

## Vulnerability Scan Report

Name: Missing Anti-clickjacking Header

Risk: Medium

Description: The response does not protect against 'ClickJacking' attacks. It should include either the X-Frame-Options header or the Content-Security-Policy header.

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options headers. Ensure that your web server, application server, load balancer, etc. is configured to set the appropriate header.

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including drive-by downloads, data injection, and other malicious scripts.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This header helps to prevent the browser from interpreting the content as a different MIME type than what is specified in the Content-Type header.

Solution: Ensure that the application/web server sets the Content-Type header appropriately, and the X-Content-Type-Options header to 'nosniff'.

Name: Missing Anti-clickjacking Header

Risk: Medium

Description: The response does not protect against 'ClickJacking' attacks. It should include either the X-Frame-Options header or the Content-Security-Policy header.

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options headers. Ensure that your web server, application server, load balancer, etc. is configured to set the appropriate header.

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including drive-by downloads, data injection, and other malicious scripts.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including drive-by downloads, data injection, and other malicious scripts.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including drive-by downloads, data injection, and other malicious scripts.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. The

Solution: Ensure that the application/web server sets the Content-Type header appropriately,

Name: Missing Anti-clickjacking Header

Risk: Medium

Description: The response does not protect against 'ClickJacking' attacks. It should include either

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options H

Name: Charset Mismatch (Header Versus Meta Content-Type Charset)

Risk: Informational

Description: This check identifies responses where the HTTP Content-Type header declares a

Solution: Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect a

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Absence of Anti-CSRF Tokens

Risk: Medium

Description: No Anti-CSRF tokens were found in a HTML submission form.■A cross-site requ

Solution: Phase: Architecture and Design■Use a vetted library or framework that does not allo

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP r

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. T

Solution: Ensure that the application/web server sets the Content-Type header appropriately,

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Missing Anti-clickjacking Header

Risk: Medium

Description: The response does not protect against 'ClickJacking' attacks. It should include eit

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options H

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Missing Anti-clickjacking Header

Risk: Medium

Description: The response does not protect against 'ClickJacking' attacks. It should include eit

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options H

Name: Missing Anti-clickjacking Header

Risk: Medium

Description: The response does not protect against 'ClickJacking' attacks. It should include eit

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options H

Name: Missing Anti-clickjacking Header

Risk: Medium

Description: The response does not protect against 'ClickJacking' attacks. It should include eit

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options H

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Missing Anti-clickjacking Header

Risk: Medium

Description: The response does not protect against 'ClickJacking' attacks. It should include eit

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options H

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including drive-by downloads, data injection, and other malicious scripts.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to send the CSP header.

Name: Missing Anti-clickjacking Header

Risk: Medium

Description: The response does not protect against 'ClickJacking' attacks. It should include either the 'X-Frame-Options' or 'Content-Security-Policy' header.

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options headers.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to not leak version information.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to not leak version information.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to not leak version information.

Name: Charset Mismatch (Header Versus Meta Content-Type Charset)

Risk: Informational

Description: This check identifies responses where the HTTP Content-Type header declares a charset that does not match the charset declared in the meta tag.

Solution: Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or XML.

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By" HTTP response header fields.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to not leak information.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to not leak version information.

Name: Charset Mismatch (Header Versus Meta Content-Type Charset)

Risk: Informational

Description: This check identifies responses where the HTTP Content-Type header declares a

Solution: Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or

Name: Charset Mismatch (Header Versus Meta Content-Type Charset)

Risk: Informational

Description: This check identifies responses where the HTTP Content-Type header declares a

Solution: Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or

Name: Charset Mismatch (Header Versus Meta Content-Type Charset)

Risk: Informational

Description: This check identifies responses where the HTTP Content-Type header declares a

Solution: Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or

Name: Charset Mismatch (Header Versus Meta Content-Type Charset)

Risk: Informational

Description: This check identifies responses where the HTTP Content-Type header declares a

Solution: Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or

Name: Charset Mismatch (Header Versus Meta Content-Type Charset)

Risk: Informational

Description: This check identifies responses where the HTTP Content-Type header declares a

Solution: Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. T

Solution: Ensure that the application/web server sets the Content-Type header appropriately,

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP r

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP r

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Missing Anti-clickjacking Header

Risk: Medium

Description: The response does not protect against 'ClickJacking' attacks. It should include either the X-Frame-Options header or the Content-Security-Policy header.

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options Headers.

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including drive-by downloads, data injection, and malicious redirects.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to send the CSP header.

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including drive-by downloads, data injection, and malicious redirects.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to send the CSP header.

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including drive-by downloads, data injection, and malicious redirects.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to send the CSP header.

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including drive-by downloads, data injection, and malicious redirects.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to send the CSP header.

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By" HTTP Response Header Field(s).

Solution: Ensure that your web server, application server, load balancer, etc. is configured to not send the "X-Powered-By" header.

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including drive-by downloads, data injection, and malicious redirects.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to send the CSP header.

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including drive-by downloads, data injection, and malicious redirects.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to send the CSP header.

Name: Missing Anti-clickjacking Header

Risk: Medium

Description: The response does not protect against 'ClickJacking' attacks. It should include either the X-Frame-Options header or the Content-Security-Policy header.

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options headers.

Name: Missing Anti-clickjacking Header

Risk: Medium

Description: The response does not protect against 'ClickJacking' attacks. It should include either the X-Frame-Options header or the Content-Security-Policy header.

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options headers.

Name: Missing Anti-clickjacking Header

Risk: Medium

Description: The response does not protect against 'ClickJacking' attacks. It should include either the X-Frame-Options header or the Content-Security-Policy header.

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options headers.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header.

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including drive-by-download attacks, cross-site scripting (XSS), and data injection attacks.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the CSP header.

Name: Absence of Anti-CSRF Tokens

Risk: Medium

Description: No Anti-CSRF tokens were found in a HTML submission form.■A cross-site request forgery (CSRF) attack occurs when a malicious user tricks a legitimate user into performing actions on a web application that the user did not intend to perform.

Solution: Phase: Architecture and Design■Use a vetted library or framework that does not allow for CSRF attacks.

Name: Modern Web Application

Risk: Informational

Description: The application appears to be a modern web application. If you need to explore it further, you may want to use a tool like Burp Suite.

Solution: This is an informational alert and so no changes are required.

Name: Absence of Anti-CSRF Tokens

Risk: Medium

Description: No Anti-CSRF tokens were found in a HTML submission form.■A cross-site request forgery (CSRF) attack occurs when a malicious user tricks a legitimate user into performing actions on a web application that the user did not intend to perform.

Solution: Phase: Architecture and Design■Use a vetted library or framework that does not allow for CSRF attacks.

Name: Absence of Anti-CSRF Tokens

Risk: Medium

Description: No Anti-CSRF tokens were found in a HTML submission form.■A cross-site request forgery (CSRF) attack occurs when an attacker makes a request to a web application, as if it originates from a trusted client.

Solution: Phase: Architecture and Design■Use a vetted library or framework that does not allow for CSRF attacks.

Name: Absence of Anti-CSRF Tokens

Risk: Medium

Description: No Anti-CSRF tokens were found in a HTML submission form.■A cross-site request forgery (CSRF) attack occurs when an attacker makes a request to a web application, as if it originates from a trusted client.

Solution: Phase: Architecture and Design■Use a vetted library or framework that does not allow for CSRF attacks.

Name: Absence of Anti-CSRF Tokens

Risk: Medium

Description: No Anti-CSRF tokens were found in a HTML submission form.■A cross-site request forgery (CSRF) attack occurs when an attacker makes a request to a web application, as if it originates from a trusted client.

Solution: Phase: Architecture and Design■Use a vetted library or framework that does not allow for CSRF attacks.

Name: Missing Anti-clickjacking Header

Risk: Medium

Description: The response does not protect against 'ClickJacking' attacks. It should include either the X-Frame-Options header or the Content-Security-Policy header.

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options headers.

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including drive-by-download attacks, cross-site scripting (XSS), and data injection attacks.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to send the CSP header.

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This header is used to prevent the browser from MIME-sniffing the content of the response.

Solution: Ensure that the application/web server sets the Content-Type header appropriately, and the X-Content-Type-Options header to 'nosniff'.

Name: Charset Mismatch (Header Versus Meta Content-Type Charset)

Risk: Informational

Description: This check identifies responses where the HTTP Content-Type header declares a charset that does not match the charset declared in the meta tag.

Solution: Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or XML.

Name: Charset Mismatch (Header Versus Meta Content-Type Charset)

Risk: Informational

Description: This check identifies responses where the HTTP Content-Type header declares a charset that does not match the charset declared in the meta tag.

Solution: Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or XML.



Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header.

Name: Absence of Anti-CSRF Tokens

Risk: Medium

Description: No Anti-CSRF tokens were found in a HTML submission form.■A cross-site request forgery (CSRF) attack is a type of attack that forces the victim's browser to make an unwanted request to a trusted web site.

Solution: Phase: Architecture and Design■Use a vetted library or framework that does not allow for CSRF attacks.

Name: Absence of Anti-CSRF Tokens

Risk: Medium

Description: No Anti-CSRF tokens were found in a HTML submission form.■A cross-site request forgery (CSRF) attack is a type of attack that forces the victim's browser to make an unwanted request to a trusted web site.

Solution: Phase: Architecture and Design■Use a vetted library or framework that does not allow for CSRF attacks.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header.

Name: Missing Anti-clickjacking Header

Risk: Medium

Description: The response does not protect against 'ClickJacking' attacks. It should include either the X-Frame-Options header or the Content-Security-Policy header.

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options headers. Ensure that your web server, application server, load balancer, etc. is configured to send one of these headers.

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including drive-by-download attacks, cross-site scripting (XSS), and data injection attacks.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to send the Content-Security-Policy header.

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including drive-by-download attacks, cross-site scripting (XSS), and data injection attacks.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to send the Content-Security-Policy header.

Name: Charset Mismatch (Header Versus Meta Content-Type Charset)

Risk: Informational

Description: This check identifies responses where the HTTP Content-Type header declares a charset that does not match the charset declared in the meta tag.

Solution: Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or XML.

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This header instructs the browser not to sniff the content type of the response.

Solution: Ensure that the application/web server sets the Content-Type header appropriately, and the X-Content-Type-Options header to 'nosniff'.

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This header instructs the browser not to sniff the content type of the response.

Solution: Ensure that the application/web server sets the Content-Type header appropriately, and the X-Content-Type-Options header to 'nosniff'.

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This header instructs the browser not to sniff the content type of the response.

Solution: Ensure that the application/web server sets the Content-Type header appropriately, and the X-Content-Type-Options header to 'nosniff'.

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This header instructs the browser not to sniff the content type of the response.

Solution: Ensure that the application/web server sets the Content-Type header appropriately, and the X-Content-Type-Options header to 'nosniff'.

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. The

Solution: Ensure that the application/web server sets the Content-Type header appropriately,

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP r

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP r

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. The

Solution: Ensure that the application/web server sets the Content-Type header appropriately,

Name: Charset Mismatch (Header Versus Meta Content-Type Charset)

Risk: Informational

Description: This check identifies responses where the HTTP Content-Type header declares a

Solution: Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or

Name: Absence of Anti-CSRF Tokens

Risk: Medium

Description: No Anti-CSRF tokens were found in a HTML submission form.■A cross-site requ

Solution: Phase: Architecture and Design■Use a vetted library or framework that does not allo

Name: Absence of Anti-CSRF Tokens

Risk: Medium

Description: No Anti-CSRF tokens were found in a HTML submission form.■A cross-site requ

Solution: Phase: Architecture and Design■Use a vetted library or framework that does not allo

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect a

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By"

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By"

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By"

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By"

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By"

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. T

Solution: Ensure that the application/web server sets the Content-Type header appropriately,

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. T

Solution: Ensure that the application/web server sets the Content-Type header appropriately,

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By"

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including drive-by downloads, where malicious websites use social engineering to lure visitors into downloading code that hijacks a browser. A web browser running CSP is able to prevent automatic downloading of code, and to prevent the execution of scripts from domains not known to the application developer.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to send the CSP header.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to not leak version information.

Name: Modern Web Application

Risk: Informational

Description: The application appears to be a modern web application. If you need to explore it further, you may want to look for more information.

Solution: This is an informational alert and so no changes are required.

Name: Absence of Anti-CSRF Tokens

Risk: Medium

Description: No Anti-CSRF tokens were found in a HTML submission form.■A cross-site request forgery (CSRF) attack occurs when a malicious user tricks a legitimate user into performing actions on a web application in which the user is authenticated.

Solution: Phase: Architecture and Design■Use a vetted library or framework that does not allow for CSRF attacks.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to not leak version information.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to not leak version information.

Name: Missing Anti-clickjacking Header

Risk: Medium

Description: The response does not protect against 'ClickJacking' attacks. It should include either the X-Frame-Options header or the Content-Security-Policy header.

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options headers.

Name: Missing Anti-clickjacking Header

Risk: Medium

Description: The response does not protect against 'ClickJacking' attacks. It should include either the X-Frame-Options header or the Content-Security-Policy header.

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options headers.

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By"

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By"

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Missing Anti-clickjacking Header

Risk: Medium

Description: The response does not protect against 'ClickJacking' attacks. It should include eit

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options H

Name: Missing Anti-clickjacking Header

Risk: Medium

Description: The response does not protect against 'ClickJacking' attacks. It should include eit

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options H

Name: Absence of Anti-CSRF Tokens

Risk: Medium

Description: No Anti-CSRF tokens were found in a HTML submission form.■A cross-site requ

Solution: Phase: Architecture and Design■Use a vetted library or framework that does not allo

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. T

Solution: Ensure that the application/web server sets the Content-Type header appropriately,

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP r

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP r

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. T

Solution: Ensure that the application/web server sets the Content-Type header appropriately,

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. T

Solution: Ensure that the application/web server sets the Content-Type header appropriately,

Name: Charset Mismatch (Header Versus Meta Content-Type Charset)

Risk: Informational

Description: This check identifies responses where the HTTP Content-Type header declares a

Solution: Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or

Name: Charset Mismatch (Header Versus Meta Content-Type Charset)

Risk: Informational

Description: This check identifies responses where the HTTP Content-Type header declares a

Solution: Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or

Name: Missing Anti-clickjacking Header

Risk: Medium

Description: The response does not protect against 'ClickJacking' attacks. It should include eit

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options H

Name: Missing Anti-clickjacking Header

Risk: Medium

Description: The response does not protect against 'ClickJacking' attacks. It should include eit

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options H

Name: Charset Mismatch (Header Versus Meta Content-Type Charset)

Risk: Informational

Description: This check identifies responses where the HTTP Content-Type header declares a

Solution: Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or

Name: Charset Mismatch (Header Versus Meta Content-Type Charset)

Risk: Informational

Description: This check identifies responses where the HTTP Content-Type header declares a

Solution: Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By" HTTP response header fields.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "X-Powered-By" header.

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows the browser to sniff the content type.

Solution: Ensure that the application/web server sets the Content-Type header appropriately, and the X-Content-Type-Options header to 'nosniff'.

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows the browser to sniff the content type.

Solution: Ensure that the application/web server sets the Content-Type header appropriately, and the X-Content-Type-Options header to 'nosniff'.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header.

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including drive-by downloads and data injection attacks.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including drive-by downloads and data injection attacks.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Name: Missing Anti-clickjacking Header

Risk: Medium

Description: The response does not protect against 'ClickJacking' attacks. It should include either the X-Frame-Options header or the Content-Security-Policy header.

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options headers. Ensure that your web server, application server, load balancer, etc. is configured to set one of these headers.



Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Charset Mismatch (Header Versus Meta Content-Type Charset)

Risk: Informational

Description: This check identifies responses where the HTTP Content-Type header declares a

Solution: Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or

Name: Charset Mismatch (Header Versus Meta Content-Type Charset)

Risk: Informational

Description: This check identifies responses where the HTTP Content-Type header declares a

Solution: Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or

Name: Missing Anti-clickjacking Header

Risk: Medium

Description: The response does not protect against 'ClickJacking' attacks. It should include eit

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options H

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: User Controllable HTML Element Attribute (Potential XSS)

Risk: Informational

Description: This check looks at user-supplied input in query string parameters and POST dat

Solution: Validate all input and sanitize output it before writing to any HTML attributes.

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows the browser to sniff the content type of the response and potentially execute malicious scripts.

Solution: Ensure that the application/web server sets the Content-Type header appropriately, and the X-Content-Type-Options header is set to 'nosniff'.

Name: Absence of Anti-CSRF Tokens

Risk: Medium

Description: No Anti-CSRF tokens were found in a HTML submission form. A cross-site request forgery (CSRF) attack occurs when an attacker forces a victim's browser to make an unwanted request to a trusted web site.

Solution: Phase: Architecture and Design Use a vetted library or framework that does not allow for CSRF attacks.

Name: Absence of Anti-CSRF Tokens

Risk: Medium

Description: No Anti-CSRF tokens were found in a HTML submission form. A cross-site request forgery (CSRF) attack occurs when an attacker forces a victim's browser to make an unwanted request to a trusted web site.

Solution: Phase: Architecture and Design Use a vetted library or framework that does not allow for CSRF attacks.

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including drive-by downloads, data injection, and malicious redirects.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to send the CSP header.

Name: Absence of Anti-CSRF Tokens

Risk: Medium

Description: No Anti-CSRF tokens were found in a HTML submission form. A cross-site request forgery (CSRF) attack occurs when an attacker forces a victim's browser to make an unwanted request to a trusted web site.

Solution: Phase: Architecture and Design Use a vetted library or framework that does not allow for CSRF attacks.

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including drive-by downloads, data injection, and malicious redirects.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to send the CSP header.

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including drive-by downloads, data injection, and malicious redirects.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to send the CSP header.

Name: Absence of Anti-CSRF Tokens

Risk: Medium

Description: No Anti-CSRF tokens were found in a HTML submission form. A cross-site request forgery (CSRF) attack occurs when an attacker forces a victim's browser to make an unwanted request to a trusted web site.

Solution: Phase: Architecture and Design Use a vetted library or framework that does not allow for CSRF attacks.

Name: Charset Mismatch (Header Versus Meta Content-Type Charset)

Risk: Informational

Description: This check identifies responses where the HTTP Content-Type header declares a

Solution: Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or

Name: User Controllable HTML Element Attribute (Potential XSS)

Risk: Informational

Description: This check looks at user-supplied input in query string parameters and POST data

Solution: Validate all input and sanitize output it before writing to any HTML attributes.

Name: Missing Anti-clickjacking Header

Risk: Medium

Description: The response does not protect against 'ClickJacking' attacks. It should include either

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options H

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP r

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP r

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Absence of Anti-CSRF Tokens

Risk: Medium

Description: No Anti-CSRF tokens were found in a HTML submission form.■A cross-site requ

Solution: Phase: Architecture and Design■Use a vetted library or framework that does not allo

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP r

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Modern Web Application

Risk: Informational

Description: The application appears to be a modern web application. If you need to explore it

Solution: This is an informational alert and so no changes are required.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to not leak version information via the "Server" HTTP response header field.

Name: Absence of Anti-CSRF Tokens

Risk: Medium

Description: No Anti-CSRF tokens were found in a HTML submission form.■A cross-site request forgery (CSRF) attack occurs when an attacker makes an unauthorized request to a web application on behalf of a legitimate user.

Solution: Phase: Architecture and Design■Use a vetted library or framework that does not allow for CSRF attacks.

Name: Absence of Anti-CSRF Tokens

Risk: Medium

Description: No Anti-CSRF tokens were found in a HTML submission form.■A cross-site request forgery (CSRF) attack occurs when an attacker makes an unauthorized request to a web application on behalf of a legitimate user.

Solution: Phase: Architecture and Design■Use a vetted library or framework that does not allow for CSRF attacks.

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including drive-by downloads, data injection, and other malicious scripts.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content Security Policy (CSP) header.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to not leak version information via the "Server" HTTP response header field.

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows the browser to sniff the content type of the response.

Solution: Ensure that the application/web server sets the Content-Type header appropriately, and the X-Content-Type-Options header to 'nosniff'.

Name: Charset Mismatch (Header Versus Meta Content-Type Charset)

Risk: Informational

Description: This check identifies responses where the HTTP Content-Type header declares a charset that does not match the charset declared in the meta tags of the HTML document.

Solution: Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or XML documents.

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows the browser to sniff the content type of the response.

Solution: Ensure that the application/web server sets the Content-Type header appropriately, and the X-Content-Type-Options header to 'nosniff'.

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. The

Solution: Ensure that the application/web server sets the Content-Type header appropriately,

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. The

Solution: Ensure that the application/web server sets the Content-Type header appropriately,

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP r

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP r

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. The

Solution: Ensure that the application/web server sets the Content-Type header appropriately,

Name: Modern Web Application

Risk: Informational

Description: The application appears to be a modern web application. If you need to explore it

Solution: This is an informational alert and so no changes are required.

Name: Modern Web Application

Risk: Informational

Description: The application appears to be a modern web application. If you need to explore it

Solution: This is an informational alert and so no changes are required.

Name: Absence of Anti-CSRF Tokens

Risk: Medium

Description: No Anti-CSRF tokens were found in a HTML submission form.■A cross-site requ

Solution: Phase: Architecture and Design■Use a vetted library or framework that does not allo

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. The

Solution: Ensure that the application/web server sets the Content-Type header appropriately,

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect a

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Missing Anti-clickjacking Header

Risk: Medium

Description: The response does not protect against 'ClickJacking' attacks. It should include eit

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options H

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. The

Solution: Ensure that the application/web server sets the Content-Type header appropriately,

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. The

Solution: Ensure that the application/web server sets the Content-Type header appropriately,

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP r

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP r

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Absence of Anti-CSRF Tokens

Risk: Medium

Description: No Anti-CSRF tokens were found in a HTML submission form.■A cross-site requ

Solution: Phase: Architecture and Design■Use a vetted library or framework that does not all

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP r

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Absence of Anti-CSRF Tokens

Risk: Medium

Description: No Anti-CSRF tokens were found in a HTML submission form.■A cross-site requ

Solution: Phase: Architecture and Design■Use a vetted library or framework that does not all

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP r

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By"

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP r

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Charset Mismatch (Header Versus Meta Content-Type Charset)

Risk: Informational

Description: This check identifies responses where the HTTP Content-Type header declares a

Solution: Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By"

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Missing Anti-clickjacking Header

Risk: Medium

Description: The response does not protect against 'ClickJacking' attacks. It should include eit

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options H

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. T

Solution: Ensure that the application/web server sets the Content-Type header appropriately,

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. T

Solution: Ensure that the application/web server sets the Content-Type header appropriately,

Name: Missing Anti-clickjacking Header

Risk: Medium

Description: The response does not protect against 'ClickJacking' attacks. It should include eit

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options H



Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header.

Name: Absence of Anti-CSRF Tokens

Risk: Medium

Description: No Anti-CSRF tokens were found in a HTML submission form.■A cross-site request forgery (CSRF) attack is an attack that forces an end user to execute unwanted actions on a web application in which they are currently authenticated.

Solution: Phase: Architecture and Design■Use a vetted library or framework that does not allow for CSRF attacks.

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. The browser may be vulnerable to MIME-sniffing attacks.

Solution: Ensure that the application/web server sets the Content-Type header appropriately, and the X-Content-Type-Options header to 'nosniff'.

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By" HTTP response header fields.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "X-Powered-By" header.

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including drive-by-download attacks, cross-site scripting (XSS), and data URI attacks.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. The browser may be vulnerable to MIME-sniffing attacks.

Solution: Ensure that the application/web server sets the Content-Type header appropriately, and the X-Content-Type-Options header to 'nosniff'.

Name: Missing Anti-clickjacking Header

Risk: Medium

Description: The response does not protect against 'ClickJacking' attacks. It should include either the X-Frame-Options header or the Content-Security-Policy header.

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options headers. Ensure that your web server, application server, load balancer, etc. is configured to set one of these headers.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header.

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including drive-by downloads, data injection, and other malicious scripts.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to send the CSP header.

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By" HTTP response header fields.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to not send the "X-Powered-By" header.

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By" HTTP response header fields.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to not send the "X-Powered-By" header.

Name: User Controllable HTML Element Attribute (Potential XSS)

Risk: Informational

Description: This check looks at user-supplied input in query string parameters and POST data to see if it contains HTML attributes.

Solution: Validate all input and sanitize output before writing to any HTML attributes.

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including drive-by downloads, data injection, and other malicious scripts.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to send the CSP header.

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By" HTTP response header fields.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to not send the "X-Powered-By" header.

Name: Missing Anti-clickjacking Header

Risk: Medium

Description: The response does not protect against 'ClickJacking' attacks. It should include either the 'X-Frame-Options' or 'Content-Security-Policy' header.

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options headers.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to not send the "Server" header.

Name: Absence of Anti-CSRF Tokens

Risk: Medium

Description: No Anti-CSRF tokens were found in a HTML submission form.■A cross-site request

Solution: Phase: Architecture and Design■Use a vetted library or framework that does not allow

Name: Missing Anti-clickjacking Header

Risk: Medium

Description: The response does not protect against 'ClickJacking' attacks. It should include either

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options H

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. T

Solution: Ensure that the application/web server sets the Content-Type header appropriately,

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP r

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Missing Anti-clickjacking Header

Risk: Medium

Description: The response does not protect against 'ClickJacking' attacks. It should include either

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options H

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP r

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. T

Solution: Ensure that the application/web server sets the Content-Type header appropriately,

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header.

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows the browser to sniff the content type.

Solution: Ensure that the application/web server sets the Content-Type header appropriately, and the X-Content-Type-Options header to 'nosniff'.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header.

Name: Charset Mismatch (Header Versus Meta Content-Type Charset)

Risk: Informational

Description: This check identifies responses where the HTTP Content-Type header declares a charset that does not match the charset declared in the meta tags.

Solution: Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or XML.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header.

Name: Modern Web Application

Risk: Informational

Description: The application appears to be a modern web application. If you need to explore it, you may want to use a modern web browser.

Solution: This is an informational alert and so no changes are required.

Name: Charset Mismatch (Header Versus Meta Content-Type Charset)

Risk: Informational

Description: This check identifies responses where the HTTP Content-Type header declares a charset that does not match the charset declared in the meta tags.

Solution: Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or XML.

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows the browser to sniff the content type.

Solution: Ensure that the application/web server sets the Content-Type header appropriately, and the X-Content-Type-Options header to 'nosniff'.

Name: Missing Anti-clickjacking Header

Risk: Medium

Description: The response does not protect against 'ClickJacking' attacks. It should include either the X-Frame-Options header or the Content-Security-Policy header.

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options headers. Ensure that your web server, application server, load balancer, etc. is configured to set one of these headers.

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This header prevents the browser from interpreting the content as a different MIME type than what is declared in the Content-Type header.

Solution: Ensure that the application/web server sets the Content-Type header appropriately, and that the X-Content-Type-Options header is set to 'nosniff'.

Name: Charset Mismatch (Header Versus Meta Content-Type Charset)

Risk: Informational

Description: This check identifies responses where the HTTP Content-Type header declares a charset that does not match the charset declared in the meta tags in the HTML document.

Solution: Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or XML documents.

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By" HTTP response header fields. This header field is used to identify the software that generated the response.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to not send the X-Powered-By header field.

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This header prevents the browser from interpreting the content as a different MIME type than what is declared in the Content-Type header.

Solution: Ensure that the application/web server sets the Content-Type header appropriately, and that the X-Content-Type-Options header is set to 'nosniff'.

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By" HTTP response header fields. This header field is used to identify the software that generated the response.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to not send the X-Powered-By header field.

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This header prevents the browser from interpreting the content as a different MIME type than what is declared in the Content-Type header.

Solution: Ensure that the application/web server sets the Content-Type header appropriately, and that the X-Content-Type-Options header is set to 'nosniff'.

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including drive-by downloads and data injection attacks.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including drive-by downloads, data injection, and malicious redirects.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to send the CSP header.

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This header instructs the browser not to sniff the content type of the response.

Solution: Ensure that the application/web server sets the Content-Type header appropriately, and the X-Content-Type-Options header to 'nosniff'.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to not leak version information.

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By" HTTP response header fields.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to not leak information.

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including drive-by downloads, data injection, and malicious redirects.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to send the CSP header.

Name: Charset Mismatch (Header Versus Meta Content-Type Charset)

Risk: Informational

Description: This check identifies responses where the HTTP Content-Type header declares a charset that does not match the charset declared in the meta tag.

Solution: Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or XML.

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By" HTTP response header fields.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to not leak information.

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By" HTTP response header fields.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to not leak information.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header.

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By" HTTP response header fields.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "X-Powered-By" header.

Name: Missing Anti-clickjacking Header

Risk: Medium

Description: The response does not protect against 'ClickJacking' attacks. It should include either the X-Frame-Options or Content-Security-Policy header.

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options headers.

Name: Absence of Anti-CSRF Tokens

Risk: Medium

Description: No Anti-CSRF tokens were found in a HTML submission form. A cross-site request forgery (CSRF) attack may be possible against this application.

Solution: Phase: Architecture and Design Use a vetted library or framework that does not allow CSRF attacks.

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By" HTTP response header fields.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "X-Powered-By" header.

Name: Absence of Anti-CSRF Tokens

Risk: Medium

Description: No Anti-CSRF tokens were found in a HTML submission form. A cross-site request forgery (CSRF) attack may be possible against this application.

Solution: Phase: Architecture and Design Use a vetted library or framework that does not allow CSRF attacks.

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This may allow the browser to sniff the content type.

Solution: Ensure that the application/web server sets the Content-Type header appropriately, and the X-Content-Type-Options header to 'nosniff'.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header.

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including drive-by downloads, where malicious websites use social engineering to lure visitors into downloading malware from the Internet.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to send the CSP header.

Name: Absence of Anti-CSRF Tokens

Risk: Medium

Description: No Anti-CSRF tokens were found in a HTML submission form. A cross-site request forgery (CSRF) attack tricks an unsuspecting user into submitting a form to a vulnerable web application.

Solution: Phase: Architecture and Design Use a vetted library or framework that does not allow for CSRF attacks.

Name: Missing Anti-clickjacking Header

Risk: Medium

Description: The response does not protect against 'ClickJacking' attacks. It should include either the X-Frame-Options header or the Content-Security-Policy header.

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options headers.

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This header helps to prevent the browser from interpreting the content as a different MIME type than the one declared in the Content-Type header.

Solution: Ensure that the application/web server sets the Content-Type header appropriately, and the X-Content-Type-Options header to 'nosniff'.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to not send the Server header.

Name: Authentication Request Identified

Risk: Informational

Description: The given request has been identified as an authentication request. The 'Other Information' field contains details about the request.

Solution: This is an informational alert rather than a vulnerability and so there is nothing to fix.

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including drive-by downloads, where malicious websites use social engineering to lure visitors into downloading malware from the Internet.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to send the CSP header.

Name: Modern Web Application

Risk: Informational

Description: The application appears to be a modern web application. If you need to explore it further, you can use the 'Other Information' field.

Solution: This is an informational alert and so no changes are required.



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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By"

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Absence of Anti-CSRF Tokens

Risk: Medium

Description: No Anti-CSRF tokens were found in a HTML submission form.■A cross-site requ

Solution: Phase: Architecture and Design■Use a vetted library or framework that does not allo

Name: Missing Anti-clickjacking Header

Risk: Medium

Description: The response does not protect against 'ClickJacking' attacks. It should include eit

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options H

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. T

Solution: Ensure that the application/web server sets the Content-Type header appropriately,

Name: Absence of Anti-CSRF Tokens

Risk: Medium

Description: No Anti-CSRF tokens were found in a HTML submission form.■A cross-site requ

Solution: Phase: Architecture and Design■Use a vetted library or framework that does not allo

Name: Absence of Anti-CSRF Tokens

Risk: Medium

Description: No Anti-CSRF tokens were found in a HTML submission form.■A cross-site requ

Solution: Phase: Architecture and Design■Use a vetted library or framework that does not allo

Name: Charset Mismatch (Header Versus Meta Content-Type Charset)

Risk: Informational

Description: This check identifies responses where the HTTP Content-Type header declares a

Solution: Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By"

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. The

Solution: Ensure that the application/web server sets the Content-Type header appropriately,

Name: Missing Anti-clickjacking Header

Risk: Medium

Description: The response does not protect against 'ClickJacking' attacks. It should include either

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options H

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP r

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP r

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Missing Anti-clickjacking Header

Risk: Medium

Description: The response does not protect against 'ClickJacking' attacks. It should include either

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options H

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP r

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Charset Mismatch (Header Versus Meta Content-Type Charset)

Risk: Informational

Description: This check identifies responses where the HTTP Content-Type header declares a

Solution: Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or

Name: Absence of Anti-CSRF Tokens

Risk: Medium

Description: No Anti-CSRF tokens were found in a HTML submission form.■A cross-site request forgery (CSRF) attack occurs when an attacker makes an unauthorized request to a web application on behalf of an authenticated user.

Solution: Phase: Architecture and Design■Use a vetted library or framework that does not allow CSRF attacks.

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including drive-by downloads, data injection, and malicious scripts.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to send the CSP header.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to not leak version information.

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By" HTTP response header fields.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to not leak information.

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows the browser to sniff the content type.

Solution: Ensure that the application/web server sets the Content-Type header appropriately, and the X-Content-Type-Options header to 'nosniff'.

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows the browser to sniff the content type.

Solution: Ensure that the application/web server sets the Content-Type header appropriately, and the X-Content-Type-Options header to 'nosniff'.

Name: Charset Mismatch (Header Versus Meta Content-Type Charset)

Risk: Informational

Description: This check identifies responses where the HTTP Content-Type header declares a charset that does not match the charset declared in the meta tags.

Solution: Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or XML.

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows the browser to sniff the content type.

Solution: Ensure that the application/web server sets the Content-Type header appropriately, and the X-Content-Type-Options header to 'nosniff'.

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including drive-by downloads, data injection, and malicious redirects.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to send the CSP header.

Name: Charset Mismatch (Header Versus Meta Content-Type Charset)

Risk: Informational

Description: This check identifies responses where the HTTP Content-Type header declares a charset that does not match the charset declared in the meta tag.

Solution: Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or XML.

Name: Absence of Anti-CSRF Tokens

Risk: Medium

Description: No Anti-CSRF tokens were found in a HTML submission form. A cross-site request forgery (CSRF) attack occurs when an attacker uses a web application to perform an unwanted action on a web application in which the attacker is authenticated.

Solution: Phase: Architecture and Design Use a vetted library or framework that does not allow for CSRF attacks.

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This header is used to prevent the browser from MIME-sniffing the content of the response and to ensure that the browser uses the declared Content-Type of the response.

Solution: Ensure that the application/web server sets the Content-Type header appropriately, and the X-Content-Type-Options header is set to 'nosniff'.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to not leak version information via the "Server" HTTP response header field.

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including drive-by downloads, data injection, and malicious redirects.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to send the CSP header.

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By" HTTP response header fields.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to not leak information via the "X-Powered-By" HTTP response header fields.

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By" HTTP response header fields.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to not leak information via the "X-Powered-By" HTTP response header fields.

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By"

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect a

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Absence of Anti-CSRF Tokens

Risk: Medium

Description: No Anti-CSRF tokens were found in a HTML submission form.■A cross-site requ

Solution: Phase: Architecture and Design■Use a vetted library or framework that does not allo

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By"

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Absence of Anti-CSRF Tokens

Risk: Medium

Description: No Anti-CSRF tokens were found in a HTML submission form.■A cross-site requ

Solution: Phase: Architecture and Design■Use a vetted library or framework that does not allo

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. T

Solution: Ensure that the application/web server sets the Content-Type header appropriately,

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP r

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Absence of Anti-CSRF Tokens

Risk: Medium

Description: No Anti-CSRF tokens were found in a HTML submission form.■A cross-site requ

Solution: Phase: Architecture and Design■Use a vetted library or framework that does not allo

Name: Absence of Anti-CSRF Tokens

Risk: Medium

Description: No Anti-CSRF tokens were found in a HTML submission form.■A cross-site request forgery (CSRF) attack is a type of attack that allows an attacker to perform actions on behalf of a user without their knowledge or consent.

Solution: Phase: Architecture and Design■Use a vetted library or framework that does not allow for CSRF attacks.

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By" HTTP response header fields.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to not leak this information.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to not leak this information.

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows the browser to sniff the content type of the response.

Solution: Ensure that the application/web server sets the Content-Type header appropriately, and that the X-Content-Type-Options header is set to 'nosniff'.

Name: Absence of Anti-CSRF Tokens

Risk: Medium

Description: No Anti-CSRF tokens were found in a HTML submission form.■A cross-site request forgery (CSRF) attack is a type of attack that allows an attacker to perform actions on behalf of a user without their knowledge or consent.

Solution: Phase: Architecture and Design■Use a vetted library or framework that does not allow for CSRF attacks.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to not leak this information.

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows the browser to sniff the content type of the response.

Solution: Ensure that the application/web server sets the Content-Type header appropriately, and that the X-Content-Type-Options header is set to 'nosniff'.

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By" HTTP response header fields.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to not leak this information.

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. The

Solution: Ensure that the application/web server sets the Content-Type header appropriately,

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP r

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. T

Solution: Ensure that the application/web server sets the Content-Type header appropriately,

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Missing Anti-clickjacking Header

Risk: Medium

Description: The response does not protect against 'ClickJacking' attacks. It should include eit

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options H

Name: Missing Anti-clickjacking Header

Risk: Medium

Description: The response does not protect against 'ClickJacking' attacks. It should include eit

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options H

Name: Missing Anti-clickjacking Header

Risk: Medium

Description: The response does not protect against 'ClickJacking' attacks. It should include either the X-Frame-Options header or the Content-Security-Policy header.

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options headers. Ensure that your web server, application server, load balancer, etc. is configured to send these headers.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to not leak version information via the "Server" HTTP response header field.

Name: Missing Anti-clickjacking Header

Risk: Medium

Description: The response does not protect against 'ClickJacking' attacks. It should include either the X-Frame-Options header or the Content-Security-Policy header.

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options headers. Ensure that your web server, application server, load balancer, etc. is configured to send these headers.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to not leak version information via the "Server" HTTP response header field.

Name: Missing Anti-clickjacking Header

Risk: Medium

Description: The response does not protect against 'ClickJacking' attacks. It should include either the X-Frame-Options header or the Content-Security-Policy header.

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options headers. Ensure that your web server, application server, load balancer, etc. is configured to send these headers.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to not leak version information via the "Server" HTTP response header field.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to not leak version information via the "Server" HTTP response header field.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to not leak version information via the "Server" HTTP response header field.



Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to not leak version information via the "Server" HTTP response header field.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to not leak version information via the "Server" HTTP response header field.

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows the browser to sniff the content type of the response.

Solution: Ensure that the application/web server sets the Content-Type header appropriately, and the X-Content-Type-Options header to 'nosniff'.

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including drive-by downloads and data injection attacks.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content Security Policy (CSP) header.

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows the browser to sniff the content type of the response.

Solution: Ensure that the application/web server sets the Content-Type header appropriately, and the X-Content-Type-Options header to 'nosniff'.

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows the browser to sniff the content type of the response.

Solution: Ensure that the application/web server sets the Content-Type header appropriately, and the X-Content-Type-Options header to 'nosniff'.

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows the browser to sniff the content type of the response.

Solution: Ensure that the application/web server sets the Content-Type header appropriately, and the X-Content-Type-Options header to 'nosniff'.

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows the browser to sniff the content type of the response.

Solution: Ensure that the application/web server sets the Content-Type header appropriately, and the X-Content-Type-Options header to 'nosniff'.

Name: Charset Mismatch (Header Versus Meta Content-Type Charset)

Risk: Informational

Description: This check identifies responses where the HTTP Content-Type header declares a

Solution: Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect a

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect a

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. T

Solution: Ensure that the application/web server sets the Content-Type header appropriately,

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. T

Solution: Ensure that the application/web server sets the Content-Type header appropriately,

Name: Charset Mismatch (Header Versus Meta Content-Type Charset)

Risk: Informational

Description: This check identifies responses where the HTTP Content-Type header declares a

Solution: Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By"

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By"

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By"

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By"

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect a

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By"

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect a

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP r

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header.

Name: Missing Anti-clickjacking Header

Risk: Medium

Description: The response does not protect against 'ClickJacking' attacks. It should include either the X-Frame-Options header or the Content-Security-Policy header.

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options headers. Ensure that your web server, application server, load balancer, etc. is configured to include one of these headers.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header.

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows browsers to sniff the content type of the response.

Solution: Ensure that the application/web server sets the Content-Type header appropriately, and the X-Content-Type-Options header to 'nosniff'.

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows browsers to sniff the content type of the response.

Solution: Ensure that the application/web server sets the Content-Type header appropriately, and the X-Content-Type-Options header to 'nosniff'.

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows browsers to sniff the content type of the response.

Solution: Ensure that the application/web server sets the Content-Type header appropriately, and the X-Content-Type-Options header to 'nosniff'.

Name: Absence of Anti-CSRF Tokens

Risk: Medium

Description: No Anti-CSRF tokens were found in a HTML submission form. A cross-site request forgery (CSRF) attack is possible.

Solution: Phase: Architecture and Design Use a vetted library or framework that does not allow for CSRF attacks.

Name: Absence of Anti-CSRF Tokens

Risk: Medium

Description: No Anti-CSRF tokens were found in a HTML submission form.■A cross-site request

Solution: Phase: Architecture and Design■Use a vetted library or framework that does not allow

Name: Missing Anti-clickjacking Header

Risk: Medium

Description: The response does not protect against 'ClickJacking' attacks. It should include either

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options H

Name: Missing Anti-clickjacking Header

Risk: Medium

Description: The response does not protect against 'ClickJacking' attacks. It should include either

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options H

Name: Missing Anti-clickjacking Header

Risk: Medium

Description: The response does not protect against 'ClickJacking' attacks. It should include either

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options H

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. T

Solution: Ensure that the application/web server sets the Content-Type header appropriately,

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By"

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect a

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP r

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP r

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Charset Mismatch (Header Versus Meta Content-Type Charset)

Risk: Informational

Description: This check identifies responses where the HTTP Content-Type header declares a

Solution: Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP r

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Charset Mismatch (Header Versus Meta Content-Type Charset)

Risk: Informational

Description: This check identifies responses where the HTTP Content-Type header declares a

Solution: Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By"

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Missing Anti-clickjacking Header

Risk: Medium

Description: The response does not protect against 'ClickJacking' attacks. It should include either the X-Frame-Options header or the Content-Security-Policy header.

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options headers. Ensure that your web server, application server, load balancer, etc. is configured to send one of these headers.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to not send the "Server" header field.

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows the browser to sniff the content type of the response.

Solution: Ensure that the application/web server sets the Content-Type header appropriately, and the X-Content-Type-Options header to 'nosniff'.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to not send the "Server" header field.

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows the browser to sniff the content type of the response.

Solution: Ensure that the application/web server sets the Content-Type header appropriately, and the X-Content-Type-Options header to 'nosniff'.

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including drive-by downloads and data injection attacks.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to send the Content-Security-Policy header.

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows the browser to sniff the content type of the response.

Solution: Ensure that the application/web server sets the Content-Type header appropriately, and the X-Content-Type-Options header to 'nosniff'.

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including drive-by downloads and data injection attacks.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to send the Content-Security-Policy header.

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. The

Solution: Ensure that the application/web server sets the Content-Type header appropriately,

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. The

Solution: Ensure that the application/web server sets the Content-Type header appropriately,

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Absence of Anti-CSRF Tokens

Risk: Medium

Description: No Anti-CSRF tokens were found in a HTML submission form.■A cross-site requ

Solution: Phase: Architecture and Design■Use a vetted library or framework that does not allo

Name: Absence of Anti-CSRF Tokens

Risk: Medium

Description: No Anti-CSRF tokens were found in a HTML submission form.■A cross-site requ

Solution: Phase: Architecture and Design■Use a vetted library or framework that does not allo



Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header.

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By" HTTP response header fields.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "X-Powered-By" header.

Name: Modern Web Application

Risk: Informational

Description: The application appears to be a modern web application. If you need to explore it further, you may want to use a tool like Burp Suite.

Solution: This is an informational alert and so no changes are required.

Name: Modern Web Application

Risk: Informational

Description: The application appears to be a modern web application. If you need to explore it further, you may want to use a tool like Burp Suite.

Solution: This is an informational alert and so no changes are required.

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This may allow an attacker to perform a MIME-sniffing attack to reveal sensitive data.

Solution: Ensure that the application/web server sets the Content-Type header appropriately, and the X-Content-Type-Options header to 'nosniff'.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header.

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By" HTTP response header fields.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "X-Powered-By" header.

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. The

Solution: Ensure that the application/web server sets the Content-Type header appropriately,

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. The

Solution: Ensure that the application/web server sets the Content-Type header appropriately,

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By"

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By"

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect a

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect a

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect a

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP r

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to not leak version information via the "Server" HTTP response header field.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to not leak version information via the "Server" HTTP response header field.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to not leak version information via the "Server" HTTP response header field.

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including drive-by downloads and data injection attacks.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content Security Policy (CSP) header.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to not leak version information via the "Server" HTTP response header field.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to not leak version information via the "Server" HTTP response header field.

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including drive-by downloads and data injection attacks.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content Security Policy (CSP) header.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to not leak version information via the "Server" HTTP response header field.

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP r

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP r

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP r

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP r

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to not leak version information via the "Server" HTTP response header field.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to not leak version information via the "Server" HTTP response header field.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to not leak version information via the "Server" HTTP response header field.

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including drive-by downloads and data injection attacks.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content Security Policy (CSP) header.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to not leak version information via the "Server" HTTP response header field.

Name: Missing Anti-clickjacking Header

Risk: Medium

Description: The response does not protect against 'ClickJacking' attacks. It should include either the X-Frame-Options header or the Content-Security-Policy header.

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options headers.

Name: Charset Mismatch (Header Versus Meta Content-Type Charset)

Risk: Informational

Description: This check identifies responses where the HTTP Content-Type header declares a charset that does not match the charset declared in the meta tags.

Solution: Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or XML.

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including drive-by downloads and data injection attacks.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content Security Policy (CSP) header.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header.

Name: Missing Anti-clickjacking Header

Risk: Medium

Description: The response does not protect against 'ClickJacking' attacks. It should include either the X-Frame-Options or the Content-Security-Policy header.

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options headers. Ensure that your web server, application server, load balancer, etc. is configured to set one of these headers.

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows the browser to sniff the content type of the response.

Solution: Ensure that the application/web server sets the Content-Type header appropriately, and the X-Content-Type-Options header to 'nosniff'.

Name: Charset Mismatch (Header Versus Meta Content-Type Charset)

Risk: Informational

Description: This check identifies responses where the HTTP Content-Type header declares a charset that does not match the charset declared in the meta tags of the HTML document.

Solution: Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or XML documents.

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By" HTTP response header fields.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "X-Powered-By" header.

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including drive-by downloads and data injection attacks.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header.

Name: Absence of Anti-CSRF Tokens

Risk: Medium

Description: No Anti-CSRF tokens were found in a HTML submission form.■A cross-site request

Solution: Phase: Architecture and Design■Use a vetted library or framework that does not allow

Name: Missing Anti-clickjacking Header

Risk: Medium

Description: The response does not protect against 'ClickJacking' attacks. It should include either

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options H

Name: Missing Anti-clickjacking Header

Risk: Medium

Description: The response does not protect against 'ClickJacking' attacks. It should include either

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options H

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP r

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect a

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Charset Mismatch (Header Versus Meta Content-Type Charset)

Risk: Informational

Description: This check identifies responses where the HTTP Content-Type header declares a

Solution: Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. T

Solution: Ensure that the application/web server sets the Content-Type header appropriately,

Name: Directory Browsing

Risk: Medium

Description: It is possible to view a listing of the directory contents. Directory listings may reve

Solution: Configure the web server to disable directory browsing.

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including drive-by downloads, data injection, and other malicious scripts.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the CSP header.

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By" HTTP response header fields.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to not set the "X-Powered-By" header.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to not set the "Server" header.

Name: Modern Web Application

Risk: Informational

Description: The application appears to be a modern web application. If you need to explore it further, you can use the "View Page Source" link in the alert.

Solution: This is an informational alert and so no changes are required.

Name: Missing Anti-clickjacking Header

Risk: Medium

Description: The response does not protect against 'ClickJacking' attacks. It should include either the 'X-Frame-Options' or 'Content-Security-Policy' header.

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options headers.

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This header helps to prevent the browser from interpreting the content as a different MIME type than what is specified in the Content-Type header.

Solution: Ensure that the application/web server sets the Content-Type header appropriately, and the X-Content-Type-Options header to 'nosniff'.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to not set the "Server" header.

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including drive-by downloads, data injection, and other malicious scripts.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the CSP header.



Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. The

Solution: Ensure that the application/web server sets the Content-Type header appropriately,

Name: Directory Browsing

Risk: Medium

Description: It is possible to view a listing of the directory contents. Directory listings may reveal

Solution: Configure the web server to disable directory browsing.

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By"

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP r

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. The

Solution: Ensure that the application/web server sets the Content-Type header appropriately,

Name: Missing Anti-clickjacking Header

Risk: Medium

Description: The response does not protect against 'ClickJacking' attacks. It should include eit

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options H

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect a

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Content Security Policy (CSP) Header Not Set

Risk: Medium

Description: Content Security Policy (CSP) is an added layer of security that helps to detect a

Solution: Ensure that your web server, application server, load balancer, etc. is configured to s

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header.

Name: Directory Browsing

Risk: Medium

Description: It is possible to view a listing of the directory contents. Directory listings may reveal sensitive information.

Solution: Configure the web server to disable directory browsing.

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

Risk: Low

Description: The web/application server is leaking information via one or more "X-Powered-By" HTTP response header fields.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "X-Powered-By" header.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header.

Name: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk: Low

Description: The web/application server is leaking version information via the "Server" HTTP response header field.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header.

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows the browser to sniff the content type.

Solution: Ensure that the application/web server sets the Content-Type header appropriately, and the X-Content-Type-Options header to 'nosniff'.

Name: X-Content-Type-Options Header Missing

Risk: Low

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows the browser to sniff the content type.

Solution: Ensure that the application/web server sets the Content-Type header appropriately, and the X-Content-Type-Options header to 'nosniff'.

Name: Cross Site Scripting (Reflected)

Risk: High

Description: Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a web page.

Solution: Phase: Architecture and Design■Use a vetted library or framework that does not allow user input to be reflected directly into the page.

Name: Cross Site Scripting (Reflected)

Risk: High

Description: Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-s

Solution: Phase: Architecture and Design■Use a vetted library or framework that does not allo

Name: Cross Site Scripting (Reflected)

Risk: High

Description: Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-s

Solution: Phase: Architecture and Design■Use a vetted library or framework that does not allo

Name: Cross Site Scripting (Reflected)

Risk: High

Description: Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-s

Solution: Phase: Architecture and Design■Use a vetted library or framework that does not allo

Name: Cross Site Scripting (Reflected)

Risk: High

Description: Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-s

Solution: Phase: Architecture and Design■Use a vetted library or framework that does not allo

Name: Cross Site Scripting (Reflected)

Risk: High

Description: Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-s

Solution: Phase: Architecture and Design■Use a vetted library or framework that does not allo

Name: Cross Site Scripting (Reflected)

Risk: High

Description: Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-s

Solution: Phase: Architecture and Design■Use a vetted library or framework that does not allo

Name: Cross Site Scripting (Reflected)

Risk: High

Description: Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-s

Solution: Phase: Architecture and Design■Use a vetted library or framework that does not allo

Name: Cross Site Scripting (Reflected)

Risk: High

Description: Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-s

Solution: Phase: Architecture and Design■Use a vetted library or framework that does not allo

Name: Cross Site Scripting (Reflected)

Risk: High

Description: Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-s

Solution: Phase: Architecture and Design■Use a vetted library or framework that does not allo

Name: Cross Site Scripting (Reflected)

Risk: High

Description: Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-s

Solution: Phase: Architecture and Design■Use a vetted library or framework that does not allo

Name: Cross Site Scripting (Reflected)

Risk: High

Description: Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-s

Solution: Phase: Architecture and Design■Use a vetted library or framework that does not allo

Name: Cross Site Scripting (Reflected)

Risk: High

Description: Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-s

Solution: Phase: Architecture and Design■Use a vetted library or framework that does not allo

Name: Cross Site Scripting (Reflected)

Risk: High

Description: Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-s

Solution: Phase: Architecture and Design■Use a vetted library or framework that does not allo

Name: Cross Site Scripting (Reflected)

Risk: High

Description: Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-s

Solution: Phase: Architecture and Design■Use a vetted library or framework that does not allo

Name: Cross Site Scripting (Reflected)

Risk: High

Description: Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-s

Solution: Phase: Architecture and Design■Use a vetted library or framework that does not allo

Name: Cross Site Scripting (Reflected)

Risk: High

Description: Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-s

Solution: Phase: Architecture and Design■Use a vetted library or framework that does not allo

Name: Cross Site Scripting (Reflected)

Risk: High

Description: Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-s

Solution: Phase: Architecture and Design■Use a vetted library or framework that does not allo

Name: Cross Site Scripting (Reflected)

Risk: High

Description: Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-s

Solution: Phase: Architecture and Design■Use a vetted library or framework that does not allo

Name: Cross Site Scripting (Reflected)

Risk: High

Description: Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-s

Solution: Phase: Architecture and Design■Use a vetted library or framework that does not allo

Name: SQL Injection - MySQL

Risk: High

Description: SQL injection may be possible.

Solution: Do not trust client side input, even if there is client side validation in place.■In gener

Name: SQL Injection - MySQL

Risk: High

Description: SQL injection may be possible.

Solution: Do not trust client side input, even if there is client side validation in place.■In gener

Name: SQL Injection - MySQL

Risk: High

Description: SQL injection may be possible.

Solution: Do not trust client side input, even if there is client side validation in place.■In gener

Name: SQL Injection - MySQL

Risk: High

Description: SQL injection may be possible.

Solution: Do not trust client side input, even if there is client side validation in place.■In gener

Name: SQL Injection - MySQL

Risk: High

Description: SQL injection may be possible.

Solution: Do not trust client side input, even if there is client side validation in place.■In gener

Name: SQL Injection - MySQL

Risk: High

Description: SQL injection may be possible.

Solution: Do not trust client side input, even if there is client side validation in place.■In gener

Name: SQL Injection - MySQL

Risk: High

Description: SQL injection may be possible.

Solution: Do not trust client side input, even if there is client side validation in place.■In gener

Name: SQL Injection - MySQL

Risk: High

Description: SQL injection may be possible.

Solution: Do not trust client side input, even if there is client side validation in place.■In gener

Name: SQL Injection - MySQL

Risk: High

Description: SQL injection may be possible.

Solution: Do not trust client side input, even if there is client side validation in place.■In gener

Name: SQL Injection - MySQL

Risk: High

Description: SQL injection may be possible.

Solution: Do not trust client side input, even if there is client side validation in place.■In gener

Name: SQL Injection - MySQL

Risk: High

Description: SQL injection may be possible.

Solution: Do not trust client side input, even if there is client side validation in place.■In gener

Name: SQL Injection - MySQL

Risk: High

Description: SQL injection may be possible.

Solution: Do not trust client side input, even if there is client side validation in place.■In gener

Name: SQL Injection - MySQL

Risk: High

Description: SQL injection may be possible.

Solution: Do not trust client side input, even if there is client side validation in place.■In gener

Name: SQL Injection - MySQL

Risk: High

Description: SQL injection may be possible.

Solution: Do not trust client side input, even if there is client side validation in place.■In gener

Name: SQL Injection - MySQL

Risk: High

Description: SQL injection may be possible.

Solution: Do not trust client side input, even if there is client side validation in place.■In gener

Name: SQL Injection - MySQL

Risk: High

Description: SQL injection may be possible.

Solution: Do not trust client side input, even if there is client side validation in place.■In gener

Name: SQL Injection - MySQL

Risk: High

Description: SQL injection may be possible.

Solution: Do not trust client side input, even if there is client side validation in place.■In gener

Name: SQL Injection - MySQL

Risk: High

Description: SQL injection may be possible.

Solution: Do not trust client side input, even if there is client side validation in place.■In gener

Name: SQL Injection

Risk: High

Description: SQL injection may be possible.

Solution: Do not trust client side input, even if there is client side validation in place.■In gener

Name: SQL Injection - MySQL

Risk: High

Description: SQL injection may be possible.

Solution: Do not trust client side input, even if there is client side validation in place.■In gener

Name: SQL Injection - MySQL

Risk: High

Description: SQL injection may be possible.

Solution: Do not trust client side input, even if there is client side validation in place.■In gener

Name: SQL Injection - MySQL

Risk: High

Description: SQL injection may be possible.

Solution: Do not trust client side input, even if there is client side validation in place.■In gener

Name: SQL Injection - MySQL

Risk: High

Description: SQL injection may be possible.

Solution: Do not trust client side input, even if there is client side validation in place.■In gener

Name: SQL Injection - MySQL

Risk: High

Description: SQL injection may be possible.

Solution: Do not trust client side input, even if there is client side validation in place.■In gener

Name: XSLT Injection

Risk: Medium

Description: Injection using XSL transformations may be possible, and may allow an attacker

Solution: Sanitize and analyze every user input coming from any client-side.

Name: XSLT Injection

Risk: Medium

Description: Injection using XSL transformations may be possible, and may allow an attacker

Solution: Sanitize and analyze every user input coming from any client-side.

Name: GET for POST

Risk: Informational

Description: A request that was originally observed as a POST was also accepted as a GET.

Solution: Ensure that only POST is accepted where POST is expected.

Name: GET for POST

Risk: Informational

Description: A request that was originally observed as a POST was also accepted as a GET.

Solution: Ensure that only POST is accepted where POST is expected.

Name: GET for POST

Risk: Informational

Description: A request that was originally observed as a POST was also accepted as a GET.

Solution: Ensure that only POST is accepted where POST is expected.



Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:



Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:



Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:



Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: User Agent Fuzzer

Risk: Informational

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites,

Solution:

Name: GET for POST

Risk: Informational

Description: A request that was originally observed as a POST was also accepted as a GET.

Solution: Ensure that only POST is accepted where POST is expected.

Name: GET for POST

Risk: Informational

Description: A request that was originally observed as a POST was also accepted as a GET.

Solution: Ensure that only POST is accepted where POST is expected.