Wapiti scan report

Wapiti vulnerability report

Target: http://testaspnet.vulnweb.com/

Date of the scan: Tue, 09 Jul 2024 01:57:53 +0000. Scope of the scan: folder

---

Summary

Category	Number of vulnerabilities found
Backup file	0
Blind SQL Injection	0
Weak credentials	0
CRLF Injection	0
Content Security Policy Configuration	1
Cross Site Request Forgery	0
Potentially dangerous file	0
Command execution	0
Path Traversal	0
Htaccess Bypass	0
HTTP Secure Headers	4
HttpOnly Flag cookie	0
Open Redirect	0
Secure Flag cookie	0
SQL Injection	0
Server Side Request Forgery	0
Cross Site Scripting	0
XML External Entity	0
Internal Server Error	0
Resource consumption	0
Fingerprint web technology	0

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: testaspnet.vulnweb.com
```

```
curl "http://testaspnet.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: testaspnet.vulnweb.com
```

```
curl "http://testaspnet.vulnweb.com/"
```

Vulnerability found in /

Description HTTP Request cURL command line

```
X-XSS-Protection is not set
```

```
GET / HTTP/1.1
Host: testaspnet.vulnweb.com
```

```
curl "http://testaspnet.vulnweb.com/"
```

Vulnerability found in /

Description HTTP Request cURL command line

```
X-Content-Type-Options is not set

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

curl "http://testaspnet.vulnweb.com/"
```

Vulnerability found in /

Description HTTP Request cURL command line

```
Strict-Transport-Security is not set

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

curl "http://testaspnet.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)
