

Vulnerabilities Report

1. 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.

Tags:

OWASP_2021_A05

SYSTEMIC

CWE-693

OWASP_2017_A06

Risk: Medium

URL: <https://example.com/sitemap.xml>

Method: GET

2. 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.

Tags:

OWASP_2021_A05

SYSTEMIC

CWE-693

OWASP_2017_A06

Risk: Medium

URL: <https://example.com/robots.txt>

Method: GET

3. Retrieved from Cache

Description: The content was retrieved from a shared cache. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

Tags:

CWE-525

SYSTEMIC

WSTG-v42-ATHN-06

Risk: Informational

URL: <https://example.com/robots.txt>

Method: GET

4. Retrieved from Cache

Description: The content was retrieved from a shared cache. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

Tags:

CWE-525

SYSTEMIC

WSTG-v42-ATHN-06

Risk: Informational

URL: <https://example.com/sitemap.xml>

Method: GET

5. Strict-Transport-Security Header Not Set

Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF

standards track protocol and is specified in RFC 6797.

Tags:

OWASP_2021_A05

SYSTEMIC

CWE-319

OWASP_2017_A06

Risk: Low

URL: <https://example.com/sitemap.xml>

Method: GET

6. Strict-Transport-Security Header Not Set

Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

Tags:

OWASP_2021_A05

SYSTEMIC

CWE-319

OWASP_2017_A06

Risk: Low

URL: <https://example.com/robots.txt>

Method: GET

7. ZAP is Out of Date

Description: The version of ZAP you are using to test your app is out of date and is no longer being updated. The risk level is set based on how out of date your ZAP version is.

Tags:

CWE-1104

Risk: Low

URL: <https://example.com/sitemap.xml>

Method: GET

8. 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.

Tags:

OWASP_2021_A05

CWE-1021

SYSTEMIC

WSTG-v42-CLNT-09

OWASP_2017_A06

Risk: Medium

URL: <https://example.com/>

Method: GET

9. Re-examine Cache-control Directives

Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

Tags:

CWE-525

SYSTEMIC

WSTG-v42-ATHN-06

Risk: Informational

URL: <https://example.com/>

Method: GET

10. 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.

Tags:

OWASP_2021_A05

SYSTEMIC

CWE-693

OWASP_2017_A06

Risk: Medium

URL: <https://example.com/>

Method: GET

11. Retrieved from Cache

Description: The content was retrieved from a shared cache. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

Tags:

CWE-525

SYSTEMIC

WSTG-v42-ATHN-06

Risk: Informational

URL: <https://example.com/>

Method: GET

12. Strict-Transport-Security Header Not Set

Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

Tags:

OWASP_2021_A05

SYSTEMIC

CWE-319

OWASP_2017_A06

Risk: Low

URL: <https://example.com/>

Method: GET

13. 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.

Tags:

OWASP_2021_A05

SYSTEMIC

CWE-693

OWASP_2017_A06

Risk: Low

URL: <https://example.com/>

Method: GET