Security Scan Report

Target: http://testphp.vulnweb.com/

Scan Date: 2025-11-13 17:59:56

Framework & Technology Detection

Vulnerability Summary

High: 0 | **Medium: 116** | Low: 172 | Informational: 44

Showing 15 of 332 vulnerabilities. Prioritized by risk level.

Vulnerability Details

Content Security Policy (CSP) Header Not Set (MEDIUM)

URL: http://testphp.vulnweb.com/robots.txt

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attack...

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

Missing Anti-clickjacking Header (MEDIUM)

URL: http://testphp.vulnweb.com/

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

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by yo...

Content Security Policy (CSP) Header Not Set (MEDIUM)

URL: http://testphp.vulnweb.com/sitemap.xml

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attack...

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

Missing Anti-clickjacking Header (MEDIUM)

URL: http://testphp.vulnweb.com/categories.php

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

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by yo...

Missing Anti-clickjacking Header (MEDIUM)

URL: http://testphp.vulnweb.com/artists.php

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

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by yo...

Missing Anti-clickjacking Header (MEDIUM)

URL: http://testphp.vulnweb.com/index.php

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

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by yo...

Content Security Policy (CSP) Header Not Set (MEDIUM)

URL: http://testphp.vulnweb.com/

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attack...

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

Absence of Anti-CSRF Tokens (MEDIUM)

URL: http://testphp.vulnweb.com/

Description: No Anti-CSRF tokens were found in a HTML submission form. A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their know...

Solution: Phase: Architecture and Design Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this w...

Evidence:

Content Security Policy (CSP) Header Not Set (MEDIUM)

URL: http://testphp.vulnweb.com/index.php

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attack...

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

Content Security Policy (CSP) Header Not Set (MEDIUM)

URL: http://testphp.vulnweb.com/artists.php

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attack...

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

Content Security Policy (CSP) Header Not Set (MEDIUM)

URL: http://testphp.vulnweb.com/categories.php

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attack...

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

Absence of Anti-CSRF Tokens (MEDIUM)

URL: http://testphp.vulnweb.com/index.php

Description: No Anti-CSRF tokens were found in a HTML submission form. A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their know...

Solution: Phase: Architecture and Design Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this w...

Evidence:

Absence of Anti-CSRF Tokens (MEDIUM)

URL: http://testphp.vulnweb.com/artists.php

Description: No Anti-CSRF tokens were found in a HTML submission form. A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their know...

Solution: Phase: Architecture and Design Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this w...

Evidence:

Absence of Anti-CSRF Tokens (MEDIUM)

URL: http://testphp.vulnweb.com/categories.php

Description: No Anti-CSRF tokens were found in a HTML submission form. A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their know...

Solution: Phase: Architecture and Design Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this w...

Evidence:

Missing Anti-clickjacking Header (MEDIUM)

URL: http://testphp.vulnweb.com/AJAX/index.php

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

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by yo...