Acunetix
by Invicti

Compliance Report

OWASP TOP 10 2021

Description

The primary aim of the OWASP Top 10 is to educate developers, designers, architects, managers, and organizations about the consequences of the most important web application security weaknesses. The Top 10 provides basic techniques to protect against these high risk problem areas - and also provides guidance on where to go from here.

Disclaimer

This document or any of its content cannot account for, or be included in any form of legal advice. The outcome of a vulnerability scan (or security evaluation) should be utilized to ensure that diligent measures are taken to lower the risk of potential exploits carried out to compromise data.

Legal advice must be supplied according to its legal context. All laws and the environments in which they are applied, are constantly changed and revised. Therefore no information provided in this document may ever be used as an alternative to a qualified legal body or representative.

A portion of this report is taken from OWASP's Top Ten 2021 Project document, that can be found at http://www.owasp.org.

Scan Detail

Target	http://213.125.163.178:1337
Scan Type	Full Scan
Start Time	Jun 10, 2022, 10:41:35 AM GMT-7
Scan Duration	12 minutes
Requests	4824
Average Response Time	119ms
Maximum Response Time	15558ms

Compliance at a Glance

	CATEGORY
1	A01 Broken Access Control
1	A02 Cryptographic Failures
0	A03 Injection
2	A04 Insecure Design
3	A05 Security Misconfiguration
2	A06 Vulnerable and Outdated Components
1	A07 Identification and Authentication Failures
0	A08 Software and Data Integrity Failures
0	A09 Security Logging and Monitoring Failures
0	A10 Server-Side Request Forgery

Detailed Compliance Report by Category

This section is a detailed report that explains each vulnerability found according to individual compliance categories.

A01 Broken Access Control

Access control enforces policy such that users cannot act outside of their intended permissions. Failures typically lead to unauthorized information disclosure, modification, or destruction of all data or performing a business function outside the user's limits.

Clickjacking: X-Frame-Options header

Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

The server did not return an **X-Frame-Options** header with the value DENY or SAMEORIGIN, which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into untrusted sites.

CWE

CWE-1021

CVSS2

AV:N/AC:M/Au:N/C:N/I:P/A:N

Access Vector	Network
Access Complexity	Medium
Authentication	None
Confidentiality	None
Integrity Impact	Partial
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:N

Base Score	5.8
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	None
Integrity Impact	Low
Availability Impact	None

Impact

The impact depends on the affected web application.

http://213.125.163.178:1337/

Paths without secure XFO header:

- http://213.125.163.178:1337/
- http://213.125.163.178:1337/index.php

Request

```
GET / HTTP/1.1
Referer: http://213.125.163.178:1337/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/92.0.4512.0 Safari/537.36
Host: 213.125.163.178:1337
Connection: Keep-alive
```

Recommendation

Configure your web server to include an X-Frame-Options header and a CSP header with frame-ancestors directive. Consult Web references for more information about the possible values for this header.

References

The X-Frame-Options response header
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

Clickjacking
https://en.wikipedia.org/wiki/Clickjacking

OWASP Clickjacking
https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html

Frame Buster Buster
https://stackoverflow.com/questions/958997/frame-buster-buster-buster-code-needed

A02 Cryptographic Failures

The first thing is to determine the protection needs of data in transit and at rest. For example, passwords, credit card numbers, health records, personal information, and business secrets require extra protection, mainly if that data falls under privacy laws, e.g., EU's General Data Protection Regulation (GDPR), or regulations, e.g., financial data protection such as PCI Data Security Standard (PCI DSS).

Unencrypted connection

This scan target was connected to over an unencrypted connection. A potential attacker can intercept and modify data sent and received from this site.

CWE

CWE-319

CVSS2

AV:N/AC:M/Au:N/C:P/I:P/A:N

Access Vector	Network
Access Complexity	Medium
Authentication	None
Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N

Base Score	5.4
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	Low
Integrity Impact	Low
Availability Impact	None

Impact

Possible information disclosure.

http://213.125.163.178:1337/ Verified

Request

```
GET / HTTP/1.1
Referer: http://213.125.163.178:1337/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/92.0.4512.0 Safari/537.36
Host: 213.125.163.178:1337
Connection: Keep-alive
```

Recommendation

The site should send and receive data over a secure (HTTPS) connection.

A03 Injection

Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

No alerts in this category

A04 Insecure Design

Insecure design is a broad category representing different weaknesses, expressed as "missing or ineffective control design." Insecure design is not the source for all other Top 10 risk categories. There is a difference between insecure design and insecure implementation. We differentiate between design flaws and implementation defects for a reason, they have different root causes and remediation. A secure design can still have implementation defects leading to vulnerabilities that may be exploited. An insecure design cannot be fixed by a perfect implementation as by definition, needed security controls were never created to defend against specific attacks. One of the factors that contribute to insecure design is the lack of business risk profiling inherent in the software or system being developed, and thus the failure to determine what level of security design is required.

Clickjacking: X-Frame-Options header

Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

The server did not return an **X-Frame-Options** header with the value DENY or SAMEORIGIN, which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into untrusted sites.

CWE

CWE-1021

CVSS2

AV:N/AC:M/Au:N/C:N/I:P/A:N

Access Vector	Network

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:N

Base Score	5.8

Access Complexity	Medium
Authentication	None
Confidentiality	None
Integrity Impact	Partial
Availability Impact	None

Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	None
Integrity Impact	Low
Availability Impact	None

Impact

The impact depends on the affected web application.

http://213.125.163.178:1337/

Paths without secure XFO header:

- http://213.125.163.178:1337/
- http://213.125.163.178:1337/index.php

Request

```
GET / HTTP/1.1
Referer: http://213.125.163.178:1337/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/92.0.4512.0 Safari/537.36
Host: 213.125.163.178:1337
Connection: Keep-alive
```

Recommendation

Configure your web server to include an X-Frame-Options header and a CSP header with frame-ancestors directive. Consult Web references for more information about the possible values for this header.

References

The X-Frame-Options response header
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

Clickjacking
https://en.wikipedia.org/wiki/Clickjacking

OWASP Clickjacking
https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html

Frame Buster Buster
https://stackoverflow.com/questions/958997/frame-buster-buster-buster-code-needed

Content Security Policy (CSP) not implemented

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.

Content Security Policy (CSP) can be implemented by adding a **Content-Security-Policy** header. The value of this header is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for the all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:

```
Content-Security-Policy:
default-src 'self';
script-src 'self' https://code.jquery.com;
```

It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP header is missing from the response. It's recommended to implement Content Security Policy (CSP) into your web application.

CWE
CWE-1021

CVSS2
AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Impact

CSP can be used to prevent and/or mitigate attacks that involve content/code injection, such as cross-site scripting/XSS attacks, attacks that require embedding a malicious resource, attacks that involve malicious use of iframes, such as clickjacking attacks, and others.

---

http://213.125.163.178:1337/

Paths without CSP header:

- http://213.125.163.178:1337/
- http://213.125.163.178:1337/index.php

Request

```
GET / HTTP/1.1
Referer: http://213.125.163.178:1337/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/92.0.4512.0 Safari/537.36
Host: 213.125.163.178:1337
Connection: Keep-alive
```

Recommendation

It's recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the **Content-Security-Policy** HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page.

References

Content Security Policy (CSP)
https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP

Implementing Content Security Policy
https://hacks.mozilla.org/2016/02/implementing-content-security-policy/

A05 Security Misconfiguration

Security misconfiguration is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securly configured, but they must be patched and upgraded in a timely fashion.

Cookies without HttpOnly flag set

One or more cookies don't have the HttpOnly flag set. When a cookie is set with the HttpOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies.

CWE

CWE-1004

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Impact

Cookies can be accessed by client-side scripts.

http://213.125.163.178:1337/ Verified

Cookies without HttpOnly flag set:

- http://213.125.163.178:1337/

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IjhIM1lNUEVvNGFLWDRBTmtYbDdieVE9PSIsInZhbHVlIjoiTEY2QURzak9jVGRMQVF
jMURVV0xwMGQwek5WVndQVytOeHBiY2VKUVpHTTdyY1BIb1lqU1c2dGJNMVplakFTeGFWWktoL29wQmJ2
NURVVnBGcHVqazhVbUV0T0tFakdNMm9PQy9yWk9PUVQvR1lUcEhTajJ6QkVHSkJzemRXM2wiLCJtYWMiO
iI4MGI5MzBlYWFmN2E3YjU0ODkyMzc1NWQ5MTIzODNkZDQzNDE3Y2FiOWUwODQ3NzYyOTIzMzExYzI5MD
YxNTZhIiwidGFnIjoiIn0%3D; expires=Fri, 10 Jun 2022 19:41:48 GMT; Max-Age=7200;
path=/; samesite=lax
```

- http://213.125.163.178:1337/index.php

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IkpmcXRjcWZrejJBWVhVOWZydi9Yc2c9PSIsInZhbHVlIjoiSTZCM09iYjVmMnFYeFZ
0Y1ljMWp0WWFWYTRKbng3T211b1kwSWRiT0RObDNZdlBiQ0RWVEtWS1N5ZnhaN3Jud0Q2UVJrckQwa2tD
WDBuUjJQOWxtdkwrVFdOdzd0cklFTDQrS1RiY0Jqam5tRk9rWUdZd0RhdCt6czg0RmVzY1oiLCJtYWMiO
iI1OWQwOTAwZTRlNzAwMDQ0MWEyMGI3YjgxY2EyOTc0M2MwNWZhZjg1NDFmNDg2OWY1ZWMzM2ZhOWYzZW
UwMTAxIiwidGFnIjoiIn0%3D; expires=Fri, 10 Jun 2022 19:48:59 GMT; Max-Age=7200;
path=/; samesite=lax
```

- http://213.125.163.178:1337/

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6InlVNU1IanJ0Wm5FUUpxMUxoTHc3c0E9PSIsInZhbHVlIjoicVhjK1Z3bnJCSTViK0E
relNJSit4QVk3TzNhSnlUT3lzNUl6ZEhpZUN2dlcreUVqK1NHT3YwS1BkNTRDaDFYbnpudm9tN3NKQmtD
U3VKVEV6QTNsWjBFT2FHQjdqWWl0WGNRKzFCL3BGZ2ZJcEVFVWFaNlQ0ZDl2TTNCR0JVWjUiLCJtYWMiO
iJiYjU5ZDQ2ZGIyMGNkOTIxMTFlNDUwOGVkOTI0ZTQyMzM5ODRkM2NlNmMzNzcwYjY5ZjhmY2M4YTY1YW
E5ZDFhIiwidGFnIjoiIn0%3D; expires=Fri, 10 Jun 2022 19:51:35 GMT; Max-Age=7200;
path=/; samesite=lax
```

- http://213.125.163.178:1337/index.php

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IjlzZDZHMmJFd1JnbU82MUMyYlBwdVE9PSIsInZhbHVlIjoieEY3UVNpWmR4WFRaVEt
zRVlyVkcySG1CcWpTM2JGZHJoTHpsLzcwQXdvdldCTzdkRjJVS0UvU2JpZDBiekk5MXV2Um9Nbi9LT1M4
OExRa3VtWForbkhWeUErQ2NyUDBGUnVoL3FSdjYySjBHUktoMHR5RUZCUkJxeGJMcFFJK1IiLCJtYWMiO
iJhMDgzN2FiMGUyYjFhNzQ0MGMzNDNmNWY2Zjg2NWY3ZTM1MzJiOTcwMWJjYmM2NDA4YTJkNGZjMzEzNG
FlYzIwIiwidGFnIjoiIn0%3D; expires=Fri, 10 Jun 2022 19:51:42 GMT; Max-Age=7200;
path=/; samesite=lax
```

Request

```
GET / HTTP/1.1
Referer: http://213.125.163.178:1337/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/92.0.4512.0 Safari/537.36
Host: 213.125.163.178:1337
Connection: Keep-alive
```

Recommendation

If possible, you should set the HttpOnly flag for these cookies.

Content Security Policy (CSP) not implemented

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.

Content Security Policy (CSP) can be implemented by adding a **Content-Security-Policy** header. The value of this header is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for the all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:

```
Content-Security-Policy:
default-src 'self';
script-src 'self' https://code.jquery.com;
```

It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP header is missing from the response. It's recommended to implement Content Security Policy (CSP) into your web application.

CWE

CWE-1021

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Impact

CSP can be used to prevent and/or mitigate attacks that involve content/code injection, such as cross-site scripting/XSS attacks, attacks that require embedding a malicious resource, attacks that involve malicious use of iframes, such as clickjacking attacks, and others.

http://213.125.163.178:1337/

Paths without CSP header:

- http://213.125.163.178:1337/
- http://213.125.163.178:1337/index.php

Request

```
GET / HTTP/1.1
Referer: http://213.125.163.178:1337/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/92.0.4512.0 Safari/537.36
Host: 213.125.163.178:1337
Connection: Keep-alive
```

Recommendation

It's recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the **Content-Security-Policy** HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page.

References

Content Security Policy (CSP)
https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP

Implementing Content Security Policy
https://hacks.mozilla.org/2016/02/implementing-content-security-policy/

No HTTP Redirection

It was detected that your web application uses HTTP protocol, but doesn't automatically redirect users to HTTPS.

CWE
CWE-16

CVSS2
AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None

Integrity Impact	None
Availability Impact	None

User Interaction	Required
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Impact

In some circumstances, it could be used for a man-in-the-middle (MitM) attack

http://213.125.163.178:1337/

Request

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/92.0.4512.0 Safari/537.36
Host: 213.125.163.178:1337
Connection: Keep-alive
```

Recommendation

It's recommended to implement best practices of HTTP Redirection into your web application. Consult web references for more information

References

HTTP Redirections
https://infosec.mozilla.org/guidelines/web_security#http-redirections

A06 Vulnerable and Outdated Components

Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts.

Cookies without HttpOnly flag set

One or more cookies don't have the HttpOnly flag set. When a cookie is set with the HttpOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies.

CWE

CWE-1004

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Impact

Cookies can be accessed by client-side scripts.

---

http://213.125.163.178:1337/ Verified

Cookies without HttpOnly flag set:

- http://213.125.163.178:1337/

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IjhIM1lNUEVvNGFLWDRBTmtYbDdieVE9PSIsInZhbHVlIjoiTEY2QURzak9jVGRMQVF
jMURVV0xwMGQwek5WVndQVytOeHBiY2VKUVpHTTdyY1BIb1lqU1c2dGJNMVplakFTeGFWWktoL29wQmJ2
NURVVnBGcHVqazhVbUV0T0tFakdNMm9PQy9yWk9PUVQvR1lUcEhTajJ6QkVHSkJzemRXM2wiLCJtYWMiO
iI4MGI5MzBlYWFmN2E3YjU0ODkyMzc1NWQ5MTIzODNkZDQzNDE3Y2FiOWUwODQ3NzYyOTIzMzExYzI5MD
YxNTZhIiwidGFnIjoiIn0%3D; expires=Fri, 10 Jun 2022 19:41:48 GMT; Max-Age=7200;
path=/; samesite=lax
```

- http://213.125.163.178:1337/index.php

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IkpmcXRjcWZrejJBWVhVOWZydi9Yc2c9PSIsInZhbHVlIjoiSTZCM09iYjVmMnFYeFZ
```

```
0Y1ljMWp0WWFWYTRKbng3T211b1kwSWRiT0RObDNZdlBiQ0RWVEtWS1N5ZnhaN3Jud0Q2UVJrckQwa2tD
WDBuUjJQOWxtdkwrVFdOdzd0cklFTDQrS1RiY0Jqam5tRk9rWUdZd0RhdCt6czg0RmVzY1oiLCJtYWMiO
iI1OWQwOTAwZTRlNzAwMDQ0MWEyMGI3YjgxY2EyOTc0M2MwNWZhZjg1NDFmNDg2OWY1ZWMzM2ZhOWYzZW
UwMTAxIiwidGFnIjoiIn0%3D; expires=Fri, 10 Jun 2022 19:48:59 GMT; Max-Age=7200;
path=/; samesite=lax
```

- http://213.125.163.178:1337/

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6InlVNU1IanJ0Wm5FUUpxMUxoTHc3c0E9PSIsInZhbHVlIjoicVhjK1Z3bnJCSTViK0E
relNJSit4QVk3TzNhSnlUT3lzNUl6ZEhpZUN2dlcreUVqK1NHT3YwS1BkNTRDaDFYbnpudm9tN3NKQmtD
U3VKVEV6QTNsWjBFT2FHQjdqWWl0WGNRKzFCL3BGZ2ZJcEVFVWFaNlQ0ZDl2TTNCR0JVWjUiLCJtYWMiO
iJiYjU5ZDQ2ZGIyMGNkOTIxMTFlNDUwOGVkOTI0ZTQyMzM5ODRkM2NlNmMzNzcwYjY5ZjhmY2M4YTY1YW
E5ZDFhIiwidGFnIjoiIn0%3D; expires=Fri, 10 Jun 2022 19:51:35 GMT; Max-Age=7200;
path=/; samesite=lax
```

- http://213.125.163.178:1337/index.php

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IjlzZDZHMmJFd1JnbU82MUMyYlBwdVE9PSIsInZhbHVlIjoieEY3UVNpWmR4WFRaVEt
zRVlyVkcySG1CcWpTM2JGZHJoTHpsLzcwQXdvdldCTzdkRjJVS0UvU2JpZDBiekk5MXV2Um9Nbi9LT1M4
OExRa3VtWForbkhWeUErQ2NyUDBGUnVoL3FSdjYySjBHUktoMHR5RUZCUkJxeGJMcFFJK1IiLCJtYWMiO
iJhMDgzN2FiMGUyYjFhNzQ0MGMzNDNmNWY2Zjg2NWY3ZTM1MzJiOTcwMWJjYmM2NDA4YTJkNGZjMzEzNG
FlYzIwIiwidGFnIjoiIn0%3D; expires=Fri, 10 Jun 2022 19:51:42 GMT; Max-Age=7200;
path=/; samesite=lax
```

Request

```
GET / HTTP/1.1
Referer: http://213.125.163.178:1337/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/92.0.4512.0 Safari/537.36
Host: 213.125.163.178:1337
Connection: Keep-alive
```

Recommendation

If possible, you should set the HttpOnly flag for these cookies.

Content Security Policy (CSP) not implemented

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.

Content Security Policy (CSP) can be implemented by adding a **Content-Security-Policy** header. The value of this header is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for the all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:

```
Content-Security-Policy:
default-src 'self';
script-src 'self' https://code.jquery.com;
```

It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP header is missing from the response. It's recommended to implement Content Security Policy (CSP) into your web application.

CWE

CWE-1021

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Impact

CSP can be used to prevent and/or mitigate attacks that involve content/code injection, such as cross-site scripting/XSS attacks, attacks that require embedding a malicious resource, attacks that involve malicious use of iframes, such as clickjacking attacks, and others.

http://213.125.163.178:1337/

Paths without CSP header:

- http://213.125.163.178:1337/
- http://213.125.163.178:1337/index.php

Request

```
GET / HTTP/1.1
Referer: http://213.125.163.178:1337/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/92.0.4512.0 Safari/537.36
Host: 213.125.163.178:1337
Connection: Keep-alive
```

Recommendation

It's recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the **Content-Security-Policy** HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page.

References

Content Security Policy (CSP)
https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP

Implementing Content Security Policy
https://hacks.mozilla.org/2016/02/implementing-content-security-policy/

A07 Identification and Authentication Failures

Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities.

Unencrypted connection

This scan target was connected to over an unencrypted connection. A potential attacker can intercept and modify data sent and received from this site.

CWE
CWE-319

CVSS2 **CVSS3**

AV:N/AC:M/Au:N/C:P/I:P/A:N

Access Vector	Network
Access Complexity	Medium
Authentication	None
Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	None

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N

Base Score	5.4
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	Low
Integrity Impact	Low
Availability Impact	None

Impact

Possible information disclosure.

---

http://213.125.163.178:1337/ Verified

Request

```
GET / HTTP/1.1
Referer: http://213.125.163.178:1337/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/92.0.4512.0 Safari/537.36
Host: 213.125.163.178:1337
Connection: Keep-alive
```

Recommendation

The site should send and receive data over a secure (HTTPS) connection.

A08 Software and Data Integrity Failures

Software and data integrity failures relate to code and infrastructure that does not protect against integrity violations. An example of this is where an application relies upon plugins, libraries, or modules from untrusted sources, repositories, and content delivery networks (CDNs). An insecure CI/CD pipeline can introduce the potential for unauthorized access, malicious code, or system compromise. Lastly, many applications now include auto-update functionality, where updates are downloaded without sufficient integrity verification and applied to the previously trusted application. Attackers could potentially upload their own updates to be distributed and run on all installations. Another example is where objects or data are encoded or serialized into a structure that an attacker can see and modify is vulnerable to insecure deserialization.

No alerts in this category

A09 Security Logging and Monitoring Failures

Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systesm, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

No alerts in this category

A10 Server-Side Request Forgery

SSRF flaws occur whenever a web application is fetching a remote resource without validating the user-supplied URL. It allows an attacker to coerce the application to send a crafted request to an unexpected destination, even when protected by a firewall, VPN, or another type of network access control list (ACL).

No alerts in this category

Coverage

- http://213.125.163.178:1337
  - Inputs
    - GET iv, value, mac, tag
  - index.php
    - Inputs
      - GET iv, value, mac, tag
  - robots.txt
    - Inputs
      - GET iv, value, mac, tag