Wapiti scan report

Content Security Policy Configuration

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.

Vulnerability found in /

Description HTTP Request cURL command line

CSP is not set

GET / HTTP/1.1
Host: testhtml5.vulnweb.com

curl "http://testhtml5.vulnweb.com/"

Solutions

Configuring Content Security Policy involves adding the Content-Security-Policy HTTP header to a web page and giving it values to control what resources the user agent is allowed to load for that page.

References

Mozilla: Content Security Policy (CSP)

OWASP: Content Security Policy Cheat Sheet

OWASP: How to do Content Security Policy (PDF)

HTTP Secure Headers

Description

HTTP security headers tell the browser how to behave when handling the website's content.

Vulnerability found in /

Description HTTP Request cURL command line

X-Frame-Options is not set

GET / HTTP/1.1
Host: testhtml5.vulnweb.com

curl "http://testhtml5.vulnweb.com/"

Vulnerability found in /

Description HTTP Request cURL command line
X-XSS-Protection is not set

GET / HTTP/1.1
Host: testhtml5.vulnweb.com

curl "http://testhtml5.vulnweb.com/"

Vulnerability found in /

Description HTTP Request cURL command line
X-Content-Type-Options is not set

GET / HTTP/1.1
Host: testhtml5.vulnweb.com

curl "http://testhtml5.vulnweb.com/"

Vulnerability found in /

Description HTTP Request cURL command line
Strict-Transport-Security is not set

GET / HTTP/1.1
Host: testhtml5.vulnweb.com

curl "http://testhtml5.vulnweb.com/"

Solutions

Use the recommendations for hardening your HTTP Security Headers.

References

Netsparker: HTTP Security Headers: An Easy Way to Harden Your Web Applications

KeyCDN: Hardening Your HTTP Security Headers

OWASP: HTTP SECURITY HEADERS (Protection For Browsers) (PDF)

HttpOnly Flag cookie

Description

HttpOnly is an additional flag included in a Set-Cookie HTTP response header. Using the HttpOnly flag when generating a cookie helps mitigate the risk of client side script accessing the protected cookie (if the browser supports it).

Vulnerability found in /

Description HTTP Request cURL command line

HttpOnly flag is not set in the cookie : username

GET / HTTP/1.1
Host: testhtml5.vulnweb.com

curl "http://testhtml5.vulnweb.com/"

Solutions

While creation of the cookie, make sure to set the HttpOnly Flag to True.

References

OWASP: Testing for Cookies Attributes

OWASP: HttpOnly

Secure Flag cookie

Description

The secure flag is an option that can be set by the application server when sending a new cookie to the user within an HTTP Response. The purpose of the secure flag is to prevent cookies from being observed by unauthorized parties due to the transmission of a the cookie in clear text.

Vulnerability found in /

Description HTTP Request cURL command line

Secure flag is not set in the cookie : username

GET / HTTP/1.1

Host: testhtml5.vulnweb.com

curl "http://testhtml5.vulnweb.com/"

Solutions

When generating the cookie, make sure to set the Secure Flag to True.

References

OWASP: Testing for Cookies Attributes

OWASP: Secure Cookie Attribute
