Experiment 6

Student Name: Sahul Kumar Parida **UID: 20BCS4919**
Branch: CSE **Section/Group: WM-904/B**
Semester: 5th **Date of Performance: 08/11/2022**
Subject Name: Web and Mobile Security Lab
Subject Code: 20CSP-333

Aim:

Perform Penetration testing on a web application to gather information about the system (Foot Printing).

Objective:

To perform penetration testing and foot printing on any Web Application.

Software/Hardware Requirements:

Kali Linux, D-tech tools or any pen Testing tools and any platform using Python 2.7

Tools to be used:

1. D-Tech

2. NMAP

3. Metasploit

4. Wire Shark

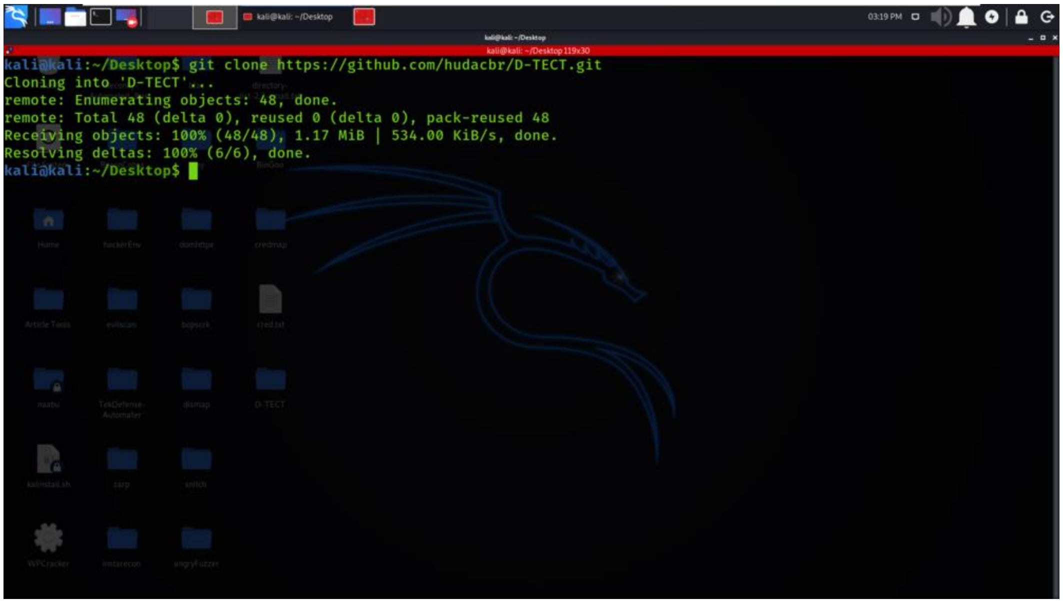
Introduction:

Web application penetration testing is the practice of simulating attacks on a system in an attempt to gain access to sensitive data, with the purpose of determining whether a system is secure. These attacks are performed either internally or externally on a system, and they help provide information about the target system, identify vulnerabilities within them, and uncover exploits that could actually compromise the system. It is an essential health check of a system that informs testers whether remediation and security measures are needed.

Steps/Method/Coding:

Installation of D-TECT Tool on Kali Linux OS
Step 1: Use the following command to install the tool in your Kali Linux operating system.

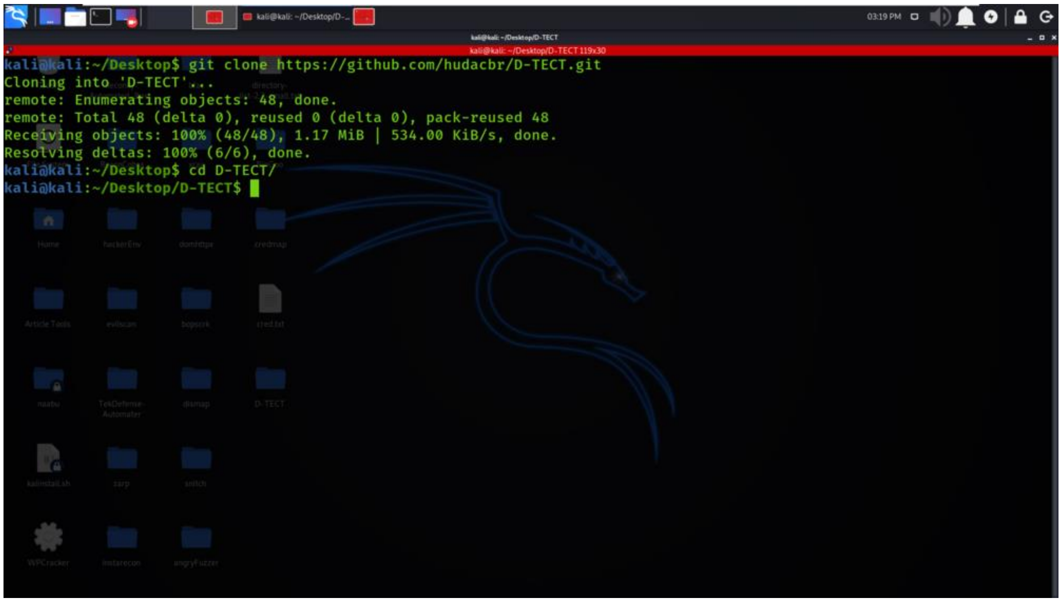
git clone https://github.com/shawarkhanethicalhacker/D-TECT-1.git



```
kali@kali:~/Desktop$ git clone https://github.com/hudacbr/D-TECT.git
Cloning into 'D-TECT'...
remote: Enumerating objects: 48, done.
remote: Total 48 (delta 0), reused 0 (delta 0), pack-reused 48
Receiving objects: 100% (48/48), 1.17 MiB | 534.00 KiB/s, done.
Resolving deltas: 100% (6/6), done.
kali@kali:~/Desktop$ 
```

Step 2: Now use the following command to move into the directory of the tool. You have to move in the directory in order to run the tool.

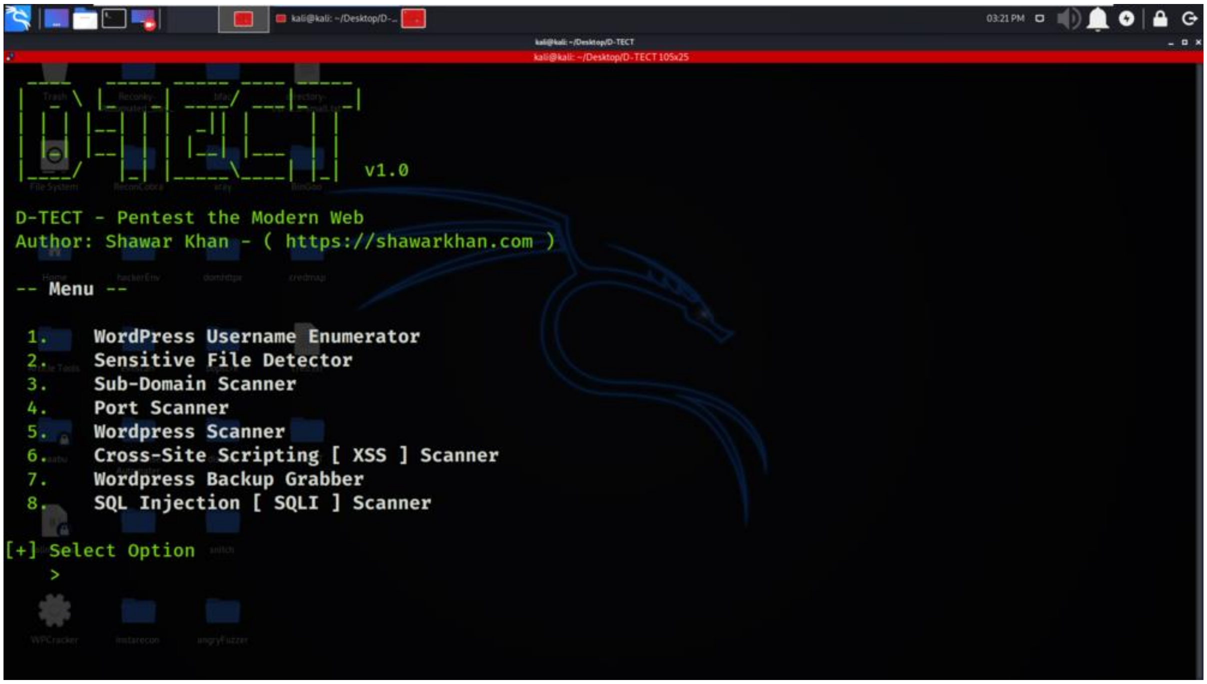
cd D-TECT-1


kali@kali: ~/Desktop/D-...
03:19 PM
kali@kali: ~/Desktop/D-TECT
kali@kali: ~/Desktop/D-TECT 119x30

```
kali@kali:~/Desktop$ git clone https://github.com/hudacbr/D-TECT.git
Cloning into 'D-TECT'...
remote: Enumerating objects: 48, done.
remote: Total 48 (delta 0), reused 0 (delta 0), pack-reused 48
Receiving objects: 100% (48/48), 1.17 MiB | 534.00 KiB/s, done.
Resolving deltas: 100% (6/6), done.
kali@kali:~/Desktop$ cd D-TECT/
kali@kali:~/Desktop/D-TECT$ 
```

Step 3: Now you are in the directory of the tool. Use the following command to run the tool.

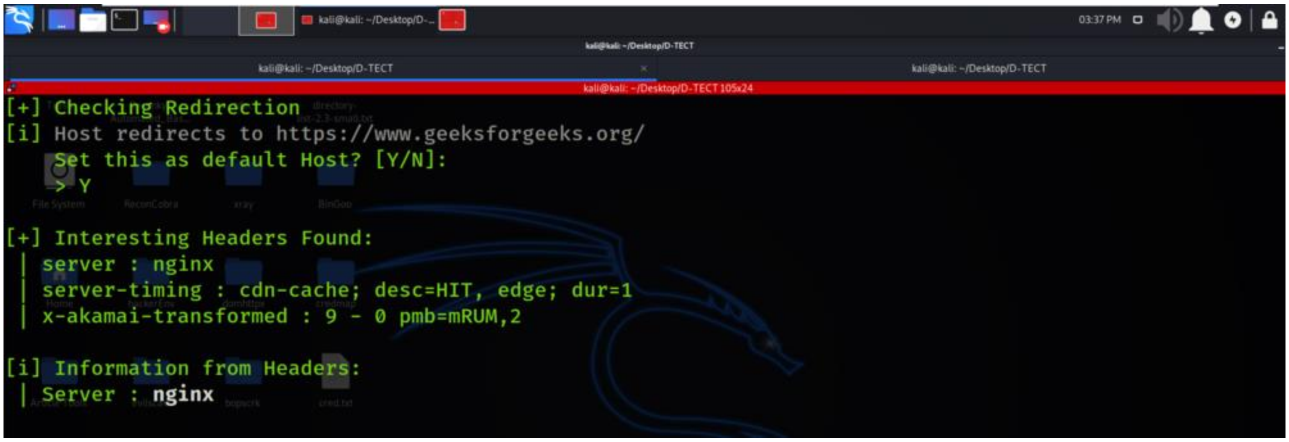
./d-tect.py


kali@kali: ~/Desktop/D-TECT
kali@kali: ~/Desktop/D-TECT 105x25
03:21 PM

```
                                         v1.0

D-TECT - Pentest the Modern Web
Author: Shawar Khan - ( https://shawarkhan.com )

-- Menu --

 1.    WordPress Username Enumerator
 2.    Sensitive File Detector
 3.    Sub-Domain Scanner
 4.    Port Scanner
 5.    Wordpress Scanner
 6.    Cross-Site Scripting [ XSS ] Scanner
 7.    Wordpress Backup Grabber
 8.    SQL Injection [ SQLI ] Scanner

[+] Select Option
    >
```

Working with D-TECT Tool on Kali Linux OS
Example 1: Banner Grabbing
Select Option 1

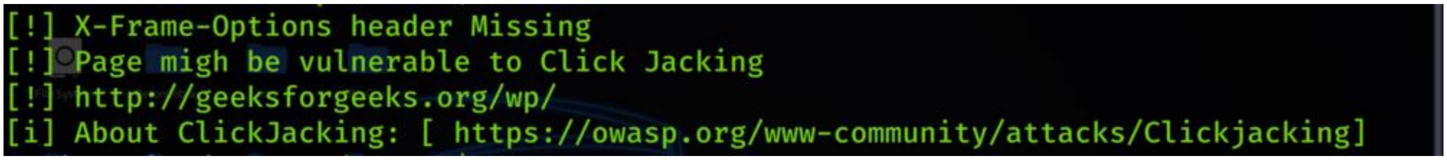
Tool have gathered the Banner Information about the target domain geeksforgeeks.org


kali@kali: ~/Desktop/D-TECT
kali@kali: ~/Desktop/D-TECT
kali@kali: ~/Desktop/D-TECT
kali@kali: ~/Desktop/D-TECT 105x24
03:37 PM

```
[+] Checking Redirection
[i] Host redirects to https://www.geeksforgeeks.org/
    Set this as default Host? [Y/N]:
    > Y

[+] Interesting Headers Found:
 | server : nginx
 | server-timing : cdn-cache; desc=HIT, edge; dur=1
 | x-akamai-transformed : 9 - 0 pmb=mRUM,2

[i] Information from Headers:
 | Server : nginx
```

Example 2: ClickJacking Detection
Select Option 5

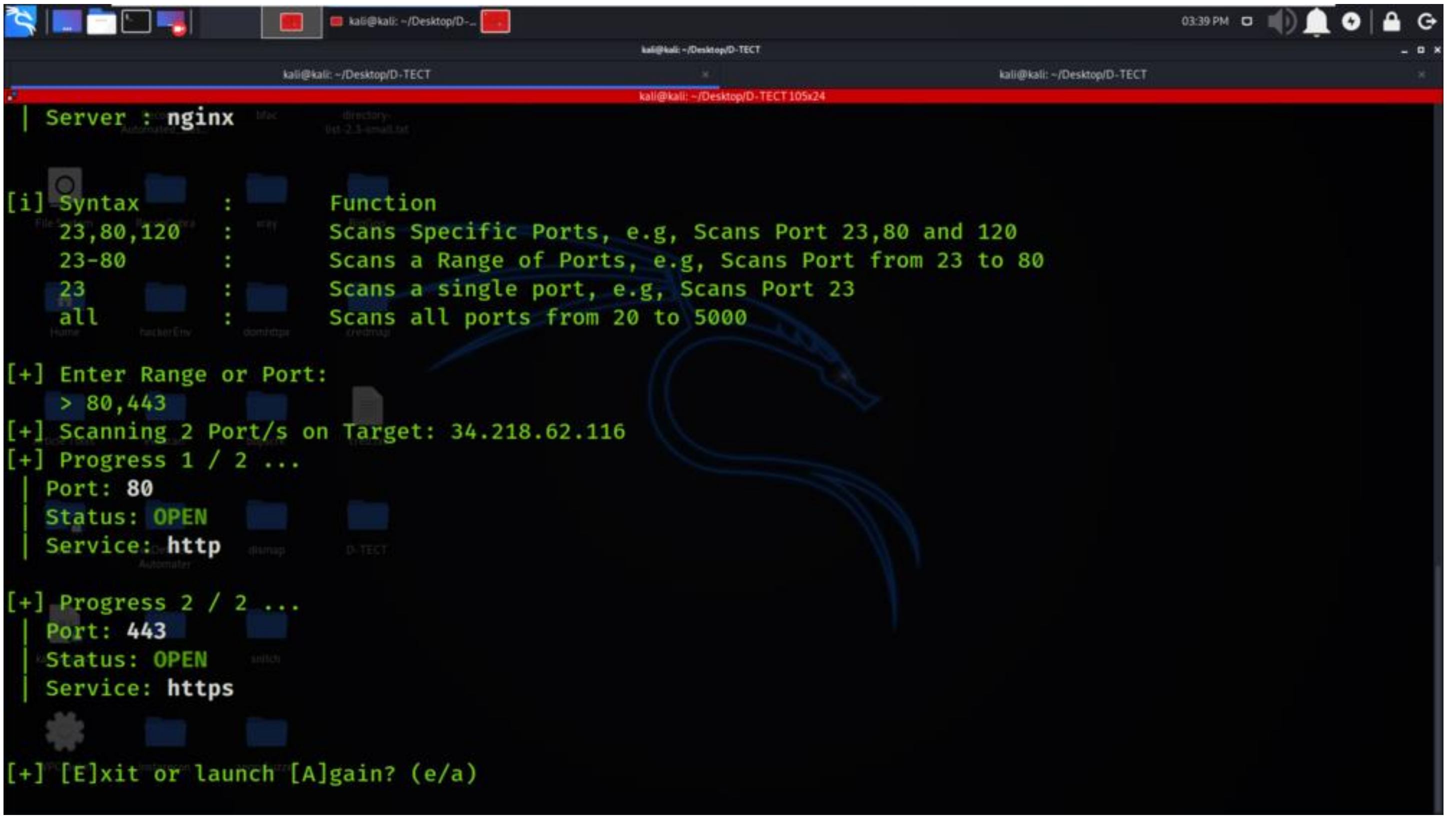
There is ClickJacking Vulnerability Detection on the domain.



```
[!] X-Frame-Options header Missing
[!] Page migh be vulnerable to Click Jacking
[!] http://geeksforgeeks.org/wp/
[i] About ClickJacking: [ https://owasp.org/www-community/attacks/Clickjacking]
```

Example 3: Port Scanner
Select Option 4

Open Ports are been scanned and displayed in the below screenshot.

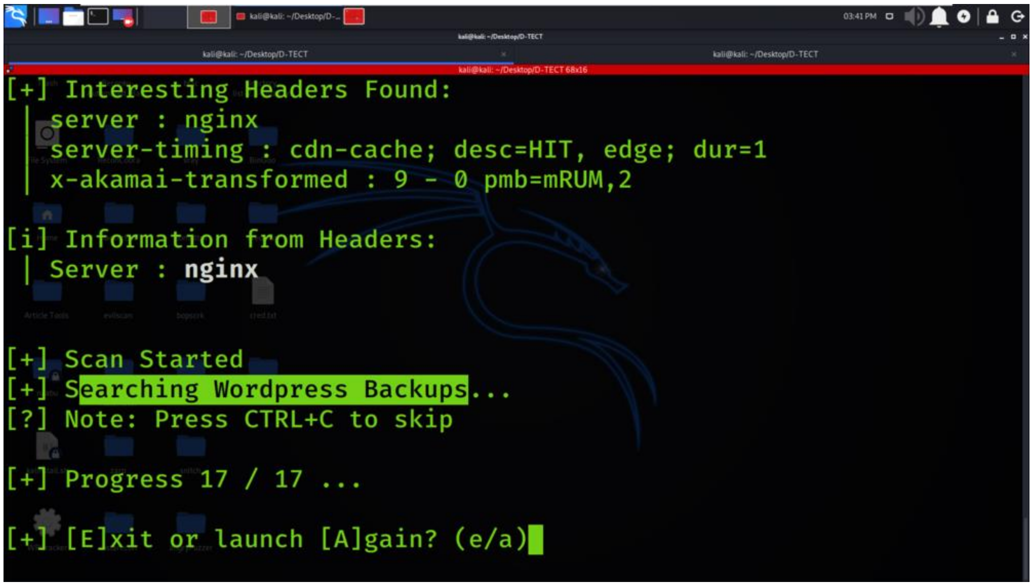


03:39 PM
kali@kali: ~/Desktop/D-TECT
kali@kali: ~/Desktop/D-TECT
kali@kali: ~/Desktop/D-TECT
kali@kali: ~/Desktop/D-TECT 105x24

```
 | Server : nginx


[i] Syntax         :       Function
    23,80,120      :       Scans Specific Ports, e.g, Scans Port 23,80 and 120
    23-80          :       Scans a Range of Ports, e.g, Scans Port from 23 to 80
    23             :       Scans a single port, e.g, Scans Port 23
    all            :       Scans all ports from 20 to 5000

[+] Enter Range or Port:
    > 80,443
[+] Scanning 2 Port/s on Target: 34.218.62.116
[+] Progress 1 / 2 ...
  | Port: 80
  | Status: OPEN
  | Service: http

[+] Progress 2 / 2 ...
  | Port: 443
  | Status: OPEN
  | Service: https


[+] [E]xit or launch [A]gain? (e/a)
```

Example 4: WP Backup Grabber
Select Option 7

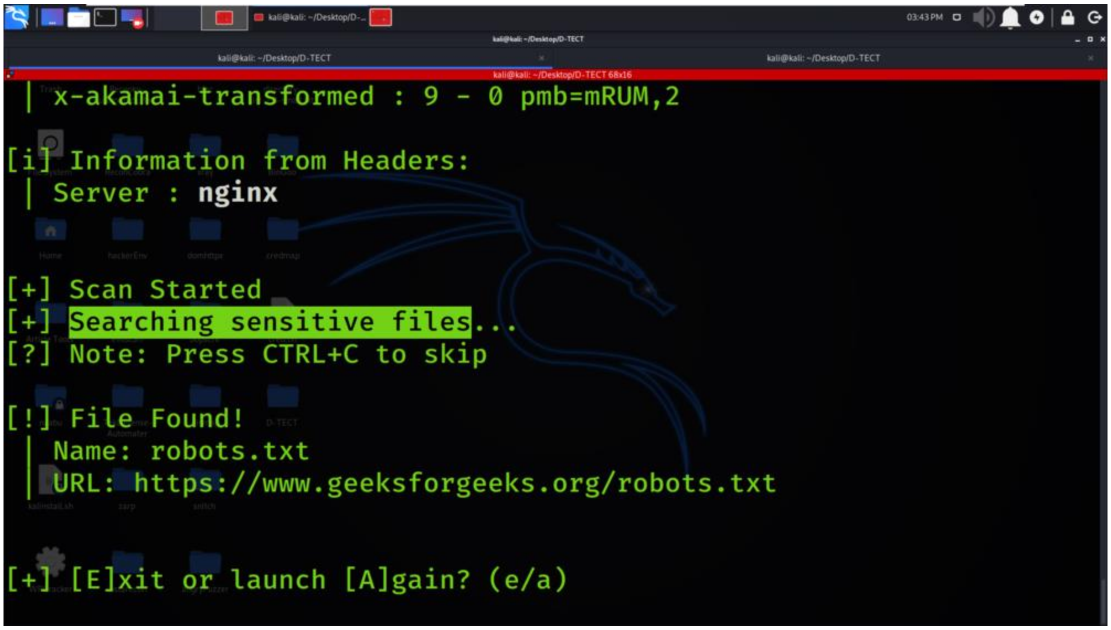
WordPress Backup Grabber is performed in the below screenshot.


kali@kali: ~/Desktop/D-TECT
kali@kali: ~/Desktop/D-TECT
kali@kali: ~/Desktop/D-TECT
kali@kali: ~/Desktop/D-TECT 68x16
03:41 PM

```
[+] Interesting Headers Found:
 | server : nginx
 | server-timing : cdn-cache; desc=HIT, edge; dur=1
 | x-akamai-transformed : 9 - 0 pmb=mRUM,2

[i] Information from Headers:
 | Server : nginx


[+] Scan Started
[+] Searching Wordpress Backups...
[?] Note: Press CTRL+C to skip

[+] Progress 17 / 17 ...

[+] [E]xit or launch [A]gain? (e/a)
```

Example 5: Sensitive File Detection
Select Option 2

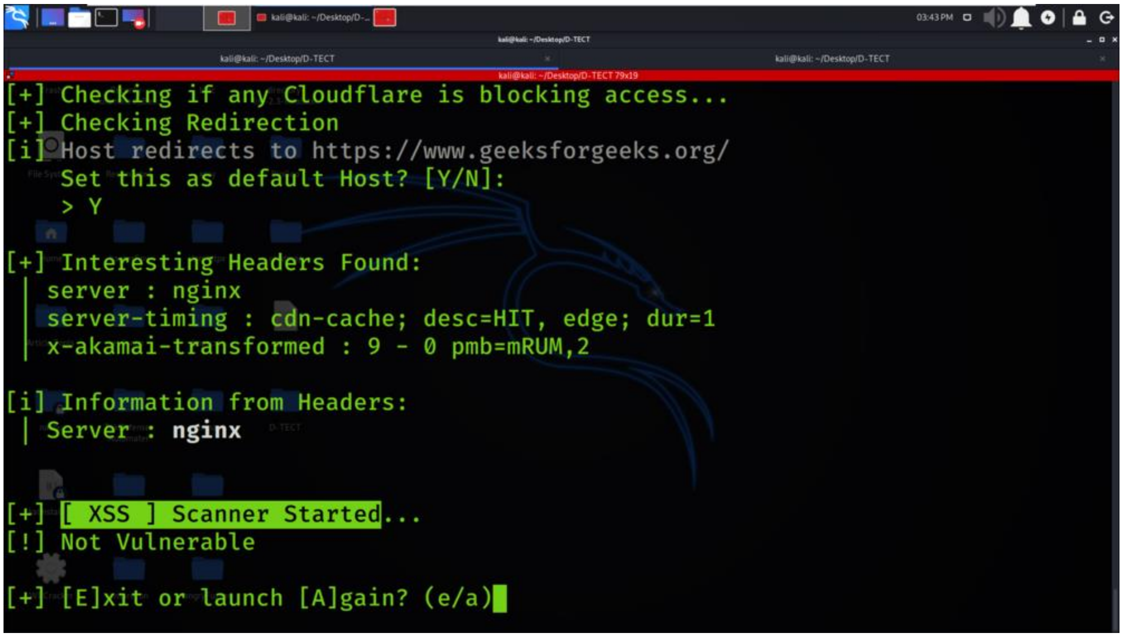
Critical files which can contain sensitive information is listed in the below screenshot.


kali@kali: ~/Desktop/D-TECT
kali@kali: ~/Desktop/D-TECT
kali@kali: ~/Desktop/D-TECT
kali@kali: ~/Desktop/D-TECT 68x16
03:43 PM

```
 | x-akamai-transformed : 9 - 0 pmb=mRUM,2

[i] Information from Headers:
 | Server : nginx


[+] Scan Started
[+] Searching sensitive files...
[?] Note: Press CTRL+C to skip

[!] File Found!
 | Name: robots.txt
 | URL: https://www.geeksforgeeks.org/robots.txt


[+] [E]xit or launch [A]gain? (e/a)
```

Example 6: Cross-Site Scripting [XSS] Scanner
Select Option 6

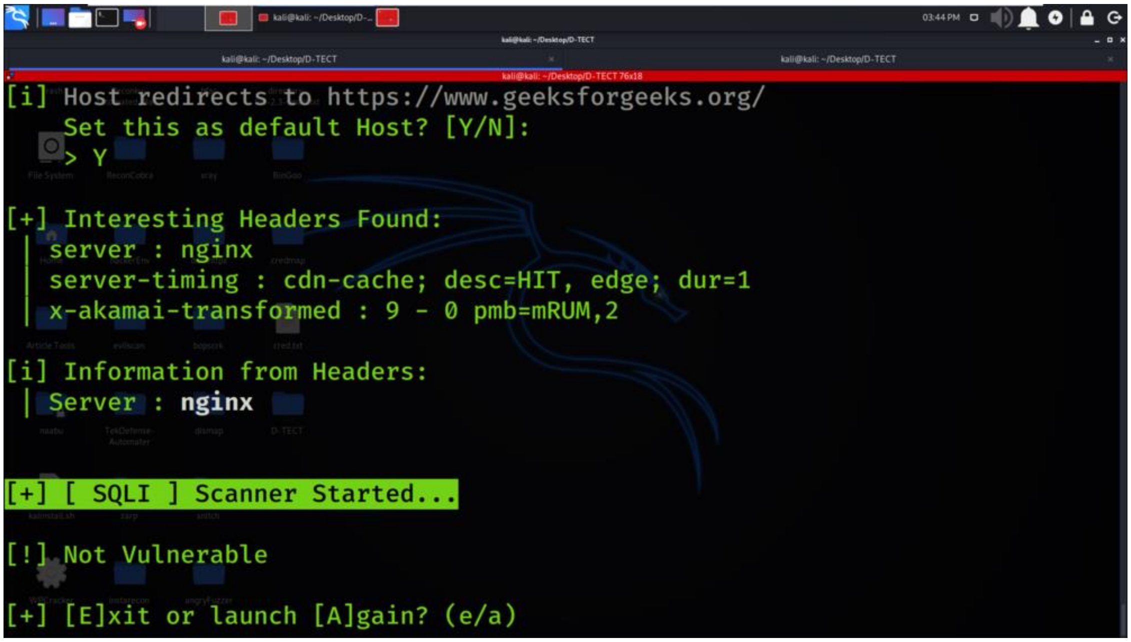
XSS Scanning is been performed on the domain geeksforgeeks.org.


kali@kali: ~/Desktop/D-TECT
kali@kali: ~/Desktop/D-TECT 79x19
03:43 PM

```
[+] Checking if any Cloudflare is blocking access...
[+] Checking Redirection
[i] Host redirects to https://www.geeksforgeeks.org/
    Set this as default Host? [Y/N]:
    > Y

[+] Interesting Headers Found:
  | server : nginx
  | server-timing : cdn-cache; desc=HIT, edge; dur=1
  | x-akamai-transformed : 9 - 0 pmb=mRUM,2

[i] Information from Headers:
  | Server : nginx


[+] [ XSS ] Scanner Started...
[!] Not Vulnerable

[+] [E]xit or launch [A]gain? (e/a)
```

Example 7: SQL Injection [SQLI] Scanner
Select Option 8

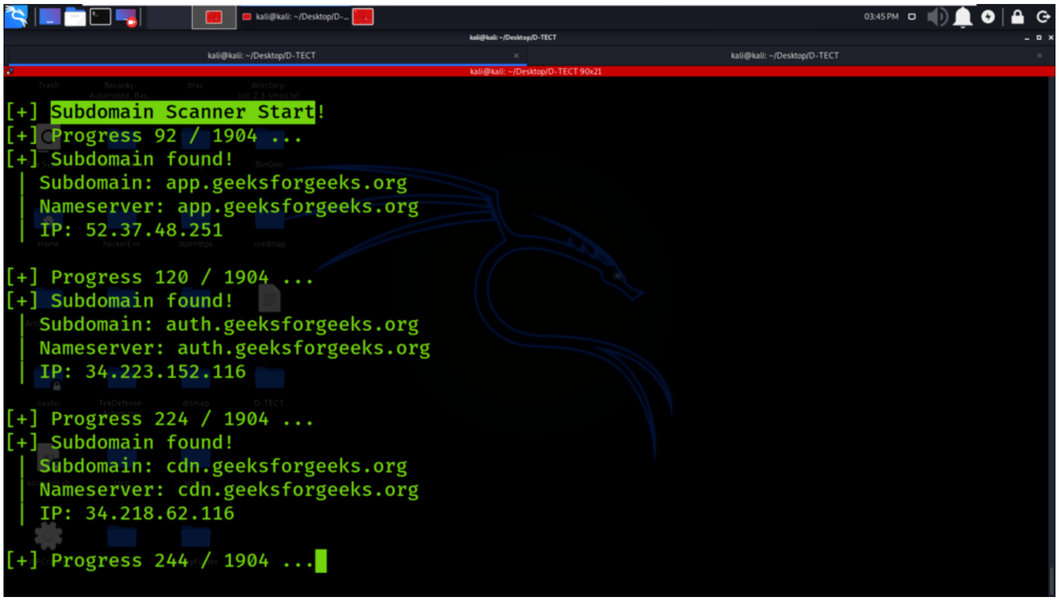
SQL Injection Scanning is been performed on the domain geeksforgeeks.org.


kali@kali: ~/Desktop/D-TECT
kali@kali: ~/Desktop/D-TECT 76x18
03:44 PM

```
[i] Host redirects to https://www.geeksforgeeks.org/
    Set this as default Host? [Y/N]:
    > Y

[+] Interesting Headers Found:
  | server : nginx
  | server-timing : cdn-cache; desc=HIT, edge; dur=1
  | x-akamai-transformed : 9 - 0 pmb=mRUM,2

[i] Information from Headers:
  | Server : nginx


[+] [ SQLI ] Scanner Started...

[!] Not Vulnerable

[+] [E]xit or launch [A]gain? (e/a)
```

Example 8: Sub-domain Scanner
Select Option 3

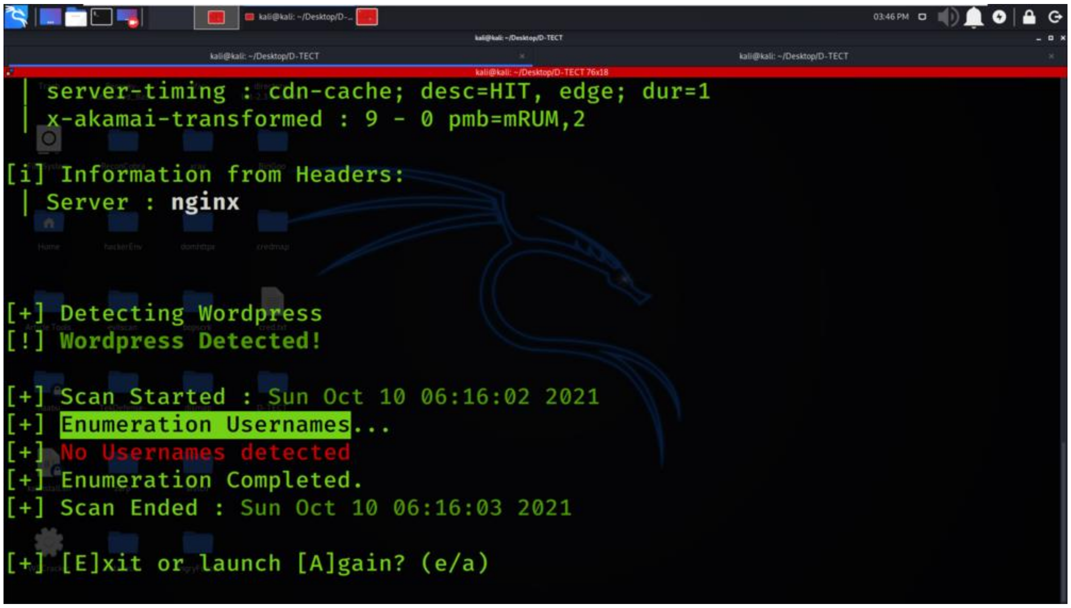
Subdomains associated with the geeksforgeeks.org are been detected and displayed in the below screenshot.


kali@kali: ~/Desktop/D-TECT
kali@kali: ~/Desktop/D-TECT 90x21
03:45 PM

```
[+] Subdomain Scanner Start!
[+] Progress 92 / 1904 ...
[+] Subdomain found!
 | Subdomain: app.geeksforgeeks.org
 | Nameserver: app.geeksforgeeks.org
 | IP: 52.37.48.251

[+] Progress 120 / 1904 ...
[+] Subdomain found!
 | Subdomain: auth.geeksforgeeks.org
 | Nameserver: auth.geeksforgeeks.org
 | IP: 34.223.152.116

[+] Progress 224 / 1904 ...
[+] Subdomain found!
 | Subdomain: cdn.geeksforgeeks.org
 | Nameserver: cdn.geeksforgeeks.org
 | IP: 34.218.62.116

[+] Progress 244 / 1904 ...
```

Example 9: WP Username Enumeration
Select Option 1

Usernames associated with the WordPress are been enumerated.

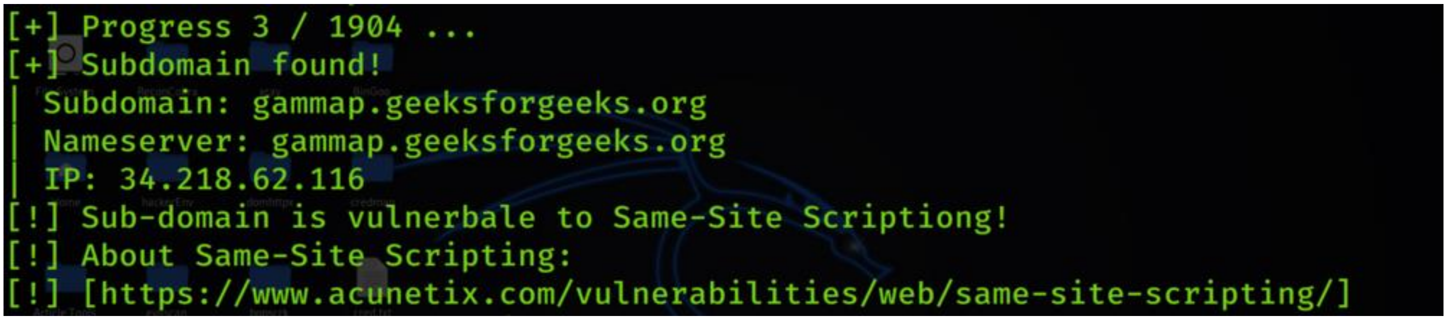

kali@kali: ~/Desktop/D-TECT
kali@kali: ~/Desktop/D-TECT 76x18
03:46 PM

```
 | server-timing : cdn-cache; desc=HIT, edge; dur=1
 | x-akamai-transformed : 9 - 0 pmb=mRUM,2

[i] Information from Headers:
 | Server : nginx


[+] Detecting Wordpress
[!] Wordpress Detected!

[+] Scan Started : Sun Oct 10 06:16:02 2021
[+] Enumeration Usernames...
[+] No Usernames detected
[+] Enumeration Completed.
[+] Scan Ended : Sun Oct 10 06:16:03 2021

[+] [E]xit or launch [A]gain? (e/a)
```

Example 10: Same Site Scripting detection
Select Option 3

Same Site Scripting Vulnerability detection is been performed on the subdomains of geeksforgeeks.org

Output screenshot:



```
[+] Progress 3 / 1904 ...
[+] Subdomain found!
| Subdomain: gammap.geeksforgeeks.org
| Nameserver: gammap.geeksforgeeks.org
| IP: 34.218.62.116
[!] Sub-domain is vulnerbale to Same-Site Scriptiong!
[!] About Same-Site Scripting:
[!] [https://www.acunetix.com/vulnerabilities/web/same-site-scripting/]
```

Learning Outcomes:

Finally, as a penetration tester, you should collect and log all vulnerabilities in the system. Don’t ignore any scenario considering that it won’t be executed by the end-users. If you are a penetration tester, please help our readers with your experience, tips, and sample test cases on how to perform Penetration Testing effectively.