

Security Scan of web app

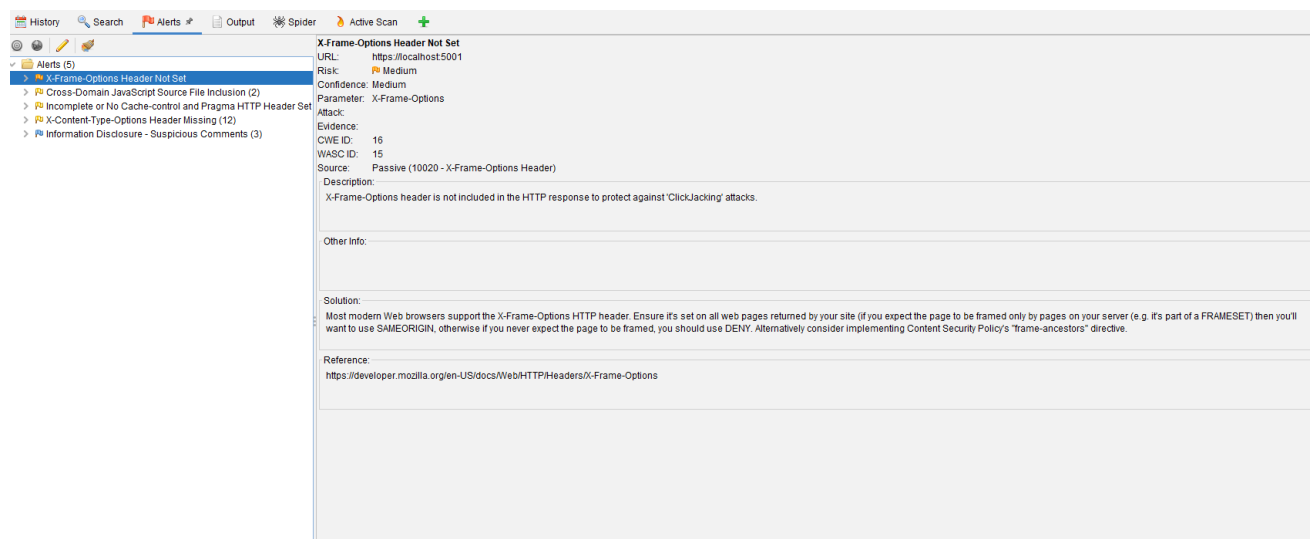
OWASP Zed Attack Proxy

Employee Connectivity Tracker

X00149863 Pavel Ivanov

Results:

X-Frame-Options Header not set:



The screenshot shows the OWASP ZAP Alerts window. The left sidebar lists several alerts, with 'X-Frame-Options Header Not Set' selected. The main panel displays the details for this alert:

- Alerts (5)**
 - X-Frame-Options Header Not Set
 - Cross-Domain JavaScript Source File Inclusion (2)
 - Incomplete or No Cache-control and Pragma HTTP Header Set
 - X-Content-Type-Options Header Missing (12)
 - Information Disclosure - Suspicious Comments (3)

X-Frame-Options Header Not Set

URL: <https://localhost5001>

Risk: **Medium**

Confidence: Medium

Parameter: X-Frame-Options

Attack:

Evidence:

CWE ID: 16

WASC ID: 15

Source: Passive (10020 - X-Frame-Options Header)

Description:

X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.

Other Info:

Solution:

Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.

Reference:

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options>

Solution:

<https://dotnetcoretutorials.com/2017/01/08/set-x-frame-options-asp-net-core/>

Cross-Domain JavaScript source file inclusion:

The screenshot displays a web page source code in the top pane, with a red box highlighting a script tag: `<script src='https://www.gstatic.com/charts/loader.js'></script>`. The bottom pane shows an alert titled "Cross-Domain JavaScript Source File Inclusion".

Alert Details:

- URL: `https://localhost:5001`
- Risk: Low
- Confidence: Medium
- Parameter: `https://kit.fontawesome.com/a076d05399.js`
- Attack: `<script src='https://www.gstatic.com/charts/loader.js'></script>`
- Evidence: `<script type='text/javascript' src='https://www.gstatic.com/charts/loader.js'></script>`
- WASC ID: 829
- Source: Passive (10017 - Cross-Domain JavaScript Source File Inclusion)
- Description: The page includes one or more script files from a third-party domain.
- Other Info:
- Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
- Reference:

These are not an issue as the included files are from trusted sources.

Incomplete or No Cache-control and Pragma HTTP Header set:

The screenshot displays an alert titled "Incomplete or No Cache-control and Pragma HTTP Header Set".

Alert Details:

- URL: `https://localhost:5001`
- Risk: Low
- Confidence: Medium
- Parameter: Cache-Control
- Attack:
- Evidence: 200 OK
- WASC ID: 525
- CWE ID: 13
- Source: Passive (10015 - Incomplete or No Cache-control and Pragma HTTP Header Set)
- Description: The cache-control and pragma HTTP header have not been set properly or are missing allowing the browser and proxies to cache content.
- Other Info:
- Solution: Whenever possible ensure the cache-control HTTP header is set with no-cache, no-store, must-revalidate, and that the pragma HTTP header is set with no-cache.
- Reference: https://cheatsheetsseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching

TODO: Find out how this can be resolved.

X-Content-Type-Options Header missing

The screenshot shows the Burp Suite interface with the 'Alerts' tab selected. A list of alerts is on the left, and the details of the selected alert are on the right. The alert is titled 'X-Content-Type-Options Header Missing' and is categorized under 'Information Disclosure - Suspicious Comments (3)'. The details pane shows the following information:

- URL:** https://localhost5001
- Risk:** Low
- Confidence:** Medium
- Parameter:** X-Content-Type-Options
- Attack:**
- Evidence:**
 - CWE ID: 16
 - WASC ID: 15
 - Source: Passive (10021 - X-Content-Type-Options Header Missing)
- Description:**

The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
- Other Info:**

This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
- Solution:**

Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.
- Reference:**
 - http://msdn.microsoft.com/en-us/library/ie/gg522941%28v=vs.85%29.aspx
 - https://owasp.org/www-community/Security-Headers

Solution:

<https://dotnetcoretutorials.com/2017/01/20/set-x-content-type-options-asp-net-core/>

Suspicious Comments

The screenshot shows the Burp Suite interface with the 'Alerts' tab selected. A list of alerts is on the left, and the details of the selected alert are on the right. The alert is titled 'Information Disclosure - Suspicious Comments' and is categorized under 'Information Disclosure - Suspicious Comments (3)'. The details pane shows the following information:

- URL:** https://localhost5001/scripts/script.js
- Risk:** Informational
- Confidence:** Low
- Parameter:**
- Attack:**
- Evidence:** from
- CWE ID:** 200
- WASC ID:** 13
- Source:** Passive (10027 - Information Disclosure - Suspicious Comments)
- Description:**

The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
- Other Info:**

The following pattern was used: 'bFROM/b and was detected in the element starting with: 'if Code adapted from https://developers.google.com/chart/interactive/docs/gallery', see evidence field for the suspicious comments/snippet.
- Solution:**

Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
- Reference:**

None of the comments are posing an issue.