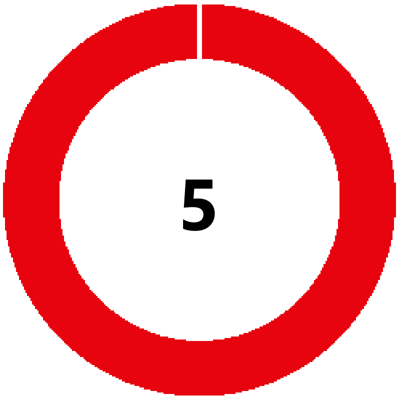
Target: **http://localhost**

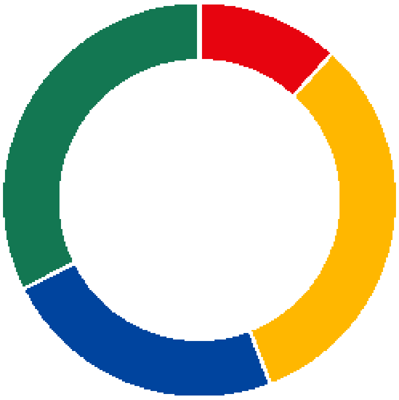
Date: **Thu May 16 2024**

Found Issues: **111**

scan **finished** within **2’ 44”** after **2903** requests.



Risk



Issue Severity

Executive Summary

SmartScanner conducted a scan on localhost to find security weaknesses and vulnerabilities. The scan took 2 minutes and 44 seconds. After performing 2903 requests, SmartScanner found 111 issues in which 13 of them are highly severe. The overall security risk of localhost is 5 out of 5. It is recommended to fix the found issues as soon as possible to mitigate the security risk. Technical details, as well as remediation of results, can be found in the following. *

* DISCLAIMER: This report is only limited to the results of SmartScanner findings.

List of Issues

1– Cross Site Scripting

- 1.1– http://localhost
- 1.2– http://localhost/feed/
- 1.3– http://localhost/user/name/index.php
- 1.4– http://localhost/xss/base64.php?name=YmFzZTY0LWVuY29kZWQtdmFsdWU
- 1.5– http://localhost/xss/index.php?name=test
- 1.6– http://localhost/xss/script-inline.php?u=testa

2– Weak Password

- 2.1– http://localhost/auth/
- 2.2– http://localhost/formauth/

3– Unicode Transformation Issue

- 3.1– http://localhost/ping/?i=127.0.0.1

4– Insecure Deserialization

- 4.1– http://localhost/dashboard/json.php

5– Unvalidated Redirection

- 5.1– http://localhost/redir/?u=http://localhost/

6– Local File Inclusion

- 6.1– http://localhost/display/?f=a.html

7– OS Command Execution

- 7.1– http://localhost/ping/?i=127.0.0.1

8– Detailed Application Error

- 8.1– http://localhost/display/?f=a.html
- 8.2– http://localhost/display/index.php
- 8.3– http://localhost/feed/
- 8.4– http://localhost/formauth/
- 8.5– http://localhost/formauth/bypassBlock.php
- 8.6– http://localhost/formauth/bypassBlock.php
- 8.7– http://localhost/formauth/enumerate.php
- 8.8– http://localhost/formauth/enumerate.php
- 8.9– http://localhost/ping/?i=127.0.0.1
- 8.10– http://localhost/ping/index.php
- 8.11– http://localhost/redir/?u=http://localhost/
- 8.12– http://localhost/user/name/index.php
- 8.13– http://localhost/xss/base64.php?name[]=YmFzZTY0LWVuY29kZWQtdmFsdWU
- 8.14– http://localhost/xss/index.php?name=test
- 8.15– http://localhost/xss/script-inline.php?u=testa

9– Host Header Injection

- 9.1– http://localhost
- 9.2– http://localhost/.htaccess
- 9.3– http://localhost/sitemap.xml

25– Sensitive Unreferenced Resource Found

- 25.1– http://localhost/admin/
- 25.2– http://localhost/admin/login.php
- 25.3– http://localhost/phpmyadmin/
- 25.4– http://localhost/show/db.sql

26– Cookie without HttpOnly Flag

- 26.1– http://localhost/dashboard/
- 26.2– http://localhost/dashboard/
- 26.3– http://localhost/dashboard/json.php
- 26.4– http://localhost/tmp/

27– Auto Complete Enabled Password Input

- 27.1– http://localhost/formauth/bypassBlock.php
- 27.2– http://localhost/formauth/enumerate.php

28– Directory Listing of Sensitive Files

- 28.1– http://localhost/admin/
- 28.2– http://localhost/show/

29– Directory Listing

- 29.1– http://localhost/icons/
- 29.2– http://localhost/icons/small/

30– Content-Security-Policy Header is Missing

- 30.1– http://localhost

31– X-Frame-Options Header is Missing

- 31.1– http://localhost

32– Subresource Integrity is Missing

- 32.1– http://localhost/ssi/

33– Cookie without SameSite Flag

- 33.1– http://localhost/dashboard/json.php

34– Apache Version Disclosure

- 34.1– http://localhost

35– Insecure Inline Frame

- 35.1– http://localhost/iframe/index.html

36– TRACE Method Allowed

- 36.1– http://localhost/

37– Windows Path Disclosure

- 37.1– http://localhost
- 37.2– http://localhost/display/?f='%22!?-%25s
- 37.3– http://localhost/display/index.php
- 37.4– http://localhost/feed/
- 37.5– http://localhost/formauth/
- 37.6– http://localhost/formauth/bypassBlock.php

- 37.7– http://localhost/formauth/enumerate.php
- 37.8– http://localhost/ping/?i[]=127.0.0.1
- 37.9– http://localhost/redir/?u[]=http://localhost/
- 37.10– http://localhost/server-info
- 37.11– http://localhost/user/name/index.php
- 37.12– http://localhost/xss/base64.php?name[]=YmFzZTY0LWVuY29kZWQtdmFsdWU
- 37.13– http://localhost/xss/index.php?name[]=test
- 37.14– http://localhost/xss/script-inline.php?u[]=testa

38– Email Address Disclosure

- 38.1– http://localhost
- 38.2– http://localhost/icons/
- 38.3– http://localhost/server-info
- 38.4– http://localhost/tmp/

39– Content Character Encoding is not Defined

- 39.1– http://localhost/iframe/index.html
- 39.2– http://localhost/iframe/secure.html
- 39.3– http://localhost/ssi/

40– Unreferenced Resource Found

- 40.1– http://localhost/admin/change.php
- 40.2– http://localhost/Redirected/
- 40.3– http://localhost/tmp/

41– X-Content-Type-Options Header is Missing

- 41.1– http://localhost

42– Missing or Insecure Cache-Control Header

- 42.1– http://localhost/dashboard/json.php

43– Referrer-Policy Header is Missing

- 43.1– http://localhost

44– Private IPv4 Address Disclosure

- 44.1– http://localhost

45– Private IPv6 Address Disclosure

- 45.1– http://localhost

46– X-XSS-Protection Header is Set

- 46.1– http://localhost/xss/index.php?name=test

47– X-Powered-By Header Found

- 47.1– http://localhost

48– File Upload Functionality

- 48.1– http://localhost

49– SQL Command Disclosure

- 49.1– http://localhost

50– PHP Version Disclosure

1.1 Cross Site Scripting

SEVERITY	High
URL	http://localhost
PARAMETER (HEADER)	User-Agent
INJECTION	"'/<jxqz9464>=()

DETAILS

The `"'/<jxqz9464>=()` was set as parameter `User-Agent` value and, it was reflected in the response.

REQUEST / RESPONSE

#1

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Content-Length: 0
User-Agent: "'/<jxqz9464>=()
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:07 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 7813
Keep-Alive: timeout=5, max=94
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

...[truncated]...
module-title">XSS in header</div>
        <div class="module-body">
        "'/<jxqz9464>=()        </div>
  </div>


  <div class="module">
        <div class="module-title">XSS in
...[truncated]...
```

DESCRIPTION

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it. OWASP

RECOMMENDATION

Before using user input for rendering the page, use libraries for sanitizing and encoding untrusted data into HTML.

The primary defenses against XSS are described in the OWASP XSS Prevention Cheat Sheet.

The OWASP ESAPI project has produced a set of reusable security components in several languages, including validation and escaping routines to prevent parameter tampering and the injection of XSS attacks. [OWASP]

1.2 Cross Site Scripting

SEVERITY	High
URL	http://localhost/feed/
PARAMETER (POST)	name
INJECTION	"'/<jxqz30603>=()

DETAILS

The `"'/<jxqz30603>=()` was set as parameter `name` value and, it was reflected in the response.

REQUEST / RESPONSE

#1

```
POST /feed/ HTTP/1.1
Authorization: valid-token
Content-Type: applicatioN/json
Referer: http://localhost/feed/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 43
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
Content-Length: 43

{
    "name": "IicvPGp4cXozMDYwMz49KCk="
}
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:08:04 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 400
Keep-Alive: timeout=5, max=38
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<html>

hi "'/<jxqz30603>=()
        <script>
  async function req(name) {
    const body = {
      name: btoa(name)
    }
    let myInit = {
      method: 'P
...[truncated]...
```

DESCRIPTION

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it. [OWASP]

RECOMMENDATION

Before using user input for rendering the page, use libraries for sanitizing and encoding untrusted data into HTML.
The primary defenses against XSS are described in the OWASP XSS Prevention Cheat Sheet.
The OWASP ESAPI project has produced a set of reusable security components in several languages, including validation and escaping routines to prevent parameter tampering and the injection of XSS attacks. [OWASP]

1.3 Cross Site Scripting

SEVERITY	High
URL	http://localhost/user/name/index.php
PARAMETER (POST)	name
INJECTION	"'/<jxqz24353>=()

DETAILS

The `"'/<jxqz24353>=()` was set as parameter `name` value and, it was reflected in the response.

REQUEST / RESPONSE

#1

```
POST /user/name/index.php HTTP/1.1
Authorization: valid-token
Content-Type: application/x-www-form-urlencoded
Referer: http://localhost/user/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 30
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
Content-Length: 30

name=%22'/%3Cjxqz24353%3E%3D()
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:08:02 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 17
Keep-Alive: timeout=5, max=94
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

"'/<jxqz24353>=()
```

DESCRIPTION

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it. OWASP

RECOMMENDATION

Before using user input for rendering the page, use libraries for sanitizing and encoding untrusted data into HTML.

The primary defenses against XSS are described in the OWASP XSS Prevention Cheat Sheet.
The OWASP ESAPI project has produced a set of reusable security components in several languages, including validation and escaping routines to prevent parameter tampering and the injection of XSS attacks. OWASP

1.4 Cross Site Scripting

SEVERITY	High
URL	http://localhost/xss/base64.php?name=YmFzZTY0LWVuY29kZWQtdmFsdWU
PARAMETER (QUERY)	name
INJECTION	"'/<jxqz32026>=()

DETAILS

The `"'/<jxqz32026>=()` was set as parameter `name` value and, it was reflected in the response.

REQUEST / RESPONSE

#1

```
GET /xss/base64.php?name=IicvPGp4cXozMjAyNj49KCk%3D HTTP/1.1
Referer: http://localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:14 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 23
Keep-Alive: timeout=5, max=64
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

hello "'/<jxqz32026>=()
```

DESCRIPTION

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it. OWASP

RECOMMENDATION

Before using user input for rendering the page, use libraries for sanitizing and encoding untrusted data into HTML.
The primary defenses against XSS are described in the OWASP XSS Prevention Cheat Sheet.

The OWASP ESAPI project has produced a set of reusable security components in several languages, including validation and escaping routines to prevent parameter tampering and the injection of XSS attacks. [OWASP]

1.5 Cross Site Scripting

SEVERITY	High
URL	http://localhost/xss/index.php?name=test
PARAMETER (QUERY)	name
INJECTION	"'/<jxqz4630>=()

DETAILS

The `"'/<jxqz4630>=()` was set as parameter `name` value and, it was reflected in the response.

REQUEST / RESPONSE

#1

```
GET /xss/index.php?name=%22'/%3Cjxqz4630%3E%3D() HTTP/1.1
Referer: http://localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:16 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
X-XSS-Protection: 1
Content-Length: 22
Keep-Alive: timeout=5, max=31
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

hello "'/<jxqz4630>=()
```

DESCRIPTION

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it. OWASP

RECOMMENDATION

Before using user input for rendering the page, use libraries for sanitizing and encoding untrusted data into HTML.
The primary defenses against XSS are described in the OWASP XSS Prevention Cheat Sheet.

The OWASP ESAPI project has produced a set of reusable security components in several languages, including validation and escaping routines to prevent parameter tampering and the injection of XSS attacks. OWASP

1.6 Cross Site Scripting

SEVERITY	High
URL	http://localhost/xss/script-inline.php?u=testa
PARAMETER (QUERY)	u
INJECTION	a';alert(1);//

DETAILS

The `a';alert(1);//` was set as parameter `u` value and, it was reflected in the response.

REQUEST / RESPONSE

#1

```
GET /xss/script-inline.php?u=a';alert(1);// HTTP/1.1
Referer: http://localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:16 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 80
Keep-Alive: timeout=5, max=95
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

hi
<script>
    let name = 'a';alert(1);//';
    console.log(name)
</script>
```

DESCRIPTION

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it. OWASP

RECOMMENDATION

Before using user input for rendering the page, use libraries for sanitizing and encoding untrusted data into HTML.

The primary defenses against XSS are described in the OWASP XSS Prevention Cheat Sheet.
The OWASP ESAPI project has produced a set of reusable security components in several languages, including validation and escaping routines to prevent parameter tampering and the injection of XSS attacks. [OWASP]

2.1 Weak Password

SEVERITY	High
URL	http://localhost/auth/
PASS	password
USER	admin

DETAILS

An easily guessable user/password was found.

REQUEST / RESPONSE

#1

```
GET /auth/ HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:13 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 64
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<p>Hello admin.</p><p>You entered password as your password.</p>
```

DESCRIPTION

The application does not enforce using a strong password, which makes it easier for attackers to find users' passwords.

RECOMMENDATION

To mitigate the risk of easily guessed passwords facilitating unauthorized access there are two solutions: introduce additional authentication controls (i.e. two-factor authentication) or introduce a strong password policy. The simplest and cheapest of these is the introduction of a strong password policy that ensures password length, complexity, reuse and aging; although ideally both of them should be implemented. OWASP

2.2 Weak Password

SEVERITY	High
URL	http://localhost/formauth/
REFERER	http://localhost/formauth/
PASS	123456
USER	admin

DETAILS

An easily guessable user/password was found.

REQUEST / RESPONSE

#1

```
POST /formauth/ HTTP/1.1
Referer: http://localhost/formauth/
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 21
Content-Length: 21

usr=admin&pass=123456
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:15 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 45
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

Welcome <a href="protected.php">protected</a>
```

DESCRIPTION

The application does not enforce using a strong password, which makes it easier for attackers to find users' passwords.

RECOMMENDATION

To mitigate the risk of easily guessed passwords facilitating unauthorized access there are two solutions: introduce additional authentication controls (i.e. two-factor authentication) or introduce a strong password policy. The simplest and cheapest of these is the introduction of a strong password policy that ensures password length, complexity, reuse and aging; although ideally both of them should be implemented. OWASP

3.1 Unicode Transformation Issue

SEVERITY	High
URL	http://localhost/ping/?i=127.0.0.1
PARAMETER (QUERY)	i
INJECTION	smta%EF%BC%9Cb%CA%BAc%CA%B9d%ef%bb%bfetms769
PROOF	a<b"c'd?e

DETAILS

The parameter `i` incorectly transforms unicode values.

- The Fullwidth Less-Than Sign (U+FF1C) was transformed to Less-Than Sign `<` (U+003C) when entered as UTF-8 encoded (`%EF %BC %9C`).
- The Modifier Letter Double Prime (U+02BA) was transformed to Quotation Mark `"` (U+0022) when entered as UTF-8 encoded (`%CA %BA`).
- The Modifier Letter Prime (U+02B9) was transformed to Apostrophe `'` (U+0027) when entered as UTF-8 encoded (`%CA %B9`).

REQUEST / RESPONSE

#1

```
GET /ping/?i=smta%EF%BC%9Cb%CA%BAc%CA%B9d%EF%BB%BFetms769 HTTP/1.1
Referer: http://localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:08:09 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 265
Keep-Alive: timeout=5, max=89
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<html><body><pre>
Ping request could not find host smta<b"c'd?etms769. Please check the name and try again.
Ping request could not find host smta<b"c'd?
...[truncated]...
```

DESCRIPTION

The Unicode Standard represents a very significant advance over all previous methods of encoding characters. For the first time, all of the world’s characters can be represented in a uniform manner, making it feasible for the vast majority of programs to be globalized: built to handle any language in the world.
In many ways, the use of Unicode makes programs much more robust and secure. When systems used a hodge-podge of different charsets for representing characters, there were security and corruption problems that resulted from differences between those charsets, or from the way in which programs converted to and from them.
However, because Unicode contains such a large number of characters, and incorporates the varied writing systems of the world, incorrect usage can expose programs or systems to possible security attacks like below one:

- Visual Security Issues
- UTF-8 Exploits
- Text Comparison (Sorting, Searching, Matching)
- Buffer Overflows
- Deletion of Code Points

Hackers can use these attacks to bypass WAFs and exploit XSS and SQL Injection vulnerabilities.

RECOMMENDATION

Check all the functions where the input is passed through and make sure all unicode security considerations in the reference are applied.
If you are using a library, make sure it is up to date.

4.1 Insecure Deserialization

SEVERITY	High
URL	http://localhost/dashboard/json.php
PARAMETER (COOKIE)	id
INJECTION	{"userId":12,"userName":"customevalue"}

DETAILS

SmartScanner tampered with a value in the `userName` property of the serialized JSON object in the parameter `id (Cookie)` and, the server accepted it without integrity checking. Then the server replied with the tampered data in the body.

REQUEST / RESPONSE

#1

```
GET /dashboard/json.php HTTP/1.1
Referer: http://localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: id=eyJ1c2VySWQiOjEyLCJ1c2VyTmFtZSI6ImN1c3RvbWV2YWx1ZSJ9; PHPSESSID=e2n36q648gvr9u8rk3hsdmbo
eo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:07 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 18
Keep-Alive: timeout=5, max=90
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

Hello customevalue
```

DESCRIPTION

Insecure deserialization occurs when an application deserializes a user-supplied object string without checking its integrity. It allows attackers to manipulate the system state and execute remote commands.

RECOMMENDATION

Change the application architecture and make it not dependent on object serialization from an untrusted source. Or at least use object deserialization where only primitive data types are acceptable. If you have to use object deserialization, make sure to implement integrity checks such as digital signatures on any serialized objects to prevent data tampering. Also, log any deserialization errors and monitor them.

5.1 Unvalidated Redirection

SEVERITY	High
URL	http://localhost/redir/?u=http://localhost/
PARAMETER (QUERY)	u
INJECTION	www.example.com

DETAILS

The URL will be redirected when the value of parameter `u` is set to `www.example.com`

REQUEST / RESPONSE

#1

```
GET /redir/?u=www.example.com HTTP/1.1
Referer: http://localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 301 Moved Permanently
Date: Thu, 16 May 2024 10:08:02 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Location: www.example.com
Content-Length: 0
Keep-Alive: timeout=5, max=89
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

DESCRIPTION

Unvalidated redirects and forwards are possible when a web application accepts untrusted input that could cause the web application to redirect the request to a URL contained within untrusted input. By modifying untrusted URL input to a malicious site, an attacker may successfully launch a phishing scam and steal user credentials. OWASP

RECOMMENDATION

Use a mapping between user input and redirection target. You can also use a white-list for user input. If none is applicable, notify the user before redirection.

6.1 Local File Inclusion

SEVERITY	High
URL	http://localhost/display/?f=a.html
PARAMETER (QUERY)	f
INJECTION	../../../../../../../../windows/win.ini
PROOF	[mci extensions]

DETAILS

The `../../../../../../../../windows/win.ini` was injected into the parameter `f` and `[mci extensions]` was found in the response which indicates the target is vulnerable against Local File Inclusion.

REQUEST / RESPONSE

#1

```
GET /display/?f=../../../../../../../../windows/win.ini HTTP/1.1
Referer: http://localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:16 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 103
Keep-Alive: timeout=5, max=90
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

hello vas
; for 16-bit app support
[fonts]
[extensions]
[mci extensions]
[files]
[Mail]
MAPI=1
```

DESCRIPTION

The File Inclusion vulnerability allows an attacker to include a file, usually exploiting a “dynamic file inclusion” mechanisms implemented in the target application. The vulnerability occurs due to the use of user-supplied input without proper validation. OWASP

In a Local File Inclusion the content of the local file is reflected in the response. The application might execute the content of the file if it contains code.

RECOMMENDATION

The most effective solution to eliminate file inclusion vulnerabilities is to avoid passing user-submitted input to any filesystem/framework API. If this is not possible the application can maintain an allow list of files, that may be included by the page, and then use an identifier (for example the index number) to access to the selected file. Any request containing an invalid identifier has to be rejected, in this way there is no attack surface for malicious users to manipulate the path. [OWASP]

7.1 OS Command Execution

SEVERITY	High
URL	http://localhost/ping/?i=127.0.0.1
PARAMETER (QUERY)	i
INJECTION	a|ver
PROOF	Microsoft Windows [Version

DETAILS

The server replied with the result of executing the injected command `a|ver` into the parameter `i`.

REQUEST / RESPONSE

1

```
GET /ping/?i=a%7Cver HTTP/1.1
Referer: http://localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:08:10 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 175
Keep-Alive: timeout=5, max=87
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<html><body><pre>

Microsoft Windows [Version 10.0.22621.3527]
Microsoft Windows [Version 10.0.22621.3527]</pre>
<p>normal,blind: &ver&ping 127.0.0.1</p>
<
...[truncated]...
```

DESCRIPTION

Command injection is an attack in which the goal is execution of arbitrary commands on the host operating system via a vulnerable application. Command injection attacks are possible when an application passes unsafe user supplied data (forms, cookies, HTTP headers etc.) to a system shell. In this attack, the attacker-supplied operating system commands are usually executed with the privileges of the vulnerable application. Command injection attacks are possible largely due to insufficient input validation. OWASP

RECOMMENDATION

Ideally, a developer should use existing API for their language. For example (Java): Rather than use Runtime.exec() to issue a ‘mail’ command, use the available Java API located at javax.mail.*
If no such available API exists, the developer should scrub all input for malicious characters. Implementing a positive security model would be most efficient. Typically, it is much easier to define the legal characters than the illegal characters. OWASP

8.1 Detailed Application Error

SEVERITY	Medium
URL	http://localhost/display/?f=a.html
PARAMETER (QUERY)	f
APPLICATION ERROR	Warning</b>: include('&quot;!?-%s): Failed to open stream: No such file or directory in <b>C:\xampp\htdocs\display\index.php</b> on line
INJECTION	'"!?-%s
PROGRAMMING LANGUAGE	PHP

DETAILS

When the `'"!?-%s` was set as the parameter `f` value, the application faced with an error.

REQUEST / RESPONSE

#1

```
GET /display/?f='%22!?-%25s HTTP/1.1
Referer: http://localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:16 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 355
Keep-Alive: timeout=5, max=13
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

hello vas
<br />
<b>Warning</b>:  include('&quot;!?-%s): Failed to open stream: No such file or directory in <b>C:\x
ampp\htdocs\display\index.php</b> on line <
...[truncated]...
```

DESCRIPTION

Unhandled exceptions have two primary risks.

- **Denial of service:** When an unhandled exception occurs, it might cause memory leakage or consume server resources by performing more process than usual.

- **Leaking information:** Unhandled exceptions can generate error messages with sensitive information. When these error messages are shown to users, attackers can take advantage of them to develop their attack on the target.

RECOMMENDATION

You should properly handle all types of exceptions and display a generic error message. You can find more details in the following.

ASP.NET

For ASP.NET, you can disable detailed errors by setting the mode attribute of the `customErrors` to `on` or `RemoteOnly`.

Example configuration:

```
<configuration>
  <system.web>
    <customErrors defaultRedirect="YourErrorPage.aspx"
                  mode="RemoteOnly">
      <error statusCode="500"
             redirect="InternalErrorPage.aspx"/>
    </customErrors>
  </system.web>
</configuration>
```

PHP

In PHP you can disable errors by adding the below lines to your code:

```
ini_set('display_errors', 0);
ini_set('display_startup_errors', 0);
error_reporting(0);
```

You can also disable error reporting in the `php.ini` file by using the below config.

```
display_errors = off
```

Java

You can set a default exception handler using the `Thread.setDefaultUncaughtExceptionHandler` method to capture all unchecked and runtime errors.

8.2 Detailed Application Error

SEVERITY	Medium
URL	http://localhost/display/index.php
REFERER	http://localhost
APPLICATION ERROR	Warning</b>: Undefined array key "f" in <b>C:\xampp\htdocs\display\index.php</b> on line
PROGRAMMING LANGUAGE	PHP

REQUEST / RESPONSE

#1

```
GET /display/index.php HTTP/1.1
Referer: http://localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:09:36 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 334
Keep-Alive: timeout=5, max=36
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

hello vas
<br />
<b>Warning</b>:  Undefined array key "f" in <b>C:\xampp\htdocs\display\index.php</b> on line <b>4</
b><br />
<br />
<b>Fatal error</b>:  Uncaug
...[truncated]...
```

DESCRIPTION

Unhandled exceptions have two primary risks.

- **Denial of service:** When an unhandled exception occurs, it might cause memory leakage or consume server resources by performing more process than usual.
- **Leaking information:** Unhandled exceptions can generate error messages with sensitive information. When these error messages are shown to users, attackers can take advantage of them to develop their attack on the target.

RECOMMENDATION

You should properly handle all types of exceptions and display a generic error message. You can find more details in the following.

ASP.NET

For ASP.NET, you can disable detailed errors by setting the mode attribute of the `customErrors` to `on` or `RemoteOnly`.

Example configuration:

```
<configuration>
  <system.web>
    <customErrors defaultRedirect="YourErrorPage.aspx"
                  mode="RemoteOnly">
      <error statusCode="500"
             redirect="InternalErrorPage.aspx"/>
    </customErrors>
  </system.web>
</configuration>
```

PHP

In PHP you can disable errors by adding the below lines to your code:

```
ini_set('display_errors', 0);
ini_set('display_startup_errors', 0);
error_reporting(0);
```

You can also disable error reporting in the `php.ini` file by using the below config.

```
display_errors = off
```

Java

You can set a default exception handler using the `Thread.setDefaultUncaughtExceptionHandler` method to capture all unchecked and runtime errors.

8.3 Detailed Application Error

SEVERITY	Medium
URL	http://localhost/feed/
REFERER	http://localhost/feed/
PARAMETER (POST)	name
APPLICATION ERROR	Warning</b>: Undefined property: stdClass::$name in <b>C:\xampp\htdocs\feed\index.php</b> on line
PROGRAMMING LANGUAGE	PHP

REQUEST / RESPONSE

#1

```
POST /feed/ HTTP/1.1
Authorization: valid-token
Content-Type: applicatioN/json
Referer: http://localhost/feed/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 4
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
Content-Length: 4

{
}
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:08:04 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 508
Keep-Alive: timeout=5, max=41
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<html>

<br />
<b>Warning</b>:  Undefined property: stdClass::$name in <b>C:\xampp\htdocs\feed\index.php</b> on li
ne <b>13</b><br />
hi
        <script>
  async f
...[truncated]...
```

DESCRIPTION

Unhandled exceptions have two primary risks.

- **Denial of service:** When an unhandled exception occurs, it might cause memory leakage or consume server resources by performing more process than usual.

- **Leaking information:** Unhandled exceptions can generate error messages with sensitive information. When these error messages are shown to users, attackers can take advantage of them to develop their attack on the target.

RECOMMENDATION

You should properly handle all types of exceptions and display a generic error message. You can find more details in the following.

ASP.NET

For ASP.NET, you can disable detailed errors by setting the mode attribute of the `customErrors` to `on` or `RemoteOnly`.

Example configuration:

```
<configuration>
  <system.web>
    <customErrors defaultRedirect="YourErrorPage.aspx"
                  mode="RemoteOnly">
      <error statusCode="500"
             redirect="InternalErrorPage.aspx"/>
    </customErrors>
  </system.web>
</configuration>
```

PHP

In PHP you can disable errors by adding the below lines to your code:

```
ini_set('display_errors', 0);
ini_set('display_startup_errors', 0);
error_reporting(0);
```

You can also disable error reporting in the `php.ini` file by using the below config.

```
display_errors = off
```

Java

You can set a default exception handler using the `Thread.setDefaultUncaughtExceptionHandler` method to capture all unchecked and runtime errors.

8.4 Detailed Application Error

SEVERITY	Medium
URL	http://localhost/formauth/
REFERER	http://localhost
APPLICATION ERROR	Warning</b>: Undefined array key "usr" in <b>C:\xampp\htdocs\formauth\index.php</b> on line
PROGRAMMING LANGUAGE	PHP

REQUEST / RESPONSE

#1

```
GET /formauth/ HTTP/1.1
Referer: http://localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:13 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 447
Keep-Alive: timeout=5, max=84
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<br />
<b>Warning</b>:  Undefined array key "usr" in <b>C:\xampp\htdocs\formauth\index.php</b> on line <b>
3</b><br />
<html>
<body>
        <form method="POST">
        <b
...[truncated]...
```

DESCRIPTION

Unhandled exceptions have two primary risks.

- **Denial of service:** When an unhandled exception occurs, it might cause memory leakage or consume server resources by performing more process than usual.
- **Leaking information:** Unhandled exceptions can generate error messages with sensitive information. When these error messages are shown to users, attackers can take advantage of them to develop their attack on the target.

RECOMMENDATION

You should properly handle all types of exceptions and display a generic error message. You can find more details in the following.

ASP.NET

For ASP.NET, you can disable detailed errors by setting the mode attribute of the `customErrors` to `on` or `RemoteOnly`.

Example configuration:

```
<configuration>
  <system.web>
    <customErrors defaultRedirect="YourErrorPage.aspx"
                  mode="RemoteOnly">
      <error statusCode="500"
             redirect="InternalErrorPage.aspx"/>
    </customErrors>
  </system.web>
</configuration>
```

PHP

In PHP you can disable errors by adding the below lines to your code:

```
ini_set('display_errors', 0);
ini_set('display_startup_errors', 0);
error_reporting(0);
```

You can also disable error reporting in the `php.ini` file by using the below config.

```
display_errors = off
```

Java

You can set a default exception handler using the `Thread.setDefaultUncaughtExceptionHandler` method to capture all unchecked and runtime errors.

8.5 Detailed Application Error

SEVERITY	Medium
URL	http://localhost/formauth/bypassBlock.php
REFERER	smta%EF%BC%9Cb%CA%BAc%CA%B9d%ef%bb%bfetms769
PARAMETER (HEADER)	Referer
APPLICATION ERROR	Warning</b>: Undefined array key "name" in <b>C:\xampp\htdocs\formauth\bypassBlock.php</b> on line
INJECTION	smta%EF%BC%9Cb%CA%BAc%CA%B9d%ef%bb%bfetms769
PROGRAMMING LANGUAGE	PHP

DETAILS

When the `smta%EF%BC%9Cb%CA%BAc%CA%B9d%ef%bb%bfetms769` was set as the parameter `Referer` value, the application faced with an error.

REQUEST / RESPONSE

#1

```
GET /formauth/bypassBlock.php HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Referer: smta%EF%BC%9Cb%CA%BAc%CA%B9d%ef%bb%bfetms769
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:07 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 463
Keep-Alive: timeout=5, max=95
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<br />
<b>Warning</b>:  Undefined array key "name" in <b>C:\xampp\htdocs\formauth\bypassBlock.php</b> on l
ine <b>4</b><br />
<br />
<b>Warning</b>:  Undefined a
...[truncated]...
```

DESCRIPTION

Unhandled exceptions have two primary risks.

- **Denial of service:** When an unhandled exception occurs, it might cause memory leakage or consume server resources by performing more process than usual.
- **Leaking information:** Unhandled exceptions can generate error messages with sensitive information. When these error messages are shown to users, attackers can take advantage of them to develop their attack on the target.

RECOMMENDATION

You should properly handle all types of exceptions and display a generic error message. You can find more details in the following.

ASP.NET

For ASP.NET, you can disable detailed errors by setting the mode attribute of the `customErrors` to `on` or `RemoteOnly`.

Example configuration:

```
<configuration>
  <system.web>
    <customErrors defaultRedirect="YourErrorPage.aspx"
                  mode="RemoteOnly">
      <error statusCode="500"
             redirect="InternalErrorPage.aspx"/>
    </customErrors>
  </system.web>
</configuration>
```

PHP

In PHP you can disable errors by adding the below lines to your code:

```
ini_set('display_errors', 0);
ini_set('display_startup_errors', 0);
error_reporting(0);
```

You can also disable error reporting in the `php.ini` file by using the below config.

```
display_errors = off
```

Java

You can set a default exception handler using the `Thread.setDefaultUncaughtExceptionHandler` method to capture all unchecked and runtime errors.

8.6 Detailed Application Error

SEVERITY	Medium
URL	http://localhost/formauth/bypassBlock.php
PARAMETER (POST)	name
APPLICATION ERROR	Warning</b>: Undefined array key "name" in <b>C:\xampp\htdocs\formauth\bypassBlock.php</b> on line
PROGRAMMING LANGUAGE	PHP

DETAILS

When the parameter `name` was removed, the application faced with an error.

REQUEST / RESPONSE

#1

```
POST /formauth/bypassBlock.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Referer: http://localhost/formauth/bypassBlock.php
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 18
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
Content-Length: 18

pass=DJrLcmno321@!
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:08:02 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 466
Keep-Alive: timeout=5, max=82
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<br />
<b>Warning</b>:  Undefined array key "name" in <b>C:\xampp\htdocs\formauth\bypassBlock.php</b> on l
ine <b>4</b><br />
<br />
<b>Warning</b>:  Undefined a
...[truncated]...
```

DESCRIPTION

Unhandled exceptions have two primary risks.

- **Denial of service:** When an unhandled exception occurs, it might cause memory leakage or consume server resources by performing more process than usual.
- **Leaking information:** Unhandled exceptions can generate error messages with sensitive information. When these error messages are shown to users, attackers can take advantage of them to develop their attack on the target.

RECOMMENDATION

You should properly handle all types of exceptions and display a generic error message. You can find more details in the following.

ASP.NET

For ASP.NET, you can disable detailed errors by setting the mode attribute of the `customErrors` to `on` or `RemoteOnly`.

Example configuration:

```
<configuration>
  <system.web>
    <customErrors defaultRedirect="YourErrorPage.aspx"
                  mode="RemoteOnly">
      <error statusCode="500"
             redirect="InternalErrorPage.aspx"/>
    </customErrors>
  </system.web>
</configuration>
```

PHP

In PHP you can disable errors by adding the below lines to your code:

```
ini_set('display_errors', 0);
ini_set('display_startup_errors', 0);
error_reporting(0);
```

You can also disable error reporting in the `php.ini` file by using the below config.

```
display_errors = off
```

Java

You can set a default exception handler using the `Thread.setDefaultUncaughtExceptionHandler` method to capture all unchecked and runtime errors.

8.7 Detailed Application Error

SEVERITY	Medium
URL	http://localhost/formauth/enumerate.php
REFERER	http://localhost
APPLICATION ERROR	Warning</b>: Undefined array key "user" in <b>C:\xampp\htdocs\formauth\enumerate.php</b> on line
PROGRAMMING LANGUAGE	PHP

REQUEST / RESPONSE

#1

```
GET /formauth/enumerate.php HTTP/1.1
Referer: http://localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:13 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 458
Keep-Alive: timeout=5, max=82
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<br />
<b>Warning</b>:  Undefined array key "user" in <b>C:\xampp\htdocs\formauth\enumerate.php</b> on lin
e <b>3</b><br />
<br />
<b>Warning</b>:  Undefined arr
...[truncated]...
```

DESCRIPTION

Unhandled exceptions have two primary risks.

- **Denial of service:** When an unhandled exception occurs, it might cause memory leakage or consume server resources by performing more process than usual.
- **Leaking information:** Unhandled exceptions can generate error messages with sensitive information. When these error messages are shown to users, attackers can take advantage of them to develop their attack on the target.

RECOMMENDATION

You should properly handle all types of exceptions and display a generic error message. You can find more details in the following.

ASP.NET

For ASP.NET, you can disable detailed errors by setting the mode attribute of the `customErrors` to `on` or `RemoteOnly`.

Example configuration:

```
<configuration>
  <system.web>
    <customErrors defaultRedirect="YourErrorPage.aspx"
                  mode="RemoteOnly">
      <error statusCode="500"
             redirect="InternalErrorPage.aspx"/>
    </customErrors>
  </system.web>
</configuration>
```

PHP

In PHP you can disable errors by adding the below lines to your code:

```
ini_set('display_errors', 0);
ini_set('display_startup_errors', 0);
error_reporting(0);
```

You can also disable error reporting in the `php.ini` file by using the below config.

```
display_errors = off
```

Java

You can set a default exception handler using the `Thread.setDefaultUncaughtExceptionHandler` method to capture all unchecked and runtime errors.

8.8 Detailed Application Error

SEVERITY	Medium
URL	http://localhost/formauth/enumerate.php
PARAMETER (POST)	user
APPLICATION ERROR	Warning</b>: Undefined array key "user" in <b>C:\xampp\htdocs\formauth\enumerate.php</b> on line
PROGRAMMING LANGUAGE	PHP

DETAILS

When the parameter `name` was removed, the application faced with an error.

REQUEST / RESPONSE

#1

```
POST /formauth/enumerate.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Referer: http://localhost/formauth/enumerate.php
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 18
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
Content-Length: 18

pass=DJrLcmno321@!
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:08:04 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 458
Keep-Alive: timeout=5, max=40
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<br />
<b>Warning</b>:  Undefined array key "user" in <b>C:\xampp\htdocs\formauth\enumerate.php</b> on lin
e <b>3</b><br />
<br />
<b>Warning</b>:  Undefined arr
...[truncated]...
```

DESCRIPTION

Unhandled exceptions have two primary risks.

- **Denial of service:** When an unhandled exception occurs, it might cause memory leakage or consume server resources by performing more process than usual.

- **Leaking information:** Unhandled exceptions can generate error messages with sensitive information. When these error messages are shown to users, attackers can take advantage of them to develop their attack on the target.

RECOMMENDATION

You should properly handle all types of exceptions and display a generic error message. You can find more details in the following.

ASP.NET

For ASP.NET, you can disable detailed errors by setting the mode attribute of the `customErrors` to `on` or `RemoteOnly`.

Example configuration:

```
<configuration>
  <system.web>
    <customErrors defaultRedirect="YourErrorPage.aspx"
                  mode="RemoteOnly">
      <error statusCode="500"
             redirect="InternalErrorPage.aspx"/>
    </customErrors>
  </system.web>
</configuration>
```

PHP

In PHP you can disable errors by adding the below lines to your code:

```
ini_set('display_errors', 0);
ini_set('display_startup_errors', 0);
error_reporting(0);
```

You can also disable error reporting in the `php.ini` file by using the below config.

```
display_errors = off
```

Java

You can set a default exception handler using the `Thread.setDefaultUncaughtExceptionHandler` method to capture all unchecked and runtime errors.

8.9 Detailed Application Error

SEVERITY	Medium
URL	http://localhost/ping/?i=127.0.0.1
PARAMETER (QUERY)	i
APPLICATION ERROR	Warning</b>: Array to string conversion in <b>C:\xampp\htdocs\ping\index.php</b> on line
PROGRAMMING LANGUAGE	PHP

DETAILS

When the parameter `name` was converted to array (`name[]`), the application faced with an error.

REQUEST / RESPONSE

#1

```
GET /ping/?i[]=127.0.0.1 HTTP/1.1
Referer: http://localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:08:06 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 354
Keep-Alive: timeout=5, max=90
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<html><body><pre>
<br />
<b>Warning</b>:  Array to string conversion in <b>C:\xampp\htdocs\ping\index.php</b> on line <b>5</
b><br />
Ping request could not fin
...[truncated]...
```

DESCRIPTION

Unhandled exceptions have two primary risks.

- **Denial of service:** When an unhandled exception occurs, it might cause memory leakage or consume server resources by performing more process than usual.
- **Leaking information:** Unhandled exceptions can generate error messages with sensitive information. When these error messages are shown to users, attackers can take advantage of

them to develop their attack on the target.

RECOMMENDATION

You should properly handle all types of exceptions and display a generic error message. You can find more details in the following.

ASP.NET

For ASP.NET, you can disable detailed errors by setting the mode attribute of the `customErrors` to `on` or `RemoteOnly`.

Example configuration:

```
<configuration>
  <system.web>
    <customErrors defaultRedirect="YourErrorPage.aspx"
                  mode="RemoteOnly">
      <error statusCode="500"
             redirect="InternalErrorPage.aspx"/>
    </customErrors>
  </system.web>
</configuration>
```

PHP

In PHP you can disable errors by adding the below lines to your code:

```
ini_set('display_errors', 0);
ini_set('display_startup_errors', 0);
error_reporting(0);
```

You can also disable error reporting in the `php.ini` file by using the below config.

```
display_errors = off
```

Java

You can set a default exception handler using the `Thread.setDefaultUncaughtExceptionHandler` method to capture all unchecked and runtime errors.

8.10 Detailed Application Error

SEVERITY	Medium
URL	http://localhost/ping/index.php
REFERER	http://localhost
APPLICATION ERROR	Warning</b>: Undefined array key "i" in <b>C:\xampp\htdocs\ping\index.php</b> on line
PROGRAMMING LANGUAGE	PHP

REQUEST / RESPONSE

#1

```
GET /ping/index.php HTTP/1.1
Referer: http://localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:09:39 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 1894
Keep-Alive: timeout=5, max=53
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<html><body><pre>
<br />
<b>Warning</b>:  Undefined array key "i" in <b>C:\xampp\htdocs\ping\index.php</b> on line <b>4</b><
br />

Usage: ping [-t] [-a] [-n c
...[truncated]...
```

DESCRIPTION

Unhandled exceptions have two primary risks.

- **Denial of service:** When an unhandled exception occurs, it might cause memory leakage or consume server resources by performing more process than usual.
- **Leaking information:** Unhandled exceptions can generate error messages with sensitive information. When these error messages are shown to users, attackers can take advantage of them to develop their attack on the target.

RECOMMENDATION

You should properly handle all types of exceptions and display a generic error message. You can find more details in the following.

ASP.NET

For ASP.NET, you can disable detailed errors by setting the mode attribute of the `customErrors` to `on` or `RemoteOnly`.

Example configuration:

```
<configuration>
  <system.web>
    <customErrors defaultRedirect="YourErrorPage.aspx"
                  mode="RemoteOnly">
      <error statusCode="500"
             redirect="InternalErrorPage.aspx"/>
    </customErrors>
  </system.web>
</configuration>
```

PHP

In PHP you can disable errors by adding the below lines to your code:

```
ini_set('display_errors', 0);
ini_set('display_startup_errors', 0);
error_reporting(0);
```

You can also disable error reporting in the `php.ini` file by using the below config.

```
display_errors = off
```

Java

You can set a default exception handler using the `Thread.setDefaultUncaughtExceptionHandler` method to capture all unchecked and runtime errors.

8.11 Detailed Application Error

SEVERITY	Medium
URL	http://localhost/redir/?u=http://localhost/
PARAMETER (QUERY)	u
APPLICATION ERROR	Warning</b>: Array to string conversion in <b>C:\xampp\htdocs\redir\index.php</b> on line
PROGRAMMING LANGUAGE	PHP

DETAILS

When the parameter `name` was converted to array (`name[]`), the application faced with an error.

REQUEST / RESPONSE

#1

```
GET /redir/?u[]=http://localhost/ HTTP/1.1
Referer: http://localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 301 Moved Permanently
Date: Thu, 16 May 2024 10:08:02 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Location: Array
Content-Length: 116
Keep-Alive: timeout=5, max=97
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<br />
<b>Warning</b>:  Array to string conversion in <b>C:\xampp\htdocs\redir\index.php</b> on line <b>7
</b><br />
```

DESCRIPTION

Unhandled exceptions have two primary risks.

- **Denial of service:** When an unhandled exception occurs, it might cause memory leakage or consume server resources by performing more process than usual.
- **Leaking information:** Unhandled exceptions can generate error messages with sensitive information. When these error messages are shown to users, attackers can take advantage of them to develop their attack on the target.

RECOMMENDATION

You should properly handle all types of exceptions and display a generic error message. You can find more details in the following.

ASP.NET

For ASP.NET, you can disable detailed errors by setting the mode attribute of the `customErrors` to `on` or `RemoteOnly`.

Example configuration:

```
<configuration>
  <system.web>
    <customErrors defaultRedirect="YourErrorPage.aspx"
                  mode="RemoteOnly">
      <error statusCode="500"
             redirect="InternalErrorPage.aspx"/>
    </customErrors>
  </system.web>
</configuration>
```

PHP

In PHP you can disable errors by adding the below lines to your code:

```
ini_set('display_errors', 0);
ini_set('display_startup_errors', 0);
error_reporting(0);
```

You can also disable error reporting in the `php.ini` file by using the below config.

```
display_errors = off
```

Java

You can set a default exception handler using the `Thread.setDefaultUncaughtExceptionHandler` method to capture all unchecked and runtime errors.

8.12 Detailed Application Error

SEVERITY	Medium
URL	http://localhost/user/name/index.php
PARAMETER (POST)	name
APPLICATION ERROR	Warning</b>: Array to string conversion in <b>C:\xampp\htdocs\user\name\index.php</b> on line
PROGRAMMING LANGUAGE	PHP

DETAILS

When the parameter `name` was converted to array (`name[]`), the application faced with an error.

REQUEST / RESPONSE

#1

```
POST /user/name/index.php HTTP/1.1
Authorization: valid-token
Content-Type: application/x-www-form-urlencoded
Referer: http://localhost/user/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 13
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
Content-Length: 13

name[]=myname
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:08:02 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 125
Keep-Alive: timeout=5, max=98
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<br />
<b>Warning</b>:  Array to string conversion in <b>C:\xampp\htdocs\user\name\index.php</b> on line <
b>4</b><br />
Array
```

DESCRIPTION

Unhandled exceptions have two primary risks.

- **Denial of service:** When an unhandled exception occurs, it might cause memory leakage or consume server resources by performing more process than usual.

- **Leaking information:** Unhandled exceptions can generate error messages with sensitive information. When these error messages are shown to users, attackers can take advantage of them to develop their attack on the target.

RECOMMENDATION

You should properly handle all types of exceptions and display a generic error message. You can find more details in the following.

ASP.NET

For ASP.NET, you can disable detailed errors by setting the mode attribute of the `customErrors` to `on` or `RemoteOnly`.

Example configuration:

```
<configuration>
  <system.web>
    <customErrors defaultRedirect="YourErrorPage.aspx"
                  mode="RemoteOnly">
      <error statusCode="500"
             redirect="InternalErrorPage.aspx"/>
    </customErrors>
  </system.web>
</configuration>
```

PHP

In PHP you can disable errors by adding the below lines to your code:

```
ini_set('display_errors', 0);
ini_set('display_startup_errors', 0);
error_reporting(0);
```

You can also disable error reporting in the `php.ini` file by using the below config.

```
display_errors = off
```

Java

You can set a default exception handler using the `Thread.setDefaultUncaughtExceptionHandler` method to capture all unchecked and runtime errors.

8.13 Detailed Application Error

SEVERITY	Medium
URL	http://localhost/xss/base64.php?name[]=YmFzZTY0LWVuY29kZWQtdmFsdWU
REFERER	http://localhost
PARAMETER (QUERY)	name
AFFECTED URLS	localhost/xss/base64.php?name[]=YmFzZTY0LWVuY29kZWQtdmFsdWU localhost/xss/base64.php
APPLICATION ERROR	Fatal error</b>: Uncaught TypeError: base64_decode(): Argument #1 ($string) must be of type string, array given in C:\xampp\htdocs\xss\base64.php:3 Stack trace: #0 C:\xampp\htdocs\xss\base64.php(3): base64_decode(Array) #1 {main} thrown in <b>C:\xampp\htdocs\xss\base64.php</b> on line
PROGRAMMING LANGUAGE	PHP

REQUEST / RESPONSE

1

```
GET /xss/base64.php?name[]=YmFzZTY0LWVuY29kZWQtdmFsdWU HTTP/1.1
Referer: http://localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:14 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 320
Keep-Alive: timeout=5, max=68
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

hello <br />
<b>Fatal error</b>:  Uncaught TypeError: base64_decode(): Argument #1 ($string) must be of type str
ing, array given in C:\xampp\htdocs\xss\base64.p
...[truncated]...
```

DESCRIPTION

Unhandled exceptions have two primary risks.

- **Denial of service:** When an unhandled exception occurs, it might cause memory leakage or consume server resources by performing more process than usual.

- **Leaking information:** Unhandled exceptions can generate error messages with sensitive information. When these error messages are shown to users, attackers can take advantage of them to develop their attack on the target.

RECOMMENDATION

You should properly handle all types of exceptions and display a generic error message. You can find more details in the following.

ASP.NET

For ASP.NET, you can disable detailed errors by setting the mode attribute of the `customErrors` to `on` or `RemoteOnly`.

Example configuration:

```
<configuration>
  <system.web>
    <customErrors defaultRedirect="YourErrorPage.aspx"
                  mode="RemoteOnly">
      <error statusCode="500"
             redirect="InternalErrorPage.aspx"/>
    </customErrors>
  </system.web>
</configuration>
```

PHP

In PHP you can disable errors by adding the below lines to your code:

```
ini_set('display_errors', 0);
ini_set('display_startup_errors', 0);
error_reporting(0);
```

You can also disable error reporting in the `php.ini` file by using the below config.

```
display_errors = off
```

Java

You can set a default exception handler using the `Thread.setDefaultUncaughtExceptionHandler` method to capture all unchecked and runtime errors.

8.14 Detailed Application Error

SEVERITY	Medium
URL	http://localhost/xss/index.php?name=test
PARAMETER (QUERY)	name
APPLICATION ERROR	Warning</b>: Array to string conversion in <b>C:\xampp\htdocs\xss\index.php</b> on line
PROGRAMMING LANGUAGE	PHP

DETAILS

When the parameter `name` was converted to array (`name[]`), the application faced with an error.

REQUEST / RESPONSE

#1

```
GET /xss/index.php?name[]=test HTTP/1.1
Referer: http://localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:16 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
X-XSS-Protection: 1
Content-Length: 125
Keep-Alive: timeout=5, max=34
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

hello <br />
<b>Warning</b>:  Array to string conversion in <b>C:\xampp\htdocs\xss\index.php</b> on line <b>4</b><br />
Array
```

DESCRIPTION

Unhandled exceptions have two primary risks.

- **Denial of service:** When an unhandled exception occurs, it might cause memory leakage or consume server resources by performing more process than usual.
- **Leaking information:** Unhandled exceptions can generate error messages with sensitive information. When these error messages are shown to users, attackers can take advantage of

them to develop their attack on the target.

RECOMMENDATION

You should properly handle all types of exceptions and display a generic error message. You can find more details in the following.

ASP.NET

For ASP.NET, you can disable detailed errors by setting the mode attribute of the `customErrors` to `on` or `RemoteOnly`.

Example configuration:

```
<configuration>
  <system.web>
    <customErrors defaultRedirect="YourErrorPage.aspx"
                  mode="RemoteOnly">
      <error statusCode="500"
             redirect="InternalErrorPage.aspx"/>
    </customErrors>
  </system.web>
</configuration>
```

PHP

In PHP you can disable errors by adding the below lines to your code:

```
ini_set('display_errors', 0);
ini_set('display_startup_errors', 0);
error_reporting(0);
```

You can also disable error reporting in the `php.ini` file by using the below config.

```
display_errors = off
```

Java

You can set a default exception handler using the `Thread.setDefaultUncaughtExceptionHandler` method to capture all unchecked and runtime errors.

8.15 Detailed Application Error

SEVERITY	Medium
URL	http://localhost/xss/script-inline.php?u=testa
PARAMETER (QUERY)	u
APPLICATION ERROR	Warning</b>: Array to string conversion in <b>C:\xampp\htdocs\xss\script-inline
PROGRAMMING LANGUAGE	PHP

DETAILS

When the parameter `name` was converted to array (`name[]`), the application faced with an error.

REQUEST / RESPONSE

#1

```
GET /xss/script-inline.php?u[]=testa HTTP/1.1
Referer: http://localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:16 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 193
Keep-Alive: timeout=5, max=55
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

hi
<script>
    let name = '<br />
<b>Warning</b>:  Array to string conversion in <b>C:\xampp\htdocs\xss\script-inline.php</b> on line
<b>3</b><br />
Array';
...[truncated]...
```

DESCRIPTION

Unhandled exceptions have two primary risks.

- **Denial of service:** When an unhandled exception occurs, it might cause memory leakage or consume server resources by performing more process than usual.

- **Leaking information:** Unhandled exceptions can generate error messages with sensitive information. When these error messages are shown to users, attackers can take advantage of them to develop their attack on the target.

RECOMMENDATION

You should properly handle all types of exceptions and display a generic error message. You can find more details in the following.

ASP.NET

For ASP.NET, you can disable detailed errors by setting the mode attribute of the `customErrors` to `on` or `RemoteOnly`.

Example configuration:

```
<configuration>
  <system.web>
    <customErrors defaultRedirect="YourErrorPage.aspx"
                  mode="RemoteOnly">
      <error statusCode="500"
             redirect="InternalErrorPage.aspx"/>
    </customErrors>
  </system.web>
</configuration>
```

PHP

In PHP you can disable errors by adding the below lines to your code:

```
ini_set('display_errors', 0);
ini_set('display_startup_errors', 0);
error_reporting(0);
```

You can also disable error reporting in the `php.ini` file by using the below config.

```
display_errors = off
```

Java

You can set a default exception handler using the `Thread.setDefaultUncaughtExceptionHandler` method to capture all unchecked and runtime errors.

9.1 Host Header Injection

SEVERITY	Medium
URL	http://localhost

DETAILS

The value injected in the `Host` header is reflected in the response.

REQUEST / RESPONSE

1

```
GET / HTTP/1.1
Origin: dkGjcdj2y3djasdcO
X-Forwarded-Host: dkGjcdj2y3djasdcX
Forwarded: for=dkGjcdj2y3djasdcF
Connection: Close
Accept: */*
Host: dkGjcdj2y3djasdc
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:08 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 7927
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en" >

<head>
  <meta charset="UTF-8">
  <title>Complete test cases</title>
  <style>
body {
  margin: 0 auto;
  max-width: 56em;
  padding: 1em 0;
}

.grid {
  /* Grid Fallback */
  display: flex;
  flex-wrap: wrap;

  /* Supports Grid */
  display: grid;
  grid-template-columns: repeat(auto-fill, minmax(200px, 1fr));
  grid-auto-rows: minmax(150px, auto);
  grid-gap: 1em;
}

.module {
  /* Demo-Specific Styles */
  background: #eaeaea;
}

.module div {
        padding: 5px;
        display: flex;
        align-items: center;
        justify-content: center;
        flex-direction: column;
}
```

```
.module-title {
        min-height: 40px;
        background-color: tomato;
        color:white;
        font-weight: bold;
}

.module-body {
        display: flex;
        align-i
```

DESCRIPTION

When processing an incoming HTTP request, the webserver needs to know which component or virtual host should complete the request. The `Host` HTTP header is used for this purpose.
All HTTP headers including the `Host` header are user-controlled data. If the application uses the value of any HTTP header without validation, a header injection attack occurs.
Host header injection allows attackers to manipulate the response to perform arbitrary redirection, cache poisoning, and information disclosure.

RECOMMENDATION

Do not rely on the value of headers. If you have to do so, accept a whitelisted value only.

9.2 Host Header Injection

SEVERITY	Medium
URL	http://localhost/.htaccess

DETAILS

The value injected in the `Host` header is reflected in the response.

REQUEST / RESPONSE

1

```
GET /.htaccess HTTP/1.1
Origin: dkGjcdj2y3djasdcO
X-Forwarded-Host: dkGjcdj2y3djasdcX
Forwarded: for=dkGjcdj2y3djasdcF
Connection: Close
Accept: */*
Host: dkGjcdj2y3djasdc
```

```
HTTP/1.1 403 Forbidden
Date: Thu, 16 May 2024 10:08:05 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
Content-Length: 305
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access this resource.</p>
<hr>
<address>Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30 Server at dkgjcdj2y3djasdc Port 80</address
>
</body></html>
```

DESCRIPTION

When processing an incoming HTTP request, the webserver needs to know which component or virtual host should complete the request. The `Host` HTTP header is used for this purpose.
All HTTP headers including the `Host` header are user-controlled data. If the application uses the value of any HTTP header without validation, a header injection attack occurs.
Host header injection allows attackers to manipulate the response to perform arbitrary redirection, cache poisoning, and information disclosure.

RECOMMENDATION

Do not rely on the value of headers. If you have to do so, accept a whitelisted value only.

9.3 Host Header Injection

SEVERITY	Medium
URL	http://localhost/sitemap.xml

DETAILS

The value injected in the `Host` header is reflected in the response.

REQUEST / RESPONSE

#1

```
GET /sitemap.xml HTTP/1.1
Origin: dkGjcdj2y3djasdcO
X-Forwarded-Host: dkGjcdj2y3djasdcX
Forwarded: for=dkGjcdj2y3djasdcF
Connection: Close
Accept: */*
Host: dkGjcdj2y3djasdc
```

```
HTTP/1.1 404 Not Found
Date: Thu, 16 May 2024 10:07:09 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
Content-Length: 302
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30 Server at dkgjcdj2y3djasdc Port 80</address
>
</body></html>
```

DESCRIPTION

When processing an incoming HTTP request, the webserver needs to know which component or virtual host should complete the request. The `Host` HTTP header is used for this purpose.
All HTTP headers including the `Host` header are user-controlled data. If the application uses the value of any HTTP header without validation, a header injection attack occurs.
Host header injection allows attackers to manipulate the response to perform arbitrary redirection, cache poisoning, and information disclosure.

RECOMMENDATION

Do not rely on the value of headers. If you have to do so, accept a whitelisted value only.

9.4 Host Header Injection

SEVERITY	Medium
URL	http://localhost/ssi

DETAILS

The value injected in the `Host` header is reflected in the response.

REQUEST / RESPONSE

1

```
GET /ssi HTTP/1.1
Origin: dkGjcdj2y3djasdcO
X-Forwarded-Host: dkGjcdj2y3djasdcX
Forwarded: for=dkGjcdj2y3djasdcF
Connection: Close
Accept: */*
Host: dkGjcdj2y3djasdc
```

```
HTTP/1.1 301 Moved Permanently
Date: Thu, 16 May 2024 10:07:07 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
Location: http://dkgjcdj2y3djasdc/ssi/
Content-Length: 342
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="http://dkgjcdj2y3djasdc/ssi/">here</a>.</p>
<hr>
<address>Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30 Server at dkgjcdj2y3djasdc Port 80</address
>
</body></html>
```

DESCRIPTION

When processing an incoming HTTP request, the webserver needs to know which component or virtual host should complete the request. The `Host` HTTP header is used for this purpose.
All HTTP headers including the `Host` header are user-controlled data. If the application uses the value of any HTTP header without validation, a header injection attack occurs.
Host header injection allows attackers to manipulate the response to perform arbitrary redirection, cache poisoning, and information disclosure.

RECOMMENDATION

Do not rely on the value of headers. If you have to do so, accept a whitelisted value only.

10.1 Password Sent Over HTTP

SEVERITY	Medium
URL	http://localhost/formauth/

REQUEST / RESPONSE

#1

```
GET /formauth/ HTTP/1.1
Referer: http://localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:13 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 447
Keep-Alive: timeout=5, max=84
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<br />
<b>Warning</b>:  Undefined array key "usr" in <b>C:\xampp\htdocs\formauth\index.php</b> on line <b>
3</b><br />
<html>
<body>
        <form method="POST">
        <b
...[truncated]...
```

DESCRIPTION

Attackers can sniff and capture sensitive information like passwords when they're served and transmitted over the unencrypted HTTP traffic.

RECOMMENDATION

Enforce using HTTPS.

10.2 Password Sent Over HTTP

SEVERITY	Medium
URL	http://localhost/formauth/bypassBlock.php

REQUEST / RESPONSE

#1

```
GET /formauth/bypassBlock.php HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Referer: smta%EF%BC%9Cb%CA%BAc%CA%B9d%ef%bb%bfetms769
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:07 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 463
Keep-Alive: timeout=5, max=95
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<br />
<b>Warning</b>:  Undefined array key "name" in <b>C:\xampp\htdocs\formauth\bypassBlock.php</b> on l
ine <b>4</b><br />
<br />
<b>Warning</b>:  Undefined a
...[truncated]...
```

DESCRIPTION

Attackers can sniff and capture sensitive information like passwords when they’re served and transmitted over the unencrypted HTTP traffic.

RECOMMENDATION

Enforce using HTTPS.

10.3 Password Sent Over HTTP

SEVERITY	Medium
URL	http://localhost/formauth/enumerate.php

REQUEST / RESPONSE

#1

```
GET /formauth/enumerate.php HTTP/1.1
Referer: http://localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:13 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 458
Keep-Alive: timeout=5, max=82
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<br />
<b>Warning</b>:  Undefined array key "user" in <b>C:\xampp\htdocs\formauth\enumerate.php</b> on lin
e <b>3</b><br />
<br />
<b>Warning</b>:  Undefined arr
...[truncated]...
```

DESCRIPTION

Attackers can sniff and capture sensitive information like passwords when they're served and transmitted over the unencrypted HTTP traffic.

RECOMMENDATION

Enforce using HTTPS.

11.1 Session Cookie without Secure Flag

SEVERITY	Medium
URL	http://localhost/formauth/bypassBlock.php
COOKIE	PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo

REQUEST / RESPONSE

#1

```
GET /formauth/bypassBlock.php HTTP/1.1
Referer: http://localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:07 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Set-Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 593
Keep-Alive: timeout=5, max=98
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<br />
<b>Warning</b>:  Undefined array key "name" in <b>C:\xampp\htdocs\formauth\bypassBlock.php</b> on l
ine <b>4</b><br />
<br />
<b>Warning</b>:  Undefined a
...[truncated]...
```

DESCRIPTION

The `Secure` cookie flag prevents the browser from sending the cookie over an unencrypted connection. A cookie with a `Secure` flag is sent to the server only with an encrypted request over the HTTPS protocol. Therefore it can’t easily be accessed by a man-in-the-middle attacker.

RECOMMENDATION

Set `Secure` flag for the cookie.

11.2 Session Cookie without Secure Flag

SEVERITY	Medium
URL	http://localhost/phpmyadmin/
COOKIE	phpMyAdmin=4o8r1dsf0pa7psm2obll989v6i

REQUEST / RESPONSE

#1

```
GET /phpmyadmin/ HTTP/1.1
Referer:
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:08:27 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Expires: Thu, 16 May 2024 10:08:28 +0000
Cache-Control: no-store, no-cache, must-revalidate, pre-check=0, post-check=0, max-age=0
Last-Modified: Thu, 16 May 2024 10:08:28 +0000
Set-Cookie: phpMyAdmin=4o8r1dsf0pa7psm2obll989v6i; path=/phpmyadmin/; HttpOnly; SameSite=Strict
Set-Cookie: phpMyAdmin=4o8r1dsf0pa7psm2obll989v6i; path=/phpmyadmin/; HttpOnly; SameSite=Strict
Set-Cookie: pma_lang=en; expires=Sat, 15-Jun-2024 10:08:27 GMT; Max-Age=2592000; path=/phpmyadmin/;
HttpOnly; SameSite=Strict
X-ob_mode: 1
X-Frame-Options: DENY
Referrer-Policy: no-referrer
Content-Security-Policy: default-src 'self' ;script-src 'self' 'unsafe-inline' 'unsafe-eval' ;style
-src 'self' 'unsafe-inline' ;img-src 'self' data:  *.tile.openstreetmap.org;object-src 'none';
X-Content-Security-Policy: default-src 'self' ;options inline-script eval-script;referrer no-referr
er;img-src 'self' data:  *.tile.openstreetmap.org;object-src 'none';
X-WebKit-CSP: default-src 'self' ;script-src 'self'  'unsafe-inline' 'unsafe-eval';referrer no-refe
rrer;style-src 'self' 'unsafe-inline' ;img-src 'self' data:  *.tile.openstreetmap.org;object-src 'n
one';
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Permitted-Cross-Domain-Policies: none
X-Robots-Tag: noindex, nofollow
Pragma: no-cache
Content-Encoding: gzip
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=27
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8

<!doctype html>
<html lang="en" dir="ltr">
<head>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <meta name="
...[truncated]...
```

DESCRIPTION

The `Secure` cookie flag prevents the browser from sending the cookie over an unencrypted connection. A cookie with a `Secure` flag is sent to the server only with an encrypted request over the HTTPS protocol. Therefore it can’t easily be accessed by a man-in-the-middle attacker.

RECOMMENDATION

Set `Secure` flag for the cookie.

12.1 Session Cookie without HttpOnly Flag

SEVERITY	Medium
URL	http://localhost/formauth/bypassBlock.php
COOKIE	PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo

REQUEST / RESPONSE

#1

```
GET /formauth/bypassBlock.php HTTP/1.1
Referer: http://localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:07 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Set-Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 593
Keep-Alive: timeout=5, max=98
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<br />
<b>Warning</b>:  Undefined array key "name" in <b>C:\xampp\htdocs\formauth\bypassBlock.php</b> on l
ine <b>4</b><br />
<br />
<b>Warning</b>:  Undefined a
...[truncated]...
```

DESCRIPTION

The `HttpOnly` cookie flag prevents JavaScript `Document.cookie` API from accessing the cookie. When this flag is set, the cookie is only sent to the server. In many cases, cookies are not needed on the client-side. Session cookies are a good example of cookies that don't need to be available to JavaScript. Using the `HttpOnly` flag can help to mitigate Cross-Site-Scripting(XSS) attacks.

RECOMMENDATION

Set `HttpOnly` flag for the cookie.

13.1 Session Cookie without SameSite Flag

SEVERITY	Medium
URL	http://localhost/formauth/bypassBlock.php
COOKIE	PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo

REQUEST / RESPONSE

#1

```
GET /formauth/bypassBlock.php HTTP/1.1
Referer: http://localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:07 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Set-Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 593
Keep-Alive: timeout=5, max=98
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<br />
<b>Warning</b>:  Undefined array key "name" in <b>C:\xampp\htdocs\formauth\bypassBlock.php</b> on l
ine <b>4</b><br />
<br />
<b>Warning</b>:  Undefined a
...[truncated]...
```

DESCRIPTION

The `SameSite` cookie flag with the right value prevents the browser from sending the cookie in cross-origin requests. It provides some protection against cross-site request forgery attacks (CSRF).

RECOMMENDATION

Set `SameSite` flag for the cookie.

14.1 No Redirection from HTTP to HTTPS

SEVERITY	Medium
URL	http://localhost

DESCRIPTION

When HTTPS is enabled but, HTTP requests are not redirected to HTTPS automatically, users have to open the HTTPS URL explicitly. Otherwise, communication is not encrypted and can be captured by an attacker who has access to a network interface.

RECOMMENDATION

Enforce using HTTPS. You can do it by redirecting any HTTP request to HTTPS using your application or web server configuration. You can also use the **Strict-Transport-Security** HTTP response header as an extra security defense.

15.1 Brute Force Prevention Bypassed

SEVERITY	Medium
URL	http://localhost/formauth/bypassBlock.php
REFERER	http://localhost/formauth/bypassBlock.php

DETAILS

The server uses the session to limit login attempts. This can be easily bypassed by not sending the session token to the server.

REQUEST / RESPONSE

#1

```
POST /formauth/bypassBlock.php HTTP/1.1
Referer: http://localhost/formauth/bypassBlock.php
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 15
Cookie: PHPSESSID=sh7320pe1qgpvn3bdsjdhbkb73;
Content-Length: 15

name=root&pass=
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:10 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 216
Keep-Alive: timeout=5, max=90
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<html>
<body>
        <form method="POST">
        you have been locked<br>        username: <input name="name"><br>
        password: <input name="pass" type="password"><br>
        <input
...[truncated]...
```

#2

```
POST /formauth/bypassBlock.php HTTP/1.1
Referer: http://localhost/formauth/bypassBlock.php
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 15
Cookie: PHPSESSID=tp88ivhtn018878srnmkca490v;
Content-Length: 15

name=root&pass=
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:10 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Expires: Thu, 19 Nov 1981 08:52:00 GMT
```

```
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 213
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<html>
<body>
        <form method="POST">
        Invalid user/pass<br>   username: <input name="name"><br>
        password: <input name="pass" type="password"><br>
        <input typ
...[truncated]...
```

DESCRIPTION

The software does not implement sufficient measures to prevent multiple failed authentication attempts within in a short time frame, making it more susceptible to brute force attacks. MITRE

RECOMMENDATION

Try using a CAPTCHA or lockout target user account or source IP address.

16.1 Basic Authentication Over HTTP

SEVERITY	Medium
URL	http://localhost/auth/
REFERER	http://localhost

REQUEST / RESPONSE

#1

```
GET /auth/ HTTP/1.1
Referer: http://localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 401 Unauthorized
Date: Thu, 16 May 2024 10:07:13 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
WWW-Authenticate: Basic realm="My Realm"
Content-Length: 39
Connection: close
Content-Type: text/html; charset=UTF-8

Text to send if user hits Cancel button
```

DESCRIPTION

HTTP traffic can often be sniffed and captured by an attacker who has access to a network interface. In HTTP basic authentication, user credentials are sent in Base64 encoding which, can easily be decoded into plain text.

RECOMMENDATION

Enforce using HTTPS.

17.1 Apache server-status enabled

SEVERITY	Medium
URL	http://localhost/server-status

REQUEST / RESPONSE

#1

```
GET /server-status HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:07 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
Keep-Alive: timeout=5, max=87
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=ISO-8859-1

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html><head>
<title>Apache Status</title>
</head><body>
<h1>Apache Server Status for localhost (via ::1)
...[truncated]...
```

DESCRIPTION

Sensitive information is exposed on this page. Attackers can use this information to extend their attack.

RECOMMENDATION

Disable `server-status` in the Apache config file. Another mitigation is to limit access to `/server-status` URL.

18.1 Vulnerable OpenSSL Version

SEVERITY	Medium
URL	http://localhost
VERSION IN USE	3.1.3

REQUEST / RESPONSE

#1

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:07 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 7908
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en" >

<head>
  <meta charset="UTF-8">
  <title>Complete test cases</title>
  <style>
body {
  margin: 0 auto;
  max-width:
...[truncated]...
```

DESCRIPTION

The **OpenSSL** version used is outdated and has security flaws.

RECOMMENDATION

Update the OpenSSL to any of the below versions.

- **>0.9.6m**
- **>0.9.7k**
- **>0.9.8ze**
- **>1.0.0q**
- **>1.0.1t**
- **>1.0.2zi**
- **>1.1.0k**

- **>1.1.1w**
- **>3.0.12**
- **>3.1.4**
- **>3.2.0**

19.1 Apache server-info enabled

SEVERITY	Medium
URL	http://localhost/server-info

REQUEST / RESPONSE

#1

```
GET /server-info HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:07 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
Keep-Alive: timeout=5, max=97
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=ISO-8859-1

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xh
...[truncated]...
```

DESCRIPTION

Sensitive information is exposed on this page. Attackers can use this information to extend their attack.

RECOMMENDATION

Disable `server-info` in the Apache config file. Another mitigation is to limit access to `/server-info` URL.

20.1 Source Code Disclosure

SEVERITY	Medium
URL	http://localhost
CODE	<?php

REQUEST / RESPONSE

#1

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:07 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 7908
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

...[truncated]...
"module-title">Source Code Disclosure</div>
        <div class="module-body">
        <span><?php echo something; ?></span>
        </div>
  </div>
  <div class="module">
        <di
...[truncated]...
```

DESCRIPTION

Source code on a web server often contains sensitive information and should not be accessible to users.

RECOMMENDATION

Check source code for syntax typos and server settings for misconfigurations to fix the issues.

21.1 Vulnerable PHP Version

SEVERITY	Medium
URL	http://localhost
VERSION IN USE	8.0.30

REQUEST / RESPONSE

#1

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:07 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 7908
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en" >

<head>
  <meta charset="UTF-8">
  <title>Complete test cases</title>
  <style>
body {
  margin: 0 auto;
  max-width:
...[truncated]...
```

DESCRIPTION

The **PHP** version used is outdated and has security flaws.

RECOMMENDATION

Update the PHP to any of below versions.

- **>=8.1.22**
- **>=8.2.8**

22.1 User Enumeration

SEVERITY	Medium
URL	http://localhost/formauth/enumerate.php
REFERER	http://localhost/formauth/enumerate.php
FOUND USER	admin

DETAILS

The server generates different responses for user `admin` and `nonexistinguser`. it means that the user `admin` exists in the application.

REQUEST / RESPONSE

#1

```
POST /formauth/enumerate.php HTTP/1.1
Referer: http://localhost/formauth/enumerate.php
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 38
Content-Length: 38

user=admin&pass=InvalidPa$s12f%23Kdkf4
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:13 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 212
Keep-Alive: timeout=5, max=97
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<html>
<body>
        <form method="POST">
        Invalid password<br>    username: <input name="user"><br>
        password: <input name="pass" type="password"><br>
        <input type
...[truncated]...
```

#2

```
POST /formauth/enumerate.php HTTP/1.1
Referer: http://localhost/formauth/enumerate.php
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 48
Content-Length: 48

user=nonexistinguser&pass=InvalidPa$s12f%23Kdkf4
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:13 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 212
Keep-Alive: timeout=5, max=96
Connection: Keep-Alive
```

```
Content-Type: text/html; charset=UTF-8

<html>
<body>
        <form method="POST">
        Invalid username<br>    username: <input name="user"><br>
        password: <input name="pass" type="password"><br>
        <input type
...[truncated]...
```

DESCRIPTION

Often, web applications reveal when a username exists on system, either as a consequence of mis-configuration or as a design decision. For example, sometimes, when we submit wrong credentials, we receive a message that states that either the username is present on the system or the provided password is wrong. The information obtained can be used by an attacker to gain a list of users on system. This information can be used to attack the web application, for example, through a brute force or default username and password attack. OWASP

RECOMMENDATION

Ensure the application returns consistent generic error messages in response to invalid account name, password or other user credentials entered during the log in process.
Ensure default system accounts and test accounts are deleted prior to releasing the system into production (or exposing it to an untrusted network). OWASP

23.1 No HTTPS

SEVERITY	Medium
URL	http://localhost
AFFECTED URLS (22)	localhost/dashboard/json.php localhost/show/ localhost/xss/base64.php?name=YmFzZTY0LWVuY29kZWQtdmFsdWU localhost/iframe/secure.html localhost/msg/ZGRkZGRkZGRkZA== localhost/ping/?i=127.0.0.1 localhost/formauth/ localhost/ssi/ localhost/xss/script-inline.php?u=testa localhost/formauth/enumerate.php localhost/display/?f=a.html localhost/xss/?name=test localhost localhost/user/ localhost/formauth/bypassBlock.php localhost/auth/ localhost/iframe/ localhost/user/name/ localhost/contact/?q=1 localhost/icons/small/ ...

DESCRIPTION

In HTTP communications, traffic is not encrypted and can be captured by an attacker who has access to a network interface.

RECOMMENDATION

Enable HTTPS and enforce using it.

24.1 Cookie without Secure Flag

SEVERITY	Low
URL	http://localhost/dashboard/
COOKIE	profile=Tzo4OiJzdGRDbGFzcyI6Mjp7czo4OiJ1c2VyTmFtZSI7czo4OiJ0ZXN0dXNlciI7czo2OiJ1c2VySWQiO2k6MTI7fQ%3D%3D

REQUEST / RESPONSE

#1

```
GET /dashboard/ HTTP/1.1
Referer: http://localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: id=eyJ1c2VyTmFtZSI6InRlc3R1c2VyIiwidXNlcklkIjoxMn0%3D; PHPSESSID=e2n36q648gvr9u8rk3hsdmboe
o;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:08:05 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Set-Cookie: profile=Tzo4OiJzdGRDbGFzcyI6Mjp7czo4OiJ1c2VyTmFtZSI7czo4OiJ0ZXN0dXNlciI7czo2OiJ1c2VySWQ
iO2k6MTI7fQ%3D%3D
Set-Cookie: p3=rO0ABXNyAAlTb21lQ2xhc3MAAAAAAAAAAQIABkkAAWJJAAFpTAABZHQAEkxqYXZhL2xhbmcvRG91YmxlO0wA
BGhoaGh0ABJMamF2YS9sYW5nL1N0cmluZztMAAFzcQB%2BAAJMAANzdHJxAH4AAnhwAAAAe3%2F%2F%2F%2F9zcgAQamF2YS5sY
W5nLkRvdWJsZYCzwkopa%2FsEAgABRAAFdmFsdWV4cgAQamF2YS5sYW5nLk51bWJlcoaslR0LlOCLAgAAeHC%2F8AAAAAAAAHQA
BmhoaGhoaHQABUFCQ0RFdAAGc3RyaW5n
Content-Length: 14
Keep-Alive: timeout=5, max=16
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

Hello testuser
```

DESCRIPTION

The `Secure` cookie flag prevents the browser from sending the cookie over an unencrypted connection. A cookie with a `Secure` flag is sent to the server only with an encrypted request over the HTTPS protocol. Therefore it can't easily be accessed by a man-in-the-middle attacker.

RECOMMENDATION

Set `Secure` flag for the cookie.

24.2 Cookie without Secure Flag

SEVERITY	Low
URL	http://localhost/dashboard/
COOKIE	p3=rO0ABXNyAAlTb21lQ2xhc3MAAAAAAAAAAQIABkkAAWJJAAFpTAABZHQAEkxqYXZhL2xhbmcvRG91YmxlO0wABGhoaGh0ABJMamF2YS9sYW5nL1N0cmluZztMAAFzcQB%2BAAJMAANzdHJxAH4AAnhwAAAAe3%2F%2F%2F%2F9zcgAQamF2YS5sYW5nLkRvdWJsZYCzwkopa%2FsEAgABRAAFdmFsdWV4cgAQamF2YS5sYW5nLk51bWJlcoaslR0LlOCLAgAAeHC%2F8AAAAAAAAAHQABmhoaGhoaHQABUFCQ0RFdAAGc3RyaW5n

REQUEST / RESPONSE

#1

```
GET /dashboard/ HTTP/1.1
Referer: http://localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: id=eyJ1c2VyTmFtZSI6InRlc3R1c2VyIiwidXNlcklkIjoxMn0%3D; PHPSESSID=e2n36q648gvr9u8rk3hsdmboe
o;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:08:05 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Set-Cookie: profile=Tzo4OiJzdGRDbGFzcyI6Mjp7czo4OiJ1c2VyTmFtZSI7czo4OiJ0ZXN0dXNlciI7czo2OiJ1c2VySWQ
iO2k6MTI7fQ%3D%3D
Set-Cookie: p3=rO0ABXNyAAlTb21lQ2xhc3MAAAAAAAAAAQIABkkAAWJJAAFpTAABZHQAEkxqYXZhL2xhbmcvRG91YmxlO0wA
BGhoaGh0ABJMamF2YS9sYW5nL1N0cmluZztMAAFzcQB%2BAAJMAANzdHJxAH4AAnhwAAAAe3%2F%2F%2F%2F9zcgAQamF2YS5sY
W5nLkRvdWJsZYCzwkopa%2FsEAgABRAAFdmFsdWV4cgAQamF2YS5sYW5nLk51bWJlcoaslR0LlOCLAgAAeHC%2F8AAAAAAAAAHQA
BmhoaGhoaHQABUFCQ0RFdAAGc3RyaW5n
Content-Length: 14
Keep-Alive: timeout=5, max=16
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

Hello testuser
```

DESCRIPTION

The `Secure` cookie flag prevents the browser from sending the cookie over an unencrypted connection. A cookie with a `Secure` flag is sent to the server only with an encrypted request over the HTTPS protocol. Therefore it can't easily be accessed by a man-in-the-middle attacker.

RECOMMENDATION

Set `Secure` flag for the cookie.

24.3 Cookie without Secure Flag

SEVERITY	Low
URL	http://localhost/dashboard/json.php
COOKIE	id=eyJ1c2VyTmFtZSI6InRlc3R1c2VyIiwidXNlcklkIjoxMn0%3D

REQUEST / RESPONSE

#1

```
GET /dashboard/json.php HTTP/1.1
Referer: http://localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: id=rawplain; PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:07 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Set-Cookie: id=eyJ1c2VyTmFtZSI6InRlc3R1c2VyIiwidXNlcklkIjoxMn0%3D
Content-Length: 14
Keep-Alive: timeout=5, max=83
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

Hello testuser
```

DESCRIPTION

The `Secure` cookie flag prevents the browser from sending the cookie over an unencrypted connection. A cookie with a `Secure` flag is sent to the server only with an encrypted request over the HTTPS protocol. Therefore it can’t easily be accessed by a man-in-the-middle attacker.

RECOMMENDATION

Set `Secure` flag for the cookie.

24.4 Cookie without Secure Flag

SEVERITY	Low
URL	http://localhost/phpmyadmin/
COOKIE	pma_lang=en

REQUEST / RESPONSE

#1

```
GET /phpmyadmin/ HTTP/1.1
Referer: 
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:08:27 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Expires: Thu, 16 May 2024 10:08:28 +0000
Cache-Control: no-store, no-cache, must-revalidate, pre-check=0, post-check=0, max-age=0
Last-Modified: Thu, 16 May 2024 10:08:28 +0000
Set-Cookie: phpMyAdmin=4o8r1dsf0pa7psm2obll989v6i; path=/phpmyadmin/; HttpOnly; SameSite=Strict
Set-Cookie: phpMyAdmin=4o8r1dsf0pa7psm2obll989v6i; path=/phpmyadmin/; HttpOnly; SameSite=Strict
Set-Cookie: pma_lang=en; expires=Sat, 15-Jun-2024 10:08:27 GMT; Max-Age=2592000; path=/phpmyadmin/;
HttpOnly; SameSite=Strict
X-ob_mode: 1
X-Frame-Options: DENY
Referrer-Policy: no-referrer
Content-Security-Policy: default-src 'self' ;script-src 'self' 'unsafe-inline' 'unsafe-eval' ;style
-src 'self' 'unsafe-inline' ;img-src 'self' data:  *.tile.openstreetmap.org;object-src 'none';
X-Content-Security-Policy: default-src 'self' ;options inline-script eval-script;referrer no-referr
er;img-src 'self' data:  *.tile.openstreetmap.org;object-src 'none';
X-WebKit-CSP: default-src 'self' ;script-src 'self'  'unsafe-inline' 'unsafe-eval';referrer no-refe
rrer;style-src 'self' 'unsafe-inline' ;img-src 'self' data:  *.tile.openstreetmap.org;object-src 'n
one';
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Permitted-Cross-Domain-Policies: none
X-Robots-Tag: noindex, nofollow
Pragma: no-cache
Content-Encoding: gzip
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=27
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8

<!doctype html>
<html lang="en" dir="ltr">
<head>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <meta name="
...[truncated]...
```

DESCRIPTION

The `Secure` cookie flag prevents the browser from sending the cookie over an unencrypted connection. A cookie with a `Secure` flag is sent to the server only with an encrypted request over the HTTPS protocol. Therefore it can’t easily be accessed by a man-in-the-middle attacker.

RECOMMENDATION

Set `Secure` flag for the cookie.

24.5 Cookie without Secure Flag

SEVERITY	Low
URL	http://localhost/tmp/
COOKIE	this_should_not_be=1

REQUEST / RESPONSE

#1

```
GET /tmp/ HTTP/1.1
Referer:
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: this_should_not_be=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa; PHPSESSI
D=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:09:24 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Set-Cookie: this_should_not_be=1
Content-Length: 11
Keep-Alive: timeout=5, max=57
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

aaa@sss.com
```

DESCRIPTION

The `Secure` cookie flag prevents the browser from sending the cookie over an unencrypted connection. A cookie with a `Secure` flag is sent to the server only with an encrypted request over the HTTPS protocol. Therefore it can’t easily be accessed by a man-in-the-middle attacker.

RECOMMENDATION

Set `Secure` flag for the cookie.

25.1 Sensitive Unreferenced Resource Found

SEVERITY	Low
URL	http://localhost/admin/

REQUEST / RESPONSE

#1

```
GET /admin/ HTTP/1.1
Referer: http://localhost/admin
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:08:22 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
Content-Length: 1403
Keep-Alive: timeout=5, max=98
Connection: Keep-Alive
Content-Type: text/html;charset=UTF-8

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
 <head>
  <title>Index of /admin</title>
 </head>
 <body>
<h1>Index of /admin</h1>
  <table>
   <
...[truncated]...
```

DESCRIPTION

Attackers can often predict unreferenced resources on web applications. These files may disclose sensitive information that can facilitate a focused attack against the application. Unreferenced pages may contain powerful functionality that can be used to attack the application. OWASP

RECOMMENDATION

The security of systems should not be based on the obscurity of resource locations. Remove or limit access to the file.

25.2 Sensitive Unreferenced Resource Found

SEVERITY	Low
URL	http://localhost/admin/login.php

REQUEST / RESPONSE

#1

```
GET /admin/login.php HTTP/1.1
Referer: http://localhost/admin/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:08:22 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 0
Keep-Alive: timeout=5, max=50
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

DESCRIPTION

Attackers can often predict unreferenced resources on web applications. These files may disclose sensitive information that can facilitate a focused attack against the application. Unreferenced pages may contain powerful functionality that can be used to attack the application. [OWASP]

RECOMMENDATION

The security of systems should not be based on the obscurity of resource locations. Remove or limit access to the file.

25.3 Sensitive Unreferenced Resource Found

SEVERITY Low

URL http://localhost/phpmyadmin/

REQUEST / RESPONSE

#1

```
GET /phpmyadmin/ HTTP/1.1
Referer: http://localhost/phpmyadmin
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:08:28 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Expires: Thu, 16 May 2024 10:08:29 +0000
Cache-Control: no-store, no-cache, must-revalidate, pre-check=0, post-check=0, max-age=0
Last-Modified: Thu, 16 May 2024 10:08:29 +0000
Set-Cookie: phpMyAdmin=prqtdhngpp3jds6cmbpulra02h; path=/phpmyadmin/; HttpOnly; SameSite=Strict
Set-Cookie: phpMyAdmin=prqtdhngpp3jds6cmbpulra02h; path=/phpmyadmin/; HttpOnly; SameSite=Strict
Set-Cookie: pma_lang=en; expires=Sat, 15-Jun-2024 10:08:28 GMT; Max-Age=2592000; path=/phpmyadmin/;
HttpOnly; SameSite=Strict
X-ob_mode: 1
X-Frame-Options: DENY
Referrer-Policy: no-referrer
Content-Security-Policy: default-src 'self' ;script-src 'self' 'unsafe-inline' 'unsafe-eval' ;style
-src 'self' 'unsafe-inline' ;img-src 'self' data:  *.tile.openstreetmap.org;object-src 'none';
X-Content-Security-Policy: default-src 'self' ;options inline-script eval-script;referrer no-referr
er;img-src 'self' data:  *.tile.openstreetmap.org;object-src 'none';
X-WebKit-CSP: default-src 'self' ;script-src 'self'  'unsafe-inline' 'unsafe-eval';referrer no-refe
rrer;style-src 'self' 'unsafe-inline' ;img-src 'self' data:  *.tile.openstreetmap.org;object-src 'n
one';
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Permitted-Cross-Domain-Policies: none
X-Robots-Tag: noindex, nofollow
Pragma: no-cache
Content-Encoding: gzip
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=56
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8

<!doctype html>
<html lang="en" dir="ltr">
<head>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <meta name="
...[truncated]...
```

DESCRIPTION

Attackers can often predict unreferenced resources on web applications. These files may disclose sensitive information that can facilitate a focused attack against the application. Unreferenced pages may contain powerful functionality that can be used to attack the application. OWASP

RECOMMENDATION

The security of systems should not be based on the obscurity of resource locations. Remove or limit access to the file.

25.4 Sensitive Unreferenced Resource Found

SEVERITY	Low
URL	http://localhost/show/db.sql

REQUEST / RESPONSE

#1

```
GET /show/ HTTP/1.1
Referer: http://localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:13 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
Content-Length: 975
Keep-Alive: timeout=5, max=93
Connection: Keep-Alive
Content-Type: text/html;charset=UTF-8

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
 <head>
  <title>Index of /show</title>
 </head>
 <body>
<h1>Index of /show</h1>
  <table>
   <tr
...[truncated]...
```

DESCRIPTION

Attackers can often predict unreferenced resources on web applications. These files may disclose sensitive information that can facilitate a focused attack against the application. Unreferenced pages may contain powerful functionality that can be used to attack the application. OWASP

RECOMMENDATION

The security of systems should not be based on the obscurity of resource locations. Remove or limit access to the file.

26.1 Cookie without HttpOnly Flag

SEVERITY	Low
URL	http://localhost/dashboard/
COOKIE	profile=Tzo4OiJzdGRDbGFzcyI6Mjp7czo4OiJ1c2VyTmFtZSI7czo4OiJ0ZXN0dXNlciI7czo2OiJ1c2VySWQiO2k6MTI7fQ%3D%3D

REQUEST / RESPONSE

#1

```
GET /dashboard/ HTTP/1.1
Referer: http://localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: id=eyJ1c2VyTmFtZSI6InRlc3R1c2VyIiwidXNlcklkIjoxMn0%3D; PHPSESSID=e2n36q648gvr9u8rk3hsdmboe
o;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:08:05 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Set-Cookie: profile=Tzo4OiJzdGRDbGFzcyI6Mjp7czo4OiJ1c2VyTmFtZSI7czo4OiJ0ZXN0dXNlciI7czo2OiJ1c2VySWQ
iO2k6MTI7fQ%3D%3D
Set-Cookie: p3=rO0ABXNyAAlTb21lQ2xhc3MAAAAAAAAAAQIABkkAAWJJAAFpTAABZHQAEkxqYXZhL2xhbmcvRG91YmxlO0wA
BGhoaGh0ABJMamF2YS9sYW5nL1N0cmluZztMAAFzcQB%2BAAJMAANzdHJxAH4AAnhwAAAAe3%2F%2F%2F%2F9zcgAQamF2YS5sY
W5nLkRvdWJsZYCzwkopa%2FsEAgABRAAFdmFsdWV4cgAQamF2YS5sYW5nLk51bWJlcoaslR0LlOCLAgAAeHC%2F8AAAAAAAAHQA
BmhoaGhoaHQABUFCQ0RFdAAGc3RyaW5n
Content-Length: 14
Keep-Alive: timeout=5, max=16
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

Hello testuser
```

DESCRIPTION

The `HttpOnly` cookie flag prevents JavaScript `Document.cookie` API from accessing the cookie. When this flag is set, the cookie is only sent to the server. In many cases, cookies are not needed on the client-side. Session cookies are a good example of cookies that don't need to be available to JavaScript. Using the `HttpOnly` flag can help to mitigate Cross-Site-Scripting(XSS) attacks.

RECOMMENDATION

Set `HttpOnly` flag for the cookie.

26.2 Cookie without HttpOnly Flag

SEVERITY	Low
URL	http://localhost/dashboard/
COOKIE	p3=rO0ABXNyAAlTb21lQ2xhc3MAAAAAAAAAAQIABkkAAWJJAAFpTAABZHQAEkxqYXZhL2xhbmcvRG91YmxlO0wABGhoaGh0ABJMamF2YS9sYW5nL1N0cmluZztMAAFzcQB%2BAAJMAANzdHJxAH4AAnhwAAAAe3%2F%2F%2F%2F9zcgAQamF2YS5sYW5nLkRvdWJsZYCzwkopa%2FsEAgABRAAFdmFsdWV4cgAQamF2YS5sYW5nLk51bWJlcoaslR0LlOCLAgAAeHC%2F8AAAAAAAAAAHQABmhoaGhoaHQABUFCQ0RFdAAGc3RyaW5n

REQUEST / RESPONSE

#1

```
GET /dashboard/ HTTP/1.1
Referer: http://localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: id=eyJ1c2VyTmFtZSI6InRlc3R1c2VyIiwidXNlcklkIjoxMn0%3D; PHPSESSID=e2n36q648gvr9u8rk3hsdmboe
o;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:08:05 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Set-Cookie: profile=Tzo4OiJzdGRDbGFzcyI6Mjp7czo4OiJ1c2VyTmFtZSI7czo4OiJ0ZXN0dXNlciI7czo2OiJ1c2VySWQ
iO2k6MTI7fQ%3D%3D
Set-Cookie: p3=rO0ABXNyAAlTb21lQ2xhc3MAAAAAAAAAAQIABkkAAWJJAAFpTAABZHQAEkxqYXZhL2xhbmcvRG91YmxlO0wA
BGhoaGh0ABJMamF2YS9sYW5nL1N0cmluZztMAAFzcQB%2BAAJMAANzdHJxAH4AAnhwAAAAe3%2F%2F%2F%2F9zcgAQamF2YS5sY
W5nLkRvdWJsZYCzwkopa%2FsEAgABRAAFdmFsdWV4cgAQamF2YS5sYW5nLk51bWJlcoaslR0LlOCLAgAAeHC%2F8AAAAAAAAAAHQA
BmhoaGhoaHQABUFCQ0RFdAAGc3RyaW5n
Content-Length: 14
Keep-Alive: timeout=5, max=16
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

Hello testuser
```

DESCRIPTION

The `HttpOnly` cookie flag prevents JavaScript `Document.cookie` API from accessing the cookie. When this flag is set, the cookie is only sent to the server. In many cases, cookies are not needed on the client-side. Session cookies are a good example of cookies that don't need to be available to JavaScript. Using the `HttpOnly` flag can help to mitigate Cross-Site-Scripting(XSS) attacks.

RECOMMENDATION

Set `HttpOnly` flag for the cookie.

26.3 Cookie without HttpOnly Flag

SEVERITY	Low
URL	http://localhost/dashboard/json.php
COOKIE	id=eyJ1c2VyTmFtZSI6InRlc3R1c2VyIiwidXNlcklkIjoxMn0%3D

REQUEST / RESPONSE

#1

```
GET /dashboard/json.php HTTP/1.1
Referer: http://localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: id=rawplain; PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:07 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Set-Cookie: id=eyJ1c2VyTmFtZSI6InRlc3R1c2VyIiwidXNlcklkIjoxMn0%3D
Content-Length: 14
Keep-Alive: timeout=5, max=83
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

Hello testuser
```

DESCRIPTION

The `HttpOnly` cookie flag prevents JavaScript `Document.cookie` API from accessing the cookie. When this flag is set, the cookie is only sent to the server. In many cases, cookies are not needed on the client-side. Session cookies are a good example of cookies that don't need to be available to JavaScript. Using the `HttpOnly` flag can help to mitigate Cross-Site-Scripting(XSS) attacks.

RECOMMENDATION

Set `HttpOnly` flag for the cookie.

26.4 Cookie without HttpOnly Flag

SEVERITY	Low
URL	http://localhost/tmp/
COOKIE	this_should_not_be=1

REQUEST / RESPONSE

#1

```
GET /tmp/ HTTP/1.1
Referer:
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: this_should_not_be=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa; PHPSESSI
D=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:09:24 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Set-Cookie: this_should_not_be=1
Content-Length: 11
Keep-Alive: timeout=5, max=57
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

aaa@sss.com
```

DESCRIPTION

The `HttpOnly` cookie flag prevents JavaScript `Document.cookie` API from accessing the cookie. When this flag is set, the cookie is only sent to the server. In many cases, cookies are not needed on the client-side. Session cookies are a good example of cookies that don’t need to be available to JavaScript. Using the `HttpOnly` flag can help to mitigate Cross-Site-Scripting(XSS) attacks.

RECOMMENDATION

Set `HttpOnly` flag for the cookie.

27.1 Auto Complete Enabled Password Input

SEVERITY	Low
URL	http://localhost/formauth/bypassBlock.php

REQUEST / RESPONSE

#1

```
GET /formauth/bypassBlock.php HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Referer: smta%EF%BC%9Cb%CA%BAc%CA%B9d%ef%bb%bfetms769
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:07 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 463
Keep-Alive: timeout=5, max=95
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<br />
<b>Warning</b>:  Undefined array key "name" in <b>C:\xampp\htdocs\formauth\bypassBlock.php</b> on l
ine <b>4</b><br />
<br />
<b>Warning</b>:  Undefined a
...[truncated]...
```

DESCRIPTION

The user browser can save and remember the entered values for user input fields with autocomplete enabled attributes. This might reveal sensitive information like passwords, especially in public and multi-user computers.

RECOMMENDATION

Add the attribute `autocomplete="off"` for sensitive form inputs.

27.2 Auto Complete Enabled Password Input

SEVERITY	Low
URL	http://localhost/formauth/enumerate.php

REQUEST / RESPONSE

#1

```
GET /formauth/enumerate.php HTTP/1.1
Referer: http://localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:13 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 458
Keep-Alive: timeout=5, max=82
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<br />
<b>Warning</b>:  Undefined array key "user" in <b>C:\xampp\htdocs\formauth\enumerate.php</b> on lin
e <b>3</b><br />
<br />
<b>Warning</b>:  Undefined arr
...[truncated]...
```

DESCRIPTION

The user browser can save and remember the entered values for user input fields with autocomplete enabled attributes. This might reveal sensitive information like passwords, especially in public and multi-user computers.

RECOMMENDATION

Add the attribute `autocomplete="off"` for sensitive form inputs.

28.1 Directory Listing of Sensitive Files

SEVERITY	Low
URL	http://localhost/admin/

DETAILS

Directory listing discloses sensitive or dynamic application files.

REQUEST / RESPONSE

#1

```
GET /admin/ HTTP/1.1
Referer: 
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:08:22 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
Content-Length: 1403
Keep-Alive: timeout=5, max=54
Connection: Keep-Alive
Content-Type: text/html;charset=UTF-8

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
 <head>
  <title>Index of /admin</title>
 </head>
 <body>
<h1>Index of /admin</h1>
  <table>
   <
...[truncated]...
```

DESCRIPTION

A directory listing provides an attacker with the complete index of all the resources located inside of the directory. The specific risks and consequences vary depending on which files are listed and accessible. MITRE

RECOMMENDATION

Create a default index file or disable directory listing in web server configurations.

28.2 Directory Listing of Sensitive Files

SEVERITY	Low
URL	http://localhost/show/

DETAILS

Directory listing discloses sensitive or dynamic application files.

REQUEST / RESPONSE

#1

```
GET /show/ HTTP/1.1
Referer: http://localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:13 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
Content-Length: 975
Keep-Alive: timeout=5, max=93
Connection: Keep-Alive
Content-Type: text/html;charset=UTF-8

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
 <head>
  <title>Index of /show</title>
 </head>
 <body>
<h1>Index of /show</h1>
  <table>
   <tr
...[truncated]...
```

DESCRIPTION

A directory listing provides an attacker with the complete index of all the resources located inside of the directory. The specific risks and consequences vary depending on which files are listed and accessible. MITRE

RECOMMENDATION

Create a default index file or disable directory listing in web server configurations.

29.1 Directory Listing

SEVERITY	Low
URL	http://localhost/icons/

REQUEST / RESPONSE

#1

```
GET /icons/ HTTP/1.1
Referer: http://localhost/show/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:08:05 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
Keep-Alive: timeout=5, max=75
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html;charset=UTF-8

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
 <head>
  <title>Index of /icons</title>
 </head>
 <body>
<h1>Index of /icons</h1>
  <table>
   <
...[truncated]...
```

DESCRIPTION

A directory listing provides an attacker with the complete index of all the resources located inside of the directory. The specific risks and consequences vary depending on which files are listed and accessible. MITRE

RECOMMENDATION

Create a default index file or disable directory listing in web server configurations.

29.2 Directory Listing

SEVERITY	Low
URL	http://localhost/icons/small/

REQUEST / RESPONSE

#1

```
GET /icons/small/ HTTP/1.1
Referer: http://localhost/icons/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:08:05 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html;charset=UTF-8

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
 <head>
  <title>Index of /icons/small</title>
 </head>
 <body>
<h1>Index of /icons/small</h1>

...[truncated]...
```

DESCRIPTION

A directory listing provides an attacker with the complete index of all the resources located inside of the directory. The specific risks and consequences vary depending on which files are listed and accessible. MITRE

RECOMMENDATION

Create a default index file or disable directory listing in web server configurations.

30.1 Content-Security-Policy Header is Missing

SEVERITY	Low
URL	http://localhost
AFFECTED URLS (21)	localhost/contact/ localhost/xss/ localhost/dashboard/json.php localhost/ping/ localhost/show/ localhost/xss/base64.php localhost/xss/script-inline.php localhost/iframe/secure.html localhost/msg/ZGRkZGRkZGRkZA== localhost/formauth/ localhost/ssi/ localhost/formauth/enumerate.php localhost localhost/user/ localhost/formauth/bypassBlock.php localhost/display/ localhost/iframe/ localhost/user/name/ localhost/icons/small/ localhost/feed/ ...

REQUEST / RESPONSE

#1

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:07 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 7908
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en" >

<head>
  <meta charset="UTF-8">
  <title>Complete test cases</title>
  <style>
body {
  margin: 0 auto;
  max-width:
...[truncated]...
```

DESCRIPTION

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement to distribution of malware. Mozilla

RECOMMENDATION

Configure your server to send this header for all pages. You can see references for possible values.

31.1 X-Frame-Options Header is Missing

SEVERITY	Low
URL	http://localhost
AFFECTED URLS (21)	localhost/contact/ localhost/xss/ localhost/dashboard/json.php localhost/ping/ localhost/show/ localhost/xss/base64.php localhost/xss/script-inline.php localhost/iframe/secure.html localhost/msg/ZGRkZGRkZGRkZA== localhost/formauth/ localhost/ssi/ localhost/formauth/enumerate.php localhost localhost/user/ localhost/formauth/bypassBlock.php localhost/display/ localhost/iframe/ localhost/user/name/ localhost/icons/small/ localhost/feed/ ...

REQUEST / RESPONSE

#1

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Content-Length: 0

```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:07 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 7908
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en" >

<head>
  <meta charset="UTF-8">
  <title>Complete test cases</title>
  <style>
body {
  margin: 0 auto;
  max-width:
...[truncated]...
```

DESCRIPTION

The `X-Frame-Options` HTTP response header can be used to indicate whether or not a browser should be allowed to render a page in a `<frame>`, `<iframe>`, `<embed>` or `<object>`. Sites can use this to avoid click-jacking attacks, by ensuring that their content is not embedded into other sites.

Mozilla

RECOMMENDATION

Configure your server to send this header for all pages. You can see references for possible values.

32.1 Subresource Integrity is Missing

SEVERITY	Low
URL	http://localhost/ssi/
EXTERNAL RESOURCES	https://code.jquery.com/ui/1.13.0-alpha.1/themes/smoothness/jquery-ui.css https://unpkg.com/vue@3.0.2

REQUEST / RESPONSE

#1

```
GET /ssi/ HTTP/1.1
Referer: http://localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Content-Length: 0
User-Agent: {{800944-1}}
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:07 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
Last-Modified: Wed, 13 Apr 2022 08:24:26 GMT
ETag: "147-5dc84e7d62df8"
Accept-Ranges: bytes
Content-Length: 327
Keep-Alive: timeout=5, max=81
Connection: Keep-Alive
Content-Type: text/html

<html>

<head>
<script type="text/javascript" src="https://unpkg.com/vue@3.0.2"></script>
<link type="text/css" rel="stylesheet" href="https://code.jquery.com/ui/1.13.0-alpha.1/themes/smoot
hne
...[truncated]...
```

DESCRIPTION

Subresource Integrity (SRI) is a security feature that enables browsers to verify that resources they fetch (for example, from a CDN) are delivered without unexpected manipulation. It works by allowing you to provide a cryptographic hash that a fetched resource must match. Moilla

RECOMMENDATION

Add a base64-encoded hash of the resource in the value of the `integrity` attribute of the `<script>` or `<link>` element. You can ask the resource provider for the hash of the file or calculate it on your own. Please references for details.

33.1 Cookie without SameSite Flag

SEVERITY	Low
URL	http://localhost/dashboard/json.php
COOKIE	

REQUEST / RESPONSE

1

```
GET /dashboard/json.php HTTP/1.1
Referer: http://localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: id=rawplain; PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:07 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Set-Cookie: id=eyJ1c2VyTmFtZSI6InRlc3R1c2VyIiwidXNlcklkIjoxMn0%3D
Content-Length: 14
Keep-Alive: timeout=5, max=83
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

Hello testuser
```

DESCRIPTION

The `SameSite` cookie flag with the right value prevents the browser from sending the cookie in cross-origin requests. It provides some protection against cross-site request forgery attacks (CSRF).

RECOMMENDATION

Set `SameSite` flag for the cookie.

34.1 Apache Version Disclosure

SEVERITY	Low
URL	http://localhost
VERSION	2.4.58 (win64)

REQUEST / RESPONSE

#1

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:07 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 7908
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en" >

<head>
  <meta charset="UTF-8">
  <title>Complete test cases</title>
  <style>
body {
  margin: 0 auto;
  max-width:
...[truncated]...
```

DESCRIPTION

A bad configured web server can leak Apache version number in the `Server` HTTP header or in the body of error pages. Attackers use this information for finding vulnerabilities in Apache web server.

RECOMMENDATION

Open the Apache configuration file (`httpd.conf` or `apache2.conf`) and add below lines to it.

```
ServerTokens Prod
ServerSignature Off
```

Restart the web server.

35.1 Insecure Inline Frame

SEVERITY	Low
URL	http://localhost/iframe/index.html
IFRAME URL	https://example.com

DETAILS

An `iframe` tag is loading an external URL without `sandbox` attribute.

REQUEST / RESPONSE

#1

```
GET /iframe/index.html HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Referer: {{369293-1}}
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:07 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
Last-Modified: Tue, 14 Feb 2023 11:56:25 GMT
ETag: "5f-5f4a7a72e3f11"
Accept-Ranges: bytes
Content-Length: 95
Keep-Alive: timeout=5, max=86
Connection: Keep-Alive
Content-Type: text/html

<html>
    <body>
        <iframe src="https://example.com"></iframe>
    </body>

</html>
```

DESCRIPTION

An inline frame tag (`iframe`) on the page refers to an external resource, and no `sandbox` is set. This allows the external URL to trick users into doing unwanted actions like submitting passwords.

RECOMMENDATION

Set `sandbox` attribute for iframes with external URL.

36.1 TRACE Method Allowed

SEVERITY	Low
URL	http://localhost/

REQUEST / RESPONSE

#1

```
TRACE / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:08 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
Keep-Alive: timeout=5, max=85
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: message/http

TRACE / HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla
...[truncated]...
```

DESCRIPTION

HTTP TRACE method allows a client to see the whole request that the webserver has received. The main purpose of this feature is for testing or diagnostic information.
This method can reveal sensitive information like Cookies and Authorization tokens to clients when they’re not supposed to access these data. This is often called a **Cross-Site Tracing (XST)** attack.

RECOMMENDATION

Disable the TRACE method in the webserver configuration.
For the Apache web server, add the below line to the main configuration file.

```
TraceEnable off
```

For Microsoft IIS open **ISS Manager**, go to **Request Filtering**, and change the configuration for TRACK and TRACE verbs in **HTTP Verbs**.

37.1 Windows Path Disclosure

SEVERITY	Informational
URL	http://localhost
PATH	C:\xampp\htdocs

REQUEST / RESPONSE

#1

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:07 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 7908
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

...[truncated]...
C:\xampp\htdocs\</span>
        <span>/var/log/www/</spa
...[truncated]...
```

DESCRIPTION

File and directory paths reveal information about the structure of the file system of the underlying OS. This information does not create any direct impact on the target, though it provides valuable information attackers can use in their attack.

RECOMMENDATION

If it's not displayed intentionally, fix the reason causing the disclosure and make sure the path is not revealed due to errors and misconfigurations.

37.2 Windows Path Disclosure

SEVERITY	Informational
URL	http://localhost/display/?f='%22!?-%25s
FOUND IN (29)	localhost/display/?f=%7B%7B561181-1%7D%7D localhost/display/?f=99999 or 1%3E0-- a localhost/display/?f=a.html'; if (1%3D1) waitfor delay '00:00:03'-- localhost/display/?f=a.html' and 1%3E1-- a localhost/display/?f=smta＜b″c′detms769 localhost/display/?f=a%26ping 2130706433%26%23'%26ping 2130706434%26a%26%23%22%26ping 2130706435%26a%5C localhost/display/?f=a.html or 1%3DExtractValue(1,CoNCaT(0x3a,(md5(122459)))) localhost/display/?f=99999 or 1%3E0 localhost/display/?f=99999' or '1'%3E'0 localhost/display/?f=99999' or 1%3E0-- a localhost/display/?f='%22!?-%25s localhost/display/?f=a.html' and '1'%3E'1 localhost/display/?f=a.html; if (1%3D1) waitfor delay '00:00:03'-- localhost/display/?f=a.html and 1%3E1 localhost/display/?f='XOR((SELECT(1)FROM(SELECT(if(now()%3Dsysdate(),sleep(3),0)))A))OR' localhost/display/?f=%25%7B561181-1%7D localhost/display/?f=a.html and 1%3E1-- a localhost/display/?f=a%7Cver localhost/display/?f=99999%22 or %221%22%3E%220 localhost/display/?f=a.html%22 and %221%22%3E%221 ...
PATH	C:\xampp\php\PEAR C:\xampp\htdocs\display\index.php

REQUEST / RESPONSE

#1

```
GET /display/?f='%22!?-%25s HTTP/1.1
Referer: http://localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:16 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 355
Keep-Alive: timeout=5, max=13
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

```
...[truncated]...
C:\xampp\htdocs\display\index.php</b> on line <b>4</b><br />
<br />
<b>Warning</b>:  include(): Failed opening ''&quot;!?-%s' for inclusion (include_path='C:\xampp\php
\PEAR') in <b>
...[truncated]...
```

DESCRIPTION

File and directory paths reveal information about the structure of the file system of the underlying OS. This information does not create any direct impact on the target, though it provides valuable information attackers can use in their attack.

RECOMMENDATION

If it’s not displayed intentionally, fix the reason causing the disclosure and make sure the path is not revealed due to errors and misconfigurations.

37.3 Windows Path Disclosure

SEVERITY	Informational
URL	http://localhost/display/index.php
PATH	C:\xampp\htdocs\display\index.php

REQUEST / RESPONSE

#1

```
GET /display/index.php HTTP/1.1
Referer: http://localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:09:36 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 334
Keep-Alive: timeout=5, max=36
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

...[truncated]...
C:\xampp\htdocs\display\index.php</b> on line <b>4</b><br />
<br />
<b>Fatal error</b>:  Uncaught ValueError: Path cannot be empty in C:\xampp\htdocs\display\index.ph
p:4
Stack trace:
#0 {main}
  thrown in <b>
...[truncated]...
```

DESCRIPTION

File and directory paths reveal information about the structure of the file system of the underlying OS. This information does not create any direct impact on the target, though it provides valuable information attackers can use in their attack.

RECOMMENDATION

If it’s not displayed intentionally, fix the reason causing the disclosure and make sure the path is not revealed due to errors and misconfigurations.

37.4 Windows Path Disclosure

SEVERITY	Informational
URL	http://localhost/feed/
PATH	C:\xampp\htdocs\feed\index.php

REQUEST / RESPONSE

#1

```
POST /feed/ HTTP/1.1
Authorization: valid-token
Content-Type: applicatioN/json
Referer: http://localhost/feed/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 4
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
Content-Length: 4

{
}
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:08:04 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 508
Keep-Alive: timeout=5, max=41
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

...[truncated]...
C:\xampp\htdocs\feed\index.php</b> on line <b>13</
...[truncated]...
```

DESCRIPTION

File and directory paths reveal information about the structure of the file system of the underlying OS. This information does not create any direct impact on the target, though it provides valuable information attackers can use in their attack.

RECOMMENDATION

If it’s not displayed intentionally, fix the reason causing the disclosure and make sure the path is not revealed due to errors and misconfigurations.

37.5 Windows Path Disclosure

SEVERITY	Informational
URL	http://localhost/formauth/
PATH	C:\xampp\htdocs\formauth\index.php

REQUEST / RESPONSE

#1

```
GET /formauth/ HTTP/1.1
Referer: http://localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:13 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 447
Keep-Alive: timeout=5, max=84
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

...[truncated]...
C:\xampp\htdocs\formauth\index.php</b> on line <b>3</b><br />
<html>
<body>
        <form method="POST">
        <br />
<b>Warning</b>:  Undefined variable $error in <b>
...[truncated]...
```

DESCRIPTION

File and directory paths reveal information about the structure of the file system of the underlying OS. This information does not create any direct impact on the target, though it provides valuable information attackers can use in their attack.

RECOMMENDATION

If it’s not displayed intentionally, fix the reason causing the disclosure and make sure the path is not revealed due to errors and misconfigurations.

37.6 Windows Path Disclosure

SEVERITY	Informational
URL	http://localhost/formauth/bypassBlock.php
PATH	C:\xampp\htdocs\formauth\bypassBlock.php

REQUEST / RESPONSE

#1

```
GET /formauth/bypassBlock.php HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Referer: smta%EF%BC%9Cb%CA%BAc%CA%B9d%ef%bb%bfetms769
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:07 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 463
Keep-Alive: timeout=5, max=95
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

...[truncated]...
C:\xampp\htdocs\formauth\bypassBlock.php</b> on line <b>4</b><br />
<br />
<b>Warning</b>:  Undefined array key "name" in <b>
...[truncated]...
```

DESCRIPTION

File and directory paths reveal information about the structure of the file system of the underlying OS. This information does not create any direct impact on the target, though it provides valuable information attackers can use in their attack.

RECOMMENDATION

If it’s not displayed intentionally, fix the reason causing the disclosure and make sure the path is not revealed due to errors and misconfigurations.

37.7 Windows Path Disclosure

SEVERITY	Informational
URL	http://localhost/formauth/enumerate.php
PATH	C:\xampp\htdocs\formauth\enumerate.php

REQUEST / RESPONSE

#1

```
GET /formauth/enumerate.php HTTP/1.1
Referer: http://localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:13 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 458
Keep-Alive: timeout=5, max=82
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

...[truncated]...
C:\xampp\htdocs\formauth\enumerate.php</b> on line <b>3</b><br />
<br />
<b>Warning</b>:  Undefined array key "user" in <b>
...[truncated]...
```

DESCRIPTION

File and directory paths reveal information about the structure of the file system of the underlying OS. This information does not create any direct impact on the target, though it provides valuable information attackers can use in their attack.

RECOMMENDATION

If it’s not displayed intentionally, fix the reason causing the disclosure and make sure the path is not revealed due to errors and misconfigurations.

37.8 Windows Path Disclosure

SEVERITY	Informational
URL	http://localhost/ping/?i[]=127.0.0.1
FOUND IN	localhost/ping/ localhost/ping/?i[]=127.0.0.1
PATH	C:\xampp\htdocs\ping\index.php

REQUEST / RESPONSE

#1

```
GET /ping/?i[]=127.0.0.1 HTTP/1.1
Referer: http://localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:08:06 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 354
Keep-Alive: timeout=5, max=90
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

...[truncated]...
C:\xampp\htdocs\ping\index.php</b> on line <b>5</b
...[truncated]...
```

DESCRIPTION

File and directory paths reveal information about the structure of the file system of the underlying OS. This information does not create any direct impact on the target, though it provides valuable information attackers can use in their attack.

RECOMMENDATION

If it’s not displayed intentionally, fix the reason causing the disclosure and make sure the path is not revealed due to errors and misconfigurations.

37.9 Windows Path Disclosure

SEVERITY	Informational
URL	http://localhost/redir/?u[]=http://localhost/
FOUND IN	localhost/redir/?u=QvXuSbA%0D%0AQvXuSbA localhost/redir/?u[]=http://localhost/
PATH	C:\xampp\htdocs\redir\index.php

REQUEST / RESPONSE

#1

```
GET /redir/?u[]=http://localhost/ HTTP/1.1
Referer: http://localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 301 Moved Permanently
Date: Thu, 16 May 2024 10:08:02 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Location: Array
Content-Length: 116
Keep-Alive: timeout=5, max=97
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

...[truncated]...
C:\xampp\htdocs\redir\index.php</b> on line <b>7</
...[truncated]...
```

DESCRIPTION

File and directory paths reveal information about the structure of the file system of the underlying OS. This information does not create any direct impact on the target, though it provides valuable information attackers can use in their attack.

RECOMMENDATION

If it’s not displayed intentionally, fix the reason causing the disclosure and make sure the path is not revealed due to errors and misconfigurations.

37.10 Windows Path Disclosure

SEVERITY	Informational
URL	http://localhost/server-info
PATH (25)	C:/xampp/apache/conf/extra/httpd-mpm.conf C:/xampp/webalizer C:/xampp/apache C:/xampp/apache/conf/extra/httpd-ssl.conf C:/xampp/cgi-bin C:/xampp/php C:/xampp/apache/bin/openssl.cnf C:/xampp/apache/logs/ssl_scache C:/xampp/licenses C:/xampp/apache/conf/extra/httpd-info.conf C:/xampp/apache/cgi-bin C:/xampp/apache/conf/extra/httpd-xampp.conf C:/xampp/apache/conf/extra/httpd-default.conf C:/xampp/apache/conf/httpd.conf C:/xampp/php/extras/mibs C:/xampp/htdocs C:/xampp/apache/logs/access.log C:/xampp/apache/logs/error.log C:/xampp/apache/conf/extra/httpd-languages.conf C:/xampp/apache/logs/ssl_request.log ...

REQUEST / RESPONSE

#1

```
GET /server-info HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:07 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
Keep-Alive: timeout=5, max=97
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=ISO-8859-1

...[truncated]...
C:/xampp/apache</tt></dt>
<dt><strong>Config File:</strong> <tt>C:/xampp/apache/conf/httpd.conf</tt></dt>
<dt><strong>Server Built With:</strong>
<tt style="white-space: pre;">
 -D APR_HAS_SENDFILE
 -D APR_HAS_MMAP
 -D APR_HAVE_IPV6 (IPv4-mapped addr
...[truncated]...
```

DESCRIPTION

File and directory paths reveal information about the structure of the file system of the underlying OS. This information does not create any direct impact on the target, though it provides valuable information attackers can use in their attack.

RECOMMENDATION

If it’s not displayed intentionally, fix the reason causing the disclosure and make sure the path is not revealed due to errors and misconfigurations.

37.11 Windows Path Disclosure

SEVERITY	Informational
URL	http://localhost/user/name/index.php
PATH	C:\xampp\htdocs\user\name\index.php

REQUEST / RESPONSE

#1

```
POST /user/name/index.php HTTP/1.1
Authorization: valid-token
Content-Type: application/x-www-form-urlencoded
Referer: http://localhost/user/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 13
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
Content-Length: 13

name[]=myname
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:08:02 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 125
Keep-Alive: timeout=5, max=98
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

...[truncated]...
C:\xampp\htdocs\user\name\index.php</b> on line <b
...[truncated]...
```

DESCRIPTION

File and directory paths reveal information about the structure of the file system of the underlying OS. This information does not create any direct impact on the target, though it provides valuable information attackers can use in their attack.

RECOMMENDATION

If it's not displayed intentionally, fix the reason causing the disclosure and make sure the path is not revealed due to errors and misconfigurations.

37.12 Windows Path Disclosure

SEVERITY	Informational
URL	http://localhost/xss/base64.php?name[]=YmFzZTY0LWVuY29kZWQtdmFsdWU
FOUND IN	localhost/xss/base64.php?name[]=YmFzZTY0LWVuY29kZWQtdmFsdWU localhost/xss/base64.php
PATH	C:\xampp\htdocs\xss\base64.php

REQUEST / RESPONSE

#1

```
GET /xss/base64.php?name[]=YmFzZTY0LWVuY29kZWQtdmFsdWU HTTP/1.1
Referer: http://localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:14 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 320
Keep-Alive: timeout=5, max=68
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

...[truncated]...
C:\xampp\htdocs\xss\base64.php:3
Stack trace:
#0 C:\xampp\htdocs\xss\base64.php(3): base64_decode(Array)
#1 {main}
  thrown in <b>
...[truncated]...
```

DESCRIPTION

File and directory paths reveal information about the structure of the file system of the underlying OS. This information does not create any direct impact on the target, though it provides valuable information attackers can use in their attack.

RECOMMENDATION

If it’s not displayed intentionally, fix the reason causing the disclosure and make sure the path is not revealed due to errors and misconfigurations.

37.13 Windows Path Disclosure

SEVERITY	Informational
URL	http://localhost/xss/index.php?name[]=test
PATH	C:\xampp\htdocs\xss\index.php

REQUEST / RESPONSE

#1

```
GET /xss/index.php?name[]=test HTTP/1.1
Referer: http://localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:16 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
X-XSS-Protection: 1
Content-Length: 125
Keep-Alive: timeout=5, max=34
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

...[truncated]...
C:\xampp\htdocs\xss\index.php</b> on line <b>4</b>
...[truncated]...
```

DESCRIPTION

File and directory paths reveal information about the structure of the file system of the underlying OS. This information does not create any direct impact on the target, though it provides valuable information attackers can use in their attack.

RECOMMENDATION

If it's not displayed intentionally, fix the reason causing the disclosure and make sure the path is not revealed due to errors and misconfigurations.

37.14 Windows Path Disclosure

SEVERITY	Informational
URL	http://localhost/xss/script-inline.php?u[]=testa
PATH	C:\xampp\htdocs\xss\script-inline.php

REQUEST / RESPONSE

#1

```
GET /xss/script-inline.php?u[]=testa HTTP/1.1
Referer: http://localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:16 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 193
Keep-Alive: timeout=5, max=55
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

...[truncated]...
C:\xampp\htdocs\xss\script-inline.php</b> on line
...[truncated]...
```

DESCRIPTION

File and directory paths reveal information about the structure of the file system of the underlying OS. This information does not create any direct impact on the target, though it provides valuable information attackers can use in their attack.

RECOMMENDATION

If it’s not displayed intentionally, fix the reason causing the disclosure and make sure the path is not revealed due to errors and misconfigurations.

38.1 Email Address Disclosure

SEVERITY	Informational
URL	http://localhost
FOUND EMAILS	admin@gmail.com

REQUEST / RESPONSE

#1

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:07 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 7908
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

...[truncated]...
admin@gmail.com">admin@gmail.com</a>
        </div>
  <
...[truncated]...
```

DESCRIPTION

Spambots can harvest email addresses from webpages and use them for sending spam emails.

RECOMMENDATION

Do not show personal email addresses. Use submission forms with CAPTCHA for receiving messages.

38.2 Email Address Disclosure

SEVERITY	Informational
URL	http://localhost/icons/
FOUND EMAILS	mike@hyperreal.org kevinh@kevcom.com

REQUEST / RESPONSE

#1

```
GET /icons/ HTTP/1.1
Referer: http://localhost/show/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:08:05 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
Keep-Alive: timeout=5, max=75
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html;charset=UTF-8

...[truncated]...
kevinh@kevcom.com).
Andy Polyakov tuned the icon colors and added few new images.</p>

<p>If you'd like to contribute additions to this set, contact the httpd
documentation project <a href="http://httpd.apache.org/docs-project/"
>http://httpd.ap
...[truncated]...
```

DESCRIPTION

Spambots can harvest email addresses from webpages and use them for sending spam emails.

RECOMMENDATION

Do not show personal email addresses. Use submission forms with CAPTCHA for receiving messages.

38.3 Email Address Disclosure

SEVERITY	Informational
URL	http://localhost/server-info
FOUND EMAILS	admin@example.com

REQUEST / RESPONSE

#1

```
GET /server-info HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:07 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
Keep-Alive: timeout=5, max=97
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=ISO-8859-1

...[truncated]...
admin@example.com</i></tt></dd>
<dd><tt>&nbsp;127:
...[truncated]...
```

DESCRIPTION

Spambots can harvest email addresses from webpages and use them for sending spam emails.

RECOMMENDATION

Do not show personal email addresses. Use submission forms with CAPTCHA for receiving messages.

38.4 Email Address Disclosure

SEVERITY	Informational
URL	http://localhost/tmp/
FOUND EMAILS	aaa@sss.com

REQUEST / RESPONSE

#1

```
GET /tmp/ HTTP/1.1
Referer:
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: this_should_not_be=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa; PHPSESSI
D=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:09:24 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Set-Cookie: this_should_not_be=1
Content-Length: 11
Keep-Alive: timeout=5, max=57
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

aaa@sss.com
```

DESCRIPTION

Spambots can harvest email addresses from webpages and use them for sending spam emails.

RECOMMENDATION

Do not show personal email addresses. Use submission forms with CAPTCHA for receiving messages.

39.1 Content Character Encoding is not Defined

SEVERITY	Informational
URL	http://localhost/iframe/index.html

REQUEST / RESPONSE

#1

```
GET /iframe/index.html HTTP/1.1
Referer: http://localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:07 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
Last-Modified: Tue, 14 Feb 2023 11:56:25 GMT
ETag: "5f-5f4a7a72e3f11"
Accept-Ranges: bytes
Content-Length: 95
Keep-Alive: timeout=5, max=98
Connection: Keep-Alive
Content-Type: text/html

<html>
    <body>
        <iframe src="https://example.com"></iframe>
    </body>

</html>
```

DESCRIPTION

Web browsers need to be aware of the encoding of characters to display it right. When the character encoding is not explicitly defined, the browser has to either guess the encoding or use a default encoding. This will allow attackers to use different encodings like UTF-7 to exploit vulnerabilities like XSS.

RECOMMENDATION

Send character encoding in HTTP header as shown below:

```
Content-Type: text/html; charset=UTF-8
```

or use HTML Meta tags like below:

```
< META http-equiv="Content-Type" content = "text/html; charset=UTF-8" >
```

39.2 Content Character Encoding is not Defined

SEVERITY	Informational
URL	http://localhost/iframe/secure.html

REQUEST / RESPONSE

#1

```
GET /iframe/secure.html HTTP/1.1
Referer: http://localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:10 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
Last-Modified: Tue, 14 Feb 2023 11:56:25 GMT
ETag: "71-5f4a7a72e3f11"
Accept-Ranges: bytes
Content-Length: 113
Keep-Alive: timeout=5, max=83
Connection: Keep-Alive
Content-Type: text/html

<html>
    <body>
        <iframe src="https://example.com"
        sandbox></iframe>
    </body>

</html>
```

DESCRIPTION

Web browsers need to be aware of the encoding of characters to display it right. When the character encoding is not explicitly defined, the browser has to either guess the encoding or use a default encoding. This will allow attackers to use different encodings like UTF-7 to exploit vulnerabilities like XSS.

RECOMMENDATION

Send character encoding in HTTP header as shown below:

```
Content-Type: text/html; charset=UTF-8
```

or use HTML Meta tags like below:

```
< META http-equiv="Content-Type" content = "text/html; charset=UTF-8" >
```

39.3 Content Character Encoding is not Defined

SEVERITY	Informational
URL	http://localhost/ssi/

REQUEST / RESPONSE

#1

```
GET /ssi/ HTTP/1.1
Referer: http://localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:07 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
Last-Modified: Wed, 13 Apr 2022 08:24:26 GMT
ETag: "147-5dc84e7d62df8"
Accept-Ranges: bytes
Content-Length: 327
Keep-Alive: timeout=5, max=96
Connection: Keep-Alive
Content-Type: text/html

<html>

<head>
<script type="text/javascript" src="https://unpkg.com/vue@3.0.2"></script>
<link type="text/css" rel="stylesheet" href="https://code.jquery.c
...[truncated]...
```

DESCRIPTION

Web browsers need to be aware of the encoding of characters to display it right. When the character encoding is not explicitly defined, the browser has to either guess the encoding or use a default encoding. This will allow attackers to use different encodings like UTF-7 to exploit vulnerabilities like XSS.

RECOMMENDATION

Send character encoding in HTTP header as shown below:

```
Content-Type: text/html; charset=UTF-8
```

or use HTML Meta tags like below:

```
< META http-equiv="Content-Type" content = "text/html; charset=UTF-8" >
```

40.1 Unreferenced Resource Found

SEVERITY	Informational
URL	http://localhost/admin/change.php

REQUEST / RESPONSE

#1

```
GET /admin/change.php HTTP/1.1
Referer: http://localhost/admin/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:08:22 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 0
Keep-Alive: timeout=5, max=51
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

DESCRIPTION

Attackers can often predict unreferenced resources on web applications. These files may disclose sensitive information that can facilitate a focused attack against the application. Unreferenced pages may contain powerful functionality that can be used to attack the application. OWASP

RECOMMENDATION

The security of systems should not be based on the obscurity of resource locations. Remove or limit access to the file.

40.2 Unreferenced Resource Found

SEVERITY	Informational
URL	http://localhost/Redirected/
REQUESTED URL	http://localhost/test.php

REQUEST / RESPONSE

#1

```
GET /Redirected/ HTTP/1.1
Referer:
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:09:24 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 81
Keep-Alive: timeout=5, max=73
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

hello
<a href="?q=1">query on same page</a>
<a href="subdir/">sub directory</a>
```

DESCRIPTION

Attackers can often predict unreferenced resources on web applications. These files may disclose sensitive information that can facilitate a focused attack against the application. Unreferenced pages may contain powerful functionality that can be used to attack the application. OWASP

RECOMMENDATION

The security of systems should not be based on the obscurity of resource locations. Remove or limit access to the file.

40.3 Unreferenced Resource Found

SEVERITY	Informational
URL	http://localhost/tmp/

REQUEST / RESPONSE

#1

```
GET /tmp/ HTTP/1.1
Referer:
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:09:24 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Set-Cookie: this_should_not_be=1
Content-Length: 11
Keep-Alive: timeout=5, max=61
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

aaa@sss.com
```

DESCRIPTION

Attackers can often predict unreferenced resources on web applications. These files may disclose sensitive information that can facilitate a focused attack against the application. Unreferenced pages may contain powerful functionality that can be used to attack the application. OWASP

RECOMMENDATION

The security of systems should not be based on the obscurity of resource locations. Remove or limit access to the file.

41.1 X-Content-Type-Options Header is Missing

SEVERITY	Informational
URL	http://localhost
AFFECTED URLS (21)	localhost/contact/ localhost/xss/ localhost/dashboard/json.php localhost/ping/ localhost/show/ localhost/xss/base64.php localhost/xss/script-inline.php localhost/iframe/secure.html localhost/msg/ZGRkZGRkZGRkZA== localhost/formauth/ localhost/ssi/ localhost/formauth/enumerate.php localhost localhost/user/ localhost/formauth/bypassBlock.php localhost/display/ localhost/iframe/ localhost/user/name/ localhost/icons/small/ localhost/feed/ ...

REQUEST / RESPONSE

#1

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:07 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 7908
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en" >

<head>
  <meta charset="UTF-8">
  <title>Complete test cases</title>
  <style>
body {
  margin: 0 auto;
  max-width:
...[truncated]...
```

DESCRIPTION

The `X-Content-Type-Options` response HTTP header is used by the server to prevent browsers from guessing the media type (MIME type).
This is known as **MIME sniffing** in which the browser guesses the correct MIME type by looking at the contents of the resource.
The absence of this header might cause browsers to transform non-executable content into executable content.

RECOMMENDATION

Configure your server to send this header with the value set to `nosniff`.

42.1 Missing or Insecure Cache-Control Header

SEVERITY	Informational
URL	http://localhost/dashboard/json.php
AFFECTED URLS (8)	localhost/user/name/ localhost/article/show/list/1/details localhost/xss/ localhost/xss/base64.php localhost/formauth/enumerate.php localhost/msg/ZGRkZGRkZGRkZA== localhost/xss/script-inline.php localhost/dashboard/json.php

DETAILS

The `Cache-Control` header is not set

REQUEST / RESPONSE

#1

```
GET /dashboard/json.php HTTP/1.1
Referer: http://localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:07 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Set-Cookie: id=eyJ1c2VyTmFtZSI6InRlc3R1c2VyIiwidXNlcklkIjoxMn0%3D
Content-Length: 14
Keep-Alive: timeout=5, max=97
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

Hello testuser
```

DESCRIPTION

Web cache or HTTP cache is a system for optimizing the web. Browsers cache contents of a resource once and reuse it on consequent requests. Caching images on the web can boost page load time. But clients should not be allowed to cache pages that display sensitive, dynamic, or user specific contents.

RECOMMENDATION

Set any of following headers to prevent clients from caching the page.

```
Cache-Control: no-cache, no-store
```

```
Cache-Control: max-age=0, must-revalidate
```

```
Cache-Control: private
```

43.1 Referrer-Policy Header is Missing

SEVERITY	Informational
URL	http://localhost
AFFECTED URLS (21)	localhost/contact/ localhost/xss/ localhost/dashboard/json.php localhost/ping/ localhost/show/ localhost/xss/base64.php localhost/xss/script-inline.php localhost/iframe/secure.html localhost/msg/ZGRkZGRkZGRkZA== localhost/formauth/ localhost/ssi/ localhost/formauth/enumerate.php localhost localhost/user/ localhost/formauth/bypassBlock.php localhost/display/ localhost/iframe/ localhost/user/name/ localhost/icons/small/ localhost/feed/ ...

REQUEST / RESPONSE

#1

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:07 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 7908
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en" >

<head>
  <meta charset="UTF-8">
  <title>Complete test cases</title>
  <style>
body {
  margin: 0 auto;
  max-width:
...[truncated]...
```

DESCRIPTION

The `Referrer-Policy` HTTP header controls how much referrer information (sent via the `Referer` header) should be included with requests. Mozilla
The `Referer` (sic) header contains the address of the previous web page from which a link to the currently requested page was followed, which has lots of fairly innocent uses including analytics, logging, or optimized caching. However, there are more problematic uses such as tracking or stealing information, or even just side effects such as inadvertently leaking sensitive information. Mozilla

RECOMMENDATION

Configure your server to send the `Referrer-Policy` header for all pages with the value set to `strict-origin-when-cross-origin`. You can see references for other possible values.

44.1 Private IPv4 Address Disclosure

SEVERITY	Informational
URL	http://localhost
IP ADDRESSES	10.10.98.19

REQUEST / RESPONSE

#1

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:07 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 7908
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

...[truncated]...
10.10.98.19</span>
        <span>FD00::4:120</span>
        </
...[truncated]...
```

DESCRIPTION

Private IP addresses are used in private networks like local area networks (LANs). A private IP address can reveal information about the IP planning scheme used in the private network.

This information does not create any direct impact on the target, though it can help attackers develop their attack.

RECOMMENDATION

This information is usually the result of an exception unless it is displayed intentionally.

Consider removing it.

45.1 Private IPv6 Address Disclosure

SEVERITY	Informational
URL	http://localhost
IP ADDRESSES	FD00::4:120

REQUEST / RESPONSE

#1

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:07 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 7908
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

...[truncated]...
FD00::4:120</span>
        </div>
  </div>
  <div clas
...[truncated]...
```

DESCRIPTION

Private IP addresses are used in private networks like local area networks (LANs). A private IP address can reveal information about the IP planning scheme used in the private network.
This information does not create any direct impact on the target, though it can help attackers develop their attack.

RECOMMENDATION

This information is usually the result of an exception unless it is displayed intentionally.
Consider removing it.

46.1 X-XSS-Protection Header is Set

SEVERITY	Informational
URL	http://localhost/xss/index.php?name=test

REQUEST / RESPONSE

#1

```
GET /xss/index.php?name=test HTTP/1.1
Referer: http://localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
Cookie: PHPSESSID=e2n36q648gvr9u8rk3hsdmboeo;
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:16 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
X-XSS-Protection: 1
Content-Length: 10
Keep-Alive: timeout=5, max=86
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

hello test
```

DESCRIPTION

The HTTP `X-XSS-Protection` response header is a feature of Internet Explorer, Chrome and Safari that stops pages from loading when they detect reflected cross-site scripting (XSS) attacks. [Mozilla]

- Chrome has removed their XSS Auditor
- Firefox has not, and will not implement X-XSS-Protection
- Edge has retired their XSS filter

This means that if you do not need to support legacy browsers, it is recommended that you use `Content-Security-Policy` without allowing `unsafe-inline` scripts instead.

RECOMMENDATION

Do not send this header or set `0` as value.

47.1 X-Powered-By Header Found

SEVERITY	Informational
URL	http://localhost
X-POWERED-BY	PHP/8.0.30

REQUEST / RESPONSE

#1

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:07 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 7908
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en" >

<head>
  <meta charset="UTF-8">
  <title>Complete test cases</title>
  <style>
body {
  margin: 0 auto;
  max-width:
...[truncated]...
```

DESCRIPTION

The `X-Powered-By` header describes the technologies used by the webserver. This information exposes the server to attackers. Using the information in this header, attackers can find vulnerabilities easier.

RECOMMENDATION

Configure the webserver to stop sending the `X-Powered-By` header.

48.1 File Upload Functionality

SEVERITY	Informational
URL	http://localhost

REQUEST / RESPONSE

#1

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:07 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 7908
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

...[truncated]...
iv class="module-body">
  <input type=file name=test>
...[truncated]...
```

DESCRIPTION

An `<input>` element with `type="file"` lets user choose one or more files from their device storage. Then, the files can be uploaded to a remote server.
An unrestricted file upload functionality can cause an *arbitrary file upload* vulnerability where malicious users can upload (and execute) any file to the server.

RECOMMENDATION

Restrict file type size that users can select.
Make sure the uploaded files are not publicly accessible on the web.

49.1 SQL Command Disclosure

SEVERITY	Informational
URL	http://localhost
SQL	Select * from users

REQUEST / RESPONSE

#1

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:07 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 7908
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

...[truncated]...
Select * from users where id=1</span>
        </div>

...[truncated]...
```

DESCRIPTION

SQL commands reveal information about the structure of the underlying database.
This information does not create any direct impact on the target, though it provides valuable information attackers can use in their attack.

RECOMMENDATION

If it’s not displayed intentionally, fix the reason causing the disclosure and make sure the SQL comand is not revealed due to errors and misconfigurations.

50.1 PHP Version Disclosure

SEVERITY	Informational
URL	http://localhost
PHP VERSION	8.0.30

DETAILS

PHP version is disclosed in the `Server header`.

REQUEST / RESPONSE

#1

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:07 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 7908
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en" >

<head>
  <meta charset="UTF-8">
  <title>Complete test cases</title>
  <style>
body {
  margin: 0 auto;
  max-width:
...[truncated]...
```

DESCRIPTION

Knowing the PHP version used by the server, attackers can find vulnerabilities easier. This information exposes the server to attackers.

RECOMMENDATION

Configure the webserver to stop revealing the PHP version.

51.1 Unix Path Disclosure

SEVERITY	Informational
URL	http://localhost
PATH	/var/log/www

REQUEST / RESPONSE

#1

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/119.0.0.0 Safari/537.36
Content-Length: 0
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:07:07 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 7908
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

...[truncated]...

...[truncated]...
```

DESCRIPTION

File and directory paths reveal information about the structure of the file system of the underlying OS. This information does not create any direct impact on the target, though it provides valuable information attackers can use in their attack.

RECOMMENDATION

If it’s not displayed intentionally, fix the reason causing the disclosure and make sure the path is not revealed due to errors and misconfigurations.

52.1 Target Information

SEVERITY	Informational
URL	http://localhost
AUTHENTICATION REQUIRED	http://localhost/auth/
COOKIES (7)	p3 phpMyAdmin profile PHPSESSID pma_lang id this_should_not_be
EMAILS	mike@hyperreal.org admin@gmail.com admin@example.com kevinh@kevcom.com aaa@sss.com
FORMS WITH PASSWORD	http://localhost/formauth/ http://localhost/formauth/bypassBlock.php http://localhost/formauth/enumerate.php
OS	Windows
PHP VERSIONS	8.0.30
PATHS (39)	C:\xampp\htdocs\user\name\index.php C:/xampp/htdocs C:/xampp/webalizer C:\xampp\htdocs C:\xampp\htdocs\xss\base64.php C:\xampp\htdocs\formauth\bypassBlock.php /var/log/www C:\xampp\htdocs\feed\index.php C:/xampp/apache/logs/ssl_scache C:/xampp/apache/cgi-bin C:\xampp\htdocs\xss\script-inline.php C:/xampp/apache/logs/error.log C:/xampp/apache/conf/extra/httpd-autoindex.conf C:\xampp\htdocs\ping\index.php C:/xampp/htdocs/xampp C:\xampp\htdocs\redir\index.php C:/xampp/apache/conf/extra/httpd-xampp.conf C:/xampp/apache/bin/openssl.cnf C:\xampp\htdocs\display\index.php

SERVER BANNER	C:/xampp/php apache/2.4.58 (win64) openssl/3.1.3 php/8.0.30
TECHNOLOGIES	PHP
USERS	admin
WEB SERVER	apache/2.4.58 (win64)
X-POWERED-BY	PHP/8.0.30