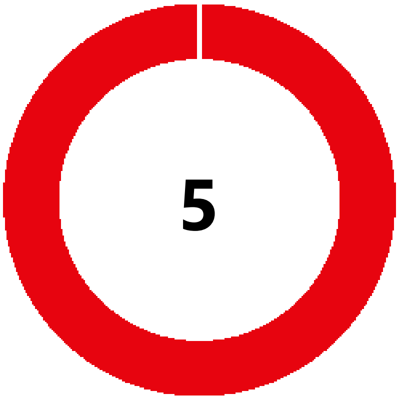
Target: **http://localhost**

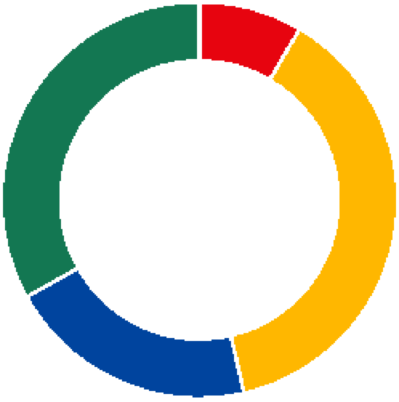
Date: **Tue Jul 26 2022**

Found Issues: **166**

scan **finished** within **16″** after **3749** requests.



Risk



Issue Severity

Executive Summary

SmartScanner conducted a scan on localhost to find security weaknesses and vulnerabilities. The scan took 16 seconds. After performing 3749 requests, SmartScanner found 166 issues in which 14 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/fetch/name/index.php
- 1.2– http://localhost/header/
- 1.3– http://localhost/template-injection/index.php?template=test
- 1.4– http://localhost/xss/base64.php?name=YmFzZTY0LWVuY29kZWQtdmFsdWU
- 1.5– http://localhost/xss/index.php?name=test

2– Insecure Deserialization

- 2.1– http://localhost/deserialization/
- 2.2– http://localhost/deserialization/json.php

3– Weak Password

- 3.1– http://localhost/basicauth/
- 3.2– http://localhost/formauth/

4– Unreferenced Source Code Disclosure

- 4.1– http://localhost/backup/index.php.bac

5– Expression Language Injection

- 5.1– http://localhost/template-injection/index.php?template=test

6– Unvalidated Redirection

- 6.1– http://localhost/redir/?u=http://127.0.0.1/

7– Remote URL Inclusion

- 7.1– http://localhost/rfi/rfd.php?f=a

8– OS Command Execution

- 8.1– http://localhost/osexec/?i=127.0.0.1

9– Detailed Application Error

- 9.1– http://localhost/deserialization/
- 9.2– http://localhost/error/?dummy=%22%27%2F%3Cjxqz21850%3E%3D%28%29
- 9.3– http://localhost/error/?dummy=1
- 9.4– http://localhost/fetch/name/index.php
- 9.5– http://localhost/fetch/name/index.php
- 9.6– http://localhost/formauth/
- 9.7– http://localhost/formauth/
- 9.8– http://localhost/formauth/
- 9.9– http://localhost/formauth/bypassBlock.php
- 9.10– http://localhost/formauth/bypassBlock.php
- 9.11– http://localhost/formauth/enumerate.php
- 9.12– http://localhost/formauth/enumerate.php
- 9.13– http://localhost/formauth/enumerate.php
- 9.14– http://localhost/formauth/enumerate.php
- 9.15– http://localhost/fuzzing/array.php?a=1
- 9.16– http://localhost/osexec/?i=127.0.0.1
- 9.17– http://localhost/osexec/index.php

9.18– http://localhost/redir/?u=http://127.0.0.1/
9.19– http://localhost/rfi/rfd.php?f=%22%27%2F%3Cjxqz19642%3E%3D%28%29
9.20– http://localhost/rfi/rfd.php?f=a
9.21– http://localhost/sqli/complex.php?q=%7B%7B394487-1%7D%7D
9.22– http://localhost/sqli/complex.php?q=1
9.23– http://localhost/sqli/complex.php?q=1
9.24– http://localhost/sqli/complex.php?q=1
9.25– http://localhost/template-injection/index.php
9.26– http://localhost/template-injection/index.php?template=test
9.27– http://localhost/xss/base64.php?
9.28– http://localhost/xss/index.php
9.29– http://localhost/xss/index.php?name=test
9.30– https://localhost/breach/?input=userinput

10– Host Header Injection

10.1– http://127.0.0.1/
10.2– http://localhost
10.3– http://localhost/
10.4– http://localhost/error/server/
10.5– http://localhost/https-pass-in-url
10.6– http://localhost/https-pass-in-url/
10.7– http://localhost/nowhere
10.8– http://localhost/phpmyadmin
10.9– http://localhost/sitemap.xml

11– Password Sent Over HTTP

11.1– http://localhost/formauth/
11.2– http://localhost/formauth/bypassBlock.php
11.3– http://localhost/formauth/enumerate.php
11.4– http://localhost/login/

12– Detailed Application and Database Error

12.1– http://localhost/error/db.php
12.2– http://localhost/error/db.php
12.3– http://localhost/error/db.php

13– Internal Server Error

13.1– http://localhost/error/server/
13.2– http://localhost/error/server/

14– Session Cookie without HttpOnly Flag

14.1– http://localhost/formauth/bypassBlock.php

15– Session Cookie without SameSite Flag

15.1– http://localhost/formauth/bypassBlock.php

16– Sensitive Old/Backup Resource Found

16.1– http://localhost/backup/index.php.bac

17– Session Cookie without Secure Flag

17.1– http://localhost/formauth/bypassBlock.php

18– No Redirection from HTTP to HTTPS

18.1– http://localhost

19– Brute Force Prevention Bypassed

19.1– http://localhost/formauth/bypassBlock.php

20– Basic Authentication Over HTTP

20.1– http://localhost/basicauth/

21– Unreferenced Login Page Found

21.1– http://localhost/login/

22– Apache server-status enabled

22.1– http://localhost/server-status

23– Vulnerable OpenSSL Version

23.1– http://localhost

24– Apache server-info enabled

24.1– http://localhost/server-info

25– Source Code Disclosure

25.1– http://localhost

26– User Enumeration

26.1– http://localhost/formauth/enumerate.php

27– phpinfo() Found

27.1– http://localhost/phpinfo/

28– Buffer Overflow

28.1– http://localhost/bof/?a=ferri

29– No HTTPS

29.1– http://localhost

30– Auto Complete Enabled Password Input

30.1– http://localhost/formauth/
30.2– http://localhost/formauth/bypassBlock.php
30.3– http://localhost/formauth/enumerate.php
30.4– http://localhost/login/
30.5– https://localhost/https-pass-in-url/

31– Cookie without HttpOnly Flag

31.1– http://localhost/cookie/domain.php
31.2– http://localhost/cookie/index.php
31.3– http://localhost/deserialization/
31.4– http://localhost/deserialization/
31.5– http://localhost/deserialization/json.php

32– Cookie without Secure Flag

32.1– http://localhost/cookie/domain.php

32.2– http://localhost/cookie/index.php
32.3– http://localhost/deserialization/
32.4– http://localhost/deserialization/
32.5– http://localhost/deserialization/json.php

33– Directory Listing of Sensitive Files

33.1– http://localhost/admin/
33.2– http://localhost/fuzzing/
33.3– http://localhost/listing-sensitive/

34– Sensitive Unreferenced Resource Found

34.1– http://localhost/admin/
34.2– http://localhost/listing-sensitive/db.sql

35– Subresource Integrity is Missing

35.1– http://localhost/redirectionBody/
35.2– http://localhost/ssi/

36– Cookie without SameSite Flag

36.1– http://localhost/cookie/domain.php
36.2– http://localhost/deserialization/json.php

37– Strict-Transport-Security Header is Missing

37.1– https://localhost/https-pass-in-url/

38– Content-Security-Policy Header is Missing

38.1– http://localhost

39– X-Frame-Options Header is Missing

39.1– http://localhost

40– Old/Backup Resource Found

40.1– http://localhost/backup/index2.php

41– Password Sent in Query

41.1– https://localhost/https-pass-in-url/

42– Redirection with Body

42.1– http://localhost/redirectionBody/

43– Passive Mixed Content

43.1– https://localhost/mix/passive.html

44– TRACE Method Allowed

44.1– http://localhost/

45– Application Error

45.1– http://localhost/fuzzing/error.php

46– Windows Path Disclosure

46.1– http://localhost
46.2– http://localhost/deserialization/
46.3– http://localhost/error/?dummy=1

- 46.4– http://localhost/error/db.php
- 46.5– http://localhost/fetch/name/index.php
- 46.6– http://localhost/formauth/
- 46.7– http://localhost/formauth/bypassBlock.php
- 46.8– http://localhost/formauth/enumerate.php
- 46.9– http://localhost/fuzzing/array.php?a%5B%5D=
- 46.10– http://localhost/osexec/?i=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fwindows%2Fwin.ini%00127.0.0.1
- 46.11– http://localhost/phpinfo/
- 46.12– http://localhost/redir/?u%5B%5D=
- 46.13– http://localhost/rfi/rfd.php?f=a
- 46.14– http://localhost/server-info
- 46.15– http://localhost/sqli/complex.php?q=%7B%7B394487-1%7D%7D
- 46.16– http://localhost/template-injection/index.php
- 46.17– http://localhost/template-injection/index.php?template%5B%5D=
- 46.18– http://localhost/xss/base64.php?
- 46.19– http://localhost/xss/index.php?name%5B%5D=
- 46.20– https://localhost/breach/?input%5B%5D=

47– Email Address Disclosure

- 47.1– http://localhost
- 47.2– http://localhost/fuzzing/increment.php?q=2
- 47.3– http://localhost/icons/
- 47.4– http://localhost/phpinfo/
- 47.5– http://localhost/server-info

48– Content Character Encoding is not Defined

- 48.1– http://localhost/ssi/
- 48.2– http://localhost/ssi/safe.html
- 48.3– https://localhost/https-pass-in-url/
- 48.4– https://localhost/mix/passive.html

49– Directory Listing

- 49.1– http://localhost/icons/
- 49.2– http://localhost/icons/small/
- 49.3– http://localhost/listing/
- 49.4– https://localhost/mix/

50– PHP Version Disclosure

- 50.1– http://localhost
- 50.2– http://localhost/phpinfo/

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

- 51.1– http://localhost

52– Missing or Insecure Cache-Control Header

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

53– Cross-Origin Resource Sharing Allowed

- 53.1– http://localhost/CORS/

54– Referrer-Policy Header is Missing

  54.1– http://localhost

55– Cookie Accessible for Subdomains

  55.1– http://localhost/cookie/domain.php

56– Private IPv4 Address Disclosure

  56.1– http://localhost

57– Private IPv6 Address Disclosure

  57.1– http://localhost

58– X-XSS-Protection Header is Set

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

59– Public-Key-Pins Header is Set

  59.1– http://localhost/HPKP/

60– Unreferenced Resource Found

  60.1– http://localhost/fuzzing/removeparam.php

61– ViewState is not Encrypted

  61.1– http://localhost/fuzzing/error.php

62– File Upload Functionality

  62.1– http://localhost

63– X-Powered-By Header Found

  63.1– http://localhost

64– Apache Version Disclosure

  64.1– http://localhost

65– Serialized Object Found

  65.1– http://localhost/deserialization/

66– SQL Command Disclosure

  66.1– http://localhost

67– Unix Path Disclosure

  67.1– http://localhost

68– Target Information

  68.1– http://localhost

69– Broken Link

  69.1– http://localhost/nowhere

70– Profanity

  70.1– http://localhost

1.1 Cross Site Scripting

SEVERITY	High
URL	http://localhost/fetch/name/index.php
PARAMETER (POST)	name
INJECTION	"'/<jxqz25788>=()

DETAILS

The `"'/<jxqz25788>=()` was set as parameter `name` value and, it was reflected in the response.

REQUEST / RESPONSE

#1

```
POST /fetch/name/index.php HTTP/1.1
Authorization: valid-token
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi
Referer:
Content-Length: 32

name="%27%2F<jxqz25788>%3D%28%29
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:07 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 17
Keep-Alive: timeout=5, max=41
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

"'/<jxqz25788>=()
```

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/header/
PARAMETER (HEADER)	User-Agent
INJECTION	"'/<jxqz13954>=()

DETAILS

The `"'/<jxqz13954>=()` was set as parameter `User-Agent` value and, it was reflected in the response.

REQUEST / RESPONSE

#1

```
GET /header/ 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
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi
Referer:
User-Agent: "'/<jxqz13954>=()
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:03 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 23
Keep-Alive: timeout=5, max=96
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

hello "'/<jxqz13954>=()
```

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/template-injection/index.php?template=test
PARAMETER (QUERY)	template
INJECTION	"'/<jxqz23000>=()

DETAILS

The `"'/<jxqz23000>=()` was set as parameter `template` value and, it was reflected in the response.

REQUEST / RESPONSE

#1

```
GET /template-injection/index.php?template=%22%27%2F%3Cjxqz23000%3E%3D%28%29 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi
Referer:
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:06 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 46
Keep-Alive: timeout=5, max=69
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

test: /?template={{1000-1}}
"'/<jxqz23000>=()
```

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-BASE64)	name
INJECTION	"'/<jxqz18529>=()

DETAILS

The `"'/<jxqz18529>=()` was set as parameter `name` value and, it was reflected in the response.

REQUEST / RESPONSE

#1

```
GET /xss/base64.php?name=IicvPGp4cXoxODUyOT49KCk%3D HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi
Referer:
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:05 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 23
Keep-Alive: timeout=5, max=82
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

hello "'/<jxqz18529>=()
```

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	"'/<jxqz6698>=()

DETAILS

The `"'/<jxqz6698>=()` was set as parameter `name` value and, it was reflected in the response.

REQUEST / RESPONSE

#1

```
GET /xss/index.php?name=%22%27%2F%3Cjxqz6698%3E%3D%28%29 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer:
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
X-XSS-Protection: 1
Content-Length: 22
Keep-Alive: timeout=5, max=94
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

hello "'/<jxqz6698>=()
```

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 Insecure Deserialization

SEVERITY	High
URL	http://localhost/deserialization/
PARAMETER (COOKIE-BASE64)	profile
INJECTION	O:8:"stdClass":2:{s:8:"userName";s:12:"customvalue1";s:6:"userId";i:12;}

DETAILS

SmartScanner tampered with a value in the serialized PHP object in the parameter `profile (Cookie-base64)` and, the server accepted it without integrity checking. Then the server replied with the tampered data in the body.

REQUEST / RESPONSE

#1

```
GET /deserialization/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer:
Cookie: profile=Tzo4OiJzdGRDbGFzcyI6Mjp7czo4OiJ1c2VyTmFtZSI7czoxMjoiY3VzdG9tdmFsdWUxIjtzOjY6InVzZXJ
JZCI7aToxMjt9; p3=rO0ABXNyAAlTb21lQ2xhc3MAAAAAAAAAAQIABkkAAWJJAAFpTAABZHQAEkxqYXZhL2xhbmcvRG91Ymxl0
0wABGhoaGh0ABJMamF2YS9sYW5nL1N0cmluZztMAAFzcQB%2BAAJMAANzdHJxAH4AAnhwAAAAe3%2F%2F%2F%2F9zcgAQamF2YS
5sYW5nLkRvdWJsZYCzwkopa%2FsEAgABRAAFdmFsdWV4cgAQamF2YS5sYW5nLk51bWJlcoaslR0LlOCLAgAAeHC%2F8AAAAAAAA
HQABmhoaGhoaHQABUFCQ0RFdAAGc3RyaW5n; id=eyJ1c2VyTmFtZSI6InRlc3R1c2VyIiwidXNlcklkIjoxMn0%3D; PHPSESS
ID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 18
Keep-Alive: timeout=5, max=57
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

Hello customvalue1
```

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.

2.2 Insecure Deserialization

SEVERITY	High
URL	http://localhost/deserialization/json.php
PARAMETER (COOKIE-BASE64)	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-base64)` and, the server accepted it without integrity checking. Then the server replied with the tampered data in the body.

REQUEST / RESPONSE

#1

```
GET /deserialization/json.php HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer:
Cookie: p3=rO0ABXNyAAlTb21lQ2xhc3MAAAAAAAAAAQIABkkAAWJJAAFpTAABZHQAEkxqYXZhL2xhbmcvRG91YmxlO0wABGho
aGh0ABJMamF2YS9sYW5nL1N0cmluZztMAAFzcQB%2BAAJMAANzdHJxAH4AAnhwAAAAe3%2F%2F%2F%2F9zcgAQamF2YS5sYW5nL
kRvdWJsZYCzwkopa%2FsEAgABRAAFdmFsdWV4cgAQamF2YS5sYW5nLk51bWJlcoaslR0LlOCLAgAAeHC%2F8AAAAAAAAHQABmho
aGhoaHQABUFCQ0RFdAAGc3RyaW5n; id=eyJ1c2VySWQiOjEyLCJ1c2VyTmFtZSI6ImN1c3RvbWV2YWx1ZSJ9; profile=Tzo4
OiJzdGRDbGFzcyI6Mjp7czo4OiJ1c2VyTmFtZSI7czo4OiJ0ZXN0dXNlciI7czo2OiJ1c2VySWQiO2k6MTI7fQ%3D%3D; PHPSE
SSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:02 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 18
Keep-Alive: timeout=5, max=87
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.

3.1 Weak Password

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

DETAILS

An easily guessable user/password was found.

REQUEST / RESPONSE

#1

```
GET /basicauth/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:05 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
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

3.2 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 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Content-Length: 21

usr=admin&pass=123456
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:02 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
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

4.1 Unreferenced Source Code Disclosure

SEVERITY	High
URL	http://localhost/backup/index.php.bac

DETAILS

This file discloses source code and is not linked anywhere.

REQUEST / RESPONSE

1

```
GET /backup/index.php.bac HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:16 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
Last-Modified: Mon, 14 Sep 2020 14:34:22 GMT
ETag: "30-5af46ee3b0f6a"
Accept-Ranges: bytes
Content-Length: 48
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/html

hello az babate samime ghalb
<?php echo 123; ?>
```

DESCRIPTION

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

RECOMMENDATION

Remove the file or limit access to it.

5.1 Expression Language Injection

SEVERITY	High
URL	http://localhost/template-injection/index.php?template=test
PARAMETER (QUERY)	template
INJECTION	{{749199-1}}
PROOF	749198

DETAILS

The `{{749199-1}}` was injected into the parameter `template`, and the server replied with the evaluated value `749198` in response. This indicates that the target is vulnerable to EL Injection.

REQUEST / RESPONSE

#1

```
GET /template-injection/index.php?template=%7B%7B749199-1%7D%7D HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi
Referer:
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:06 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 35
Keep-Alive: timeout=5, max=67
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

test: /?template={{1000-1}}
749198
```

DESCRIPTION

In programming languages, Expressions are constants, variables, operators, or functions that can perform actions and produce values. Web applications often use dynamic Expressions in their templates to create different pages easily.

When user input is used in these dynamic Expressions and templates without proper validation, a malicious user can provide crafted inputs to change the server-side Expressions. This is called Expression Language Injection (aka EL Injection) or Template Injection.

EL injections are serious vulnerabilities that allow attackers to extract pieces of information such as session tokens or execute commands on the remote server.

RECOMMENDATION

Try not to use user input to construct expressions.
If you’re using Spring Framework, disable the double resolution functionality.
If you’re using templating engines, avoid using user inputs for building templates.

6.1 Unvalidated Redirection

SEVERITY	High
URL	http://localhost/redir/?u=http://127.0.0.1/
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
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer:
```

```
HTTP/1.1 301 Moved Permanently
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Location: www.example.com
Content-Length: 0
Keep-Alive: timeout=5, max=81
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.

7.1 Remote URL Inclusion

SEVERITY	High
URL	http://localhost/rfi/rfd.php?f=a
PARAMETER (QUERY)	f
INJECTION	hTtp://example.com/?
PROOF	<h1>Example Domain</h1>

DETAILS

The `hTtp://example.com/?` was injected into the parameter `f` and `<h1>Example Domain</h1>` was found in the response which indicates the target is vulnerable against Remote URL Inclusion.

REQUEST / RESPONSE

#1

```
GET /rfi/rfd.php?f=hTtp%3A%2F%2Fexample.com%2F%3F HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi
Referer:
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:05 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 1267
Keep-Alive: timeout=5, max=49
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

...[truncated]...
uto;
        }
    }
    </style>
</head>

<body>
<div>
    <h1>Example Domain</h1>
    <p>This domain is for use in illustrative examples in documents. You
...[truncated]...
```

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 Remote URL Inclusion issue, the server fetches the remote URL and includes the content of the remote file in the response. The application might execute the content of the file if it contains codes. This allows attackers to run arbitrary codes on the server. Furthermore, this causes a Server-side request forgery issue.

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]

8.1 OS Command Execution

SEVERITY	High
URL	http://localhost/osexec/?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 /osexec/?i=a%7Cver HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi
Referer:
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:09 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 175
Keep-Alive: timeout=5, max=44
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<html><body><pre>

Microsoft Windows [Version 10.0.19044.1826]
Microsoft Windows [Version 10.0.19044.1826]</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

9.1 Detailed Application Error

SEVERITY	Medium
URL	http://localhost/deserialization/
PARAMETER (COOKIE-BASE64)	profile
APPLICATION ERROR	Notice</b>: unserialize(): Error at offset 0 of 16 bytes in <b>C:\xampp\htdocs\deserialization\index.php</b> on line <
INJECTION	"'/<jxqz8223>=()
PROGRAMMING LANGUAGE	PHP

DETAILS

When the `"'/<jxqz8223>=()` was set as the parameter `profile` value, the application faced with an error.

REQUEST / RESPONSE

#1

```
GET /deserialization/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: 
Cookie: p3=rO0ABXNyAAlTb21lQ2xhc3MAAAAAAAAAAQIABkkAAWJJAAFpTAABZHQAEkxqYXZhL2xhbmcvRG91YmxlO0wABGho
aGh0ABJMamF2YS9sYW5nL1N0cmluZztMAAFzcQB%2BAAJMAANzdHJxAH4AAnhwAAAAe3%2F%2F%2F%2F9zcgAQamF2YS5sYW5nL
kRvdWJsZYCzwkopa%2FsEAgABRAAFdmFsdWV4cgAQamF2YS5sYW5nLk51bWJlcoaslR0LlOCLAgAAeHC%2F8AAAAAAAAHQABmho
aGhoaHQABUFCQ0RFdAAGc3RyaW5n; id=eyJ1c2VyTmFtZSI6InRlc3R1c2VyIiwidXNlcklkIjoxMn0%3D; profile=IicvPG
p4cXo4MjIzPj0oKQ%3D%3D; PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Set-Cookie: profile=Tzo4OiJzdGRDbGFzcyI6Mjp7czo4OiJ1c2VyTmFtZSI7czo4OiJ0ZXN0dXNlciI7czo2OiJ1c2VySWQ
iO2k6MTI7fQ%3D%3D
Content-Length: 157
Keep-Alive: timeout=5, max=37
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<br />
<b>Notice</b>:  unserialize(): Error at offset 0 of 16 bytes in <b>C:\xampp\htdocs\deserialization
\index.php</b> on line <b>3</b><br />
Hello testuser
```

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.

9.2 Detailed Application Error

SEVERITY	Medium
URL	http://localhost/error/?dummy=%22%27%2F%3Cjxqz21850%3E%3D%28%29
PARAMETER (QUERY)	dummy
AFFECTED URLS (18)	localhost/error/?dummy=a%26ping 2130706433%26%23%27%26ping 2130706434%26a%26%23%22%26ping 2130706435%26a%5C localhost/error/?dummy=example.com%2F%3F localhost/error/?dummy=%24%7B900507-1%7D localhost/error/?dummy=%22%27%2F%3Cjxqz21850%3E%3D%28%29 localhost/error/?dummy=1 or 1%3DExtractValue%281%2CCoNCaT%280x3a%2C%28md5%28122459%29%29%29%29 localhost/error/?dummy=1%27 and 0-- a localhost/error/?dummy=99999 or 1-- a localhost/error/?dummy=%7B%7B900507-1%7D%7D localhost/error/?dummy=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fwindows%2Fwin.ini localhost/error/?dummy=1%27 rlike %28case when 1 then BENCHMARK%28450000000%2CMD5%280x41%29%29 else 0 end%29 -- a localhost/error/?dummy=1%27 or 1%3DExtractValue%281%2CCoNCaT%280x3a%2C%28md5%28122459%29%29%29%29 or 1%3D%272 localhost/error/?dummy=1 and 0-- a localhost/error/?dummy=1 or%28seLeCT 1 FROm%28seLeCT count%28%2A%29%2CCoNcaT%28%28seLeCT %28md5%28122459%29%29 FROm %60information_schema%60.tables LimIt 0%2C1%29%2Cfloor%28rand%280%29%2A2%29%29x FROm %60information_schema%60.tables group by x%29a%29 localhost/error/?dummy=hTtp%3A%2F%2Fexample.com%2F%3F localhost/error/?dummy=1%27 or%28seLeCT 1 FROm%28seLeCT count%28%2A%29%2CCoNcaT%28%28seLeCT %28md5%28122459%29%29 FROm %60information_schema%60.tables LimIt 0%2C1%29%2Cfloor%28rand%280%29%2A2%29%29x FROm %60information_schema%60.tables group by x%29a%29 or 1%3D%272 localhost/error/?dummy=1 rlike %28case when 1 then BENCHMARK%28450000000%2CMD5%280x41%29%29 else 0 end%29 -- a localhost/error/?dummy=99999%27 or 1-- a localhost/error/?dummy=a%7Cver
APPLICATION ERROR	Fatal error</b>: Uncaught Error: Undefined constant &quot;error&quot; in C:\xampp\htdocs\error\index.php:4 Stack trace: #0 {main} thrown in <b>C:\xampp\htdocs\error\index.php</b> on line <
INJECTION	"'/<jxqz21850>=()
PROGRAMMING	PHP

LANGUAGE

DETAILS

When the `"'/<jxqz21850>=()` was set as the parameter `dummy` value, the application faced with an error.

REQUEST / RESPONSE

#1

```
GET /error/?dummy=%22%27%2F%3Cjxqz21850%3E%3D%28%29 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi
Referer:
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:06 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 229
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

salam azizam
<br />
<b>Fatal error</b>:  Uncaught Error: Undefined constant &quot;error&quot; in C:\xampp\htdocs\error
\index.php:4
Stack trace:
#0 {main}
  thr
...[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.

9.3 Detailed Application Error

SEVERITY	Medium
URL	http://localhost/error/?dummy=1
REFERER	http://localhost
AFFECTED URLS	localhost/error/ localhost/error/?dummy=1
APPLICATION ERROR	Fatal error</b>: Uncaught Error: Undefined constant &quot;error&quot; in C:\xampp\htdocs\error\index.php:4 Stack trace: #0 {main} thrown in <b>C:\xampp\htdocs\error\index.php</b> on line <
PROGRAMMING LANGUAGE	PHP

REQUEST / RESPONSE

#1

```
GET /error/?dummy=1 HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:05 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 229
Keep-Alive: timeout=5, max=98
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

salam azizam
<br />
<b>Fatal error</b>:  Uncaught Error: Undefined constant &quot;error&quot; in C:\xampp\htdocs\error
\index.php:4
Stack trace:
#0 {main}
  thr
...[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.

9.4 Detailed Application Error

SEVERITY	Medium
URL	http://localhost/fetch/name/index.php
PARAMETER (POST)	name
APPLICATION ERROR	Warning</b>: Array to string conversion in <b>C:\xampp\htdocs\fetch\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 /fetch/name/index.php HTTP/1.1
Authorization: valid-token
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi
Referer:
Content-Length: 11

name%5B%5D=
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:07 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 126
Keep-Alive: timeout=5, max=42
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<br />
<b>Warning</b>:  Array to string conversion in <b>C:\xampp\htdocs\fetch\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.

9.5 Detailed Application Error

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

REQUEST / RESPONSE

#1

```
GET /fetch/name/index.php HTTP/1.1
Referer: http://localhost/fetch/
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:15 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 130
Keep-Alive: timeout=5, max=62
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<br />
<b>Warning</b>:  Undefined array key "Authorization" in <b>C:\xampp\htdocs\fetch\name\index.php</b>
on line <b>2</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.

9.6 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
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 428
Keep-Alive: timeout=5, max=78
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.

9.7 Detailed Application Error

SEVERITY	Medium
URL	http://localhost/formauth/
PARAMETER (POST)	usr
APPLICATION ERROR	Warning</b>: Undefined variable $error in <b>C:\xampp\htdocs\formauth\index.php</b> on line <
INJECTION	"'/<jxqz26379>=()
PROGRAMMING LANGUAGE	PHP

DETAILS

When the `"'/<jxqz26379>=()` was set as the parameter `usr` value, the application faced with an error.

REQUEST / RESPONSE

#1

```
POST /formauth/ HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi
Referer:
Content-Length: 50

pass=DJrLcmno321@!&usr="%27%2F<jxqz26379>%3D%28%29
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:07 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 310
Keep-Alive: timeout=5, max=19
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

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

...[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.

9.8 Detailed Application Error

SEVERITY	Medium
URL	http://localhost/formauth/
PARAMETER (POST)	pass
APPLICATION ERROR	Warning</b>: Undefined variable $error in <b>C:\xampp\htdocs\formauth\index.php</b> on line <
INJECTION	{{338185-1}}
PROGRAMMING LANGUAGE	PHP

DETAILS

When the `{{338185-1}}` was set as the parameter `pass` value, the application faced with an error.

REQUEST / RESPONSE

#1

```
POST /formauth/ HTTP/1.1
Authorization: valid-token
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi
Referer: 
Content-Length: 26

usr=Test&pass={{338185-1}}
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:07 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 310
Keep-Alive: timeout=5, max=13
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

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

...[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.

9.9 Detailed Application Error

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

REQUEST / RESPONSE

#1

```
GET /formauth/bypassBlock.php HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Set-Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi; 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=100
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.

9.10 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 `user` 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
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi
Referer:
Content-Length: 19

pass=DJrLcmno321@!&
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:07 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
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=58
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 line <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.

9.11 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
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 458
Keep-Alive: timeout=5, max=86
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.

9.12 Detailed Application Error

SEVERITY	Medium
URL	http://localhost/formauth/enumerate.php
REFERER	"'/<jxqz7191>=()
PARAMETER (HEADER)	Referer
APPLICATION ERROR	Warning</b>: Undefined array key "user" in <b>C:\xampp\htdocs\formauth\enumerate.php</b> on line <
INJECTION	"'/<jxqz7191>=()
PROGRAMMING LANGUAGE	PHP

DETAILS

When the `"'/<jxqz7191>=()` was set as the parameter `Referer` value, the application faced with an error.

REQUEST / RESPONSE

#1

```
GET /formauth/enumerate.php HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: "'/<jxqz7191>=()
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 458
Keep-Alive: timeout=5, max=74
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.

9.13 Detailed Application Error

SEVERITY	Medium
URL	http://localhost/formauth/enumerate.php
PARAMETER (HEADER)	User-Agent
APPLICATION ERROR	Warning</b>: Undefined array key "user" in <b>C:\xampp\htdocs\formauth\enumerate.php</b> on line <
INJECTION	{{771484-1}}
PROGRAMMING LANGUAGE	PHP

DETAILS

When the `{{771484-1}}` was set as the parameter `User-Agent` value, the application faced with an error.

REQUEST / RESPONSE

#1

```
GET /formauth/enumerate.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
Referer:
User-Agent: {{771484-1}}
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 458
Keep-Alive: timeout=5, max=63
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.

9.14 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 `user` 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
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi
Referer: 
Content-Length: 19

pass=DJrLcmno321@!&
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:06 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 458
Keep-Alive: timeout=5, max=85
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.

9.15 Detailed Application Error

SEVERITY	Medium
URL	http://localhost/fuzzing/array.php?a=1
PARAMETER (QUERY)	a
AFFECTED URLS	localhost/fuzzing/array.php?a%5B%5D= localhost/fuzzing/array.php?a=1
APPLICATION ERROR	Fatal error</b>: Uncaught TypeError: htmlentities(): Argument #1 ($string) must be of type string, array given in C:\xampp\htdocs\fuzzing\array.php:6 Stack trace: #0 C:\xampp\htdocs\fuzzing\array.php(6): htmlentities(Array) #1 {main} thrown in <b>C:\xampp\htdocs\fuzzing\array.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 /fuzzing/array.php?a%5B%5D= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi
Referer:
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:05 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 321
Keep-Alive: timeout=5, max=81
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<br />
<b>Fatal error</b>:  Uncaught TypeError: htmlentities(): Argument #1 ($string) must be of type stri
ng, array given in C:\xampp\htdocs\fuzzing\array.php:6
...[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.

9.16 Detailed Application Error

SEVERITY	Medium
URL	http://localhost/osexec/?i=127.0.0.1
PARAMETER (QUERY)	i
AFFECTED URLS	localhost/osexec/?i=127.0.0.1 localhost/osexec/?i=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fwindows%2Fwin.ini%00127.0.0.1 localhost/osexec/?i%5B%5D=
APPLICATION ERROR	Warning</b>: Array to string conversion in <b>C:\xampp\htdocs\osexec\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 /osexec/?i%5B%5D= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi
Referer:
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:06 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 356
Keep-Alive: timeout=5, max=52
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\osexec\index.php</b> on line <b>5
</b><br />
Ping request could not 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.

9.17 Detailed Application Error

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

REQUEST / RESPONSE

#1

```
GET /osexec/index.php HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:15 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 1896
Keep-Alive: timeout=5, max=36
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\osexec\index.php</b> on line <b>4</b
><br />

Usage: ping [-t] [-a] [-n
...[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.

9.18 Detailed Application Error

SEVERITY	Medium
URL	http://localhost/redir/?u=http://127.0.0.1/
PARAMETER (QUERY)	u
AFFECTED URLS	localhost/redir/?u%5B%5D= localhost/redir/?u=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fwindows%2Fwin.ini%00http%3A%2F%2F127.0.0.1%2F localhost/redir/?u=http://127.0.0.1/ localhost/redir/?u=%0D%0Ahttp%3A%2F%2F127.0.0.1%2F%3Ahttp%3A%2F%2F127.0.0.1%2F
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%5B%5D= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer:
```

```
HTTP/1.1 301 Moved Permanently
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Location: Array
Content-Length: 116
Keep-Alive: timeout=5, max=92
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.

9.19 Detailed Application Error

SEVERITY	Medium
URL	http://localhost/rfi/rfd.php?f=%22%27%2F%3Cjxqz19642%3E%3D%28%29
PARAMETER (QUERY)	f
AFFECTED URLS (21)	localhost/rfi/rfd.php?f=a or%28seLeCT 1 FROm%28seLeCT count%28%2A%29%2CCoNcaT%28%28seLeCT %28md5%28122459%29%29 FROm %60information_schema%60.tables LimIt 0%2C1%29%2Cfloor%28rand%280%29%2A2%29%29x FROm %60information_schema%60.tables group by x%29a%29 localhost/rfi/rfd.php?f=%24%7B783332-1%7D localhost/rfi/rfd.php?f=a%27 and 0-- a localhost/rfi/rfd.php?f=99999%27 or 1-- a localhost/rfi/rfd.php?f=99999%27 or %271 localhost/rfi/rfd.php?f=a%27 rlike %28case when 1 then BENCHMARK%28450000000%2CMD5%280x41%29%29 else 0 end%29 -- a localhost/rfi/rfd.php?f=a rlike %28case when 1 then BENCHMARK%28450000000%2CMD5%280x41%29%29 else 0 end%29 -- a localhost/rfi/rfd.php?f=a%27 and %270 localhost/rfi/rfd.php?f=a%27 or%28seLeCT 1 FROm%28seLeCT count%28%2A%29%2CCoNcaT%28%28seLeCT %28md5%28122459%29%29 FROm %60information_schema%60.tables LimIt 0%2C1%29%2Cfloor%28rand%280%29%2A2%29%29x FROm %60information_schema%60.tables group by x%29a%29 or 1%3D%272 localhost/rfi/rfd.php?f=%22%27%2F%3Cjxqz19642%3E%3D%28%29 localhost/rfi/rfd.php?f=99999 or 1 localhost/rfi/rfd.php?f=a%27 or 1%3DExtractValue%281%2CCoNCaT%280x3a%2C%28md5%28122459%29%29%29%29 or 1%3D%272 localhost/rfi/rfd.php?f=a%27 and %271 localhost/rfi/rfd.php?f=99999 or 1-- a localhost/rfi/rfd.php?f=a%7Cver localhost/rfi/rfd.php?f=a or 1%3DExtractValue%281%2CCoNCaT%280x3a%2C%28md5%28122459%29%29%29%29 localhost/rfi/rfd.php?f=a and 0-- a localhost/rfi/rfd.php?f=a and 1 localhost/rfi/rfd.php?f=%7B%7B783332-1%7D%7D localhost/rfi/rfd.php?f=a and 0 ...
APPLICATION ERROR	Warning</b>: file_get_contents(&quot;'/&lt;jxqz19642&gt;=()): Failed to open stream: No such file or directory in <b>C:\xampp\htdocs\rfi\rfd.php</b> on line <
INJECTION	"'/<jxqz19642>=()

PROGRAMMING LANGUAGE PHP

DETAILS

When the `"'/<jxqz19642>=()` was set as the parameter `f` value, the application faced with an error.

REQUEST / RESPONSE

#1

```
GET /rfi/rfd.php?f=%22%27%2F%3Cjxqz19642%3E%3D%28%29 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi
Referer:
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:05 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 194
Keep-Alive: timeout=5, max=19
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

hello vas
<br />
<b>Warning</b>:  file_get_contents(&quot;'/&lt;jxqz19642&gt;=()): Failed to open stream: No such fi
le or directory in <b>C:\xampp\htdocs\rfi\r
...[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.

9.20 Detailed Application Error

SEVERITY	Medium
URL	http://localhost/rfi/rfd.php?f=a
REFERER	http://localhost
APPLICATION ERROR	Warning</b>: file_get_contents(a): Failed to open stream: No such file or directory in <b>C:\xampp\htdocs\rfi\rfd.php</b> on line <
PROGRAMMING LANGUAGE	PHP

REQUEST / RESPONSE

#1

```
GET /rfi/rfd.php?f=a HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:05 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 167
Keep-Alive: timeout=5, max=95
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

hello vas
<br />
<b>Warning</b>:  file_get_contents(a): Failed to open stream: No such file or directory in <b>C:\xa
mpp\htdocs\rfi\rfd.php</b> on line <b>4</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.

9.21 Detailed Application Error

SEVERITY	Medium
URL	http://localhost/sqli/complex.php?q=%7B%7B394487-1%7D%7D
PARAMETER (QUERY)	q
AFFECTED URLS (20)	localhost/sqli/complex.php?q=1 or 1%3DExtractValue%281%2CCoNCaT%280x3a%2C%28md5%28122459%29%29%29%29 localhost/sqli/complex.php?q=%24%7B394487-1%7D localhost/sqli/complex.php?q=1 rlike %28case when 1 then BENCHMARK%28450000000%2CMD5%280x41%29%29 else 0 end%29 -- a localhost/sqli/complex.php?q=%7B%7B394487-1%7D%7D localhost/sqli/complex.php?q=99999 or 1-- a localhost/sqli/complex.php?q=hTtp%3A%2F%2Fexample.com%2F%3F localhost/sqli/complex.php?q=complex.php%001 localhost/sqli/complex.php?q=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fwindows%2Fwin.ini localhost/sqli/complex.php?q=1%27 or 1%3DExtractValue%281%2CCoNCaT%280x3a%2C%28md5%28122459%29%29%29%29 or 1%3D%272 localhost/sqli/complex.php?q=1%27 or%28seLeCT 1 FROm%28seLeCT count%28%2A%29%2CCoNcaT%28%28seLeCT %28md5%28122459%29%29 FROm %60information_schema%60.tables LimIt 0%2C1%29%2Cfloor%28rand%280%29%2A2%29%29x FROm %60information_schema%60.tables group by x%29a%29 or 1%3D%272 localhost/sqli/complex.php?q=1 and 0-- a localhost/sqli/complex.php?q=%22%27%2F%3Cjxqz14058%3E%3D%28%29 localhost/sqli/complex.php?q=complex.php localhost/sqli/complex.php?q=example.com%2F%3F localhost/sqli/complex.php?q=99999%27 or 1-- a localhost/sqli/complex.php?q=a%26ping 2130706433%26%23%27%26ping 2130706434%26a%26%23%22%26ping 2130706435%26a%5C localhost/sqli/complex.php?q=1%27 rlike %28case when 1 then BENCHMARK%28450000000%2CMD5%280x41%29%29 else 0 end%29 -- a localhost/sqli/complex.php?q=a%7Cver localhost/sqli/complex.php?q=1 or%28seLeCT 1 FROm%28seLeCT count%28%2A%29%2CCoNcaT%28%28seLeCT %28md5%28122459%29%29 FROm %60information_schema%60.tables LimIt 0%2C1%29%2Cfloor%28rand%280%29%2A2%29%29x FROm %60information_schema%60.tables group by x%29a%29 localhost/sqli/complex.php?q=1%27 and 0-- a
APPLICATION ERROR	Warning</b>: require(C:\xampp\htdocs\sqli/../../scripts/sqli/db.php): Failed to open stream: No such file or directory in <b>C:\xampp\htdocs\sqli\connect.php</b> on line <

INJECTION	{{394487-1}}
PROGRAMMING LANGUAGE	PHP

DETAILS

When the `{{394487-1}}` was set as the parameter `q` value, the application faced with an error.

REQUEST / RESPONSE

#1

```
GET /sqli/complex.php?q=%7B%7B394487-1%7D%7D HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi
Referer:
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:03 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 534
Keep-Alive: timeout=5, max=90
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<br />
<b>Warning</b>:  require(C:\xampp\htdocs\sqli/../../scripts/sqli/db.php): Failed to open stream: No
such file or directory in <b>C:\xampp\htdocs\sqli\con
...[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.

9.22 Detailed Application Error

SEVERITY	Medium
URL	http://localhost/sqli/complex.php?q=1
PARAMETER (HEADER)	User-Agent
APPLICATION ERROR	Warning</b>: require(C:\xampp\htdocs\sqli/../../scripts/sqli/db.php): Failed to open stream: No such file or directory in <b>C:\xampp\htdocs\sqli\connect.php</b> on line <
INJECTION	${742578-1}
PROGRAMMING LANGUAGE	PHP

DETAILS

When the `${742578-1}` was set as the parameter `User-Agent` value, the application faced with an error.

REQUEST / RESPONSE

#1

```
GET /sqli/complex.php?q=1 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
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi
Referer:
User-Agent: ${742578-1}
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:03 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 534
Keep-Alive: timeout=5, max=58
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<br />
<b>Warning</b>:  require(C:\xampp\htdocs\sqli/../../scripts/sqli/db.php): Failed to open stream: No
such file or directory in <b>C:\xampp\htdocs\sqli\con
...[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.

9.23 Detailed Application Error

SEVERITY	Medium
URL	http://localhost/sqli/complex.php?q=1
REFERER	"'/<jxqz17050>=()
PARAMETER (HEADER)	Referer
APPLICATION ERROR	Warning</b>: require(C:\xampp\htdocs\sqli/../../scripts/sqli/db.php): Failed to open stream: No such file or directory in <b>C:\xampp\htdocs\sqli\connect.php</b> on line <
INJECTION	"'/<jxqz17050>=()
PROGRAMMING LANGUAGE	PHP

DETAILS

When the `"'/<jxqz17050>=()` was set as the parameter `Referer` value, the application faced with an error.

REQUEST / RESPONSE

#1

```
GET /sqli/complex.php?q=1 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi
Referer: "'/<jxqz17050>=()
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:04 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 534
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<br />
<b>Warning</b>:  require(C:\xampp\htdocs\sqli/../../scripts/sqli/db.php): Failed to open stream: No such file or directory in <b>C:\xampp\htdocs\sqli\con
...[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.

9.24 Detailed Application Error

SEVERITY	Medium
URL	http://localhost/sqli/complex.php?q=1
REFERER	http://localhost
APPLICATION ERROR	Warning</b>: require(C:\xampp\htdocs\sqli/../../scripts/sqli/db.php): Failed to open stream: No such file or directory in <b>C:\xampp\htdocs\sqli\connect.php</b> on line <
PROGRAMMING LANGUAGE	PHP

REQUEST / RESPONSE

#1

```
GET /sqli/complex.php?q=1 HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:03 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 534
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<br />
<b>Warning</b>:  require(C:\xampp\htdocs\sqli/../../scripts/sqli/db.php): Failed to open stream: No
such file or directory in <b>C:\xampp\htdocs\sqli\con
...[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.

9.25 Detailed Application Error

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

REQUEST / RESPONSE

#1

```
GET /template-injection/index.php HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:15 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 967
Keep-Alive: timeout=5, max=67
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

test: /?template={{1000-1}}
<br />
<b>Warning</b>:  Undefined array key "template" in <b>C:\xampp\htdocs\template-injection\index.php
</b> on line <b>6</b><br />
...[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.

9.26 Detailed Application Error

SEVERITY	Medium
URL	http://localhost/template-injection/index.php?template=test
PARAMETER (QUERY)	template
AFFECTED URLS	localhost/template-injection/?template%5B%5D= localhost/template-injection/?template=test
APPLICATION ERROR	Warning</b>: Array to string conversion in <b>C:\xampp\htdocs\template-injection\vendor\twig\twig\src\Loader\ArrayLoader.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 /template-injection/index.php?template%5B%5D= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi
Referer:
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:06 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 1269
Keep-Alive: timeout=5, max=70
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

test: /?template={{1000-1}}
<br />
<b>Warning</b>:  Array to string conversion in <b>C:\xampp\htdocs\template-injection\vendor\twig\tw
ig\src\Loader\ArrayLoader
...[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.

9.27 Detailed Application Error

SEVERITY	Medium
URL	http://localhost/xss/base64.php?
PARAMETER (QUERY-BASE64)	name
AFFECTED URLS	localhost/xss/base64.php localhost/xss/base64.php?name%5B%5D=
APPLICATION ERROR	Warning</b>: Undefined array key "name" in <b>C:\xampp\htdocs\xss \base64.php</b> on line <
INJECTION	
PROGRAMMING LANGUAGE	PHP

DETAILS

When the `` was set as the parameter `name` value, the application faced with an error.

REQUEST / RESPONSE

#1

```
GET /xss/base64.php? HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi
Referer:
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:05 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 121
Keep-Alive: timeout=5, max=72
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

hello <br />
<b>Warning</b>:  Undefined array key "name" in <b>C:\xampp\htdocs\xss\base64.php</b> on line <b>3</
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.

9.28 Detailed Application Error

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

REQUEST / RESPONSE

#1

```
GET /xss/index.php HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:13 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
X-XSS-Protection: 1
Content-Length: 120
Keep-Alive: timeout=5, max=77
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

hello <br />
<b>Warning</b>:  Undefined array key "name" in <b>C:\xampp\htdocs\xss\index.php</b> on line <b>4</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.

9.29 Detailed Application Error

SEVERITY	Medium
URL	http://localhost/xss/index.php?name=test
PARAMETER (QUERY)	name
AFFECTED URLS	localhost/xss/?name%5B%5D= localhost/xss/?name=test
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%5B%5D= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer:
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
X-XSS-Protection: 1
Content-Length: 125
Keep-Alive: timeout=5, max=95
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.

9.30 Detailed Application Error

SEVERITY	Medium
URL	https://localhost/breach/?input=userinput
PARAMETER (QUERY)	input
AFFECTED URLS	localhost/breach/?input=userinput localhost/breach/?input%5B%5D=
APPLICATION ERROR	Fatal error</b>: Uncaught TypeError: htmlentities(): Argument #1 ($string) must be of type string, array given in C:\xampp\htdocs\breach\index.php:3 Stack trace: #0 C:\xampp\htdocs\breach\index.php(3): htmlentities(Array) #1 {main} thrown in <b>C:\xampp\htdocs\breach\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 /breach/?input%5B%5D= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi
Referer:
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:05 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 318
Keep-Alive: timeout=5, max=82
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<br />
<b>Fatal error</b>:  Uncaught TypeError: htmlentities(): Argument #1 ($string) must be of type string, array given in C:\xampp\htdocs\breach\index.php:3

...[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.

10.1 Host Header Injection

SEVERITY	Medium
URL	http://127.0.0.1/

DETAILS

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

REQUEST / RESPONSE

1

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

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

2092
<!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
```

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.

10.2 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
Accept: */*
Connection: Close
Forwarded: for=dkGjcdj2y3djasdcF
Host: dkGjcdj2y3djasdc
Origin: dkGjcdj2y3djasdcO
X-Forwarded-Host: dkGjcdj2y3djasdcX
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

2092
<!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
```

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.

10.3 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
Accept: */*
Connection: Close
Forwarded: for=dkGjcdj2y3djasdcF
Host: dkGjcdj2y3djasdc
Origin: dkGjcdj2y3djasdcO
X-Forwarded-Host: dkGjcdj2y3djasdcX
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:02 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

2092
<!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
```

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.

10.4 Host Header Injection

SEVERITY	Medium
URL	http://localhost/error/server/

DETAILS

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

REQUEST / RESPONSE

#1

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

```
HTTP/1.1 500 Internal Server Error
Date: Tue, 26 Jul 2022 09:31:02 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
Content-Length: 639
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>500 Internal Server Error</title>
</head><body>
<h1>Internal Server Error</h1>
<p>The server encountered an internal error or
misconfiguration and was unable to complete
your request.</p>
<p>Please contact the server administrator at
 postmaster@localhost to inform them of the time this error occurred,
 and the actions you performed just before this error.</p>
<p>More information about this error may be available
in the server error log.</p>
<hr>
<address>Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6 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.

10.5 Host Header Injection

SEVERITY	Medium
URL	http://localhost/https-pass-in-url

DETAILS

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

REQUEST / RESPONSE

#1

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

```
HTTP/1.1 301 Moved Permanently
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
Location: http://dkgjcdj2y3djasdc/https-pass-in-url/
Content-Length: 356
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/https-pass-in-url/">here</a>.</p>
<hr>
<address>Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6 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.

10.6 Host Header Injection

SEVERITY	Medium
URL	http://localhost/https-pass-in-url/

DETAILS

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

REQUEST / RESPONSE

#1

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

```
HTTP/1.1 301 Moved Permanently
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
Location: https://dkGjcdj2y3djasdc/https-pass-in-url/
Content-Length: 357
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="https://dkGjcdj2y3djasdc/https-pass-in-url/">here</a>.</p>
<hr>
<address>Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6 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.

10.7 Host Header Injection

SEVERITY	Medium
URL	http://localhost/nowhere

DETAILS

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

REQUEST / RESPONSE

#1

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

```
HTTP/1.1 404 Not Found
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
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/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6 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.

10.8 Host Header Injection

SEVERITY	Medium
URL	http://localhost/phpmyadmin

DETAILS

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

REQUEST / RESPONSE

1

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

```
HTTP/1.1 403 Forbidden
Date: Tue, 26 Jul 2022 09:31:13 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
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/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6 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.

10.9 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
Accept: */*
Connection: Close
Forwarded: for=dkGjcdj2y3djasdcF
Host: dkGjcdj2y3djasdc
Origin: dkGjcdj2y3djasdcO
X-Forwarded-Host: dkGjcdj2y3djasdcX
```

```
HTTP/1.1 404 Not Found
Date: Tue, 26 Jul 2022 09:31:02 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
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/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6 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.

11.1 Password Sent Over HTTP

SEVERITY Medium

URL http://localhost/formauth/

REQUEST / RESPONSE

#1

```
GET /formauth/ HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 428
Keep-Alive: timeout=5, max=78
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.

11.2 Password Sent Over HTTP

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

REQUEST / RESPONSE

#1

```
GET /formauth/bypassBlock.php HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Set-Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi; 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=100
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.

11.3 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
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 458
Keep-Alive: timeout=5, max=86
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.

11.4 Password Sent Over HTTP

SEVERITY	Medium
URL	http://localhost/login/

REQUEST / RESPONSE

#1

```
GET /login/ HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:12 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
Last-Modified: Mon, 25 Jan 2021 07:37:48 GMT
ETag: "58-5b9b49d4f3fb6"
Accept-Ranges: bytes
Content-Length: 88
Keep-Alive: timeout=5, max=71
Connection: Keep-Alive
Content-Type: text/html

<html>
<form>
<input type="password" name="pass">
</form>
<a href="/">a</a>
</html>
```

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.

12.1 Detailed Application and Database Error

SEVERITY	Medium
URL	http://localhost/error/db.php
REFERER	http://localhost
APPLICATION ERROR	Warning</b>: Undefined array key "q" in <b>C:\xampp\htdocs\error\db.php</b> on line <
DATABASE	MariaDB
DATABASE ERROR	You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near
PROGRAMMING LANGUAGE	PHP

REQUEST / RESPONSE

#1

```
GET /error/db.php HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 549
Keep-Alive: timeout=5, max=79
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

be name in the creator
<br />
<b>Warning</b>:  Undefined array key "q" in <b>C:\xampp\htdocs\error\db.php</b> on line <b>18</b><b
r />
<br />
<b>Fatal error</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.

12.2 Detailed Application and Database Error

SEVERITY	Medium
URL	http://localhost/error/db.php
REFERER	"'/<jxqz10394>=()
PARAMETER (HEADER)	Referer
APPLICATION ERROR	Warning</b>: Undefined array key "q" in <b>C:\xampp\htdocs\error\db.php</b> on line <
DATABASE	MariaDB
DATABASE ERROR	You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near
INJECTION	"'/<jxqz10394>=()
PROGRAMMING LANGUAGE	PHP

DETAILS

When the `"'/<jxqz10394>=()` was set as the parameter `Referer` value, the application faced with a database error

REQUEST / RESPONSE

#1

```
GET /error/db.php HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: "'/<jxqz10394>=()
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:02 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 549
Keep-Alive: timeout=5, max=86
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

be name in the creator
<br />
<b>Warning</b>:  Undefined array key "q" in <b>C:\xampp\htdocs\error\db.php</b> on line <b>18</b><b
r />
<br />
<b>Fatal error</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.

12.3 Detailed Application and Database Error

SEVERITY	Medium
URL	http://localhost/error/db.php
PARAMETER (HEADER)	User-Agent
APPLICATION ERROR	Warning</b>: Undefined array key "q" in <b>C:\xampp\htdocs\error\db.php</b> on line <
DATABASE	MariaDB
DATABASE ERROR	You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near
INJECTION	{{772990-1}}
PROGRAMMING LANGUAGE	PHP

DETAILS

When the `{{772990-1}}` was set as the parameter `User-Agent` value, the application faced with a database error

REQUEST / RESPONSE

#1

```
GET /error/db.php HTTP/1.1
Cookie: profile=Tzo4OiJzdGRDbGFzcyI6Mjp7czo4OiJ1c2VyTmFtZSI7czo4OiJ0ZXN0dXNlciI7czo2OiJ1c2VySWQiO2k
6MTI7fQ%3D%3D; p3=rO0ABXNyAAlTb21lQ2xhc3MAAAAAAAAAAQIABkkAAWJJAAFpTAABZHQAEkxqYXZhL2xhbmcvRG91YmxlO
0wABGhoaGh0ABJMamF2YS9sYW5nL1N0cmluZztMAAFzcQB%2BAAJMAANzdHJxAH4AAnhwAAAAe3%2F%2F%2F%2F9zcgAQamF2YS
5sYW5nLkRvdWJsZYCzwkopa%2FsEAgABRAAFdmFsdWV4cgAQamF2YS5sYW5nLk51bWJlcoaslR0LlOCLAgAAeHC%2F8AAAAAAAA
HQABmhoaGhoaHQABUFCQ0RFdAAGc3RyaW5n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer:
User-Agent: {{772990-1}}
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:03 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 549
Keep-Alive: timeout=5, max=40
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

be name in the creator
<br />
<b>Warning</b>:  Undefined array key "q" in <b>C:\xampp\htdocs\error\db.php</b> on line <b>18</b><b
r />
<br />
<b>Fatal error</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.

13.1 Internal Server Error

SEVERITY	Low
URL	http://localhost/error/server/
REFERER	http://localhost
HTTP ERROR	500

REQUEST / RESPONSE

#1

```
GET /error/server/ HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 500 Internal Server Error
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
Content-Length: 632
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>500 Internal Server Error</title>
</head><body>
<h1>Internal Server Error</h1>
<p>The se
...[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

Properly handle all types of exceptions and display a generic error message.

13.2 Internal Server Error

SEVERITY	Medium
URL	http://localhost/error/server/
PARAMETER (HEADER)	User-Agent
HTTP ERROR	500
INJECTION	{{366060-1}}

DETAILS

When the `{{366060-1}}` was set as the parameter `User-Agent` value, the server replied with the `500` error code.

REQUEST / RESPONSE

#1

```
GET /error/server/ 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
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi
Referer: 
User-Agent: {{366060-1}}
```

```
HTTP/1.1 500 Internal Server Error
Date: Tue, 26 Jul 2022 09:31:02 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
Content-Length: 632
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>500 Internal Server Error</title>
</head><body>
<h1>Internal Server Error</h1>
<p>The se
...[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

Properly handle all types of exceptions and display a generic error message.

14.1 Session Cookie without HttpOnly Flag

SEVERITY	Medium
URL	http://localhost/formauth/bypassBlock.php
COOKIE	PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi

REQUEST / RESPONSE

#1

```
GET /formauth/bypassBlock.php HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Set-Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi; 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=100
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.

15.1 Session Cookie without SameSite Flag

SEVERITY	Medium
URL	http://localhost/formauth/bypassBlock.php
COOKIE	PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi

REQUEST / RESPONSE

#1

```
GET /formauth/bypassBlock.php HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Set-Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi; 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=100
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.

16.1 Sensitive Old/Backup Resource Found

SEVERITY	Medium
URL	http://localhost/backup/index.php.bac
BACKUP ORIGIN	index.php

REQUEST / RESPONSE

#1

```
GET /backup/index.php.bac HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:16 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
Last-Modified: Mon, 14 Sep 2020 14:34:22 GMT
ETag: "30-5af46ee3b0f6a"
Accept-Ranges: bytes
Content-Length: 48
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/html

hello az babate samime ghalb
<?php echo 123; ?>
```

DESCRIPTION

Backup files can disclose important information like an application's source code, administrative interfaces, or even credentials to connect to the administrative interface or the database server.

RECOMMENDATION

Remove all backup files from web publicly accessible locations and make sure backup files are not automatically created or copied in these locations.

17.1 Session Cookie without Secure Flag

SEVERITY	Medium
URL	http://localhost/formauth/bypassBlock.php
COOKIE	PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi

REQUEST / RESPONSE

#1

```
GET /formauth/bypassBlock.php HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Set-Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi; 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=100
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.

18.1 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.

19.1 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 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=qk5c3297tn8do5rn0v1uj67kk9;
Content-Length: 15

name=root&pass=
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:04 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
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=83
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 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=adkda7gkks2es2jnaaop5jegjs;
Content-Length: 15

name=root&pass=
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:04 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
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.

20.1 Basic Authentication Over HTTP

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

REQUEST / RESPONSE

#1

```
GET /basicauth/ HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 401 Unauthorized
Date: Tue, 26 Jul 2022 09:31:03 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
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.

21.1 Unreferenced Login Page Found

SEVERITY	Medium
URL	http://localhost/login/

REQUEST / RESPONSE

#1

```
GET /login/ HTTP/1.1
Referer: http://localhost/login
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:13 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
Last-Modified: Mon, 25 Jan 2021 07:37:48 GMT
ETag: "58-5b9b49d4f3fb6"
Accept-Ranges: bytes
Content-Length: 88
Keep-Alive: timeout=5, max=64
Connection: Keep-Alive
Content-Type: text/html

<html>
<form>
<input type="password" name="pass">
</form>
<a href="/">a</a>
</html>
```

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.

22.1 Apache server-status enabled

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

REQUEST / RESPONSE

#1

```
GET /server-status HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
Keep-Alive: timeout=5, max=93
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.

23.1 Vulnerable OpenSSL Version

SEVERITY	Medium
URL	http://localhost
VERSION IN USE	1.1.1n

REQUEST / RESPONSE

#1

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
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**
- **>1.0.2zc**
- **>1.1.0k**
- **>1.1.1m**

- **>3.0.1**

24.1 Apache server-info enabled

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

REQUEST / RESPONSE

#1

```
GET /server-info HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
Keep-Alive: timeout=5, max=92
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.

25.1 Source Code Disclosure

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

REQUEST / RESPONSE

#1

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5

```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
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.

26.1 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 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Content-Length: 38

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

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:03 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
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 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Content-Length: 48

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

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:03 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
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]

27.1 phpinfo() Found

SEVERITY	Medium
URL	http://localhost/phpinfo/

REQUEST / RESPONSE

#1

```
GET /phpinfo/ HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

...[truncated]...
x; background-color: #ccc; border: 0; height: 1px;}
</style>
<title>PHP 8.1.6 - phpinfo()</title><meta name="ROBOTS" content="NOINDEX,NOFOLLOW,NOARCHIVE" /></he
...[truncated]...
```

DESCRIPTION

The `phpinfo()` method in the PHP programming language discloses a large amount of information about the PHP, extensions, server, and environments. Since different environments have a different setup, the `phpinfo()` can help to figure out the configurations. It can also facilitate the debugging process. Using this function call in the production environment can be dangerous because the provided information is valuable for attackers to develop their attack.

RECOMMENDATION

Remove the page or remove the `phpinfo()` function call.

28.1 Buffer Overflow

SEVERITY	Medium
URL	http://localhost/bof/?a=ferri
PARAMETER (QUERY)	a
AFFECTED URLS	localhost/bof/?a=aaa localhost/bof/?a=ferri
APPLICATION ERROR	error occured
INJECTION	aa

DETAILS

When a string of 260 characters was set as the parameter `a` value, the application faced with an error.

REQUEST / RESPONSE

#1

```
GET /bof/?a=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi
Referer:
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:04 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 34
Keep-Alive: timeout=5, max=49
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

an error occured while processing!
```

DESCRIPTION

Buffer overflow can occur when an application accepts data more than the space it has for it. It will cause the data to overflow the container which is usually the memory. Buffer overflow can be very dangerous because it can end up with command execution attacks.

RECOMMENDATION

Always check the size of the input before processing it. Do not process inputs with a length greater than what your application can handle.

29.1 No HTTPS

SEVERITY	Medium
URL	http://localhost
AFFECTED URLS (44)	localhost/deserialization/ localhost/sqli/?q=1 localhost/listing-sensitive/ localhost/phpinfo/ localhost/xss/?name=test localhost/fuzzing/increment.php localhost/error/?dummy=1 localhost/formauth/enumerate.php localhost/sqli/time.php?q=1 localhost/template-injection/?template=test localhost/fetch/name/ localhost/icons/small/ localhost/cookie/session.php localhost/cookie/ localhost localhost/formauth/ localhost/error/server/ localhost/rfi/lfi.php?f=a localhost/basicauth/ localhost/rfi/lfd.php?f=a ...

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.

30.1 Auto Complete Enabled Password Input

SEVERITY Low

URL http://localhost/formauth/

REQUEST / RESPONSE

#1

```
GET /formauth/ HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 428
Keep-Alive: timeout=5, max=78
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

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.

30.2 Auto Complete Enabled Password Input

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

REQUEST / RESPONSE

#1

```
GET /formauth/bypassBlock.php HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Set-Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi; 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=100
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.

30.3 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
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 458
Keep-Alive: timeout=5, max=86
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.

30.4 Auto Complete Enabled Password Input

SEVERITY Low

URL http://localhost/login/

REQUEST / RESPONSE

#1

```
GET /login/ HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:12 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
Last-Modified: Mon, 25 Jan 2021 07:37:48 GMT
ETag: "58-5b9b49d4f3fb6"
Accept-Ranges: bytes
Content-Length: 88
Keep-Alive: timeout=5, max=71
Connection: Keep-Alive
Content-Type: text/html

<html>
<form>
<input type="password" name="pass">
</form>
<a href="/">a</a>
</html>
```

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.

30.5 Auto Complete Enabled Password Input

SEVERITY	Low
URL	https://localhost/https-pass-in-url/

REQUEST / RESPONSE

#1

```
GET /https-pass-in-url/ HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
Last-Modified: Tue, 29 Sep 2020 12:22:45 GMT
ETag: "56-5b072d71e16f3"
Accept-Ranges: bytes
Content-Length: 86
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

<html>
<form method="GET">
<input type="password" name="password">
</form>
</html>
```

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.

31.1 Cookie without HttpOnly Flag

SEVERITY	Low
URL	http://localhost/cookie/domain.php
COOKIE	crossDomain=something

REQUEST / RESPONSE

#1

```
GET /cookie/domain.php HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Set-Cookie: crossDomain=something; domain=localhost
Content-Length: 0
Keep-Alive: timeout=5, max=94
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

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.

31.2 Cookie without HttpOnly Flag

SEVERITY	Low
URL	http://localhost/cookie/index.php
COOKIE	test=123

REQUEST / RESPONSE

#1

```
GET /cookie/index.php HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Set-Cookie: test=123
Content-Length: 11
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

test cookie
```

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.

31.3 Cookie without HttpOnly Flag

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

REQUEST / RESPONSE

#1

```
GET /deserialization/ HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
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=99
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.

31.4 Cookie without HttpOnly Flag

SEVERITY Low

URL http://localhost/deserialization/

COOKIE p3=rO0ABXNyAAlTb21lQ2xhc3MAAAAAAAAAAQIABkkAAWJJAAFpTAABZHQAEkxqYXZhL2xhbmcvRG91YmxlO0wABGhoaGh0ABJMamF2YS9sYW5nL1N0cmluZztMAAFzcQB%2BAAJMAANzdHJxAH4AAnhwAAAAe3%2F%2F%2F%2F9zcgAQamF2YS5sYW5nLkRvdWJsZYCzwkopa%2FsEAgABRAAFdmFsdWV4cgAQamF2YS5sYW5nLk51bWJlcoaslR0LlOCLAgAAeHC%2F8AAAAAAAAHQABmhoaGhoaHQABUFCQ0RFdAAGc3RyaW5n

REQUEST / RESPONSE

#1

```
GET /deserialization/ HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
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=99
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.

31.5 Cookie without HttpOnly Flag

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

REQUEST / RESPONSE

#1

```
GET /deserialization/json.php HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: profile=Tzo4OiJzdGRDbGFzcyI6Mjp7czo4OiJ1c2VyTmFtZSI7czo4OiJ0ZXN0dXNlciI7czo2OiJ1c2VySWQiO2k
6MTI7fQ%3D%3D; p3=rO0ABXNyAAlTb21lQ2xhc3MAAAAAAAAAAQIABkkAAWJJAAFpTAABZHQAEkxqYXZhL2xhbmcvRG91YmxlO
0wABGhoaGh0ABJMamF2YS9sYW5nL1N0cmluZztMAAFzcQB%2BAAJMAANzdHJxAH4AAnhwAAAAe3%2F%2F%2F%2F9zcgAQamF2YS
5sYW5nLkRvdWJsZYCzwkopa%2FsEAgABRAAFdmFsdWV4cgAQamF2YS5sYW5nLk51bWJlcoaslR0LlOCLAgAAeHC%2F8AAAAAAAA
HQABmhoaGhoaHQABUFCQ0RFdAAGc3RyaW5n;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
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

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.

32.1 Cookie without Secure Flag

SEVERITY	Low
URL	http://localhost/cookie/domain.php
COOKIE	crossDomain=something

REQUEST / RESPONSE

#1

```
GET /cookie/domain.php HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Set-Cookie: crossDomain=something; domain=localhost
Content-Length: 0
Keep-Alive: timeout=5, max=94
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

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.

32.2 Cookie without Secure Flag

SEVERITY	Low
URL	http://localhost/cookie/index.php
COOKIE	test=123

REQUEST / RESPONSE

#1

```
GET /cookie/index.php HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Set-Cookie: test=123
Content-Length: 11
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

test cookie
```

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.

32.3 Cookie without Secure Flag

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

REQUEST / RESPONSE

#1

```
GET /deserialization/ HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
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=99
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.

32.4 Cookie without Secure Flag

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

REQUEST / RESPONSE

#1

```
GET /deserialization/ HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
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=99
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.

32.5 Cookie without Secure Flag

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

REQUEST / RESPONSE

#1

```
GET /deserialization/json.php HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: profile=Tzo4OiJzdGRDbGFzcyI6Mjp7czo4OiJ1c2VyTmFtZSI7czo4OiJ0ZXN0dXNlciI7czo2OiJ1c2VySWQiO2k
6MTI7fQ%3D%3D; p3=rO0ABXNyAAlTb21lQ2xhc3MAAAAAAAAAAQIABkkAAWJJAAFpTAABZHQAEkxqYXZhL2xhbmcvRG91YmxlO
0wABGhoaGh0ABJMamF2YS9sYW5nL1N0cmluZztMAAFzcQB%2BAAJMAANzdHJxAH4AAnhwAAAAe3%2F%2F%2F%2F9zcgAQamF2YS
5sYW5nLkRvdWJsZYCzwkopa%2FsEAgABRAAFdmFsdWV4cgAQamF2YS5sYW5nLk51bWJlcoaslR0LlOCLAgAAeHC%2F8AAAAAAAA
HQABmhoaGhoaHQABUFCQ0RFdAAGc3RyaW5n;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
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

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.

33.1 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: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:11 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
Content-Length: 1403
Keep-Alive: timeout=5, max=31
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.

33.2 Directory Listing of Sensitive Files

SEVERITY	Low
URL	http://localhost/fuzzing/

DETAILS

Directory listing discloses sensitive or dynamic application files.

REQUEST / RESPONSE

#1

```
GET /fuzzing/ HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:07 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
Content-Length: 1621
Keep-Alive: timeout=5, max=67
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 /fuzzing</title>
 </head>
 <body>
<h1>Index of /fuzzing</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.

33.3 Directory Listing of Sensitive Files

SEVERITY	Low
URL	http://localhost/listing-sensitive/

DETAILS

Directory listing discloses sensitive or dynamic application files.

REQUEST / RESPONSE

#1

```
GET /listing-sensitive/ HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
Content-Length: 1001
Keep-Alive: timeout=5, max=96
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 /listing-sensitive</title>
 </head>
 <body>
<h1>Index of /listing-sensi
...[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.

34.1 Sensitive Unreferenced Resource Found

SEVERITY	Low
URL	http://localhost/admin/

REQUEST / RESPONSE

#1

```
GET /admin/ HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:11 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
Content-Length: 1403
Keep-Alive: timeout=5, max=31
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.

34.2 Sensitive Unreferenced Resource Found

SEVERITY Low

URL http://localhost/listing-sensitive/db.sql

REQUEST / RESPONSE

#1

```
GET /listing-sensitive/db.sql HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:14 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
Last-Modified: Mon, 25 Dec 2017 12:15:21 GMT
ETag: "0-561291ec5001a"
Accept-Ranges: bytes
Content-Length: 0
Keep-Alive: timeout=5, max=98
Connection: Keep-Alive
Content-Type: application/x-sql
```

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.

35.1 Subresource Integrity is Missing

SEVERITY	Low
URL	http://localhost/redirectionBody/
EXTERNAL RESOURCES	https://unpkg.com/vue

REQUEST / RESPONSE

#1

```
GET /redirectionBody/ HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 302 Found
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Location: ../
Content-Length: 3173
Keep-Alive: timeout=5, max=85
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

...[truncated]...
phone=no">
  <meta name="title" content="regex101"></head>
</head>
<body>
  <script src="https://unpkg.com/vue"></script>
  <p>Lorem ipsum dolor sit amet,
...[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.

35.2 Subresource Integrity is Missing

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

REQUEST / RESPONSE

#1

```
GET /ssi/ HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
Last-Modified: Wed, 13 Apr 2022 08:24:26 GMT
ETag: "147-5dc84e7d62df8"
Accept-Ranges: bytes
Content-Length: 327
Keep-Alive: timeout=5, max=77
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.

36.1 Cookie without SameSite Flag

SEVERITY	Low
URL	http://localhost/cookie/domain.php
COOKIE	crossDomain=something

REQUEST / RESPONSE

#1

```
GET /cookie/domain.php HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Set-Cookie: crossDomain=something; domain=localhost
Content-Length: 0
Keep-Alive: timeout=5, max=94
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

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.

36.2 Cookie without SameSite Flag

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

REQUEST / RESPONSE

#1

```
GET /deserialization/json.php HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: profile=Tzo4OiJzdGRDbGFzcyI6Mjp7czo4OiJ1c2VyTmFtZSI7czo4OiJ0ZXN0dXNlciI7czo2OiJ1c2VySWQiO2k
6MTI7fQ%3D%3D; p3=rO0ABXNyAAlTb21lQ2xhc3MAAAAAAAAAAQIABkkAAWJJAAFpTAABZHQAEkxqYXZhL2xhbmcvRG91YmxlO
0wABGhoaGh0ABJMamF2YS9sYW5nL1N0cmluZztMAAFzcQB%2BAAJMAANzdHJxAH4AAnhwAAAAe3%2F%2F%2F%2F9zcgAQamF2YS
5sYW5nLkRvdWJsZYCzwkopa%2FsEAgABRAAFdmFsdWV4cgAQamF2YS5sYW5nLk51bWJlcoaslR0LlOCLAgAAeHC%2F8AAAAAAAA
HQABmhoaGhoaHQABUFCQ0RFdAAGc3RyaW5n;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
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

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.

37.1 Strict-Transport-Security Header is Missing

SEVERITY Low

URL https://localhost/https-pass-in-url/

AFFECTED URLS localhost/breach/
localhost/https-pass-in-url/
localhost/mix/passive.html

REQUEST / RESPONSE

#1

```
GET /https-pass-in-url/ HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
Last-Modified: Tue, 29 Sep 2020 12:22:45 GMT
ETag: "56-5b072d71e16f3"
Accept-Ranges: bytes
Content-Length: 86
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

<html>
<form method="GET">
<input type="password" name="password">
</form>
</html>
```

DESCRIPTION

The HTTP Strict-Transport-Security response header (often abbreviated as HSTS) lets a web site tell browsers that it should only be accessed using HTTPS, instead of using HTTP. Mozilla

RECOMMENDATION

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

38.1 Content-Security-Policy Header is Missing

SEVERITY	Low
URL	http://localhost
AFFECTED URLS (43)	localhost/template-injection/ localhost/sqli/time.php localhost/deserialization/ localhost/breach/ localhost/bof/ localhost/xss/ localhost/xss/base64.php localhost/listing-sensitive/ localhost/phpinfo/ localhost/fuzzing/increment.php localhost/formauth/enumerate.php localhost/sqli/ localhost/mix/passive.html localhost/fetch/name/ localhost/icons/small/ localhost/cookie/session.php localhost/cookie/ localhost localhost/formauth/ localhost/error/server/ ...

REQUEST / RESPONSE

#1

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
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.

39.1 X-Frame-Options Header is Missing

SEVERITY	Low
URL	http://localhost
AFFECTED URLS (43)	localhost/template-injection/ localhost/sqli/time.php localhost/deserialization/ localhost/breach/ localhost/bof/ localhost/xss/ localhost/xss/base64.php localhost/listing-sensitive/ localhost/phpinfo/ localhost/fuzzing/increment.php localhost/formauth/enumerate.php localhost/sqli/ localhost/mix/passive.html localhost/fetch/name/ localhost/icons/small/ localhost/cookie/session.php localhost/cookie/ localhost localhost/formauth/ localhost/error/server/ ...

REQUEST / RESPONSE

#1

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
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.

40.1 Old/Backup Resource Found

SEVERITY	Low
URL	http://localhost/backup/index2.php
BACKUP ORIGIN	index.php

REQUEST / RESPONSE

#1

```
GET /backup/index2.php HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:16 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 28
Keep-Alive: timeout=5, max=66
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

hello az babate samime ghalb
```

DESCRIPTION

Backup files can disclose important information like an application’s source code, administrative interfaces, or even credentials to connect to the administrative interface or the database server.

RECOMMENDATION

Remove all backup files from web publicly accessible locations and make sure backup files are not automatically created or copied in these locations.

41.1 Password Sent in Query

SEVERITY	Low
URL	https://localhost/https-pass-in-url/

REQUEST / RESPONSE

#1

```
GET /https-pass-in-url/ HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
Last-Modified: Tue, 29 Sep 2020 12:22:45 GMT
ETag: "56-5b072d71e16f3"
Accept-Ranges: bytes
Content-Length: 86
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

<html>
<form method="GET">
<input type="password" name="password">
</form>
</html>
```

DESCRIPTION

URLs are stored in log files and might be sent in the `referer` HTTP request header to other websites. Passing sensitive information like passwords as part of the URL might disclose this information to an unauthorized actor. This risk is increased when the traffic is not encrypted.

RECOMMENDATION

Use the HTTP `POST` method and the request body for sending sensitive information.

42.1 Redirection with Body

SEVERITY Low

URL http://localhost/redirectionBody/

REQUEST / RESPONSE

#1

```
GET /redirectionBody/ HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 302 Found
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Location: ../
Content-Length: 3173
Keep-Alive: timeout=5, max=85
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html>
<head>
  <title>My first Vue app</title>
  <meta charset="UTF-8">
  <meta name="apple-mobile-web-app-capable" content="yes">
  <met
...[truncated]...
```

DESCRIPTION

An HTTP redirection (3XX status code) does not require a body. The presence of the body in a redirection HTTP response indicates execution of code after redirection. Redirection with a body can cause serious information leakage or expose access to sensitive functionalities. For example, consider an admin page that redirects unauthorized users to a login page. Without proper implementation of the redirection function, the response can show the admin page contents with all links and functionalities to an unauthorized user.

RECOMMENDATION

Exit the code execution routine after redirection.
In PHP code call `exit()` or `die()` after redirection.
In ASP.NET use `Response.Redirect("redirected-page.aspx", false)` to redirect user.

43.1 Passive Mixed Content

SEVERITY	Low
URL	https://localhost/mix/passive.html
HTTP CONTENTS	<img src="http://localhost/smart-unit-test/complete/mix/img.jpg

REQUEST / RESPONSE

#1

```
GET /mix/passive.html HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
Last-Modified: Sat, 31 Jul 2021 10:18:36 GMT
ETag: "67-5c868a8bd60d7"
Accept-Ranges: bytes
Content-Length: 103
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/html

...[truncated]...
<img src="http://localhost/smart-unit-test/complete/mix/img.jpg
...[truncated]...
```

DESCRIPTION

When a user visits a page served over HTTPS, their connection with the web server is encrypted with TLS and is therefore safeguarded from most sniffers and man-in-the-middle attacks. An HTTPS page that includes content fetched using cleartext HTTP is called a mixed content page. Pages like this are only partially encrypted, leaving the unencrypted content accessible to sniffers and man-in-the-middle attackers. That leaves the pages unsafe. Moilla
Passive contents are like images, audio, or videos. This type of content controls the appearance of the web page. That’s why they are also called display content.

RECOMMENDATION

Make sure all resources are loaded using HTTPS protocol.

44.1 TRACE Method Allowed

SEVERITY Low

URL http://localhost/

REQUEST / RESPONSE

#1

```
TRACE / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
Keep-Alive: timeout=5, max=90
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: message/http

TRACE / HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,applic
...[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**.

45.1 Application Error

SEVERITY	Low
URL	http://localhost/fuzzing/error.php
REFERER	http://localhost/fuzzing/increment.php?q=2
APPLICATION ERROR	error occured

REQUEST / RESPONSE

#1

```
GET /fuzzing/error.php HTTP/1.1
Referer: http://localhost/fuzzing/increment.php?q=2
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:06 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 244
Keep-Alive: timeout=5, max=57
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

an error occured while parsing

<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="/wEPDwUJODczNjQ5OTk0D2QWAgIDD2QWAgI
FDw8WAh4EVGV4dAUWSSBMb3ZlIE
...[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

Properly handle all types of exceptions and display a generic error message.

46.1 Windows Path Disclosure

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

REQUEST / RESPONSE

#1

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
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.

46.2 Windows Path Disclosure

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

REQUEST / RESPONSE

#1

```
GET /deserialization/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer:
Cookie: p3=rO0ABXNyAAlTb21lQ2xhc3MAAAAAAAAAAQIABkkAAWJJAAFpTAABZHQAEkxqYXZhL2xhbmcvRG91YmxlO0wABGho
aGh0ABJMamF2YS9sYW5nL1N0cmluZztMAAFzcQB%2BAAJMAANzdHJxAH4AAnhwAAAAe3%2F%2F%2F%2F9zcgAQamF2YS5sYW5nL
kRvdWJsZYCzwkopa%2FsEAgABRAAFdmFsdWV4cgAQamF2YS5sYW5nLk51bWJlcoaslR0LlOCLAgAAeHC%2F8AAAAAAAAHQABmho
aGhoaHQABUFCQ0RFdAAGc3RyaW5n; id=eyJ1c2VyTmFtZSI6InRlc3R1c2VyIiwidXNlcklkIjoxMn0%3D; profile=IicvPG
p4cXo4MjIzPj0oKQ%3D%3D; PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Set-Cookie: profile=Tzo4OiJzdGRDbGFzcyI6Mjp7czo4OiJ1c2VyTmFtZSI7czo4OiJ0ZXN0dXNlciI7czo2OiJ1c2VySWQ
iO2k6MTI7fQ%3D%3D
Content-Length: 157
Keep-Alive: timeout=5, max=37
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

...[truncated]...
C:\xampp\htdocs\deserialization\index.php</b> on l
...[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.

46.3 Windows Path Disclosure

SEVERITY	Informational
URL	http://localhost/error/?dummy=1
FOUND IN (20)	localhost/error/?dummy=a%26ping 2130706433%26%23%27%26ping 2130706434%26a%26%23%22%26ping 2130706435%26a%5C localhost/error/?dummy=example.com%2F%3F localhost/error/?dummy=%24%7B900507-1%7D localhost/error/?dummy=%22%27%2F%3Cjxqz21850%3E%3D%28%29 localhost/error/?dummy=1 localhost/error/?dummy=1 or 1%3DExtractValue%281%2CCoNCaT%280x3a%2C%28md5%28122459%29%29%29%29 localhost/error/?dummy=1%27 and 0-- a localhost/error/?dummy=99999 or 1-- a localhost/error/?dummy=%7B%7B900507-1%7D%7D localhost/error/?dummy=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fwindows%2Fwin.ini localhost/error/?dummy=1%27 rlike %28case when 1 then BENCHMARK%28450000000%2CMD5%280x41%29%29 else 0 end%29 -- a localhost/error/?dummy=1%27 or 1%3DExtractValue%281%2CCoNCaT%280x3a%2C%28md5%28122459%29%29%29%29 or 1%3D%272 localhost/error/?dummy=1 and 0-- a localhost/error/?dummy=1 or%28seLeCT 1 FROm%28seLeCT count%28%2A%29%2CCoNcaT%28%28seLeCT %28md5%28122459%29%29 FROm %60information_schema%60.tables LimIt 0%2C1%29%2Cfloor%28rand%280%29%2A2%29%29x FROm %60information_schema%60.tables group by x%29a%29 localhost/error/?dummy=hTtp%3A%2F%2Fexample.com%2F%3F localhost/error/?dummy=1%27 or%28seLeCT 1 FROm%28seLeCT count%28%2A%29%2CCoNcaT%28%28seLeCT %28md5%28122459%29%29 FROm %60information_schema%60.tables LimIt 0%2C1%29%2Cfloor%28rand%280%29%2A2%29%29x FROm %60information_schema%60.tables group by x%29a%29 or 1%3D%272 localhost/error/?dummy=1 rlike %28case when 1 then BENCHMARK%28450000000%2CMD5%280x41%29%29 else 0 end%29 -- a localhost/error/?dummy=a%7Cver localhost/error/?dummy=99999%27 or 1-- a localhost/error/
PATH	C:\xampp\htdocs\error\index.php

REQUEST / RESPONSE

#1

```
GET /error/?dummy=1 HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
```

```
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:05 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 229
Keep-Alive: timeout=5, max=98
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

...[truncated]...
C:\xampp\htdocs\error\index.php: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.

46.4 Windows Path Disclosure

SEVERITY	Informational
URL	http://localhost/error/db.php
PATH	C:\xampp\htdocs\error\db.php

REQUEST / RESPONSE

#1

```
GET /error/db.php HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 549
Keep-Alive: timeout=5, max=79
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

...[truncated]...
C:\xampp\htdocs\error\db.php</b> on line <b>18</b><br />
<br />
<b>Fatal error</b>:  Uncaught mysqli_sql_exception: You have an error in your SQL syntax; check the
manual that corresponds to your MariaDB server version for the right syntax to use nea
...[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.

46.5 Windows Path Disclosure

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

REQUEST / RESPONSE

#1

```
POST /fetch/name/index.php HTTP/1.1
Authorization: valid-token
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi
Referer:
Content-Length: 11

name%5B%5D=
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:07 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 126
Keep-Alive: timeout=5, max=42
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

...[truncated]...
C:\xampp\htdocs\fetch\name\index.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.

46.6 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
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 428
Keep-Alive: timeout=5, max=78
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.

46.7 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
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Set-Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi; 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=100
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>C:\xampp\htdocs\formauth\bypassBlock.php</b> on l
ine <b>4</b><br />
<br />
<b>Warning</b>:  Undefined array key "attempts" in
...[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.

46.8 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
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 458
Keep-Alive: timeout=5, max=86
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.

46.9 Windows Path Disclosure

SEVERITY	Informational
URL	http://localhost/fuzzing/array.php?a%5B%5D=
FOUND IN	localhost/fuzzing/array.php?a%5B%5D= localhost/fuzzing/array.php
PATH	C:\xampp\htdocs\fuzzing\array.php

REQUEST / RESPONSE

#1

```
GET /fuzzing/array.php?a%5B%5D= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi
Referer:
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:05 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 321
Keep-Alive: timeout=5, max=81
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

...[truncated]...
C:\xampp\htdocs\fuzzing\array.php:6
Stack trace:
#0 C:\xampp\htdocs\fuzzing\array.php(6): htmlentities(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.

46.10 Windows Path Disclosure

SEVERITY	Informational
URL	http://localhost/osexec/?i=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fwindows%2Fwin.ini%00127.0.0.1
FOUND IN	localhost/osexec/?i=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fwindows%2Fwin.ini%00127.0.0.1 localhost/osexec/?i%5B%5D= localhost/osexec/
PATH	C:\xampp\htdocs\osexec\index.php

REQUEST / RESPONSE

#1

```
GET /osexec/?i=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fwindows%2Fwin.ini%00127.0.0.1 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi
Referer:
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:12 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 338
Keep-Alive: timeout=5, max=17
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

...[truncated]...
C:\xampp\htdocs\osexec\index.php:5
Stack trace:
#0 C:\xampp\htdocs\osexec\index.php(5): system('ping ../../../....')
#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.

46.11 Windows Path Disclosure

SEVERITY	Informational
URL	http://localhost/phpinfo/
PATH (35)	C:\xampp\php\ext C:\xampp\php\extras\browscap.ini C:\Users\Farshad\AppData\Local\Temp C:\Users\Farshad\AppData\Local\Programs\Microsoft C:\Windows\system32 C:\Apache24\conf/openssl.cnf C:\Users\Public C:\xampp\php\logs\php_error_log C:\Users\Farshad\AppData\Local\Microsoft\WindowsApps C:\Windows\System32\WindowsPowerShell\v1.0 C:/xampp/php/extras/mibs C:\Windows\System32\OpenSSH C:\Users\Farshad\AppData\Local\GitHubDesktop\bin C:\ProgramData C:\xampp\php\PEAR C:/xampp/htdocs/phpinfo/index.php C:\xampp\php C:\Users\Farshad\AppData\Local C:/xampp/apache/bin/openssl.cnf C:\xampp\php\php.ini ...

REQUEST / RESPONSE

#1

```
GET /phpinfo/ HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

...[truncated]...
C:\xampp\php\php.ini </td></tr>
<tr><td class="e">Scan this dir for additional .ini files </td><td class="v">(none) </td></tr>
<tr><td class="e">Additional .ini files parsed </td><td class="v">(none) </td></tr>
<tr><td class="e">PHP API </td><td clas
...[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.

46.12 Windows Path Disclosure

SEVERITY	Informational
URL	http://localhost/redir/?u%5B%5D=
FOUND IN	localhost/redir/?u%5B%5D= localhost/redir/?u=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fwindows%2Fwin.ini%00http%3A%2F%2F127.0.0.1%2F localhost/redir/?u=%0D%0Ahttp%3A%2F%2F127.0.0.1%2F%3Ahttp%3A%2F%2F127.0.0.1%2F
PATH	C:\xampp\htdocs\redir\index.php

REQUEST / RESPONSE

#1

```
GET /redir/?u%5B%5D= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer:
```

```
HTTP/1.1 301 Moved Permanently
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Location: Array
Content-Length: 116
Keep-Alive: timeout=5, max=92
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.

46.13 Windows Path Disclosure

SEVERITY	Informational
URL	http://localhost/rfi/rfd.php?f=a
FOUND IN (22)	localhost/rfi/rfd.php?f=a or%28seLeCT 1 FROm%28seLeCT count%28%2A%29%2CCoNcaT%28%28seLeCT %28md5%28122459%29%29 FROm %60information_schema%60.tables LimIt 0%2C1%29%2Cfloor%28rand%280%29%2A2%29%29x FROm %60information_schema%60.tables group by x%29a%29 localhost/rfi/rfd.php?f=%24%7B783332-1%7D localhost/rfi/rfd.php?f=a%27 and 0-- a localhost/rfi/rfd.php?f=99999%27 or 1-- a localhost/rfi/rfd.php?f=99999%27 or %271 localhost/rfi/rfd.php?f=a localhost/rfi/rfd.php?f=a%27 rlike %28case when 1 then BENCHMARK%28450000000%2CMD5%280x41%29%29 else 0 end%29 -- a localhost/rfi/rfd.php?f=a rlike %28case when 1 then BENCHMARK%28450000000%2CMD5%280x41%29%29 else 0 end%29 -- a localhost/rfi/rfd.php?f=a%27 and %270 localhost/rfi/rfd.php?f=a%27 or%28seLeCT 1 FROm%28seLeCT count%28%2A%29%2CCoNcaT%28%28seLeCT %28md5%28122459%29%29 FROm %60information_schema%60.tables LimIt 0%2C1%29%2Cfloor%28rand%280%29%2A2%29%29x FROm %60information_schema%60.tables group by x%29a%29 or 1%3D%272 localhost/rfi/rfd.php?f=%22%27%2F%3Cjxqz19642%3E%3D%28%29 localhost/rfi/rfd.php?f=99999 or 1 localhost/rfi/rfd.php?f=a%27 or 1%3DExtractValue%281%2CCoNCaT%280x3a%2C%28md5%28122459%29%29%29%29 or 1%3D%272 localhost/rfi/rfd.php?f=a%27 and %271 localhost/rfi/rfd.php?f=99999 or 1-- a localhost/rfi/rfd.php?f=a%7Cver localhost/rfi/rfd.php?f=a or 1%3DExtractValue%281%2CCoNCaT%280x3a%2C%28md5%28122459%29%29%29%29 localhost/rfi/rfd.php?f=a and 0-- a localhost/rfi/rfd.php?f=a and 1 localhost/rfi/rfd.php?f=%7B%7B783332-1%7D%7D ...
PATH	C:\xampp\htdocs\rfi\rfd.php

REQUEST / RESPONSE

#1

```
GET /rfi/rfd.php?f=a HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:05 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 167
Keep-Alive: timeout=5, max=95
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

...[truncated]...
C:\xampp\htdocs\rfi\rfd.php</b> on line <b>4</b><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.

46.14 Windows Path Disclosure

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

REQUEST / RESPONSE

#1

```
GET /server-info HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
Keep-Alive: timeout=5, max=92
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.

46.15 Windows Path Disclosure

SEVERITY	Informational
URL	http://localhost/sqli/complex.php?q=%7B%7B394487-1%7D%7D
FOUND IN (21)	localhost/sqli/complex.php?q=1 localhost/sqli/complex.php?q=1 or 1%3DExtractValue%281%2CCoNCaT%280x3a%2C%28md5%28122459%29%29%29%29 localhost/sqli/complex.php?q=%24%7B394487-1%7D localhost/sqli/complex.php?q=1 rlike %28case when 1 then BENCHMARK%28450000000%2CMD5%280x41%29%29 else 0 end%29 -- a localhost/sqli/complex.php?q=%7B%7B394487-1%7D%7D localhost/sqli/complex.php?q=99999 or 1-- a localhost/sqli/complex.php?q=hTtp%3A%2F%2Fexample.com%2F%3F localhost/sqli/complex.php?q=complex.php%001 localhost/sqli/complex.php?q=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fwindows%2Fwin.ini localhost/sqli/complex.php?q=1%27 or 1%3DExtractValue%281%2CCoNCaT%280x3a%2C%28md5%28122459%29%29%29%29 or 1%3D%272 localhost/sqli/complex.php?q=1%27 or%28seLeCT 1 FROm%28seLeCT count%28%2A%29%2CCoNcaT%28%28seLeCT %28md5%28122459%29%29 FROm %60information_schema%60.tables LimIt 0%2C1%29%2Cfloor%28rand%280%29%2A2%29%29x FROm %60information_schema%60.tables group by x%29a%29 or 1%3D%272 localhost/sqli/complex.php?q=1 and 0-- a localhost/sqli/complex.php?q=%22%27%2F%3Cjxqz14058%3E%3D%28%29 localhost/sqli/complex.php?q=complex.php localhost/sqli/complex.php?q=example.com%2F%3F localhost/sqli/complex.php?q=99999%27 or 1-- a localhost/sqli/complex.php?q=a%26ping 2130706433%26%23%27%26ping 2130706434%26a%26%23%22%26ping 2130706435%26a%5C localhost/sqli/complex.php?q=1%27 rlike %28case when 1 then BENCHMARK%28450000000%2CMD5%280x41%29%29 else 0 end%29 -- a localhost/sqli/complex.php?q=a%7Cver localhost/sqli/complex.php?q=1 or%28seLeCT 1 FROm%28seLeCT count%28%2A%29%2CCoNcaT%28%28seLeCT %28md5%28122459%29%29 FROm %60information_schema%60.tables LimIt 0%2C1%29%2Cfloor%28rand%280%29%2A2%29%29x FROm %60information_schema%60.tables group by x%29a%29 ...
PATH	C:\xampp\htdocs\sqli\complex.php C:\xampp\htdocs\sqli/../../scripts/sqli/db.php C:\xampp\php\PEAR C:\xampp\htdocs\sqli\connect.php

REQUEST / RESPONSE

#1

```
GET /sqli/complex.php?q=%7B%7B394487-1%7D%7D HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi
Referer:
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:03 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 534
Keep-Alive: timeout=5, max=90
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

...[truncated]...
C:\xampp\htdocs\sqli/../../scripts/sqli/db.php): Failed to open stream: No such file or directory i
n <b>C:\xampp\htdocs\sqli\connect.php</b> on line <b>3</b><br />
<br />
<b>Fatal error</b>:  Uncaught Error: Failed opening required 'C:\xampp\htdocs\s
...[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.

46.16 Windows Path Disclosure

SEVERITY	Informational
URL	http://localhost/template-injection/index.php
PATH	C:\xampp\htdocs\template-injection\index.php C:\xampp\htdocs\template-injection\vendor\twig\twig\src\Loader\ArrayLoader.php C:\xampp\htdocs\template-injection\vendor\twig\twig\src\Environment.php

REQUEST / RESPONSE

#1

```
GET /template-injection/index.php HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:15 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 967
Keep-Alive: timeout=5, max=67
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

...[truncated]...
C:\xampp\htdocs\template-injection\index.php</b> on line <b>6</b><br />
<br />
<b>Fatal error</b>:  Uncaught Twig\Error\LoaderError: Template &quot;index&quot; is not defined. in
C:\xampp\htdocs\template-injection\vendor\twig\twig\src\Loader\ArrayLoa
...[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.

46.17 Windows Path Disclosure

SEVERITY	Informational
URL	http://localhost/template-injection/index.php?template%5B%5D=
PATH	C:\xampp\htdocs\template-injection\index.php C:\xampp\htdocs\template-injection\vendor\twig\twig\src\Loader\ArrayLoader.php C:\xampp\htdocs\template-injection\vendor\twig\twig\src\Source.php C:\xampp\htdocs\template-injection\vendor\twig\twig\src\Environment.php

REQUEST / RESPONSE

#1

```
GET /template-injection/index.php?template%5B%5D= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi
Referer:
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:06 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 1269
Keep-Alive: timeout=5, max=70
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

...[truncated]...
C:\xampp\htdocs\template-injection\vendor\twig\twig\src\Loader\ArrayLoader.php</b> on line <b>66</b><br />
<br />
<b>Fatal error</b>:  Uncaught TypeError: Twig\Source::__construct(): Argument #1 ($code) must be of type string, array given, called in
...[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.

46.18 Windows Path Disclosure

SEVERITY	Informational
URL	http://localhost/xss/base64.php?
FOUND IN	localhost/xss/base64.php localhost/xss/base64.php?name%5B%5D=
PATH	C:\xampp\htdocs\xss\base64.php

REQUEST / RESPONSE

#1

```
GET /xss/base64.php? HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi
Referer:
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:05 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 121
Keep-Alive: timeout=5, max=72
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

...[truncated]...
C:\xampp\htdocs\xss\base64.php</b> on line <b>3</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.

46.19 Windows Path Disclosure

SEVERITY	Informational
URL	http://localhost/xss/index.php?name%5B%5D=
FOUND IN	localhost/xss/ localhost/xss/?name%5B%5D=
PATH	C:\xampp\htdocs\xss\index.php

REQUEST / RESPONSE

#1

```
GET /xss/index.php?name%5B%5D= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer:
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
X-XSS-Protection: 1
Content-Length: 125
Keep-Alive: timeout=5, max=95
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.

46.20 Windows Path Disclosure

SEVERITY	Informational
URL	https://localhost/breach/?input%5B%5D=
PATH	C:\xampp\htdocs\breach\index.php

REQUEST / RESPONSE

#1

```
GET /breach/?input%5B%5D= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi
Referer:
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:05 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 318
Keep-Alive: timeout=5, max=82
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

...[truncated]...
C:\xampp\htdocs\breach\index.php:3
Stack trace:
#0 C:\xampp\htdocs\breach\index.php(3): htmlentities(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.

47.1 Email Address Disclosure

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

REQUEST / RESPONSE

#1

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
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.

47.2 Email Address Disclosure

SEVERITY	Informational
URL	http://localhost/fuzzing/increment.php?q=2
FOUND EMAILS	hidden@parameterValue.com

REQUEST / RESPONSE

#1

```
GET /fuzzing/increment.php?q=2 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi
Referer:
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:05 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 47
Keep-Alive: timeout=5, max=27
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<a href=error.php>hidden@parameterValue.com</a>
```

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.

47.3 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/listing-sensitive/
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:06 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
Keep-Alive: timeout=5, max=37
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.

47.4 Email Address Disclosure

SEVERITY	Informational
URL	http://localhost/phpinfo/
FOUND EMAILS	license@php.net

REQUEST / RESPONSE

#1

```
GET /phpinfo/ HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

...[truncated]...
license@php.net.
</p>
</td></tr>
</table>
</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.

47.5 Email Address Disclosure

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

REQUEST / RESPONSE

#1

```
GET /server-info HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
Keep-Alive: timeout=5, max=92
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.

48.1 Content Character Encoding is not Defined

SEVERITY	Informational
URL	http://localhost/ssi/

REQUEST / RESPONSE

#1

```
GET /ssi/ HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
Last-Modified: Wed, 13 Apr 2022 08:24:26 GMT
ETag: "147-5dc84e7d62df8"
Accept-Ranges: bytes
Content-Length: 327
Keep-Alive: timeout=5, max=77
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" >
```

48.2 Content Character Encoding is not Defined

SEVERITY	Informational
URL	http://localhost/ssi/safe.html

REQUEST / RESPONSE

#1

```
GET /ssi/safe.html HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:03 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
Last-Modified: Sat, 04 Sep 2021 06:58:09 GMT
ETag: "10a-5cb25f04c5641"
Accept-Ranges: bytes
Content-Length: 266
Keep-Alive: timeout=5, max=97
Connection: Keep-Alive
Content-Type: text/html

<html>

<head>
<script
                          src="https://code.jquery.com/ui/1.13.0-alpha.1/jquery-ui.min.js"
                          integrity="sha256-ahTP8JLHwIplWgufAohh+E04ayoLEUBEwcH04eU
...[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" >
```

48.3 Content Character Encoding is not Defined

SEVERITY	Informational
URL	https://localhost/https-pass-in-url/

REQUEST / RESPONSE

#1

```
GET /https-pass-in-url/ HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
Last-Modified: Tue, 29 Sep 2020 12:22:45 GMT
ETag: "56-5b072d71e16f3"
Accept-Ranges: bytes
Content-Length: 86
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

<html>
<form method="GET">
<input type="password" name="password">
</form>
</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" >
```

48.4 Content Character Encoding is not Defined

SEVERITY	Informational
URL	https://localhost/mix/passive.html

REQUEST / RESPONSE

#1

```
GET /mix/passive.html HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
Last-Modified: Sat, 31 Jul 2021 10:18:36 GMT
ETag: "67-5c868a8bd60d7"
Accept-Ranges: bytes
Content-Length: 103
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/html

<html>
passive content mix
<img src="http://localhost/smart-unit-test/complete/mix/img.jpg">
</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" >
```

49.1 Directory Listing

SEVERITY	Informational
URL	http://localhost/icons/

REQUEST / RESPONSE

#1

```
GET /icons/ HTTP/1.1
Referer: http://localhost/listing-sensitive/
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:06 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
Keep-Alive: timeout=5, max=37
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.

49.2 Directory Listing

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

REQUEST / RESPONSE

#1

```
GET /icons/small/ HTTP/1.1
Referer: http://localhost/icons/
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:08 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
Keep-Alive: timeout=5, max=96
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.

49.3 Directory Listing

SEVERITY	Informational
URL	http://localhost/listing/

REQUEST / RESPONSE

#1

```
GET /listing/ HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
Content-Length: 981
Keep-Alive: timeout=5, max=80
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 /listing</title>
 </head>
 <body>
<h1>Index of /listing</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.

49.4 Directory Listing

SEVERITY	Informational
URL	https://localhost/mix/

REQUEST / RESPONSE

#1

```
GET /mix/ HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:06 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
Content-Length: 1187
Keep-Alive: timeout=5, max=87
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 /mix</title>
 </head>
 <body>
<h1>Index of /mix</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.

50.1 PHP Version Disclosure

SEVERITY	Informational
URL	http://localhost
PHP VERSION	8.1.6

DETAILS

PHP version is disclosed in the `Server header`.

REQUEST / RESPONSE

#1

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
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.

50.2 PHP Version Disclosure

SEVERITY	Informational
URL	http://localhost/phpinfo/
PHP VERSION	Windows NT DESKTOP-NC76V6P 10.0 build 19044 (Windows 10) AMD64

DETAILS

PHP version is disclosed in the ``.

REQUEST / RESPONSE

#1

```
GET /phpinfo/ HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml"><head>
<style type="tex
...[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 X-Content-Type-Options Header is Missing

SEVERITY	Informational
URL	http://localhost
AFFECTED URLS (43)	localhost/template-injection/ localhost/sqli/time.php localhost/deserialization/ localhost/breach/ localhost/bof/ localhost/xss/ localhost/xss/base64.php localhost/listing-sensitive/ localhost/phpinfo/ localhost/fuzzing/increment.php localhost/formauth/enumerate.php localhost/sqli/ localhost/mix/passive.html localhost/fetch/name/ localhost/icons/small/ localhost/cookie/session.php localhost/cookie/ localhost localhost/formauth/ localhost/error/server/ ...

REQUEST / RESPONSE

#1

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
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`.

52.1 Missing or Insecure Cache-Control Header

SEVERITY	Informational
URL	http://localhost/xss/index.php?name=test
AFFECTED URLS (18)	localhost/fuzzing/array.php localhost/cookie/domain.php localhost/sqli/complex.php localhost/rfi/lfi.php localhost/formauth/enumerate.php localhost/sqli/time.php localhost/rfi/lfd.php localhost/xss/ localhost/fuzzing/increment.php localhost/fetch/name/ localhost/error/db.php localhost/sqli/blind.php localhost/fuzzing/error.php localhost/xss/base64.php localhost/rfi/rfd.php localhost/deserialization/json.php localhost/template-injection/ localhost/cookie/

DETAILS

The `Cache-Control` header is not set

REQUEST / RESPONSE

#1

```
GET /xss/index.php?name=test HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
X-XSS-Protection: 1
Content-Length: 10
Keep-Alive: timeout=5, max=89
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

hello test
```

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
```

53.1 Cross-Origin Resource Sharing Allowed

SEVERITY	Informational
URL	http://localhost/CORS/

REQUEST / RESPONSE

#1

```
GET /CORS/ HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:03 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Access-Control-Allow-Origin: *
Content-Length: 14
Keep-Alive: timeout=5, max=98
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

CORS enabled *
```

DESCRIPTION

Cross-Origin Resource Sharing (CORS) is a mechanism that uses additional HTTP headers to tell browsers to give a web application running at one origin, access to selected resources from a different origin. A web application executes a cross-origin HTTP request when it requests a resource that has a different origin (domain, protocol, or port) from its own. Mozilla

Cross-origin resource sharing should not be allowed unless specifically needed to minimize disclosure of sensitive information to foreign origins.

RECOMMENDATION

Consider removing the `Access-Control-Allow-Origin` header or use specific origins as value.

54.1 Referrer-Policy Header is Missing

SEVERITY	Informational
URL	http://localhost
AFFECTED URLS (43)	localhost/template-injection/ localhost/sqli/time.php localhost/deserialization/ localhost/breach/ localhost/bof/ localhost/xss/ localhost/xss/base64.php localhost/listing-sensitive/ localhost/phpinfo/ localhost/fuzzing/increment.php localhost/formauth/enumerate.php localhost/sqli/ localhost/mix/passive.html localhost/fetch/name/ localhost/icons/small/ localhost/cookie/session.php localhost/cookie/ localhost localhost/formauth/ localhost/error/server/ ...

REQUEST / RESPONSE

#1

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
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.

55.1 Cookie Accessible for Subdomains

SEVERITY	Informational
URL	http://localhost/cookie/domain.php
COOKIE	crossDomain=something

DETAILS

The `localhost` domain was set for the cookie `crossDomain`. So the cookie is accessible to any subdomain.

REQUEST / RESPONSE

#1

```
GET /cookie/domain.php HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Set-Cookie: crossDomain=something; domain=localhost
Content-Length: 0
Keep-Alive: timeout=5, max=94
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

DESCRIPTION

If the `Set-Cookie` header contains the `Domain` attribute, browsers automatically send the cookie to any subdomains of the specified domain. This allows subdomains to access data in cookies.

RECOMMENDATION

Remove the `Domain` attribute from `Set-Cookie` attribute.

56.1 Private IPv4 Address Disclosure

SEVERITY	Informational
URL	http://localhost
IP ADDRESSES	10.10.98.19

REQUEST / RESPONSE

#1

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
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.

57.1 Private IPv6 Address Disclosure

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

REQUEST / RESPONSE

#1

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
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.

58.1 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
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
X-XSS-Protection: 1
Content-Length: 10
Keep-Alive: timeout=5, max=89
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.

59.1 Public-Key-Pins Header is Set

SEVERITY	Informational
URL	http://localhost/HPKP/
HPKP	aa; max-age=1

REQUEST / RESPONSE

#1

```
GET /HPKP/ HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Public-Key-Pins: aa; max-age=1
Content-Length: 4
Keep-Alive: timeout=5, max=75
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

HPKP
```

DESCRIPTION

The HTTP `Public-Key-Pins` response header used to associate a specific cryptographic public key with a certain web server to decrease the risk of MITM attacks with forged certificates. However, it has been removed from modern browsers and is no longer supported.
Use Certificate Transparency and `Expect-CT` header instead. Mozilla

RECOMMENDATION

Consider removing the `Public-Key-Pins` header and using the `Expect-CT` header.

60.1 Unreferenced Resource Found

SEVERITY Informational

URL http://localhost/fuzzing/removeparam.php

REQUEST / RESPONSE

#1

```
GET /fuzzing/ HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:07 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
Content-Length: 1621
Keep-Alive: timeout=5, max=67
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 /fuzzing</title>
 </head>
 <body>
<h1>Index of /fuzzing</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.

61.1 ViewState is not Encrypted

SEVERITY Informational

URL http://localhost/fuzzing/error.php

REQUEST / RESPONSE

#1

```
GET /fuzzing/error.php HTTP/1.1
Referer: http://localhost/fuzzing/increment.php?q=2
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=i9fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:06 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 244
Keep-Alive: timeout=5, max=57
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

an error occured while parsing

<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="/wEPDwUJODczNjQ5OTk0D2QWAgIDD2QWAgI
FDw8WAh4EVGV4dAUWSSBMb3ZlIERvdG5ldEN1cnJ5LmNvbWRkZMHbBY9JqBTvB5/6kXnY15AUSAwa" />
<input type="file" name="f">
```

DESCRIPTION

The ViewState is a hidden form input in ASP.NET pages which is used automatically to persist information such as non-default values of controls.
It is also possible to store application data specific to a page in the ViewState.
If the ViewState is not encrypted, anyone can see stored values in it.

RECOMMENDATION

Do not store sensitive values in the ViewState and enable encryption for it.
To enable ViewState encryption for the whole application, add the below lines to the `pages` node under `system.web` of the `Web.Config`.

```
<system.web>
  <pages viewStateEncryptionMode="Always" />
</system.web>
```

To enable encryption for a specific page add the below line at the top of the page:

```
<%@Page ViewStateEncryptionMode="Always" %>
```

62.1 File Upload Functionality

SEVERITY	Informational
URL	http://localhost
AFFECTED URLS	localhost/fuzzing/error.php localhost

REQUEST / RESPONSE

#1

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
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.

63.1 X-Powered-By Header Found

SEVERITY	Informational
URL	http://localhost
X-POWERED-BY	PHP/8.1.6

REQUEST / RESPONSE

#1

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
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.

64.1 Apache Version Disclosure

SEVERITY	Informational
URL	http://localhost
VERSION	2.4.53 (win64)

REQUEST / RESPONSE

#1

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
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.

65.1 Serialized Object Found

SEVERITY	Informational
URL	http://localhost/deserialization/
PARAMETER (COOKIE-BASE64)	p3
OBJECT	rO0ABXNyAAlTb21lQ2xhc3MAAAAAAAAAAQIABkkAAWJJAAFpTAABZHQAEkxqYXZhL2xhbmcvRG91YmxlO0wABGhoaGh0ABJMamF2YS9sYW5nL1N0cmluZztMAAFzcQB%2BAAJMAANzdHJxAH4AAnhwAAAAe3%2F%2F%2F%2F9zcgAQamF2YS5sYW5nLkRvdWJsZYCzwkopa%2FsEAgABRAAFdmFsdWV4cgAQamF2YS5sYW5nLk51bWJlcoaslR0LlOCLAgAAeHC%2F8AAAAAAAAHQABmhoaGhoaHQABUFCQ0RFdAAGc3RyaW5n
OBJECT TYPE	JAVA

REQUEST / RESPONSE

#1

```
GET /deserialization/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer:
Cookie: p3=77%2B977%2B9; id=eyJ1c2VyTmFtZSI6InRlc3R1c2VyIiwidXNlcklkIjoxMn0%3D; profile=Tzo4OiJzdGR
DbGFzcyI6Mjp7czo4OiJ1c2VyTmFtZSI7czo4OiJ0ZXN0dXNlciI7czo2OiJ1c2VySWQiO2k6MTI7fQ%3D%3D; PHPSESSID=i9
fagce07s9b7u3h9lcqgphlhi;
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:02 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Content-Length: 14
Keep-Alive: timeout=5, max=91
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

Hello testuser
```

DESCRIPTION

Object serialization allows transferring complex data structures over channels like HTTP. But whenever there is a serialized object there would be a deserialization process in place. Object deserialization is prone to different vulnerabilities like command execution.

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.

66.1 SQL Command Disclosure

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

REQUEST / RESPONSE

#1

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
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.

67.1 Unix Path Disclosure

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

REQUEST / RESPONSE

#1

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

...[truncated]...
/var/log/www/</span>
        </div>
  </div>
  <div cl
...[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.

68.1 Target Information

SEVERITY	Informational
URL	http://localhost
AUTHENTICATION REQUIRED	http://localhost/basicauth/
COOKIES (6)	p3 test id PHPSESSID profile crossDomain
DATABASE	MariaDB
EMAILS (6)	admin@gmail.com admin@example.com hidden@parameterValue.com mike@hyperreal.org license@php.net kevinh@kevcom.com
FORMS WITH PASSWORD	http://localhost/formauth/ https://localhost/https-pass-in-url/ http://localhost/login/ http://localhost/formauth/enumerate.php http://localhost/formauth/bypassBlock.php
HTTPS	TLS 1.3
OS	Windows NT DESKTOP-NC76V6P 10.0 build 19044 (Windows 10) AMD64
PHP VERSIONS	8.1.6 Windows NT DESKTOP-NC76V6P 10.0 build 19044 (Windows 10) AMD64
PATHS (79)	C:\Windows\system32\cmd.exe C:/xampp/apache C:\xampp\htdocs\fetch\name\index.php C:/xampp/apache/logs/error.log C:/xampp/licenses C:\xampp\php\logs\php_error_log C:\xampp\htdocs\breach\index.php C:/xampp/apache/bin/openssl.cnf C:\xampp\htdocs\formauth\index.php C:/xampp/php C:\xampp\htdocs\error\index.php C:\xampp\htdocs\template-injection\vendor\twig\twig\src\Loader\ArrayL

	C:\Users\Farshad\OneDrive C:\xampp\apache\cgi-bin\index.php C:/xampp/apache/conf/extra/httpd-mpm.conf C:\xampp\php\extras\browscap.ini ...
SERVER BANNER	apache/2.4.53 (win64) openssl/1.1.1n php/8.1.6
SERVICES	HTTPS
TECHNOLOGIES	Java PHP
USERS	admin
WEB SERVER	apache/2.4.53 (win64)
X-POWERED-BY	PHP/8.1.6

69.1 Broken Link

SEVERITY	Informational
URL	http://localhost/nowhere
REFERER	http://localhost

REQUEST / RESPONSE

#1

```
GET /nowhere HTTP/1.1
Referer: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 404 Not Found
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
Content-Length: 295
Keep-Alive: timeout=5, max=90
Connection: Keep-Alive
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
...[truncated]...
```

DESCRIPTION

Broken hyperlinks in web pages can create a bad experience for the users. It can also affect the web page ranking in web search results.

RECOMMENDATION

Consider removing or fixing the link.

70.1 Profanity

SEVERITY	Informational
URL	http://localhost
PROFANS	fuck

REQUEST / RESPONSE

#1

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Jul 2022 09:31:01 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
X-Powered-By: PHP/8.1.6
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

...[truncated]...
fuck you</span>
        </div>
  </div>
  <div class="
...[truncated]...
```

DESCRIPTION

Profanity in web pages can create a bad experience for the users. It can also affect the web page ranking in web search results.

RECOMMENDATION

Create a policy in this regard and act accordingly.