Vulnerability Assessment
Summary Report

Submitted By
MuLearn Circle : Cyber Tribe
Code:CYCYBPRN123

Summary

This Vulnerability Assessment report presented by muLean Circle Cyber Tribe contains reports of various vulnerabilities findings present in the website https://demo.testfire.net/

Nikto Scanning

- Nikto v2.5.0

+ Target IP: 65.61.137.117
+ Target Hostname: demo.testfire.net
+ Target Port: 443

+ SSL Info: Subject: /CN=demo.testfire.net
Ciphers: ECDHE-RSA-AES256-GCM-SHA384
Issuer: /C=GB/ST=Greater Manchester/L=Salford/O=Sectigo Limited/CN=Sectigo RSA Domain Validation Secure Server CA
+ Start Time: 2024-03-16 11:57:25 (GMT-4)

+ Server: Apache-Coyote/1.1
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, OPTIONS .
+ HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on the web server.
+ HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.

+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
^X^Z
zsh: suspended nikto -h https://demo.testfire.net/

Nmap

Nmap scan report for 65.61.137.117
Host is up (0.29s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp   open   http
443/tcp open   https
8080/tcp open   http-proxy
8443/tcp closed https-alt

└─# nmap -sT -sV 65.61.137.117
Starting Nmap 7.94SVN (https://nmap.org) at 2024-03-17 00:54 EDT
Nmap scan report for 65.61.137.117
Host is up (0.32s latency).
Not shown: 987 filtered tcp ports (no-response), 10 filtered tcp ports (host-unreach)
PORT   STATE SERVICE VERSION
80/tcp   open http   Apache Tomcat/Coyote JSP engine 1.1
443/tcp open ssl/http Apache Tomcat/Coyote JSP engine 1.1
8080/tcp open http   Apache Tomcat/Coyote JSP engine 1.1

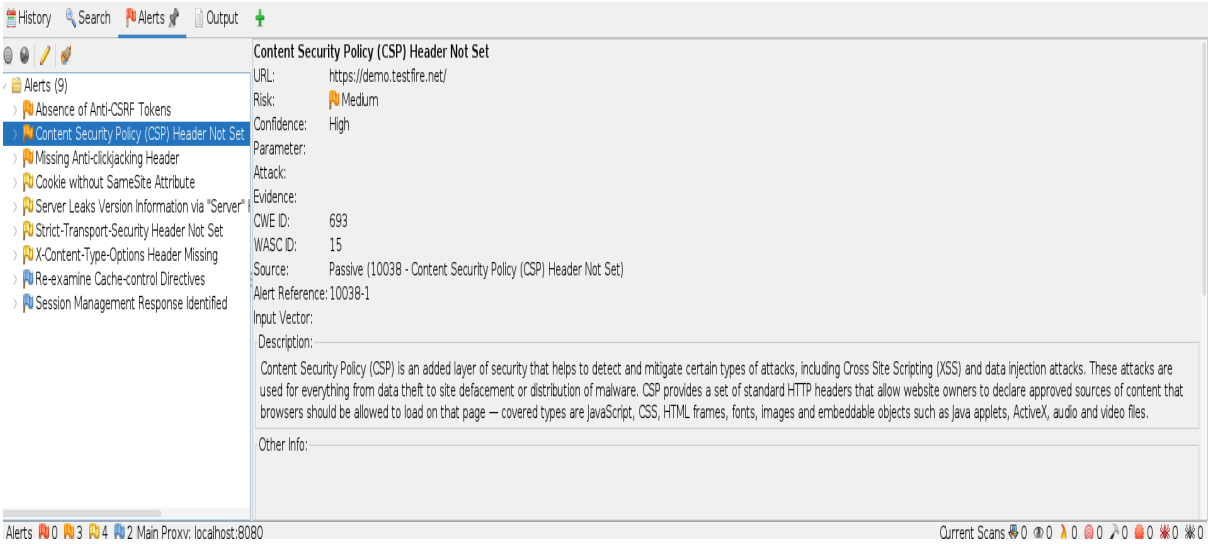
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 138.30 seconds

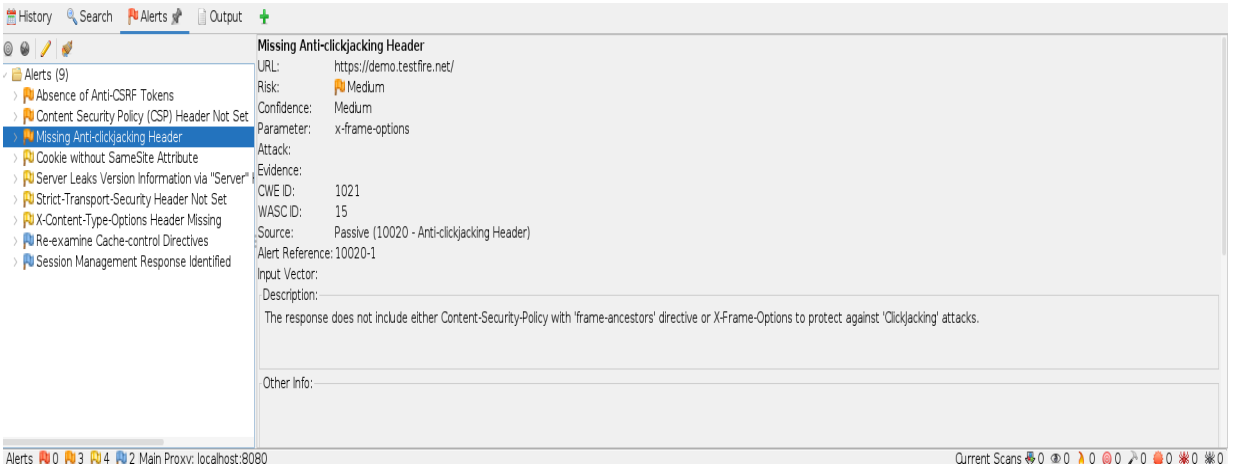
Testssl

LOGJAM (CVE-2015-4000), experimental VULNERABLE (NOT ok): common prime: RFC2409/Oakley Group 2 (1024 bits),
                                      but no DH EXPORT ciphers

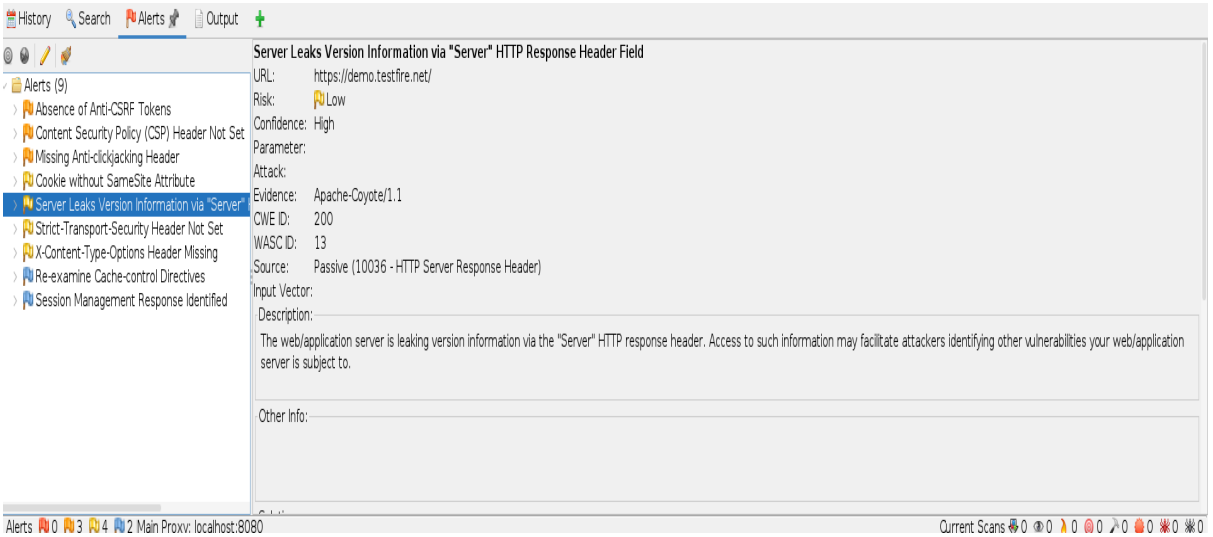
ZAP

Severity:Medium
Confidence:High
Host:https://demo.testfire.net//

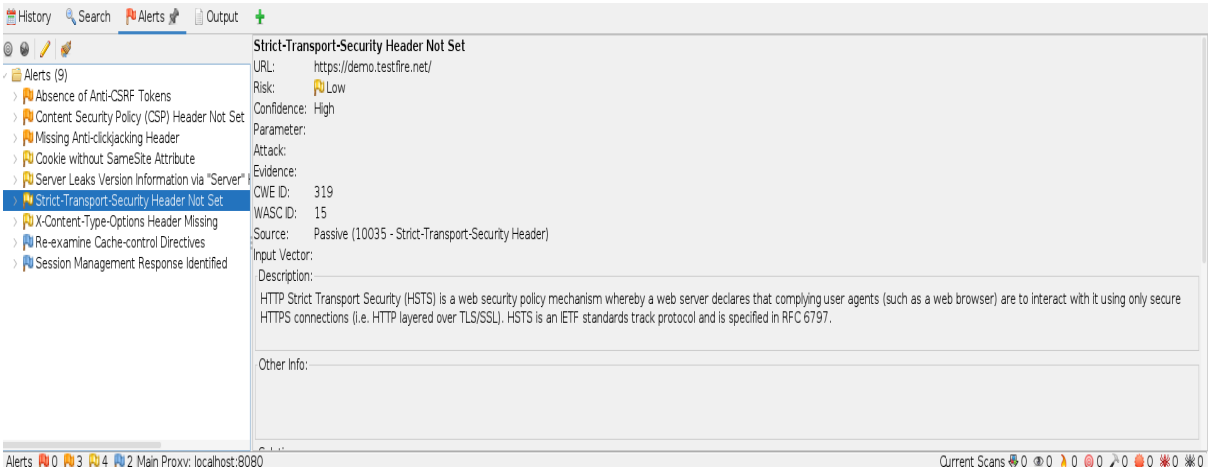



History
Search
Alerts
Output
Alerts (9)
Absence of Anti-CSRF Tokens
Content Security Policy (CSP) Header Not Set
Missing Anti-clickjacking Header
Cookie without SameSite Attribute
Server Leaks Version Information via "Server"
Strict-Transport-Security Header Not Set
X-Content-Type-Options Header Missing
Re-examine Cache-control Directives
Session Management Response Identified
Missing Anti-clickjacking Header
URL: https://demo.testfire.net/
Risk: Medium
Confidence: Medium
Parameter: x-frame-options
Attack:
Evidence:
CWE ID: 1021
WASC ID: 15
Source: Passive (10020 - Anti-clickjacking Header)
Alert Reference: 10020-1
Input Vector:
Description:
The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'Clickjacking' attacks.
Other Info:
Alerts 0 3 4 2 Main Proxy: localhost:8080
Current Scans 0 0 0 0 0 0 0 0 0


History
Search
Alerts
Output
Alerts (9)
Absence of Anti-CSRF Tokens
Content Security Policy (CSP) Header Not Set
Missing Anti-clickjacking Header
Cookie without SameSite Attribute
Server Leaks Version Information via "Server"
Strict-Transport-Security Header Not Set
X-Content-Type-Options Header Missing
Re-examine Cache-control Directives
Session Management Response Identified
Cookie without SameSite Attribute
URL: https://demo.testfire.net/
Risk: Low
Confidence: Medium
Parameter: JSESSIONID
Attack:
Evidence: Set-Cookie: JSESSIONID
CWE ID: 1275
WASC ID: 13
Source: Passive (10054 - Cookie without SameSite Attribute)
Input Vector:
Description:
A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Other Info:
Alerts 0 3 4 2 Main Proxy: localhost:8080
Current Scans 0 0 0 0 0 0 0 0 0


History
Search
Alerts
Output
Alerts (9)
Absence of Anti-CSRF Tokens
Content Security Policy (CSP) Header Not Set
Missing Anti-clickjacking Header
Cookie without SameSite Attribute
Server Leaks Version Information via "Server"
Strict-Transport-Security Header Not Set
X-Content-Type-Options Header Missing
Re-examine Cache-control Directives
Session Management Response Identified
Server Leaks Version Information via "Server" HTTP Response Header Field
URL: https://demo.testfire.net/
Risk: Low
Confidence: High
Parameter:
Attack:
Evidence: Apache-Coyote/1.1
CWE ID: 200
WASC ID: 13
Source: Passive (10036 - HTTP Server Response Header)
Input Vector:
Description:
The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Other Info:
Alerts 0 3 4 2 Main Proxy: localhost:8080
Current Scans 0 0 0 0 0 0 0 0 0


History
Search
Alerts
Output
Alerts (9)
Absence of Anti-CSRF Tokens
Content Security Policy (CSP) Header Not Set
Missing Anti-clickjacking Header
Cookie without SameSite Attribute
Server Leaks Version Information via "Server"
Strict-Transport-Security Header Not Set
X-Content-Type-Options Header Missing
Re-examine Cache-control Directives
Session Management Response Identified
Re-examine Cache-control Directives
URL: https://demo.testfire.net/
Risk: Informational
Confidence: Low
Parameter: cache-control
Attack:
Evidence:
CWE ID: 525
WASC ID: 13
Source: Passive (10015 - Re-examine Cache-control Directives)
Input Vector:
Description:
The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Other Info:
Alerts 0 3 4 2 Main Proxy: localhost:8080
Current Scans 0 0 0 0 0 0 0 0 0


History
Search
Alerts
Output
Alerts (9)
Absence of Anti-CSRF Tokens
Content Security Policy (CSP) Header Not Set
Missing Anti-clickjacking Header
Cookie without SameSite Attribute
Server Leaks Version Information via "Server"
Strict-Transport-Security Header Not Set
X-Content-Type-Options Header Missing
Re-examine Cache-control Directives
Session Management Response Identified
Strict-Transport-Security Header Not Set
URL: https://demo.testfire.net/
Risk: Low
Confidence: High
Parameter:
Attack:
Evidence:
CWE ID: 319
WASC ID: 15
Source: Passive (10035 - Strict-Transport-Security Header)
Input Vector:
Description:
HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Other Info:
Alerts 0 3 4 2 Main Proxy: localhost:8080
Current Scans 0 0 0 0 0 0 0 0 0


History
Search
Alerts
Output
Alerts (9)
Absence of Anti-CSRF Tokens
Content Security Policy (CSP) Header Not Set
Missing Anti-clickjacking Header
Cookie without SameSite Attribute
Server Leaks Version Information via "Server"
Strict-Transport-Security Header Not Set
X-Content-Type-Options Header Missing
Re-examine Cache-control Directives
Session Management Response Identified
Session Management Response Identified
URL: https://demo.testfire.net/
Risk: Informational
Confidence: Medium
Parameter: JSESSIONID
Attack:
Evidence: D3889EB246ED53B24D17B1D86F7D8150
CWE ID:
WASC ID:
Source: Passive (10112 - Session Management Response Identified)
Input Vector:
Description:
The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Other Info:
cookie:JSESSIONID
Alerts 0 3 4 2 Main Proxy: localhost:8080
Current Scans 0 0 0 0 0 0 0 0 0


History
Search
Alerts
Output
Alerts (9)
Absence of Anti-CSRF Tokens
Content Security Policy (CSP) Header Not Set
Missing Anti-clickjacking Header
Cookie without SameSite Attribute
Server Leaks Version Information via "Server"
Strict-Transport-Security Header Not Set
X-Content-Type-Options Header Missing
Re-examine Cache-control Directives
Session Management Response Identified
X-Content-Type-Options Header Missing
URL: https://demo.testfire.net/
Risk: Low
Confidence: Medium
Parameter: x-content-type-options
Attack:
Evidence:
CWE ID: 693
WASC ID: 15
Source: Passive (10021 - X-Content-Type-Options Header Missing)
Input Vector:
Description:
The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Other Info:
This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.
At "High" threshold this scan rule will not alert on client or server error responses.
Alerts 0 3 4 2 Main Proxy: localhost:8080
Current Scans 0 0 0 0 0 0 0 0 0