The Assignment on Information Security (UE19CS347)

SRN	:	PES2UG19CS312
Name	:	Suhan B Revankar
Date	:	06/05/2022
Section	:	G

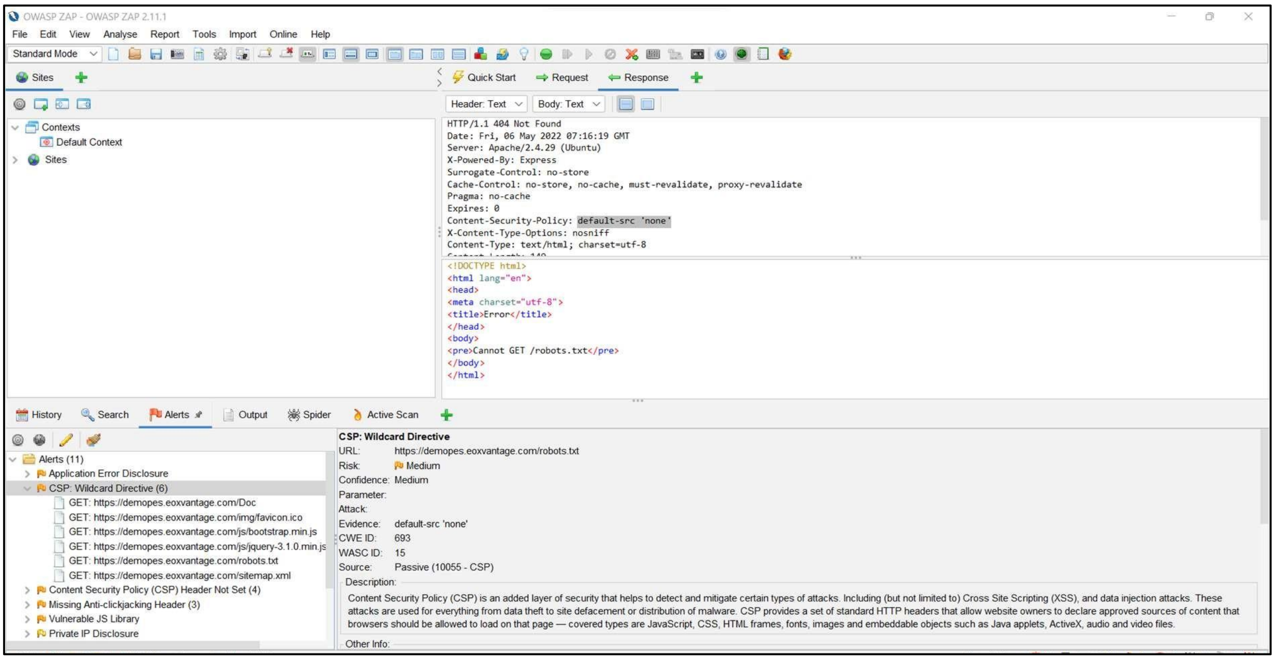
Pentest report on:

Pen testing the given websites using ZAP (Zed attack Proxy) tool. Thescreenshots for the same have been attached.

The three websites are primarily vulnerable to XSS attack as seen from the CSP header not set alerts. Content Security policy is a countermeasure to only allow trusted sources and JavaScript DOMs to be called and executed. The absence of the same makes all the three sites vulnerable.

Apart from XSS, the websites also contain anti click jacking and vulnerable JavaScript libraries which can be exploited.

1. https://demopes.eoxvantage.com/



```
HTTP/1.1 404 Not Found
Date: Fri, 06 May 2022 07:16:19 GMT
Server: Apache/2.4.29 (Ubuntu)
X-Powered-By: Express
Surrogate-Control: no-store
Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate
Pragma: no-cache
Expires: 0
Content-Security-Policy: default-src 'none'
X-Content-Type-Options: nosniff
Content-Type: text/html; charset=utf-8
```

```
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8">
<title>Error</title>
</head>
<body>
<pre>Cannot GET /robots.txt</pre>
</body>
</html>
```

Alerts (11)
- Application Error Disclosure
- CSP: Wildcard Directive (6)
  - GET: https://demopes.eoxvantage.com/Doc
  - GET: https://demopes.eoxvantage.com/img/favicon.ico
  - GET: https://demopes.eoxvantage.com/js/bootstrap.min.js
  - GET: https://demopes.eoxvantage.com/js/jquery-3.1.0.min.js
  - GET: https://demopes.eoxvantage.com/robots.txt
  - GET: https://demopes.eoxvantage.com/sitemap.xml
- Content Security Policy (CSP) Header Not Set (4)
- Missing Anti-clickjacking Header (3)
- Vulnerable JS Library
- Private IP Disclosure

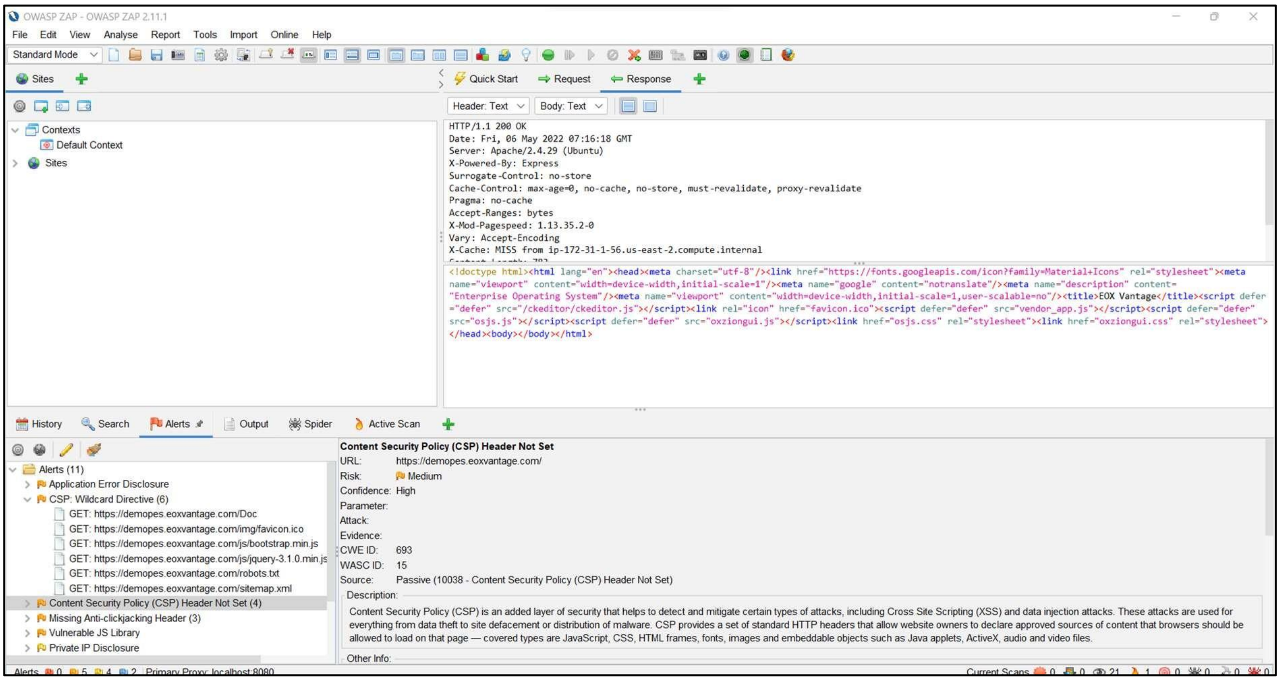
CSP: Wildcard Directive

URL:	https://demopes.eoxvantage.com/robots.txt
Risk:	Medium
Confidence:	Medium
Parameter:	
Attack:	
Evidence:	default-src 'none'
CWE ID:	693
WASC ID:	15
Source:	Passive (10055 - CSP)

Description:

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) Cross Site Scripting (XSS), and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

Other Info:



```
HTTP/1.1 200 OK
Date: Fri, 06 May 2022 07:16:18 GMT
Server: Apache/2.4.29 (Ubuntu)
X-Powered-By: Express
Surrogate-Control: no-store
Cache-Control: max-age=0, no-cache, no-store, must-revalidate, proxy-revalidate
Pragma: no-cache
Accept-Ranges: bytes
X-Mod-Pagespeed: 1.13.35.2-0
Vary: Accept-Encoding
X-Cache: MISS from ip-172-31-1-56.us-east-2.compute.internal
```

```
<!doctype html><html lang="en"><head><meta charset="utf-8"/><link href="https://fonts.googleapis.com/icon?family=Material+Icons" rel="stylesheet"><meta
name="viewport" content="width=device-width,initial-scale=1"/><meta name="google" content="notranslate"/><meta name="description" content=
"Enterprise Operating System"/><meta name="viewport" content="width=device-width,initial-scale=1,user-scalable=no"/><title>EOX Vantage</title><script defer
="defer" src="/ckeditor/ckeditor.js"></script><link rel="icon" href="favicon.ico"><script defer="defer" src="vendor_app.js"></script><script defer="defer"
src="osjs.js"></script><script defer="defer" src="oxziongui.js"></script><link href="osjs.css" rel="stylesheet"><link href="oxziongui.css" rel="stylesheet">
</head><body></body></html>
```

Alerts (11)
- Application Error Disclosure
- CSP: Wildcard Directive (6)
  - GET: https://demopes.eoxvantage.com/Doc
  - GET: https://demopes.eoxvantage.com/img/favicon.ico
  - GET: https://demopes.eoxvantage.com/js/bootstrap.min.js
  - GET: https://demopes.eoxvantage.com/js/jquery-3.1.0.min.js
  - GET: https://demopes.eoxvantage.com/robots.txt
  - GET: https://demopes.eoxvantage.com/sitemap.xml
- Content Security Policy (CSP) Header Not Set (4)
- Missing Anti-clickjacking Header (3)
- Vulnerable JS Library
- Private IP Disclosure

Content Security Policy (CSP) Header Not Set

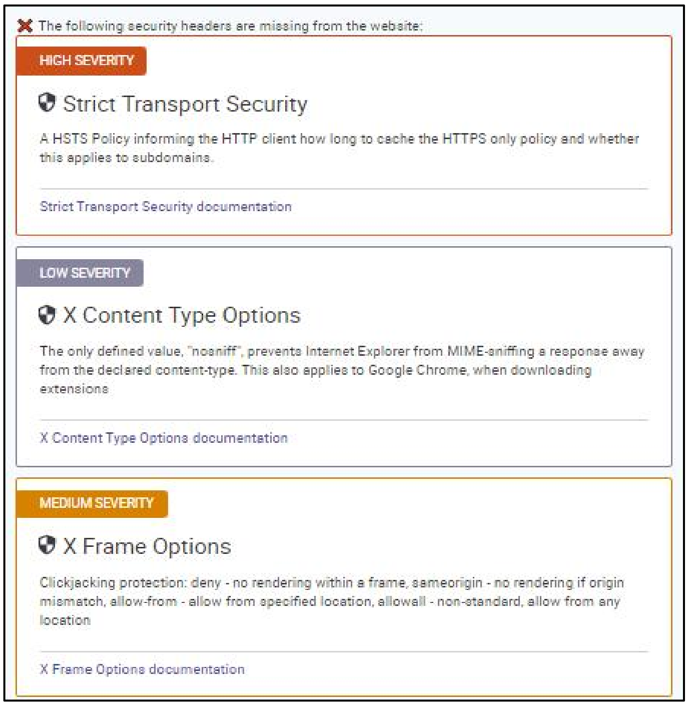
URL:	https://demopes.eoxvantage.com/
Risk:	Medium
Confidence:	High
Parameter:	
Attack:	
Evidence:	
CWE ID:	693
WASC ID:	15
Source:	Passive (10038 - Content Security Policy (CSP) Header Not Set)

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 or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

Other Info:

Alerts 0 5 4 2 Primary Proxy: localhost:8080 Current Scans 0 0 21 1 0 0 0 0



✖ The following security headers are missing from the website:

HIGH SEVERITY

Strict Transport Security

A HSTS Policy informing the HTTP client how long to cache the HTTPS only policy and whether this applies to subdomains.

Strict Transport Security documentation

LOW SEVERITY

X Content Type Options

The only defined value, "nosniff", prevents Internet Explorer from MIME-sniffing a response away from the declared content-type. This also applies to Google Chrome, when downloading extensions

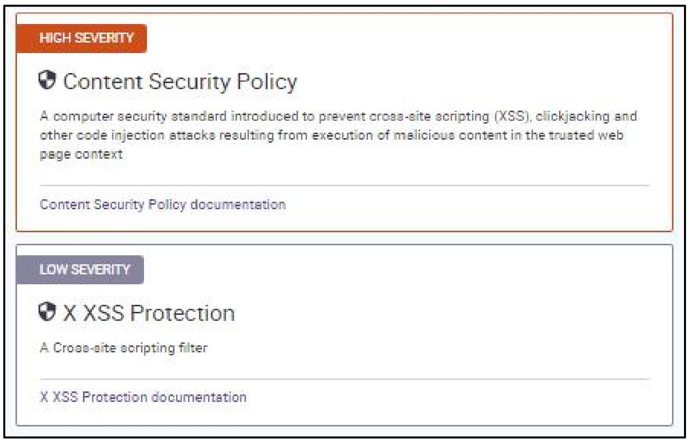
X Content Type Options documentation

MEDIUM SEVERITY

X Frame Options

Clickjacking protection: deny - no rendering within a frame, sameorigin - no rendering if origin mismatch, allow-from - allow from specified location, allowall - non-standard, allow from any location

X Frame Options documentation



HIGH SEVERITY

Content Security Policy

A computer security standard introduced to prevent cross-site scripting (XSS), clickjacking and other code injection attacks resulting from execution of malicious content in the trusted web page context

Content Security Policy documentation

LOW SEVERITY

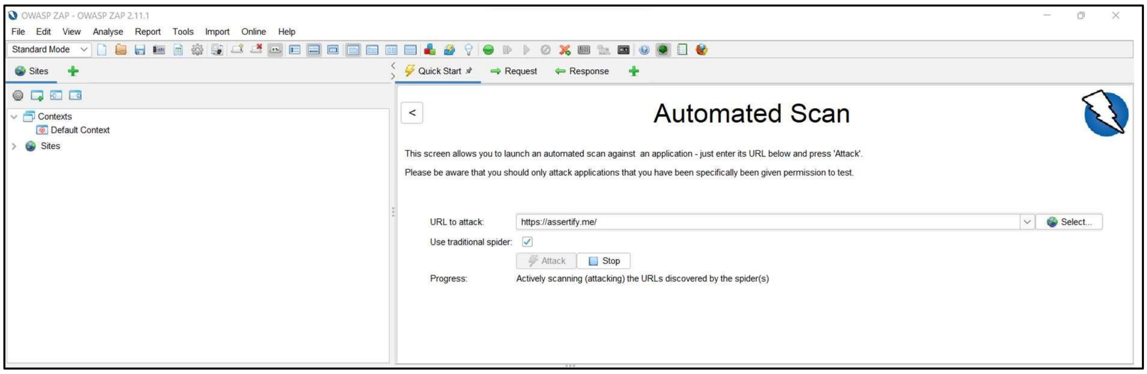
X XSS Protection

A Cross-site scripting filter

X XSS Protection documentation

It's noticed that the website is prone to attacks by cross site scripting. For, the header that thwarts this attack's missing from it. The absence of HSTS policy on the website leads any attacker to abate this website to HTTP. Hopefully, the site is safe from attacks by CSRF and SQL injection.

2. https://frizzleweather.com/



OWASP ZAP - OWASP ZAP 2.11.1
File Edit View Analyse Report Tools Import Online Help
Standard Mode
Sites
Contexts
Default Context
Sites
Quick Start
Request
Response

Automated Scan

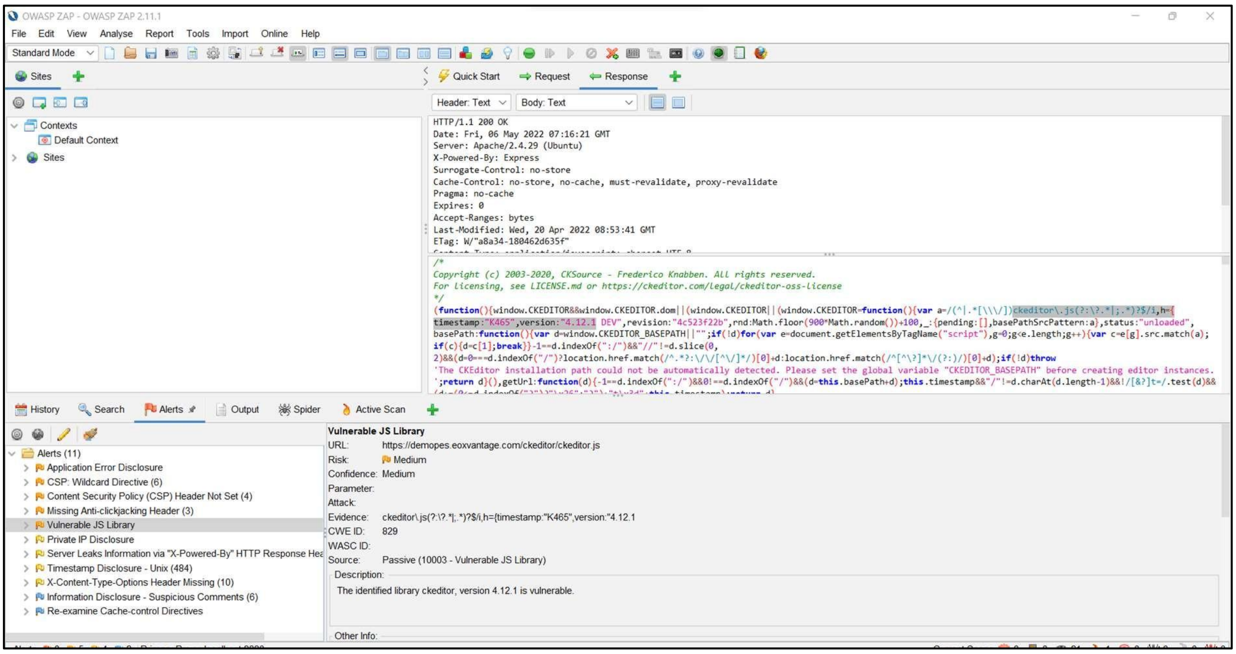
This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

URL to attack: https://assertify.me/

Use traditional spider: ☑

Progress: Actively scanning (attacking) the URLs discovered by the spider(s)



```
HTTP/1.1 200 OK
Date: Fri, 06 May 2022 07:16:21 GMT
Server: Apache/2.4.29 (Ubuntu)
X-Powered-By: Express
Surrogate-Control: no-store
Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate
Pragma: no-cache
Expires: 0
Accept-Ranges: bytes
Last-Modified: Wed, 20 Apr 2022 08:53:41 GMT
ETag: W/"a8a34-180462d635f"
```

```
/*
Copyright (c) 2003-2020, CKSource - Frederico Knabben. All rights reserved.
For licensing, see LICENSE.md or https://ckeditor.com/legal/ckeditor-oss-license
*/
(function(){window.CKEDITOR&&window.CKEDITOR.dom||(window.CKEDITOR||(window.CKEDITOR=function(){var a=/(^|.*[\\\/])ckeditor\.js(?:\?.*|;.*)?$/i,h={
timestamp:"K465",version:"4.12.1 DEV",revision:"4c523f22b",rnd:Math.floor(900*Math.random())+100,_:{pending:[],basePathSrcPattern:a},status:"unloaded",
basePath:function(){var d=window.CKEDITOR_BASEPATH||"";if(!d)for(var e=document.getElementsByTagName("script"),g=0;g<e.length;g++){var c=e[g].src.match(a);
if(c){d=c[1];break}}-1==d.indexOf(":/")&&"//"!=d.slice(0,
2)&&(d=0===d.indexOf("/")?location.href.match(/^.*?:\/\/[^\/]*/)[0]+d:location.href.match(/^[^\?]*\/(?:)/)[0]+d);if(!d)throw
'The CKEditor installation path could not be automatically detected. Please set the global variable "CKEDITOR_BASEPATH" before creating editor instances.
';return d}(),getUrl:function(d){-1==d.indexOf(":/")&&0!==d.indexOf("/")&&(d=this.basePath+d);this.timestamp&&"/"!=d.charAt(d.length-1)&&!/[&?]t=/.test(d)&&
```

- Alerts (11)
  - Application Error Disclosure
  - CSP: Wildcard Directive (6)
  - Content Security Policy (CSP) Header Not Set (4)
  - Missing Anti-clickjacking Header (3)
  - Vulnerable JS Library
  - Private IP Disclosure
  - Server Leaks Information via "X-Powered-By" HTTP Response Hea
  - Timestamp Disclosure - Unix (484)
  - X-Content-Type-Options Header Missing (10)
  - Information Disclosure - Suspicious Comments (6)
  - Re-examine Cache-control Directives

Vulnerable JS Library

URL: https://demopes.eoxvantage.com/ckeditor/ckeditor.js

Risk: Medium

Confidence: Medium

Parameter:

Attack:

Evidence: ckeditor\.js(?:\?.*|;.*)?$/i,h={timestamp:"K465",version:"4.12.1

CWE ID: 829

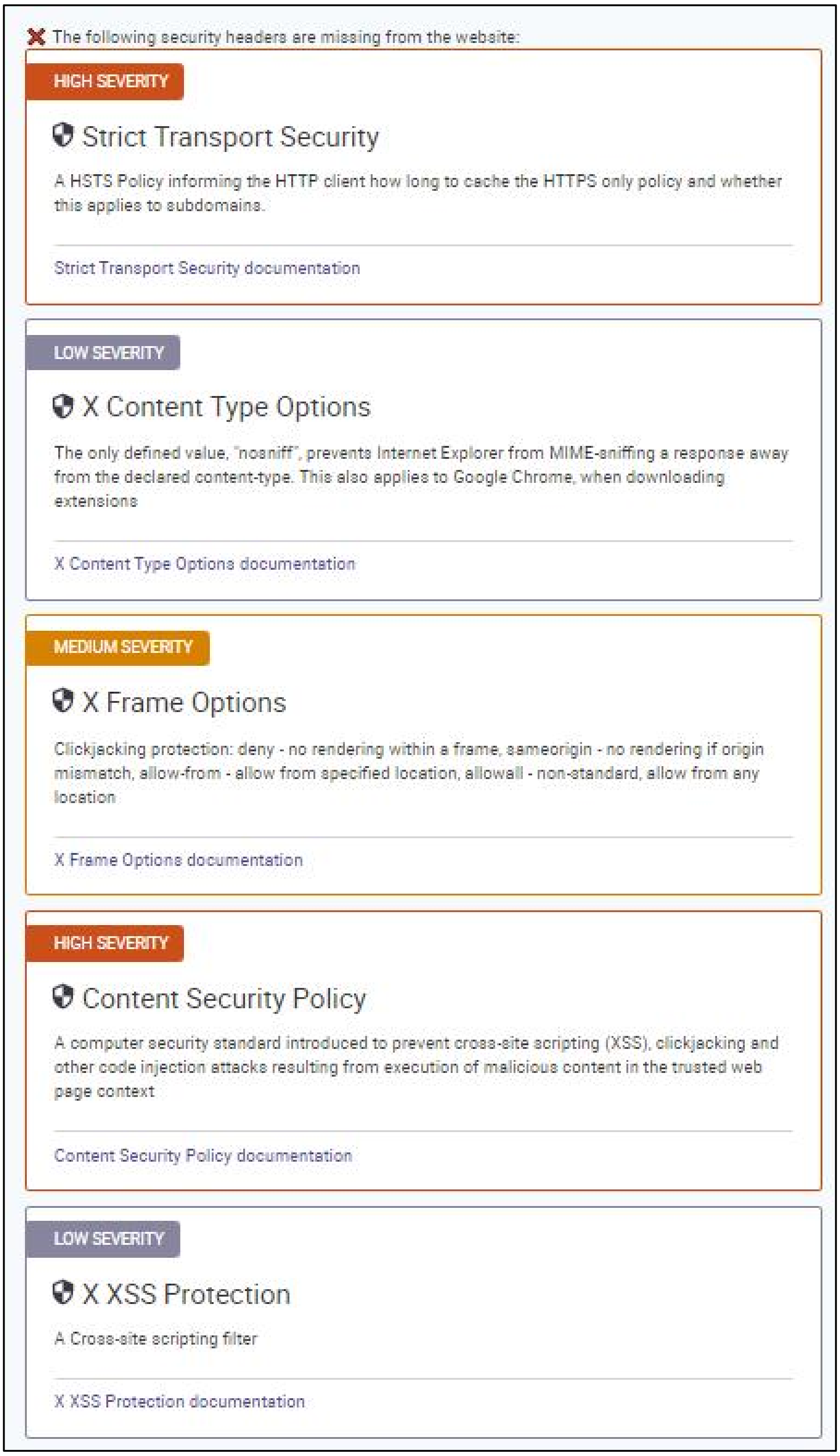
WASC ID:

Source: Passive (10003 - Vulnerable JS Library)

Description:

The identified library ckeditor, version 4.12.1 is vulnerable.

Other Info:



✖ The following security headers are missing from the website:

HIGH SEVERITY

Strict Transport Security

A HSTS Policy informing the HTTP client how long to cache the HTTPS only policy and whether this applies to subdomains.

Strict Transport Security documentation

LOW SEVERITY

X Content Type Options

The only defined value, "nosniff", prevents Internet Explorer from MIME-sniffing a response away from the declared content-type. This also applies to Google Chrome, when downloading extensions

X Content Type Options documentation

MEDIUM SEVERITY

X Frame Options

Clickjacking protection: deny - no rendering within a frame, sameorigin - no rendering if origin mismatch, allow-from - allow from specified location, allowall - non-standard, allow from any location

X Frame Options documentation

HIGH SEVERITY

Content Security Policy

A computer security standard introduced to prevent cross-site scripting (XSS), clickjacking and other code injection attacks resulting from execution of malicious content in the trusted web page context

Content Security Policy documentation

LOW SEVERITY

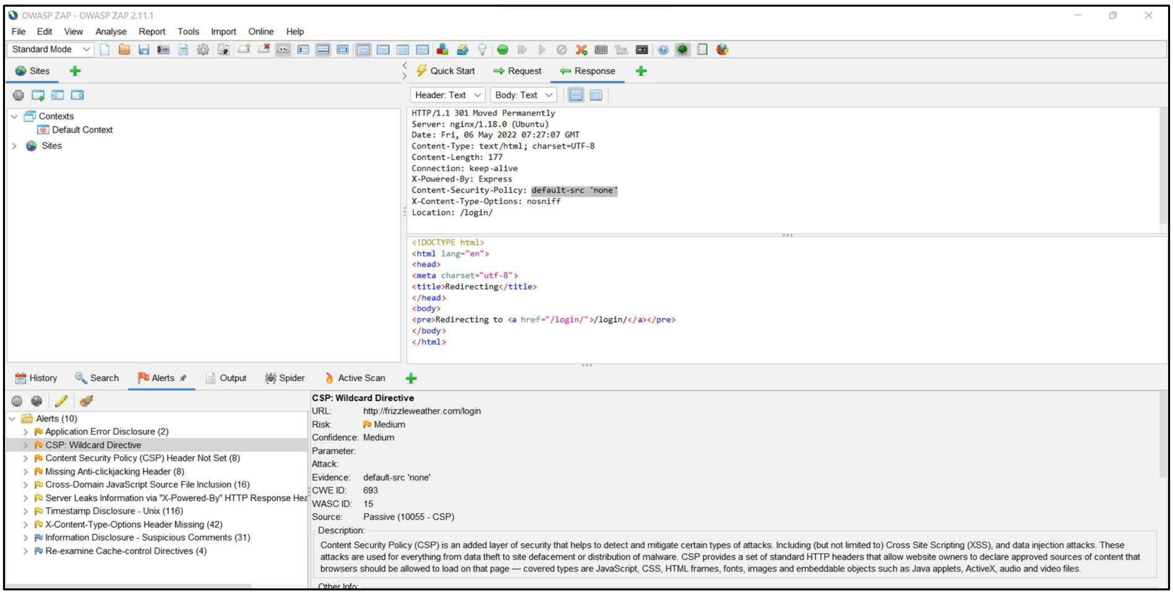
X XSS Protection

A Cross-site scripting filter

X XSS Protection documentation

As observed in the previous website, the absence of a couple of headers poses hazardous harm to this website, with XSS taking the lion's share.

3. https://assertify.me



```
HTTP/1.1 301 Moved Permanently
Server: nginx/1.18.0 (Ubuntu)
Date: Fri, 06 May 2022 07:27:07 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 177
Connection: keep-alive
X-Powered-By: Express
Content-Security-Policy: default-src 'none'
X-Content-Type-Options: nosniff
Location: /login/
```

```
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8">
<title>Redirecting</title>
</head>
<body>
<pre>Redirecting to <a href="/login/">/login/</a></pre>
</body>
</html>
```

- Alerts (10)
  - Application Error Disclosure (2)
  - CSP: Wildcard Directive
  - Content Security Policy (CSP) Header Not Set (8)
  - Missing Anti-clickjacking Header (8)
  - Cross-Domain JavaScript Source File Inclusion (16)
  - Server Leaks Information via "X-Powered-By" HTTP Response Hea
  - Timestamp Disclosure - Unix (116)
  - X-Content-Type-Options Header Missing (42)
  - Information Disclosure - Suspicious Comments (31)
  - Re-examine Cache-control Directives (4)

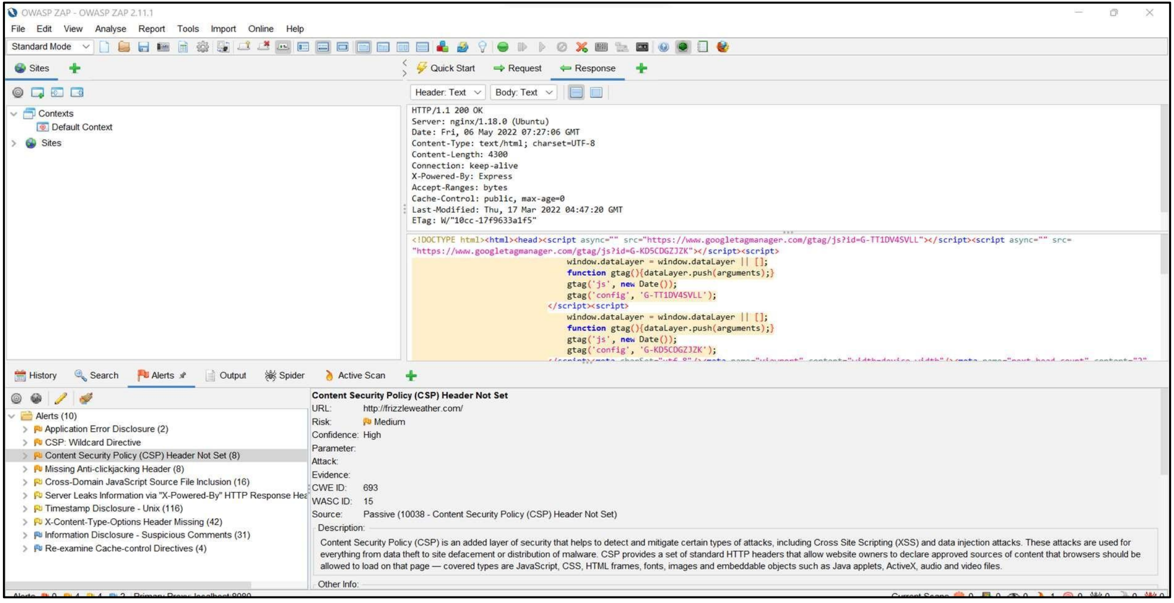
CSP: Wildcard Directive

URL: http://frizzleweather.com/login
Risk: Medium
Confidence: Medium
Parameter:
Attack:
Evidence: default-src 'none'
CWE ID: 693
WASC ID: 15
Source: Passive (10055 - CSP)

Description:

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) Cross Site Scripting (XSS), and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

Other Info:



```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Fri, 06 May 2022 07:27:06 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 4300
Connection: keep-alive
X-Powered-By: Express
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Thu, 17 Mar 2022 04:47:20 GMT
ETag: W/"10cc-17f9633a1f5"
```

```
<!DOCTYPE html><html><head><script async="" src="https://www.googletagmanager.com/gtag/js?id=G-TT1DV4SVLL"></script><script async="" src=
"https://www.googletagmanager.com/gtag/js?id=G-KD5CDGZJZK"></script><script>
                                window.dataLayer = window.dataLayer || [];
                                function gtag(){dataLayer.push(arguments);}
                                gtag('js', new Date());
                                gtag('config', 'G-TT1DV4SVLL');
                            </script><script>
                                window.dataLayer = window.dataLayer || [];
                                function gtag(){dataLayer.push(arguments);}
                                gtag('js', new Date());
                                gtag('config', 'G-KD5CDGZJZK');
```

- Alerts (10)
  - Application Error Disclosure (2)
  - CSP: Wildcard Directive
  - Content Security Policy (CSP) Header Not Set (8)
  - Missing Anti-clickjacking Header (8)
  - Cross-Domain JavaScript Source File Inclusion (16)
  - Server Leaks Information via "X-Powered-By" HTTP Response Hea
  - Timestamp Disclosure - Unix (116)
  - X-Content-Type-Options Header Missing (42)
  - Information Disclosure - Suspicious Comments (31)
  - Re-examine Cache-control Directives (4)

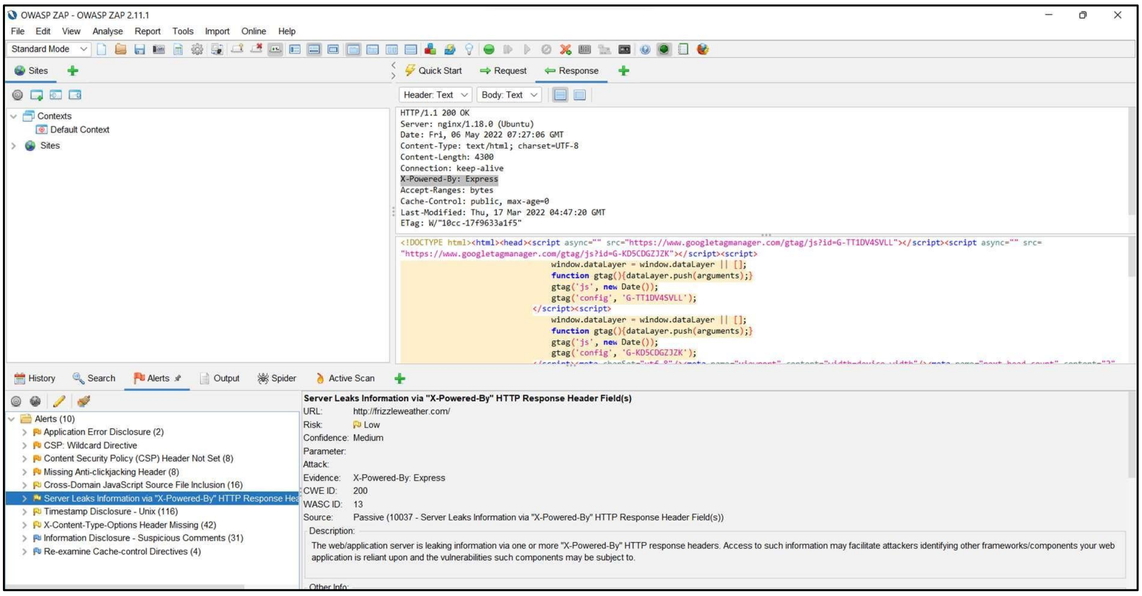
Content Security Policy (CSP) Header Not Set

URL: http://frizzleweather.com/
Risk: Medium
Confidence: High
Parameter:
Attack:
Evidence:
CWE ID: 693
WASC ID: 15
Source: Passive (10038 - Content Security Policy (CSP) Header Not Set)

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 or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

Other Info:



```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Fri, 06 May 2022 07:27:06 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 4300
Connection: keep-alive
X-Powered-By: Express
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Thu, 17 Mar 2022 04:47:20 GMT
ETag: W/"10cc-17f9633a1f5"
```

```
<!DOCTYPE html><html><head><script async="" src="https://www.googletagmanager.com/gtag/js?id=G-TT1DV4SVLL"></script><script async="" src=
"https://www.googletagmanager.com/gtag/js?id=G-KD5CDGZJZK"></script><script>
                                        window.dataLayer = window.dataLayer || [];
                                        function gtag(){dataLayer.push(arguments);}
                                        gtag('js', new Date());
                                        gtag('config', 'G-TT1DV4SVLL');
                                    </script><script>
                                        window.dataLayer = window.dataLayer || [];
                                        function gtag(){dataLayer.push(arguments);}
                                        gtag('js', new Date());
                                        gtag('config', 'G-KD5CDGZJZK');
```

Alerts (10)
- Application Error Disclosure (2)
- CSP: Wildcard Directive
- Content Security Policy (CSP) Header Not Set (8)
- Missing Anti-clickjacking Header (8)
- Cross-Domain JavaScript Source File Inclusion (16)
- Server Leaks Information via "X-Powered-By" HTTP Response Hea
- Timestamp Disclosure - Unix (116)
- X-Content-Type-Options Header Missing (42)
- Information Disclosure - Suspicious Comments (31)
- Re-examine Cache-control Directives (4)

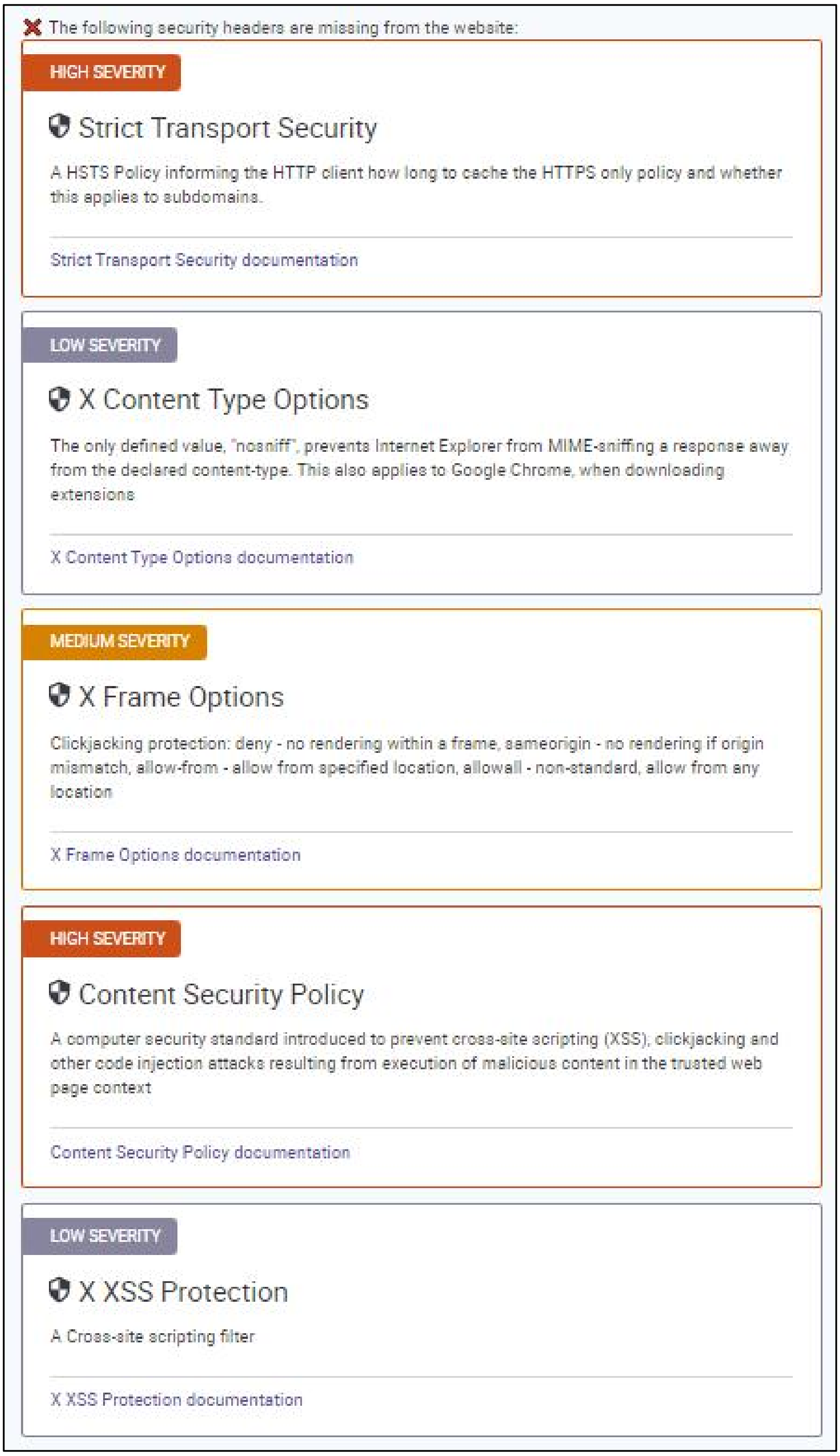
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

URL:	http://frizzleweather.com/
Risk:	Low
Confidence:	Medium
Parameter:	
Attack:	
Evidence:	X-Powered-By: Express
CWE ID:	200
WASC ID:	13
Source:	Passive (10037 - Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s))

Description:

The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.

Other Info:



✖ The following security headers are missing from the website:

HIGH SEVERITY

Strict Transport Security

A HSTS Policy informing the HTTP client how long to cache the HTTPS only policy and whether this applies to subdomains.

Strict Transport Security documentation

LOW SEVERITY

X Content Type Options

The only defined value, "nosniff", prevents Internet Explorer from MIME-sniffing a response away from the declared content-type. This also applies to Google Chrome, when downloading extensions

X Content Type Options documentation

MEDIUM SEVERITY

X Frame Options

Clickjacking protection: deny - no rendering within a frame, sameorigin - no rendering if origin mismatch, allow-from - allow from specified location, allowall - non-standard, allow from any location

X Frame Options documentation

HIGH SEVERITY

Content Security Policy

A computer security standard introduced to prevent cross-site scripting (XSS), clickjacking and other code injection attacks resulting from execution of malicious content in the trusted web page context

Content Security Policy documentation

LOW SEVERITY

X XSS Protection

A Cross-site scripting filter

X XSS Protection documentation

Once again, this website, too, is prone to XSS.