

Site: http://172.16.39.77:8080

Generated on Tue, 30 Sept 2025 18:17:19

ZAP Version: 2.16.1

ZAP by Checkmarx

Summary of Alerts

| Risk Level | Number of Alerts |
|---------------|------------------|
| High | 0 |
| Medium | 2 |
| Low | 2 |
| Informational | 0 |

Alerts

| Name | Risk Level | Number of Instances |
|--|------------|------------------------|
| Content Security Policy (CSP) Header Not Set | Medium | 3 |
| Missing Anti-clickjacking Header | Medium | 1 |
| Server Leaks Version Information via "Server" HTTP Response Header Field | Low | 3 |
| X-Content-Type-Options Header Missing | Low | 1 |

Alert Detail

| Medium | 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. |
| URL | http://172.16.39.77:8080 |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| URL | http://172.16.39.77:8080/robots.txt |
| Method | GET |

| Attack Evidence Other Info URL Method GET Attack Evidence Other Info Instances 3 Solution Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header. https://developer.mozilla.org/en-US/docs/Web/Security/CSP_Altroducing_Content_Security-Policy_Integrates_Acceptaints_Vidence_Acceptaints_ | | |
|--|---|--|
| Other Info URL http://172.16.39,77-8080/sitemap.xml Method GET Attack Evidence Other Info Instances 3 Solution Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header. https://developer.mozilla.org/en-US/docs/Web/Security/CSP //Introducing.Content.Security.Policy https://developer.mozilla.org/en-US/docs/Web/Security/CSP //Introducing.Content.Security.Policy https://deathselselsenses.owasp.org/cheatshelsets/Content.Security.Policy https://deathselselsenses.owasp.org/cheatshelsets/Content.Security.Policy.https://deathselses.org.https://deathselses.org.https://deathselses.org.https://deathselses.org.https://deathselses.org.https://deathselses.org.https://centent-security-policy.com/ CWE Id 693 WASC Id 15 Plugin Id 10038 Medium Missing Anti-click/jacking Header Description The response does not protect against 'Click/Jacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options. URL http://172.16.39,77.8080 Method GET Attack Evidence Other Info Instances 1 Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app. Solution 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 CWE Id 1021 WASC Id 15 Plugin Id 10020 | Attack | |
| Info URL Method GET Attack Evidence Other Info Instances 3 Solution Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header. Attack Evidence Other Info Instances 3 Solution Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header. Attack Evidence Attack Evidence Attack Attack Evidence Missing Anti-clickjacking Header The response does not protect against ClickJacking' attacks. It should include either Content-Security-Policy with frame-ancestors' directive or X-Frame-Options. URL http://172.16.39.77.8080 Method GET Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app. Solution 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 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 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 is 'Irane-ancestors' directive' content-in the proper in 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 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 is 'Irane-ancestors' directive. | Evidence | |
| Method GET Attack Evidence Other Info Instances 3 Solution Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header. Attos://developer.mozilla.org/en_US/docs/Web/Security/CSP //Introducing_Content_Security_Policy https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy https://www.wa.org/TR/CSP/ https://www.wa.org/TR/CSP/ https://www.wa.org/TR/CSP/ https://www.wa.org/TR/CSP/ https://web.see/articles/csp https://content-security-policy.com/ CWE Id 693 WASC Id 15 Plugin Id 10038 Medium Missing Anti-click/jacking Header Description The response does not protect against 'Click/Jacking' attacks. It should include either Content-Security-Policy with frame-ancestors' directive or X-Frame-Options. URL http://172.16.39.77.8080 Method GET Attack Evidence Other Info Instances 1 Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers, Ensure one of them is set on all web pages returned by your stie/apap. Solution 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 by Delory's 'frame-ancestors' directive' policy's 'frame-ancestors' directive' ponsider implementing Content Security Policy's 'frame-ancestors' directive' you sherwise if you never expect the page to be framed by SAMEORIGIN, otherwise if you never expect the page to be framed by you shelf-page. Reference https://developer.mozilla.org/an-US/docs/Web/HTTP/Headers/X-Frame-Options CWE Id UNASC Id 15 Plugin Id 10020 | | |
| Attack Evidence Other Info Instances 3 Solution Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header. https://developer.mozilla.or/glen-US/docs/Web/Security/CSP //Introducing_Content_Security_Policy https://www.w.a.org/TR/CSP/ //Introducing_Content_Security_Policy https://www.w.a.org/TR/CSP/ | URL | http://172.16.39.77:8080/sitemap.xml |
| Evidence Other Info Instances 3 Solution Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header. https://developer.moz/lla.org/en-US/docs/Web/Security/CSP // Introducing_Content_Security_Policy // Introducing_Content_Security_Policy // Introducing_Content_Security_Policy // Introducing_Content_Security_Policy // Introducing_Content_Security_Policy // Introducing_Content_Security_Policy // Introducing_Content_Security_Policy_Cheatsheets/Content_Security_Policy_Cheat_Sheet.html // Introducing_Content_Security_Policy_Content_Security_Content_Security_Content_Security_Content_Secu | Method | GET |
| Other Info | Attack | |
| Info Instances 3 Solution Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header. https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy_Introducing_Content_Security_Introducing_Content_Security_Introducing_C | Evidence | |
| Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header. https://developer.mozilla.org/en-US/docs/Web/Security/CSP // Introducing Content Security Policy https://cheatsheetseries.owasp.org/cheatsheets/Content Security Policy https://www.wa.org/TR/CSP/ https://content-Security-policy https://content-Security-policy with frame-ancestors' directive or X-Frame-Options Https://content-Security-policy with frame-ancestors' directive or X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app. Solution 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 DEMY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive. Reference https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options CWE Id 1021 WASC Id 15 | | |
| Content-Security-Policy header. https://developer.mozilla.org/en-US/docs/Web/Security/CSP //introducing_Content_Security_Policy https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html Reference https://www.w3.org/TR/CSP/ https://wab.cg.ithub.io/webappsec-csp/ https://wab.cg.ithub.io/webappsec-csp/ https://wab.cg.ithub.io/webappsec-csp/ https://content-security-policy.com/ CWE Id 693 WASC Id 15 Plugin Id 10038 Medium Missing Anti-click/jacking Header Description The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options. URL http://172.16.39.77:8080 Method GET Attack Evidence Other Info Instances 1 Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app. Solution 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 only by Deader implementing Content Security Policy's 'frame-ancestors' directive. Reference https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options CWE Id 1021 WASC Id 15 Plugin Id 10020 | Instances | 3 |
| Introducing_Content_Security_Policy | Solution | |
| Medium Missing Anti-clickjacking Header Description The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options. URL http://172.16.39.77:8080 Method GET Attack Evidence Other Info Instances 1 Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app. Solution 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 CWE Id 1021 WASC Id 15 Plugin Id 10020 | Reference | /Introducing Content Security Policy https://cheatsheetseries.owasp.org/cheatsheets/Content Security Policy Cheat Sheet.html https://www.w3.org/TR/CSP/ https://w3c.github.io/webappsec-csp/ https://web.dev/articles/csp https://caniuse.com/#feat=contentsecuritypolicy |
| Medium Missing Anti-clickjacking Header Description The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options. URL http://172.16.39.77:8080 Method GET Attack Evidence Other Info Instances Instances 1 Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app. Solution 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 CWE Id 1021 WASC Id 15 Plugin Id 10020 | CWE Id | <u>693</u> |
| Medium Missing Anti-clickjacking Header The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options. URL http://172.16.39.77:8080 Method GET Attack Evidence Other Info Instances 1 Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app. Solution 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 CWE Id 10020 | WASC Id | 15 |
| Description The response does not protect against 'Click Jacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options. URL http://172.16.39.77:8080 Method GET Attack Evidence Other Info Instances 1 Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app. Solution 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 CWE Id 1021 WASC Id 15 Plugin Id 10020 | Plugin Id | 10038 |
| Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options. URL http://172.16.39.77:8080 Method GET Attack Evidence Other Info Instances 1 Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app. Solution 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 CWE Id 1021 WASC Id 15 Plugin Id 10020 | | |
| Method Attack Evidence Other Info Instances 1 Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app. Solution 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 CWE Id 1021 WASC Id 15 Plugin Id 10020 | Medium | Missing Anti-clickjacking Header |
| Attack Evidence Other Info Instances 1 Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app. Solution 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 CWE Id 1021 WASC Id 15 Plugin Id 10020 | | The response does not protect against 'ClickJacking' attacks. It should include either |
| Evidence Other Info Instances 1 Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app. Solution 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 CWE Id 1021 WASC Id 15 Plugin Id 10020 | Description | The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options. |
| Other Info Instances 1 Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app. Solution 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 CWE Id 1021 WASC Id 15 Plugin Id 10020 | Description URL | The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options. http://172.16.39.77:8080 |
| Instances 1 Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app. Solution 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 CWE Id 1021 WASC Id 15 Plugin Id 10020 | Description URL Method | The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options. http://172.16.39.77:8080 |
| Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app. Solution 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 CWE Id 1021 WASC Id 15 Plugin Id 10020 | Description URL Method Attack | The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options. http://172.16.39.77:8080 |
| headers. Ensure one of them is set on all web pages returned by your site/app. Solution 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 CWE Id 1021 WASC Id 15 Plugin Id 10020 | Description URL Method Attack Evidence Other | The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options. http://172.16.39.77:8080 |
| CWE Id 1021 WASC Id 15 Plugin Id 10020 | Description URL Method Attack Evidence Other Info | The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options. http://172.16.39.77:8080 GET |
| WASC Id 15 Plugin Id 10020 | Description URL Method Attack Evidence Other Info Instances | The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options. http://172.16.39.77:8080 GET Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app. 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 |
| Plugin Id 10020 | Description URL Method Attack Evidence Other Info Instances Solution | The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options. http://172.16.39.77:8080 GET Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app. 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. |
| | Description URL Method Attack Evidence Other Info Instances Solution | The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options. http://172.16.39.77:8080 GET Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app. 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. https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options |
| Low Server Leaks Version Information via "Server" HTTP Response Header Field | Description URL Method Attack Evidence Other Info Instances Solution Reference CWE Id | The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options. http://172.16.39.77:8080 GET Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app. 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. https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options 1021 |
| 20.70. 20a.0 70.000 millioniation fla Cortor Tit it Response fleduci field | Description URL Method Attack Evidence Other Info Instances Solution Reference CWE Id WASC Id | The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options. http://172.16.39.77:8080 GET Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app. 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. https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options 1021 |
| | Description URL Method Attack Evidence Other Info Instances Solution Reference CWE Id WASC Id Plugin Id | The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options. http://172.16.39.77:8080 GET Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app. 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. https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options 1021 15 10020 |

| Description | The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to. |
|---------------|--|
| URL | http://172.16.39.77:8080 |
| Method | GET |
| Attack | |
| Evidence | Apache/2.4.49 (Unix) OpenSSL/1.1.1w PHP/7.3.31 |
| Other Info | |
| URL | http://172.16.39.77:8080/robots.txt |
| Method | GET |
| Attack | |
| Evidence | Apache/2.4.49 (Unix) OpenSSL/1.1.1w PHP/7.3.31 |
| Other Info | |
| URL | http://172.16.39.77:8080/sitemap.xml |
| Method | GET |
| Attack | |
| Evidence | Apache/2.4.49 (Unix) OpenSSL/1.1.1w PHP/7.3.31 |
| Other Info | |
| Instances | 3 |
| Solution | Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details. |
| Reference | https://httpd.apache.org/docs/current/mod/core.html#servertokens https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10) https://www.troyhunt.com/shhh-dont-let-your-response-headers/ |
| CWE Id | 497 |
| WASC Id | 13 |
| Plugin Id | 10036 |
| Low | 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. |
| URL | http://172.16.39.77:8080 |
| Method | GET |
| Attack | |
| Evidence | |
| 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. |
| Instances | 1 |
| | 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. |

| Solution | 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 | https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) https://owasp.org/www-community/Security_Headers |
| CWE Id | <u>693</u> |
| WASC Id | 15 |
| Plugin Id | <u>10021</u> |