

## **Ethical Hacking Internship**

**Sakshi Gawande**

**Institutional Affiliation :** Internship Studio

**-:Task-2:-**

**Task:** Find 3 Critical Vulnerabilities of

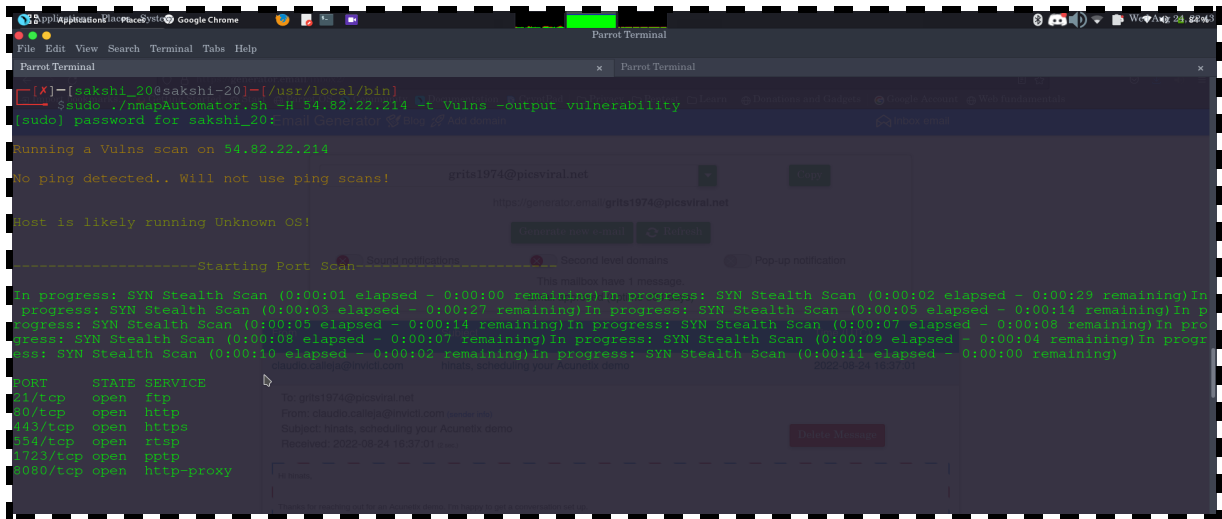
“<http://zero.webappsecurity.com/> ” website.

**Due Date :** August 24, 2022

## # Find 3 Critical Vulnerabilities of

“<http://zero.webappsecurity.com/>” website.

### ❖ Ports Scanning

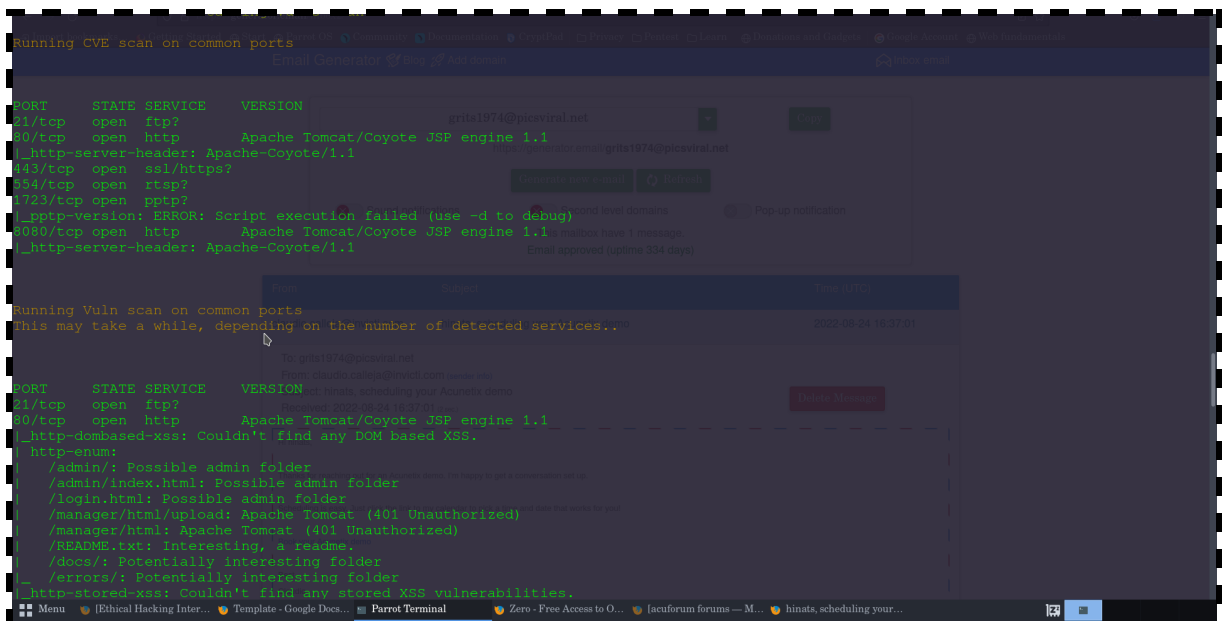


```
[*]-[sakshi_20@sakshi-20]-[/usr/local/bin]
[sudo] ~$ sudo ./nmapAutomator.sh -H 54.82.22.214 -t Vulns -o output vulnerability
[sudo] password for sakshi_20: 
Running a Vulns scan on 54.82.22.214
No ping detected.. Will not use ping scans!
Host is likely running Unknown OS!

-----Starting Port Scan-----
In progress: SYN Stealth Scan (0:00:01 elapsed - 0:00:00 remaining)In progress: SYN Stealth Scan (0:00:02 elapsed - 0:00:29 remaining)In progress: SYN Stealth Scan (0:00:03 elapsed - 0:00:27 remaining)In progress: SYN Stealth Scan (0:00:05 elapsed - 0:00:14 remaining)In progress: SYN Stealth Scan (0:00:05 elapsed - 0:00:14 remaining)In progress: SYN Stealth Scan (0:00:07 elapsed - 0:00:08 remaining)In progress: SYN Stealth Scan (0:00:08 elapsed - 0:00:07 remaining)In progress: SYN Stealth Scan (0:00:09 elapsed - 0:00:04 remaining)In progress: SYN Stealth Scan (0:00:10 elapsed - 0:00:02 remaining)In progress: SYN Stealth Scan (0:00:11 elapsed - 0:00:00 remaining)

PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
443/tcp   open  https
554/tcp   open  rtsp
1723/tcp  open  pptp
8080/tcp  open  http-proxy
```

### ❖ 1st Vulnerability



```
Running CVE scan on common ports
PORT      STATE SERVICE  VERSION
21/tcp    open  ftp?
80/tcp    open  http     Apache Tomcat/Coyote JSP engine 1.1
_ftp-server-header: Apache-Coyote/1.1
443/tcp   open  ssl/https?
554/tcp   open  rtsp?
1723/tcp  open  pptp?
_pptp-version: ERROR: Script execution failed (use -d to debug)
8080/tcp  open  http     Apache Tomcat/Coyote JSP engine 1.1
_http-server-header: Apache-Coyote/1.1

Running Vuln scan on common ports
This may take a while, depending on the number of detected services...
PORT      STATE SERVICE  VERSION
21/tcp    open  ftp?
80/tcp    open  http     Apache Tomcat/Coyote JSP engine 1.1
_http-dombased-xss: Couldn't find any DOM based XSS.
_http-enum:
/admin/: Possible admin folder
/admin/index.html: Possible admin folder
/login.html: Possible admin folder
/manager/html/upload: Apache Tomcat (401 Unauthorized)
/manager/html: Apache Tomcat (401 Unauthorized)
/README.txt: Interesting, a readme
/docs/: Potentially interesting folder
/errors/: Potentially interesting folder
_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
```

```

Parrot Terminal
File Edit View Search Terminal Tabs Help

The SSL protocol 3.0, as used in OpenSSL through 1.0.11 and other
products, uses nondeterministic CBC padding, which makes it easier
for man-in-the-middle attackers to obtain cleartext data via a
padding-oracle attack, aka the "POODLE" issue.

Disclosure date: 2014-10-14
Check results:
  TLS_RSA_WITH_AES_128_CBC_SHA
References:
  https://www.securityfocus.com/bid/70374
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
  https://www.imperialviolet.org/2014/10/14/poodle.html
  https://www.openssl.org/~bodo/ssl-poodle.pdf
http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
54/tcp open  rtsp?
1723/tcp open  RSTP?
http-version: ERROR: Script execution failed (use -d to debug)
8080/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
http-stored-xss: Couldn't find any stored XSS vulnerabilities.
http-enum:
  /admin/: Possible admin folder
  /admin/index.html: Possible admin folder
  /login.html: Possible admin folder
  /manager/html/upload: Apache Tomcat (401 Unauthorized)
  /manager/html: Apache Tomcat (401 Unauthorized)
  /README.txt: Interesting, a readme.
  /docs/: Potentially interesting folder
  /errors/: Potentially interesting folder
http-server-header: Apache-Coyote/1.1
http-csrf:
  Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=ec2-54-82-22-214.compute-1.amazonaws.com
  Found the following possible CSRF vulnerabilities:
    Path: http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/
    Form id: searchterm
    Form action: /search.html
http-dombased-xss: Couldn't find any DOM based XSS.

```

→ Vulnerable

```

Parrot Terminal
File Edit View Search Terminal Tabs Help

Scanning application launchers
Removing duplicate launchers or broken launchers
Launchers are updated
[sakshi_20@sakshi-20]~$
$dirb http://zero.webappsecurity.com/

DIRB v2.22
By The Dark Raver

START TIME: Wed Aug 24 11:11:23 2022
URL_BASE: http://zero.webappsecurity.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

---- Scanning URL: http://zero.webappsecurity.com/ ----
  http://zero.webappsecurity.com/admin (CODE:302|SIZE:0)
  http://zero.webappsecurity.com/cgi-bin (CODE:302|SIZE:0)
  http://zero.webappsecurity.com/cgi-bin/ (CODE:403|SIZE:961)
  http://zero.webappsecurity.com/docs (CODE:302|SIZE:0)
  http://zero.webappsecurity.com/errors (CODE:302|SIZE:0)
  http://zero.webappsecurity.com/help (CODE:302|SIZE:0)
  http://zero.webappsecurity.com/include (CODE:302|SIZE:0)
  http://zero.webappsecurity.com/index.html (CODE:200|SIZE:12471)
  http://zero.webappsecurity.com/manager (CODE:302|SIZE:0)
  http://zero.webappsecurity.com/resources (CODE:302|SIZE:0)
  http://zero.webappsecurity.com/server-status (CODE:200|SIZE:5523)

END TIME: Wed Aug 24 11:32:04 2022
DOWNLOADED: 4612 - FOUND: 11
[sakshi_20@sakshi-20]~$
$dirb http://zero.webappsecurity.com/

```

→ Vulnerable

Site: <http://zero.webappsecurity.com>  
Generated on Tue, 23 Aug 2022 18:53:02

### Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	4
Low	1
Informational	0
False Positives:	0

### Alerts

Name	Risk Level	Number of Instances
<a href="#">Absence of Anti-CSRF Tokens</a>	Medium	6
<a href="#">Cross-Domain Misconfiguration</a>	Medium	16
<a href="#">Missing Anti-clickjacking Header</a>	Medium	6
<a href="#">Vulnerable JS Library</a>	Medium	2
<a href="#">X-Content-Type-Options Header Missing</a>	Low	10

### Alert Detail

Medium	Absence of Anti-CSRF Tokens
Description	<p>No Anti-CSRF tokens were found in a HTML submission form.</p> <p>A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf.</p> <p>CSRF attacks are effective in a number of situations, including:</p> <ul style="list-style-type: none"> <li>* The victim has an active session on the target site.</li> <li>* The victim is authenticated via HTTP auth on the target site.</li> <li>* The victim is on the same local network as the target site.</li> </ul> <p>CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.</p>
URL	<a href="http://zero.webappsecurity.com">http://zero.webappsecurity.com</a>
Method	GET
Parameter	

→ Vulnerable

### Address

- 54.82.22.214 (ipv4)

### Hostnames

- zero.webappsecurity.com (user)
- ec2-54-82-22-214.compute-1.amazonaws.com (PTR)

### Ports

The 65353 ports scanned but not shown below are in state: **filtered**

- 65353 ports replied with: **no-responses**

Port	State (toggle closed [0]   filtered [0])	Service	Reason	Product	Version	Extra info
80	tcp open	http	syn-ack			
443	tcp open	https	syn-ack			
8080	tcp open	http-proxy	syn-ack			

## ❖ 2nd Vulnerability

Low (CVSS: 2.6) NVT: OpenSSL: ECDSA Private Key Leak (CVE-2011-1945) - Windows
<b>Product detection result</b> cpe:/a:openssl:openssl:0.9.8t Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
<b>Summary</b> OpenSSL leaks ECDSA private key through a remote timing attack.
<b>Vulnerability Detection Result</b> Installed version: 0.9.8t Fixed version: None Installation path / port: 80/tcp

## ❖ 3rd Vulnerabilities

Medium (CVSS: 4.3) NVT: Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability
<b>Product detection result</b> cpe:/a:apache:http_server:2.2.6 Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.117232)
<b>Summary</b> Apache HTTP Server is prone to a cookie information disclosure vulnerability.
<b>Vulnerability Detection Result</b> Vulnerability was detected according to the Vulnerability Detection Method.
<b>Impact</b> Successful exploitation will allow attackers to obtain sensitive information that may aid in further attacks.