TASK 1 -: You can visit Portswigger labs and Choose any 5 lab of them and solve it.

1- Vulnerabilities -:

1- Stored XSS into HTML context with nothing encoded.

2- Reflected XSS into HTML context with nothing encoded.

3- DOM XSS in document.

4 - DOM XSS in inner HTML.

5- DOM XSS in jQuery anchor

2- Description -: Cross site scripting is a type of computer security vulnerability, the attacker aims to execute malicious script in a web browser of the victim by including malicious code a legitimate web page of web application.

DOM XSS -: DOM-based XSS vulnerabilities usually arise when JavaScript takes data from an attacker-controllable source, such as the URL, and passes it to a sink that supports dynamic code execution, such **as eval() or innerHTML. This enables attackers to execute** malicious JavaScript, which typically allows them to hijack other users' accounts.

3- Severity -: Average

4– Instance -:

Vuln 1 - Submit a comment that calls the alert function when the blog post - URl - https://0a7e00f003d1396080c494d600cd0081.web-security-academy.net/post/comment/confirmation?postId=9.

Vuln 2 - I am perform a cross-site scripting attack that calls the alert function in search box.

Vuln 3 – First I'm entering alphanumeric words into search box

Then I will Right-click and inspect the element, and observe that your random string has been placed inside an `img src` attribute.

Vuln 4 - When I Enter the `<img src=1 onerror=alert(1)>` Into the search box:

Vuln 5 - I am perform the query parameter return Path to the feedback

And I am pass the query “acds1234”

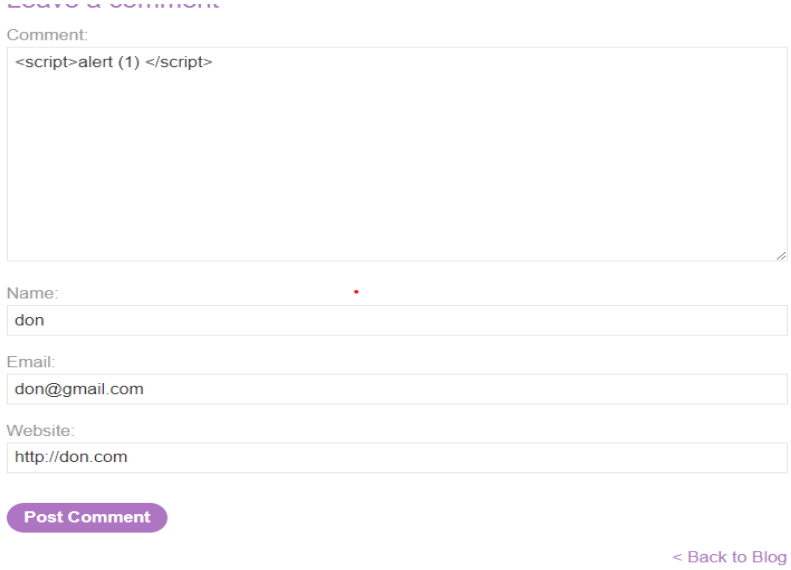
Right-click and inspect the element, and observe that your random string has been placed inside a href attribute.

Then I Change return Path to “javascript:alert(document.cookie)”

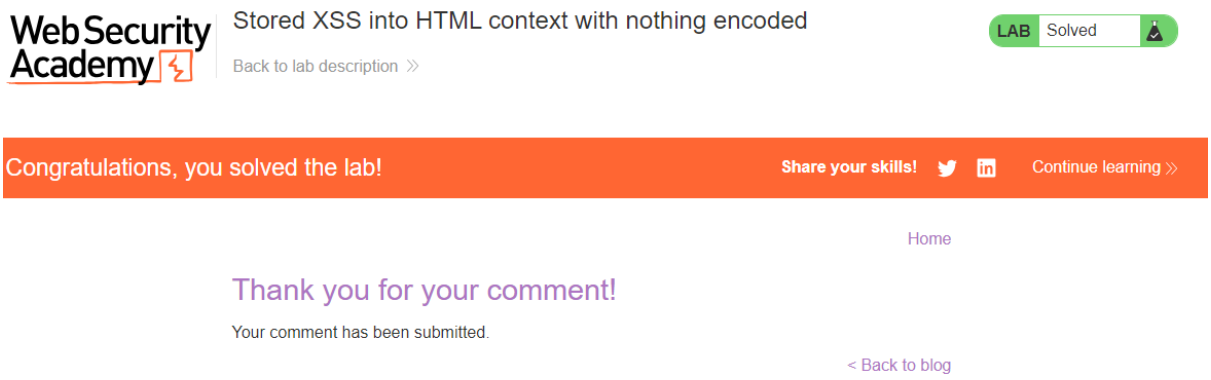
3-POC (Proof of concept) - :

1 - Stored XSS into HTML context with nothing encoded.

1 - First I trying to put alert function in comment box in the blog post



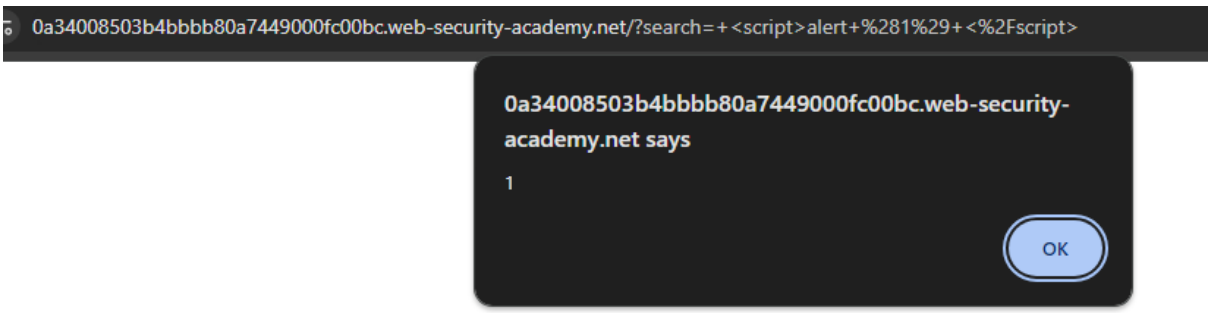
Then finally I’m success in Alert function as you can see

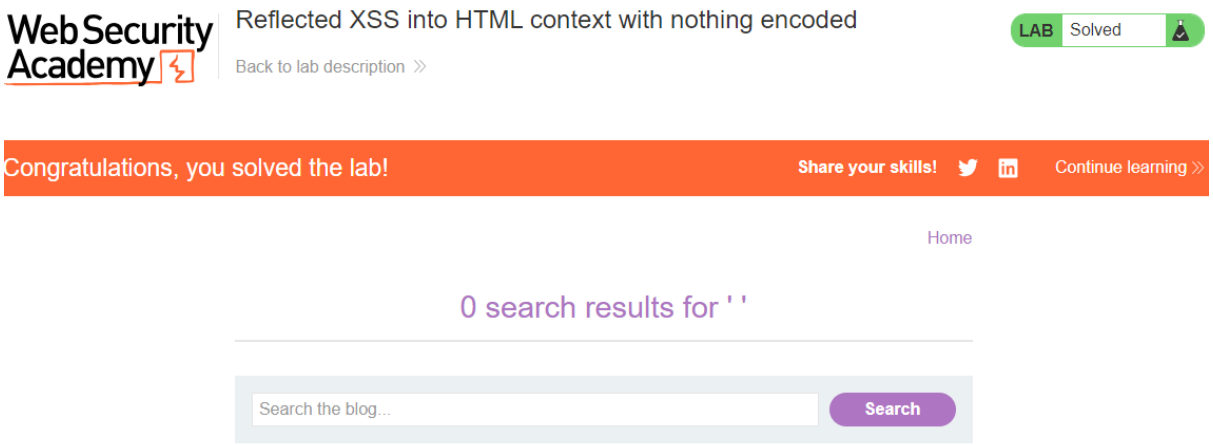


Vulnerability 2 - Reflected XSS into HTML context with nothing encoded.

– First I trying to put alert function in search box.

Then finally I'm success in Alert function as you can see



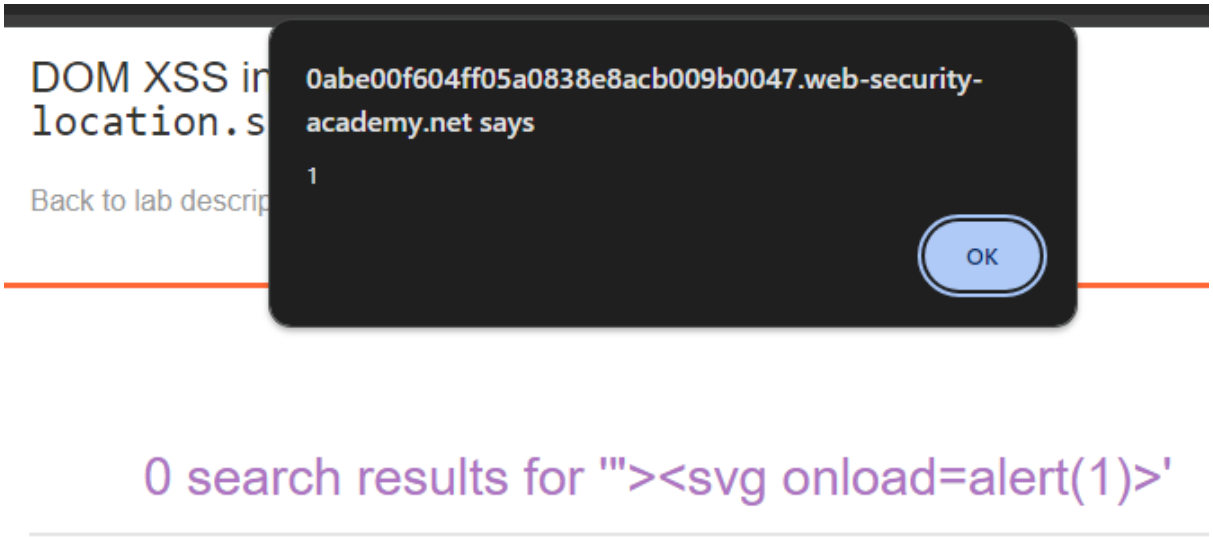


Vulnerability 3 - **DOM XSS in** document

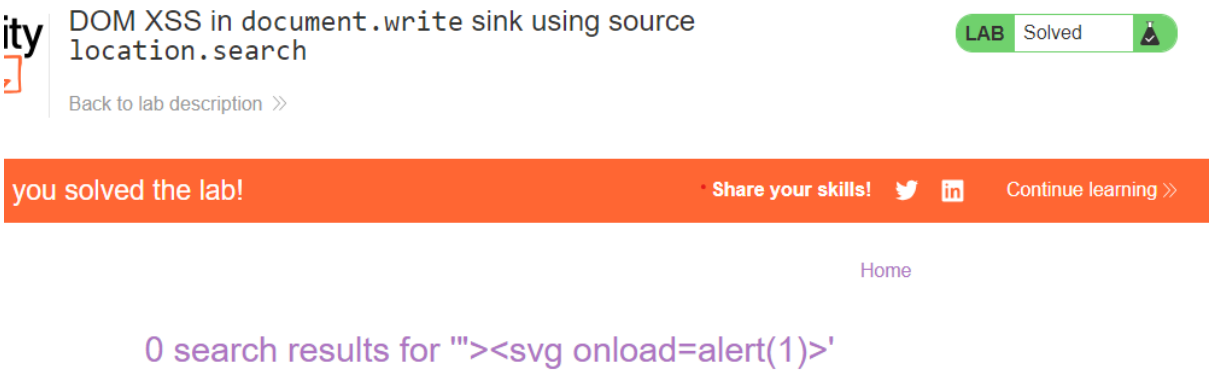
Step – I am trying to submit random alphanumeric word in search box. When I right click inspect the element Then I am observing that my string has been placed inside an img src.

As you can see

After I am putting our "><svg onload=alert(1)> command in search box



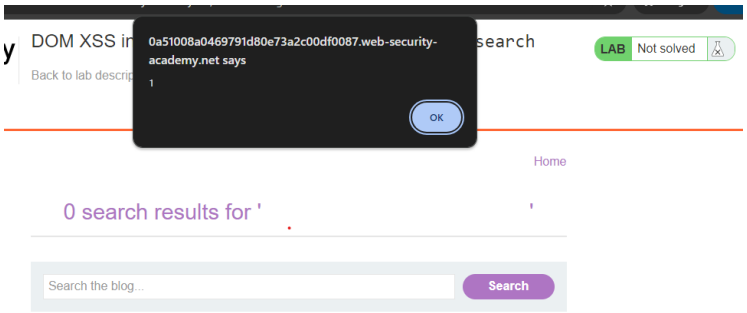
Then I m received a pop msg its indicate our alert function run successful



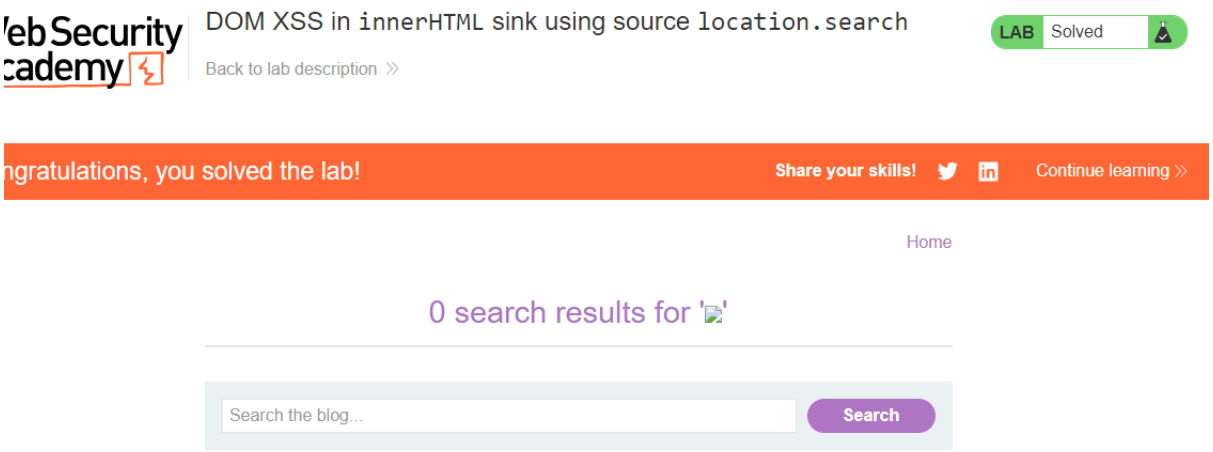
Vulnerability 4 - DOM XSS in inner HTML.

When I Enter the `<img src=1 onerror=alert(1)>` Into the search box:

I am received a pop up



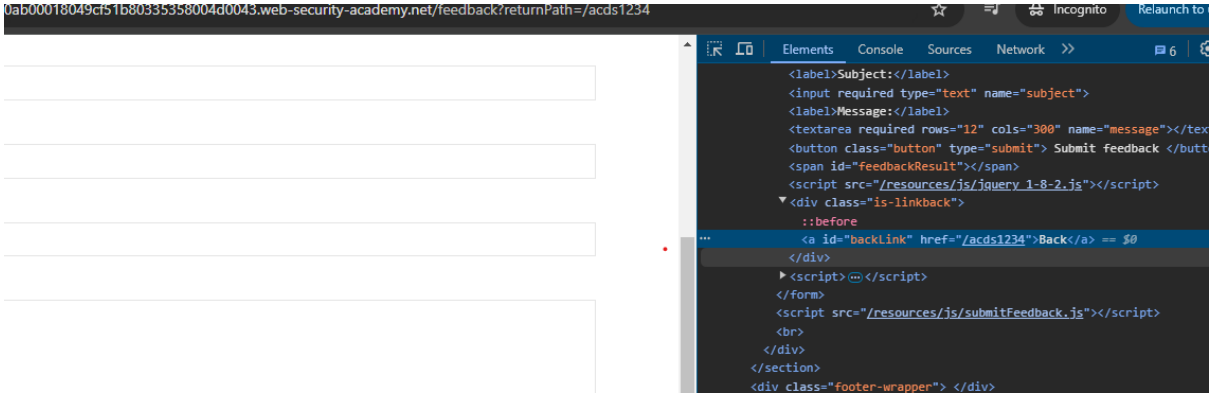
And finally I am succeed as you can see



Vulnerability 5 - DOM XSS in jQuery anchor

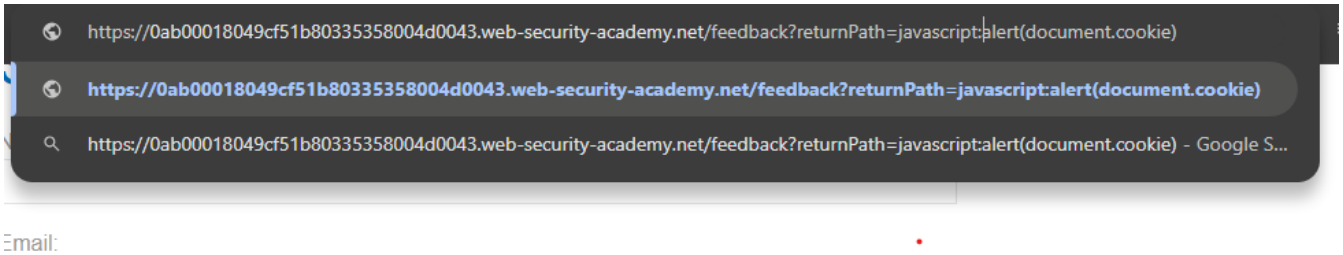
I am perform the query parameter returnPath to the feedback

And I m pass the query "acds1234"

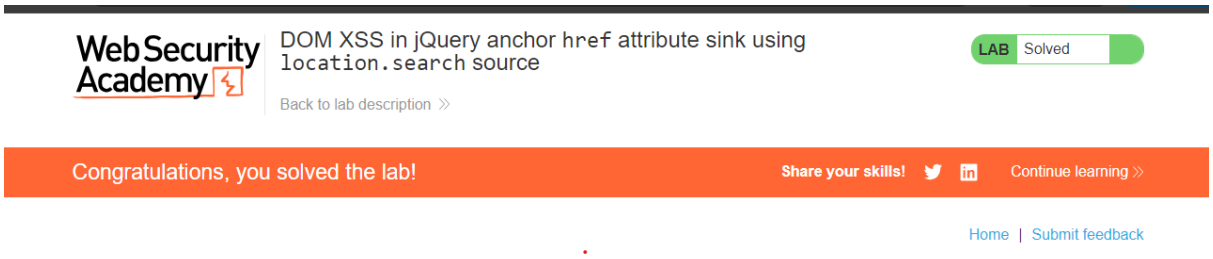


Right-click and inspect the element, and observe that your random string has been placed inside an a href attribute.

Then I Change return Path to "javascript:alert(document.cookie)"



Finally I am succeed. As you can see



6- Impact - :

- Open Redirection
- Session Hijack
- Phishing
- Defacement
- Cookie Stealing.

Task 2 – Find three high vulnerability in http://zero.webappsecurity.com

1-: Vulnerability –

- **SSL Version 2 and 3 Protocol Detection** - CVSS v3.0 Base Score: 9.8
- **SSL Medium Strength Cipher Suites Supported (SWEET32)** - CVSS v3.0 Base Score: 7.5
- **HSTS Missing from HTTPS server** – CVSS v3.0 Base Score: 6.5.
- **TLS Version 1.0 protocol Detection** - CVSS v3.0 Base Score: 6.5.
- **JQuery 1.2 < 3.5.0 Multiple XSS** - CVSS v3.0 Base Score: 6.1.

Vuln1 -: SSL Version 2 and 3 Protocol Detection - CVSS v3.0 Base Score: 9.8

Severity -: Critical.

Description -: The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including.

Impact - An insecure padding scheme with CBC ciphers. Insecure session renegotiation and resumption schemes. An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Mitigation -: Consult the application's documentation to disable SSL 2.0 and 3.0.
Use TLS 1.2 (with approved cipher suites) or higher instead

Vuln2 -: SSL Medium Strength Cipher Suites Supported (SWEET32) - CVSS v3.0 Base Score: 7.5

Severity -: Medium

Description -: The remote host support the use ciphers that offer medium strength encryption.

Impact - That it is the affected application easier to circumvent medium strength encryption if the attacker is on the same physical network.

Mitigation -: Reconfigure the affected application if possible to avoid use of medium strength cipher.

Vuln3 -: HSTS Missing from HTTPS server – CVSS v3.0 Base Score: 6.5.

Severity -: Medium

Description -: The remote web server is not enforcing HSTS, as defined by RFC 6797.

HSTS is an optional response header that can be configure on the server to instruction the browser to only communicate via HTTPS. The lack of HSTS allows downloading attacks, SSL-stripping **man-in-the-middle-attack**, and weakens cookies-hijacking protecting

Impact - SSL-stripping **man-in-the-middle-attack**, and weakens cookies-hijacking protecting

Mitigation -: Configure the remote web server to use HSTS

Vuln4 -: TLS Version 1.0 protocol Detection - CVSS v3.0 Base Score: 6.5.

Severity -: Medium

Description -: The remote service accept connections encrypted using TLS 1.0.

TLS 1.0 has a number of cryptographic design flaws. Modern emplacements of TLS 1.0 mitigate these problems. But newer version of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible

Impact - PCI DSS v3.2 required that TLS 1.0 be disabled entirely by june 30, 2018.Except for POI terminal that can be verified as not being susceptible any known exploits.

Mitigation -: Upgrading to a current, secure version of TLS that is implemented securely and configured to not accept fall back to SSL or early TLS.

Encrypting data with strong cryptography before sending over SSL/early TLS.

Setting up a strongly-encrypted session first (e.g. IPsec tunnel), then sending data over SSL within secure tunnel

Vuln5 -: JQuery 1.2 < 3.5.0 Multiple XSS - CVSS v3.0 Base Score: 6.1.

Severity -: Medium

Description -: According to the self-reported version in the script, The version on JQuery hosted web server is greater than or equal to 1.2 and prior to 3.5.0.

Impact - It is therefore, effected by multiple cross side scripting vulnerabilities.

Mitigation -: Upgrade to JQuery version 3.5.0 or latest.

Step to reproduce -:

- First I'm used **NIkto** tool for finding Vulnerability in my target website.

  Nikto –h http://zero.webappsecurity.com

- Then I trying to find hidden folder in target with the help of **gobuster** penetration testing tool.

  Gobuster –timeout 30s dir –u http://zero.webappsecurity.com –w /usr/share/wrodlists/dirb/big.txt –x txt,zip,php,html.

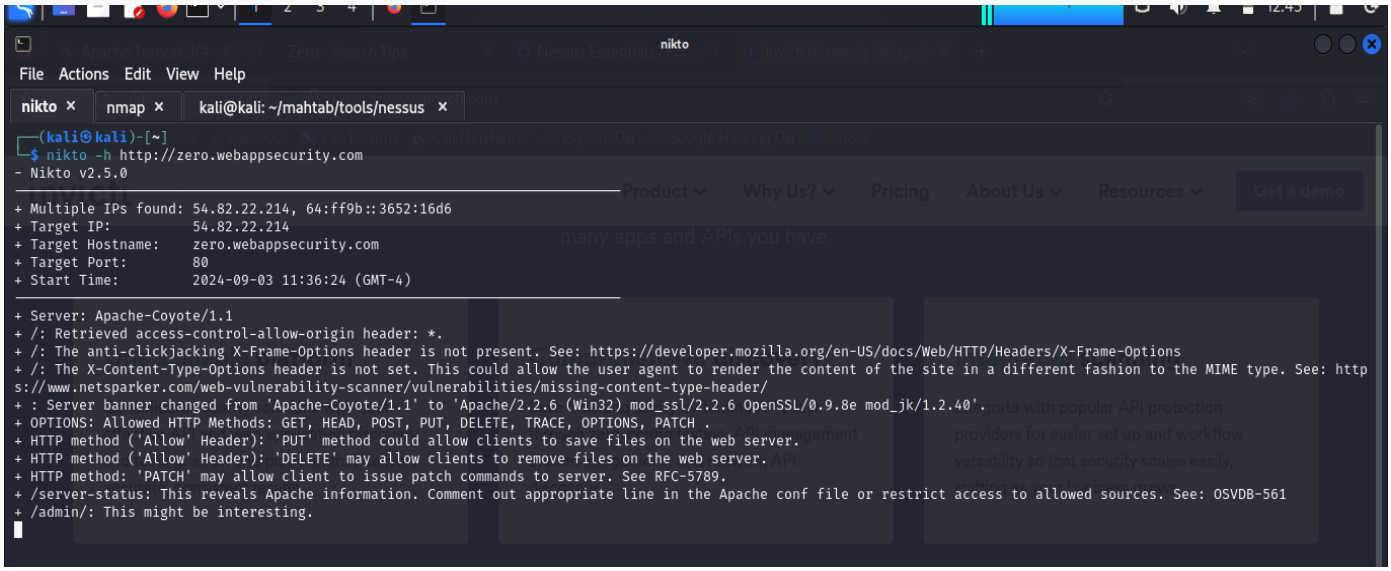
  And amazingly I'm finding some important hidden file - **/cgi.zip , /debug.txt , /feedback.html, /index.html , / login.html**. we can use for gain unauthorised access.

- Then I'm used **nmap** for gain some other information of the target website. Where I find some port, services, and week point's in system. **Like – port (80, 443 & 8080)**. Where I **seeing Tomcat Jsp engine running on port 80**. Then I'm checking on **exploit db** we got the **CVV** and other details related this vulnerability.

- Then finally I'm using **Nessus** tools for finding some other's vulnerability I target system. And I got some valuable and week point in target system. And I'm finding some other vulnerability with the help of Nessus tool.

POC -:

Nikto -



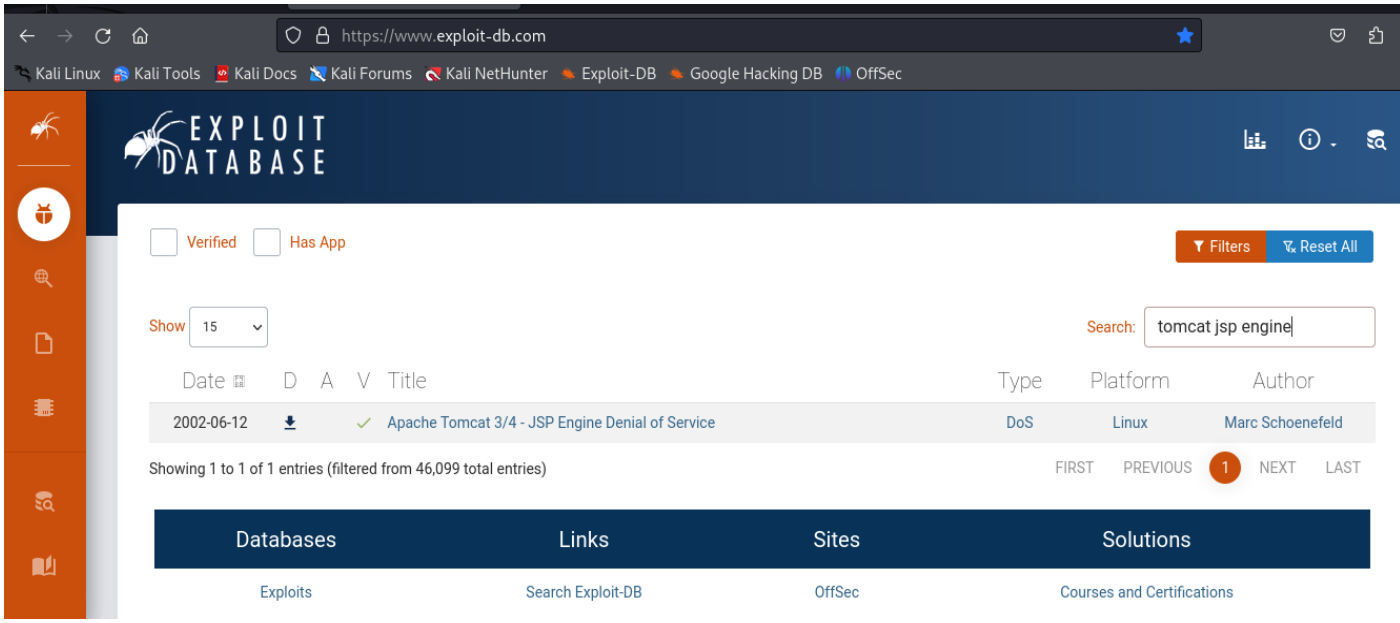
Gobuster -:

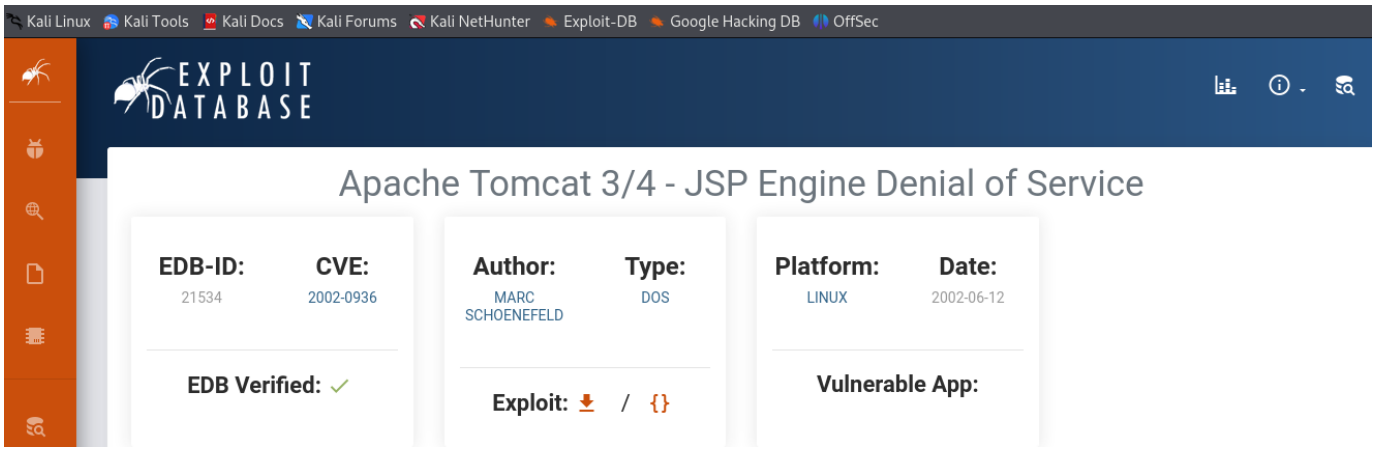
```
File  Actions  Edit  View  Help
nikto ×   nmap ×   nessus ×   gobuster ×   kali@kali: /usr/share/wordlists ×

┌──(kali㉿kali)-[~/Downloads]
└─$ gobuster --timeout 30s dir -u http://zero.webappsecurity.com -w /usr/share/wordlists/dirb/big.txt -x txt,php,zip,html
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://zero.webappsecurity.com
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              txt,php,zip,html
[+] Timeout:                 30s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/103.html             (Status: 503) [Size: 323]
/104.txt              (Status: 503) [Size: 323]
/106.txt              (Status: 503) [Size: 323]
/106.html             (Status: 503) [Size: 323]
/10668.txt            (Status: 503) [Size: 323]
```

Nmap -:

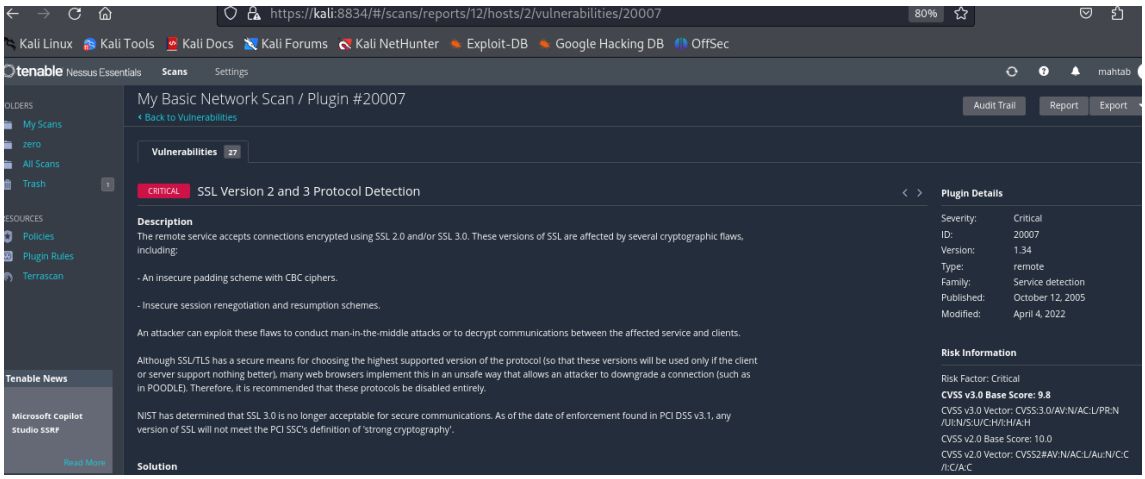
```
┌──(kali㉿kali)-[~/mahtab/project1]
└─$ cat zero.txt
# Nmap 7.94SVN scan initiated Tue Sep  3 11:44:59 2024 as: nmap -A -T4 -oN zero.txt 54.82.22.214
Nmap scan report for ec2-54-82-22-214.compute-1.amazonaws.com (54.82.22.214)
Host is up (0.42s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE  VERSION
80/tcp   open  http     Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Zero - Personal Banking - Loans - Credit Cards
| http-methods:
|_  Potentially risky methods: PUT DELETE TRACE PATCH
|_http-server-header: Apache-Coyote/1.1
443/tcp  open  ssl/http Apache httpd 2.2.6 ((Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40)
| http-methods:
|_  Potentially risky methods: TRACE
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|_    SSL2_RC4_128_WITH_MD5
|_http-title: Site doesn't have a title (text/html).
| ssl-cert: Subject: commonName=zero.webappsecurity.com/organizationName=Micro Focus LLC/stateOrProvinceName=California/countryName=US
| Subject Alternative Name: DNS:zero.webappsecurity.com
| Not valid before: 2021-04-26T00:00:00
|_Not valid after:  2022-05-04T23:59:59
|_ssl-date: 2024-09-03T15:51:43+00:00; +5m25s from scanner time.
8080/tcp open  http     Apache Tomcat/Coyote JSP engine 1.1
| http-server-header: Apache-Coyote/1.1
```

Exploit dB -:


https://www.exploit-db.com
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
EXPLOIT DATABASE
Verified Has App
Filters Reset All
Show 15
Search: tomcat jsp engine
Date D A V Title Type Platform Author
2002-06-12 Apache Tomcat 3/4 - JSP Engine Denial of Service DoS Linux Marc Schoenefeld
Showing 1 to 1 of 1 entries (filtered from 46,099 total entries)
FIRST PREVIOUS 1 NEXT LAST
Databases Links Sites Solutions
Exploits Search Exploit-DB OffSec Courses and Certifications


Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
EXPLOIT DATABASE
Apache Tomcat 3/4 - JSP Engine Denial of Service
EDB-ID: 21534
CVE: 2002-0936
Author: MARC SCHOENEFELD
Type: DOS
Platform: LINUX
Date: 2002-06-12
EDB Verified:
Exploit: / {}
Vulnerable App:

Nessus -:


https://kali:8834/#/scans/reports/12/hosts/2/vulnerabilities/20007
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
tenable Nessus Essentials Scans Settings
My Basic Network Scan / Plugin #20007
Back to Vulnerabilities
Audit Trail Report Export
Vulnerabilities 27
CRITICAL SSL Version 2 and 3 Protocol Detection
Description
The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:
- An insecure padding scheme with CBC ciphers.
- Insecure session renegotiation and resumption schemes.
An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.
Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.
NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.
Solution
Plugin Details
Severity: Critical
ID: 20007
Version: 1.34
Type: remote
Family: Service detection
Published: October 12, 2005
Modified: April 4, 2022
Risk Information
Risk Factor: Critical
CVSS v3.0 Base Score: 9.8
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS v2.0 Base Score: 10.0
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
My Scans
zero
All Scans
Trash
Policies
Plugin Rules
Terrascan
Tenable News
Microsoft Copilot Studio SSRF
Read More

https://kali:8834/#/scans/reports/12/hosts/2/vulnerabilities/42873

Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec

tenable Nessus Essentials | Scans | Settings | mahtab

FOLDERS
- My Scans
- zero
- All Scans
- Trash

RESOURCES
- Policies
- Plugin Rules
- Terrascan

Tenable News

The Data-Factor: Why Integrating

My Basic Network Scan / Plugin #42873

Back to Vulnerabilities

Audit Trail | Report | Export

Vulnerabilities 27

HIGH **SSL Medium Strength Cipher Suites Supported (SWEET32)**

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

See Also

https://www.openssl.org/blog/blog/2016/08/24/sweet32/
https://sweet32.info

Plugin Details

Severity:	High
ID:	42873
Version:	1.21
Type:	remote
Family:	General
Published:	November 23, 2009
Modified:	February 3, 2021

Risk Information

Risk Factor: Medium
CVSS v3.0 Base Score: 7.5
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

My Basic Network Scan / Plugin #142960

Back to Vulnerabilities

Audit Trail | Report

Vulnerabilities 27

MEDIUM **HSTS Missing From HTTPS Server (RFC 6797)**

Description

The remote web server is not enforcing HSTS, as defined by RFC 6797. HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

Solution

Configure the remote web server to use HSTS.

See Also

https://tools.ietf.org/html/rfc6797

Output

Plugin Details

Severity:	Medium
ID:	142960
Version:	1.12
Type:	remote
Family:	Web Servers
Published:	November 17, 202
Modified:	March 22, 2024

Risk Information

Risk Factor: Medium
CVSS v3.0 Base Score: 6.5

MEDIUM **TLS Version 1.0 Protocol Detection**

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

Solution

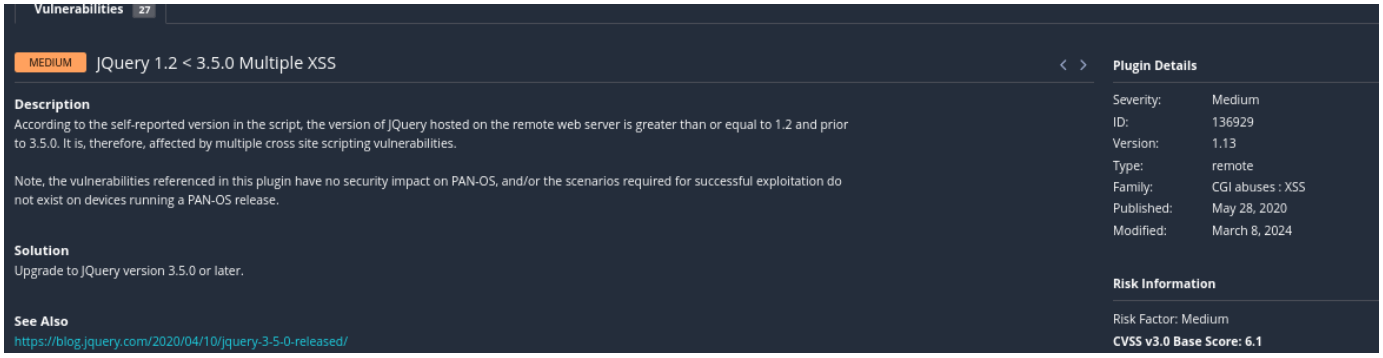
Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Plugin Details

Severity:	Medium
ID:	104743
Version:	1.10
Type:	remote
Family:	Service detection
Published:	November 22, 2017
Modified:	April 19, 2023

Risk Information

Risk Factor: Medium
CVSS v3.0 Base Score: 6.5



Vulnerabilities 27

MEDIUM JQuery 1.2 < 3.5.0 Multiple XSS

Description

According to the self-reported version in the script, the version of JQuery hosted on the remote web server is greater than or equal to 1.2 and prior to 3.5.0. It is, therefore, affected by multiple cross site scripting vulnerabilities.

Note, the vulnerabilities referenced in this plugin have no security impact on PAN-OS, and/or the scenarios required for successful exploitation do not exist on devices running a PAN-OS release.

Solution

Upgrade to JQuery version 3.5.0 or later.

See Also

https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/

Plugin Details

Severity:	Medium
ID:	136929
Version:	1.13
Type:	remote
Family:	CGI abuses : XSS
Published:	May 28, 2020
Modified:	March 8, 2024

Risk Information

Risk Factor: Medium

CVSS v3.0 Base Score: 6.1

Task 3 – Find one high vulnerability in http://testasp.vulnweb.com

Vulnerability -:

- **Dnsmasq Heap Overflow and Null-pointer Dereference on TFTP `Server` - `CVE-2009-2957`.**
- **Cross side scripting.**

`Vuln -1`

Severity -: Medium CVV score

`Description -:` Dnsmasq is a lightweight DNS forwarder and DHCP server. A vulnerabilityhas been found that may allow an attacker to execute arbitrary code on
Servers or home routers running dnsmasq[1] with the TFTP service[2][3] enabled.

`Impact -`Chances of successful exploitation increase when a long directory prefix is used for TFTP.

`References*`

```
[1] http://www.thekelleys.org.uk/dnsmasq/doc.html
[2] http://www.isi.edu/in-notes/ien/ien133.txt
[3]http://en.wikipedia.org/wiki/Trivial_File_Transfer_Protocol
```

`Mitigation -:` If the TFTP service is enabled and patching is not available Immediately, a valid workaround is to filter TFTP for untrusted hosts in the network (such as the Internet). This is the default configuration

when enabling TFTP on most home routers.

Steps To Reproduce:

- I'm using **nslookup** for finding IP address or other details.
- Then using **Nikto** tool for finding vulnerability.
- Then I'm used **NMAP** for gathering important information.
  Where is finding open port's 53 where i got **dnsmasq 2.51**.
  This is valuable vulnerability for hacker where hacker used for gain unauthorized access or other's things.

- Then I'm search on this vulnerability's dnsmasq 2.51 on **Exploitdb**.
  Where I'm saw dnsmasq exploit.

POC -:

Nslookup -

```
┌──(kali㉿kali)-[~/mahtab/project1/task2]
└─$ nslookup http://testasp.vulnweb.com
Server:         192.168.9.52
Address:        192.168.9.52#53

Non-authoritative answer:
Name:   http://testasp.vulnweb.com
Address: 44.228.249.3
Name:   http://testasp.vulnweb.com
Address: 64:ff9b::2ce4:f903
```

Nikto -:

```
┌──(kali㉿kali)-[~/mahtab/project1/task2]
└─$ nikto -h http://testasp.vulnweb.com
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 44.238.29.244, 64:ff9b::2cee:1df4
+ Target IP:          44.238.29.244
+ Target Hostname:    testasp.vulnweb.com
+ Target Port:        80
+ Start Time:         2024-09-05 12:15:59 (GMT-4)
---------------------------------------------------------------------------
+ Server: Microsoft-IIS/8.5
+ /: Retrieved x-powered-by header: ASP.NET.
+ /: 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 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: http
s://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /: Cookie ASPSESSIONIDQCSCQTRD created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /KRWesSvg.aspx: Retrieved x-aspnet-version header: 2.0.50727.
+ RFC-1918 /aspnet_client: IP address found in the 'location' header. The IP is "10.0.0.14". See: https://portswigger.net/kb/issues/00600300_private-ip-addresses-discl
osed
+ /aspnet_client: The web server may reveal its internal or real IP in the Location header via a request to with HTTP/1.0. The value is "10.0.0.14". See: http://cve.mi
tre.org/cgi-bin/cvename.cgi?name=CVE-2000-0649
+ OPTIONS: Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST .
+ OPTIONS: Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST .
```

Nmap -:

```
┌──(kali㉿kali)-[~/mahtab/project1/task2]
└─$ sudo nmap 192.168.9.52 -A -T4
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-05 12:35 EDT
Nmap scan report for 192.168.9.52
Host is up (0.0022s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
53/tcp open  domain  dnsmasq 2.51
| dns-nsid:
|_  bind.version: dnsmasq-2.51
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (95%), QEMU (91%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (95%), QEMU user mode network gateway (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
```

Exploit-DB-:

Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec

EXPLOIT DATABASE

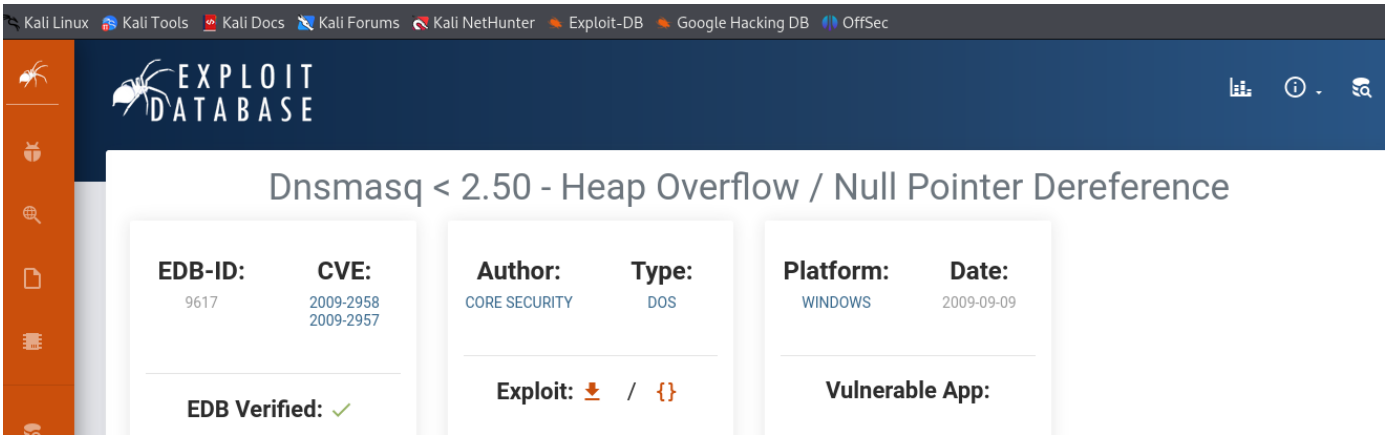
Verified | Has App | Filters | Reset All

Show 15 | Search: dnsmasq 2.5

Date	D	A	V	Title	Type	Platform	Author
2009-09-09			✓	Dnsmasq < 2.50 - Heap Overflow / Null Pointer Dereference	DoS	Windows	Core Security

Showing 1 to 1 of 1 entries (filtered from 46,099 total entries)

FIRST PREVIOUS 1 NEXT LAST



Vuln-2 -

Severity -: High

Description -: There is a cross-site scripting vulnerability on the login page of http://testasp.vulnweb.com and various regions, due to improper escaping on the URL path.

Impact - This is a high impact vulnerability as this affects the login page.

References-

- https://www.starbucks.com/account/signin
- https://www.starbucks.co.uk/account/signin

Mitigation -: An attacker can easily abuse this bug to steal user passwords, inject malicious JavaScript into the context of www.http://testasp.vulnweb.com.
Implement HTML encoding / escaping on the path.

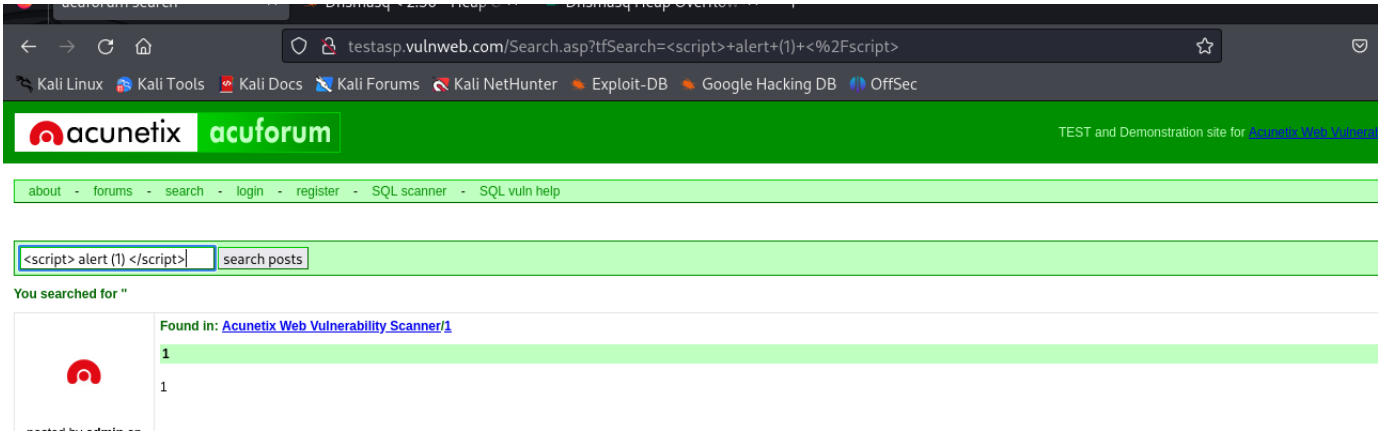
Steps To Reproduce:

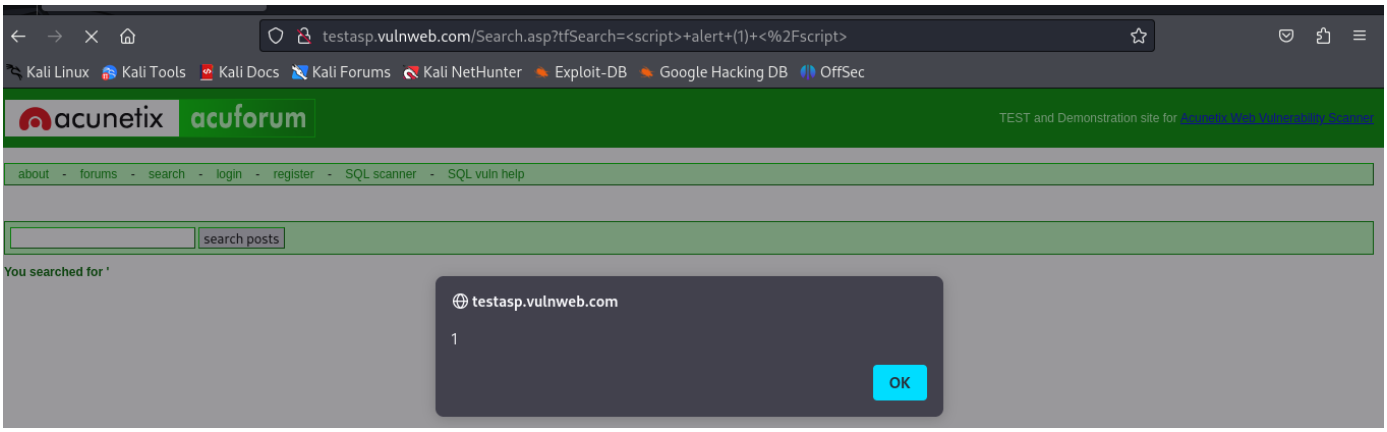
Step -1 Open Chrome or Firefox.

Step -2 visit www.http://testasp.vulnweb.com.

Step -3 The XSS will trigger and you'll get an alert() with the value of document.domain.

POC -:


testasp.vulnweb.com/Search.asp?tfSearch=<script>+alert+(1)+<%2Fscript>
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
acunetix acuforum
TEST and Demonstration site for
about - forums - search - login - register - SQL scanner - SQL vuln help
<script> alert (1) </script>
search posts
You searched for "
Found in: Acunetix Web Vulnerability Scanner/1
1
1


testasp.vulnweb.com/Search.asp?tfSearch=<script>+alert+(1)+<%2Fscript>
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
acunetix acuforum
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
about - forums - search - login - register - SQL scanner - SQL vuln help
search posts
You searched for '
testasp.vulnweb.com
1
OK