**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:**

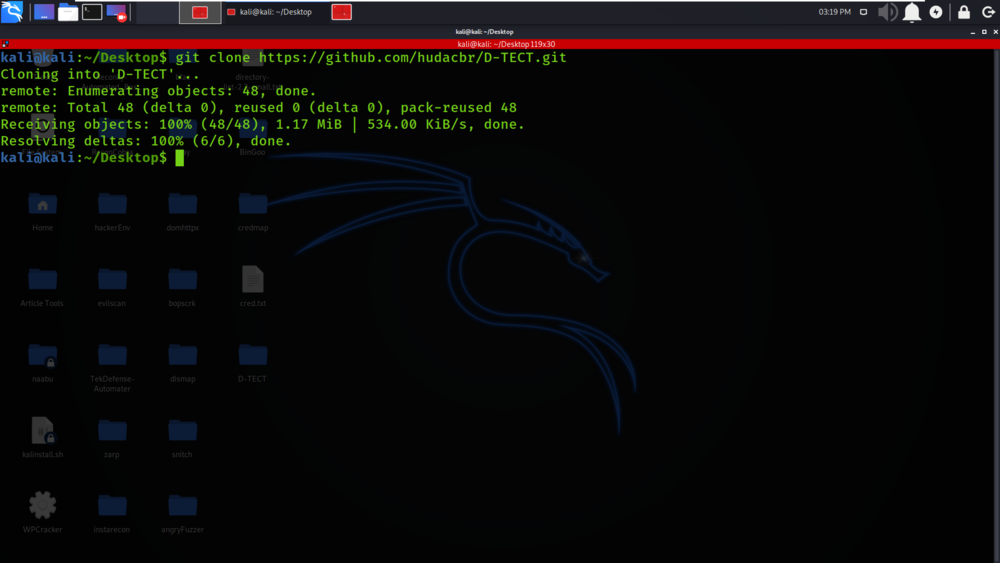
Web application penetration testing is the practice of simulating attacks on a system in an attempt to gain access to sensitive data, with the purpose of determining whether a system is secure. These attacks are performed either internally or externally on a system, and they help provide information 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**

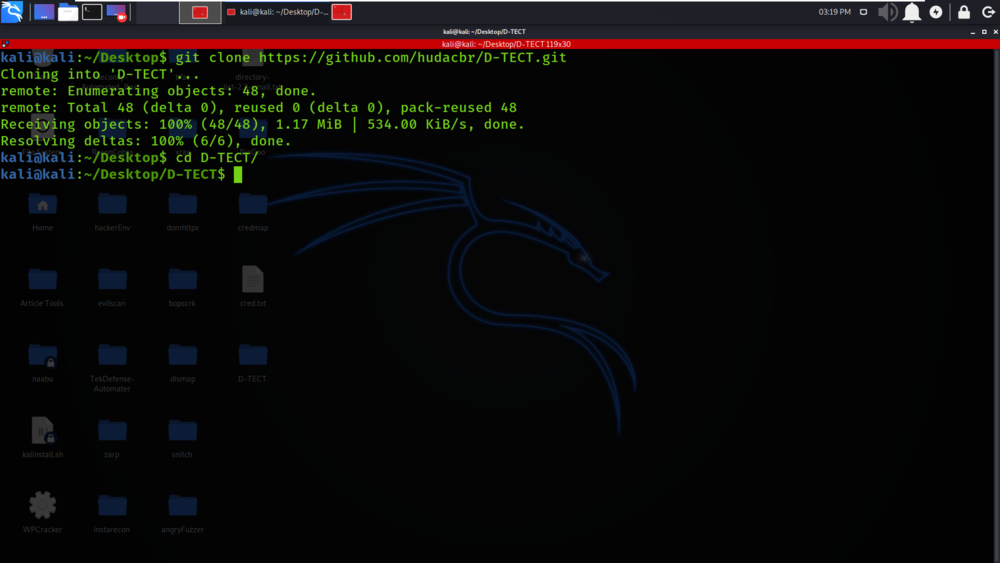
**Step 1**: Use the following command to install the tool in your Kali Linux operating system.

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



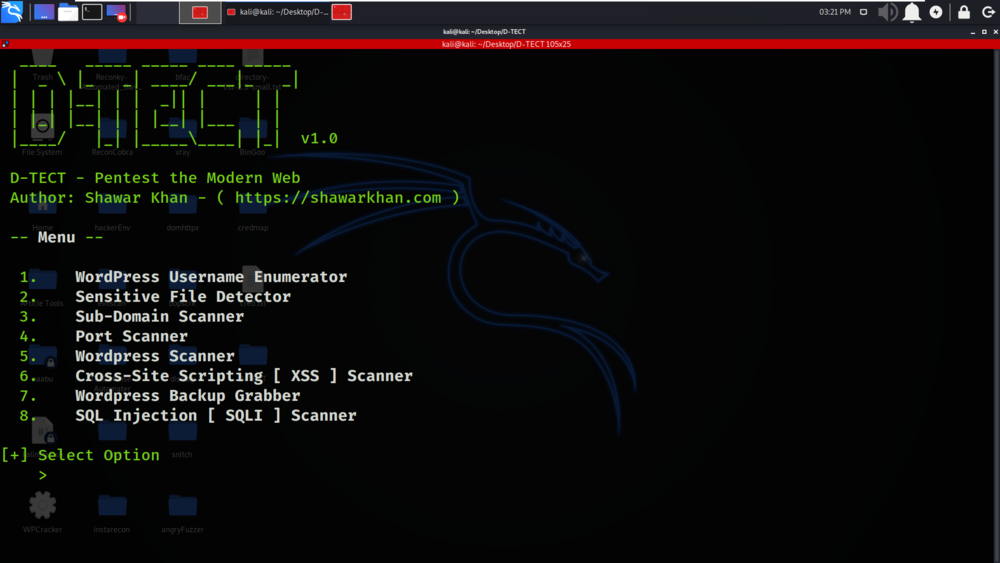
**Step 2**:  Now use the following command to move into the directory of the tool. You have to move in the directory in order to run the tool.

cd D-TECT-1



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

./d-tect.py

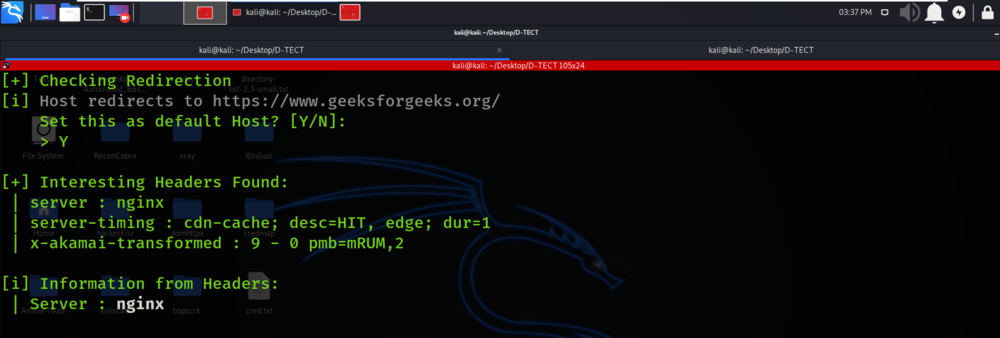


**Working with D-TECT Tool on Kali Linux OS**

**Example 1:**Banner Grabbing

Select Option 1

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



**Example 2:**ClickJacking Detection

Select Option 5

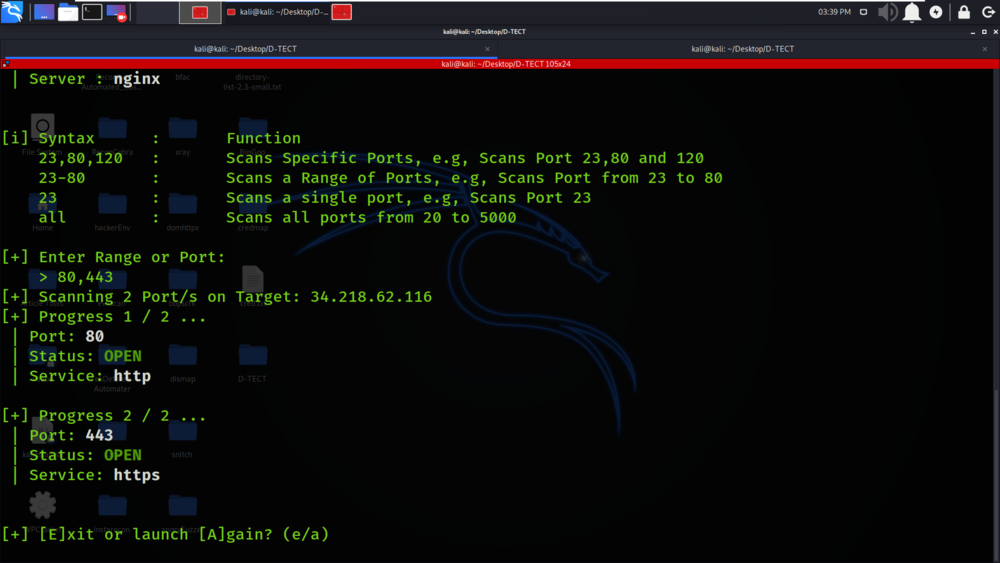
There is ClickJacking Vulnerability Detection on the domain.



**Example 3:**Port Scanner

Select Option 4

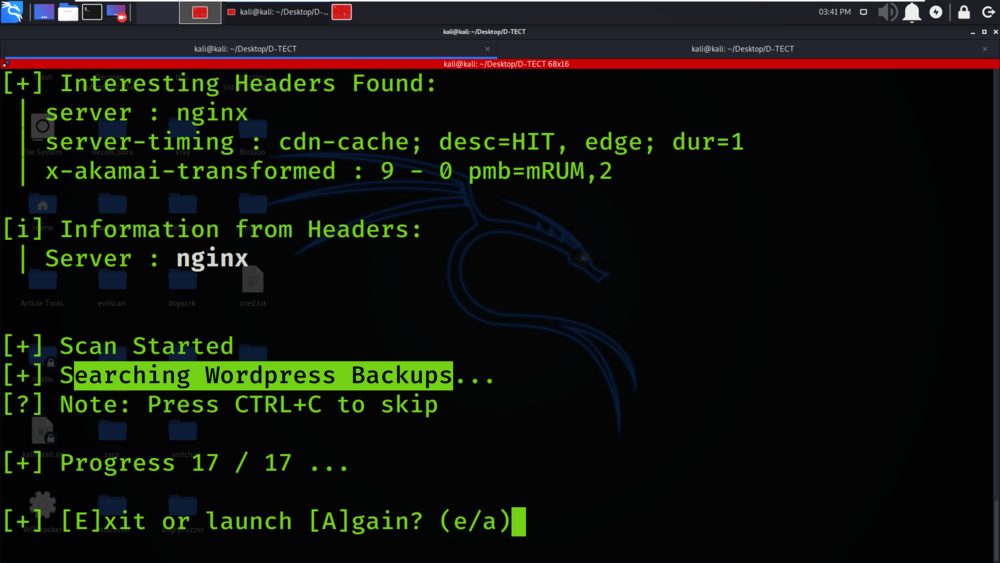
Open Ports are been scanned and displayed in the below screenshot.



**Example 4:**WP Backup Grabber

Select Option 7

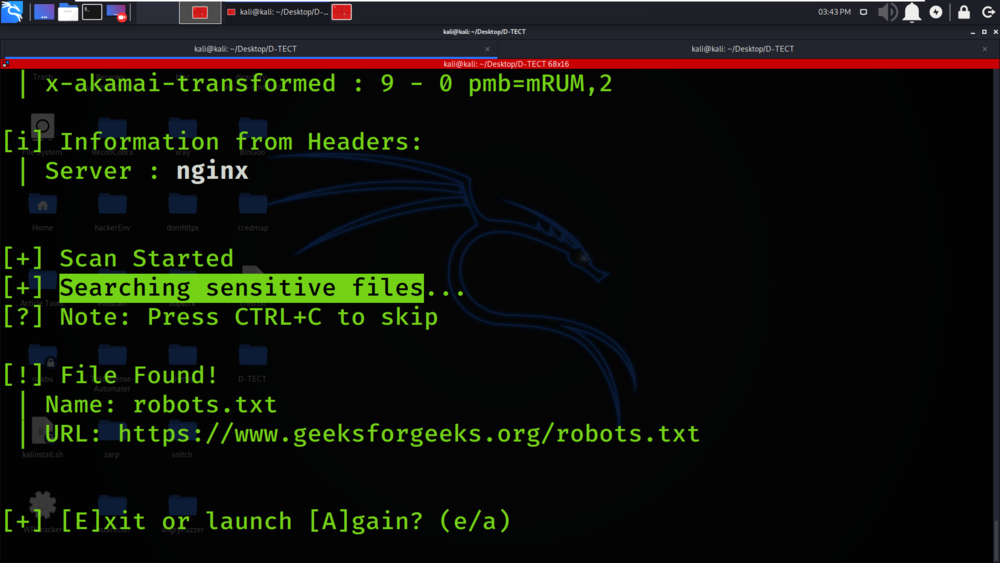
WordPress Backup Grabber is performed in the below screenshot.

****

**Example 5:**Sensitive File Detection

Select Option 2

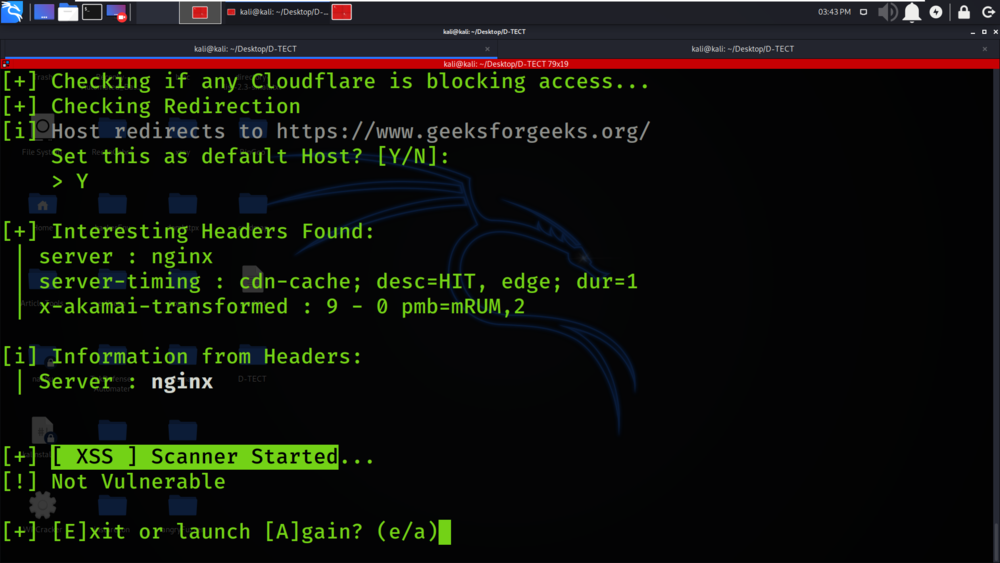
Critical files which can contain sensitive information is listed in the below screenshot.

****

**Example 6:**Cross-Site Scripting [ XSS ] Scanner

Select Option 6

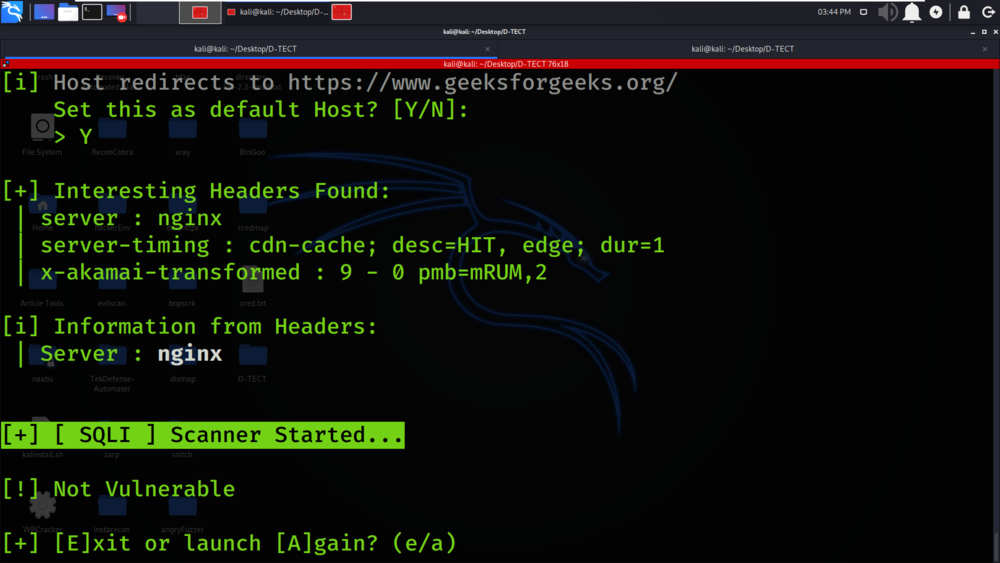
XSS Scanning is been performed on the domain geeksforgeeks.org.

****

**Example 7:**SQL Injection [ SQLI ] Scanner

Select Option 8

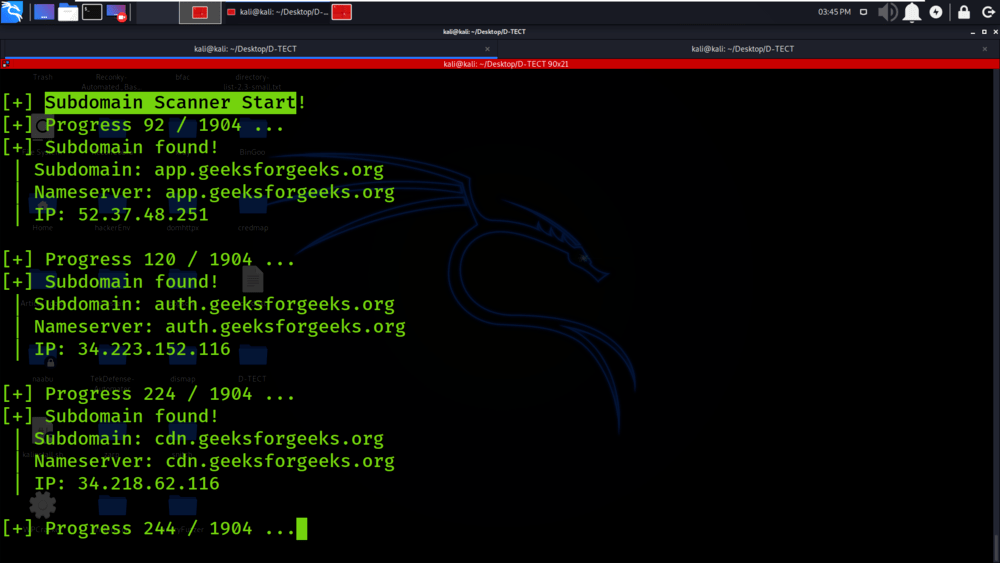
SQL Injection Scanning is been performed on the domain geeksforgeeks.org.

****

**Example 8:**Sub-domain Scanner

Select Option 3

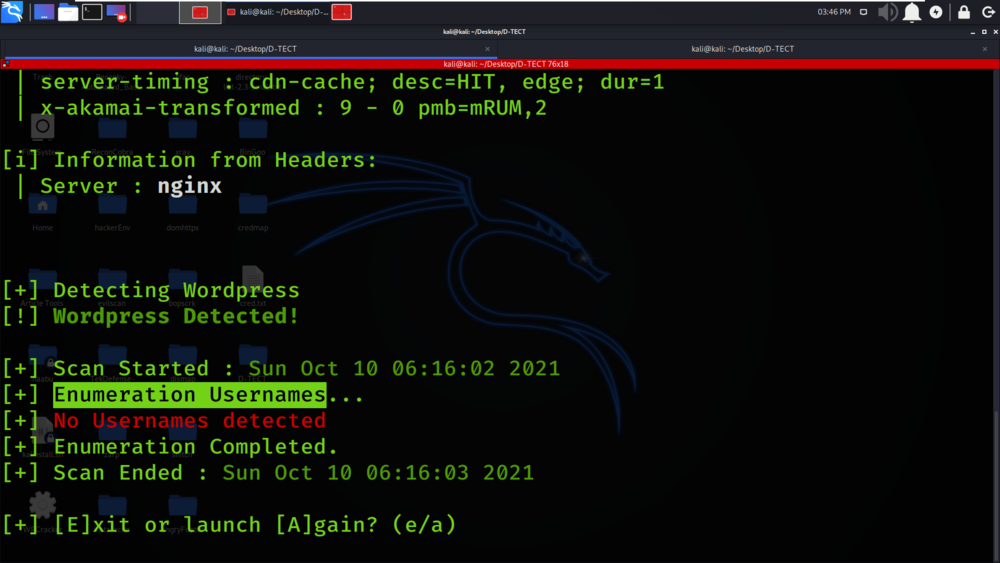
Subdomains associated with the geeksforgeeks.org are been detected and displayed in the below screenshot.



**Example 9:**WP Username Enumeration

Select Option 1

Usernames associated with the WordPress are been enumerated.

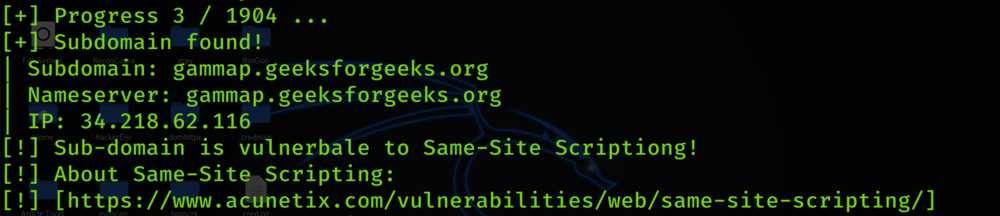
****

**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:**

****

**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.