Module 14: Hacking Web Applications

Lab 1: Footprint the Web Infrastructure

Lab Scenario

The first step in web application hacking for an ethical hacker or pen tester is to gather the maximum available information about the target organization website by performing web application footprinting using various techniques and tools. In this step, you will use techniques such as web spidering and vulnerability scanning to gather complete information about the target web application.

Web infrastructure footprinting helps you to identify vulnerable web applications, understand how they connect with peers and the technologies they use, and find vulnerabilities in specific parts of the web app architecture. These vulnerabilities can further help you to exploit and gain unauthorized access to web applications.

The labs in this exercise demonstrate how easily hackers can gather information about your web application and describe the vulnerabilities that exist in web applications.

Lab Objectives

- Perform web application reconnaissance using Nmap and Telnet
- Perform web spidering using OWASP ZAP
- Perform web application vulnerability scanning using SmartScanner

Overview of Footprinting the Web Infrastructure

Footprinting the web infrastructure allows attackers to engage in the following tasks:

- **Server Discovery**: Attackers attempt to discover the physical servers that host a web application using techniques such as Whois Lookup, DNS Interrogation, and Port Scanning
- **Service Discovery**: Attackers discover services running on web servers to determine whether they can use some of them as attack paths for hacking a web app
- **Server Identification**: Attackers use banner-grabbing to obtain server banners; this helps to identify the make and version of the web server software
- **Hidden Content Discovery**: Footprinting also allows attackers to extract content and functionality that is not directly linked to or reachable from the main visible content

Task 1: Perform Web Application Reconnaissance using Nmap and Telnet

In web application reconnaissance, you must perform various tasks such as server discovery, service discovery, server identification or banner grabbing, and hidden content discovery. A professional ethical hacker or pen tester must gather as much information as possible about the target website by performing web application footprinting using various techniques and tools.

In this task, we will perform web application reconnaissance to gather information about server IP address, DNS names, location and type of server, open ports and services, make, model, version of the web server software, and server-side technology.

1. Perform a Whois lookup to gather information about the IP address of the web server and the complete information about the domain such as its registration details, name servers, IP address, and location.

2. Use tools such as **Netcraft** (https://www.netcraft.com), **SmartWhois** (https://www.tamos.com), **WHOIS Lookup** (https://whois.domaintools.com), and **Batch IP Converter** (http://www.sabsoft.com) to perform the Whois lookup.

3. Perform DNS Interrogation to gather information about the DNS servers, DNS records, and types of servers used by the target organization. DNS zone data include DNS domain names, computer names, IP addresses, domain mail servers, service records, etc.

4. Use tools such as, **DNSRecon** (https://github.com), and **Domain Dossier** (https://centralops.net) to perform DNS interrogation.

5. Now, we will perform port scanning to gather information about the open ports and services running on the machine hosting the target website.

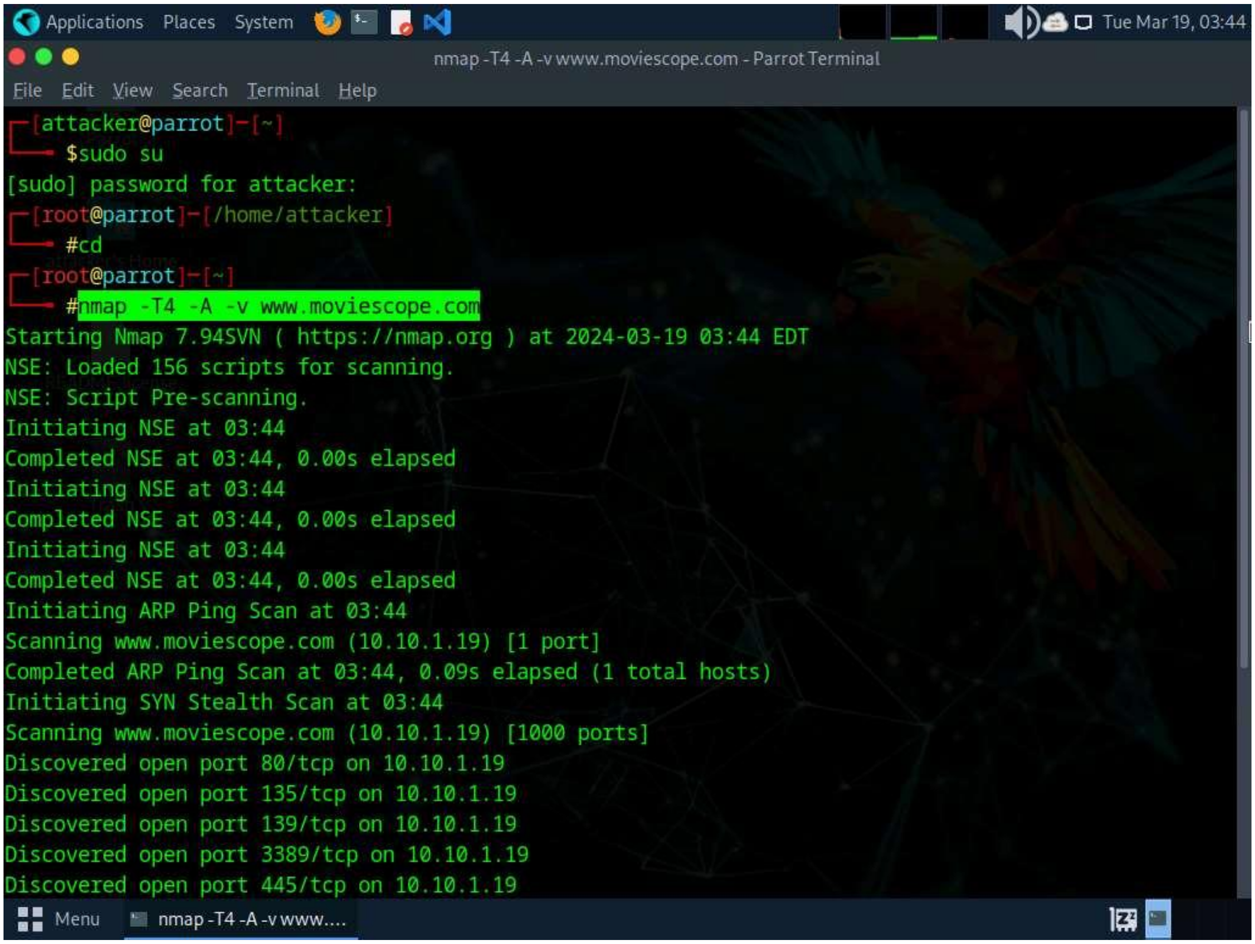
6. Click Parrot Security to switch to the **Parrot Security** machine. Open a **Terminal** window and execute **sudo su** to run the programs as a root user (When prompted, enter the password **toor**).

In this task, the target website (**www.moviescope.com**) is hosted by the victim machine (**Windows Server 2019**). Here, the host machine is the **Parrot Security** machine.

7. Now, type **cd** and press **Enter** to jump to the root directory.

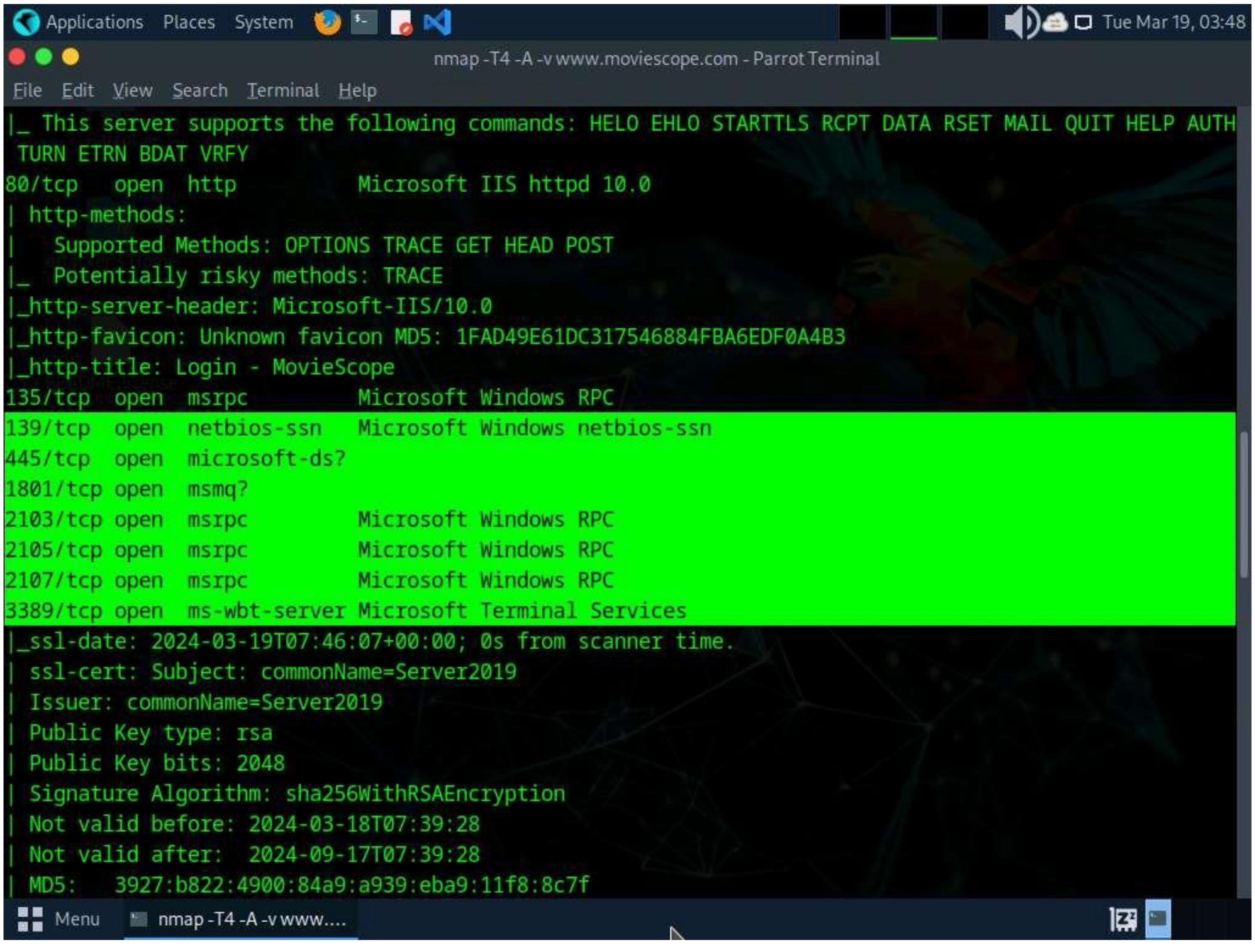
8. In the **Parrot Terminal** window, run **nmap -T4 -A -v [Target Web Application]** command (here, the target web application is **www.moviescope.com**) to perform a port and service discovery scan.

In this command, **-T4**: specifies setting time template (0-5), **-A**: specifies aggressive scan, and **-v**: enables the verbose output (include all hosts and ports in the output).


Applications Places System
Tue Mar 19, 03:44
nmap -T4 -A -v www.moviescope.com - Parrot Terminal
File Edit View Search Terminal Help
Menu
nmap -T4 -A -v www....

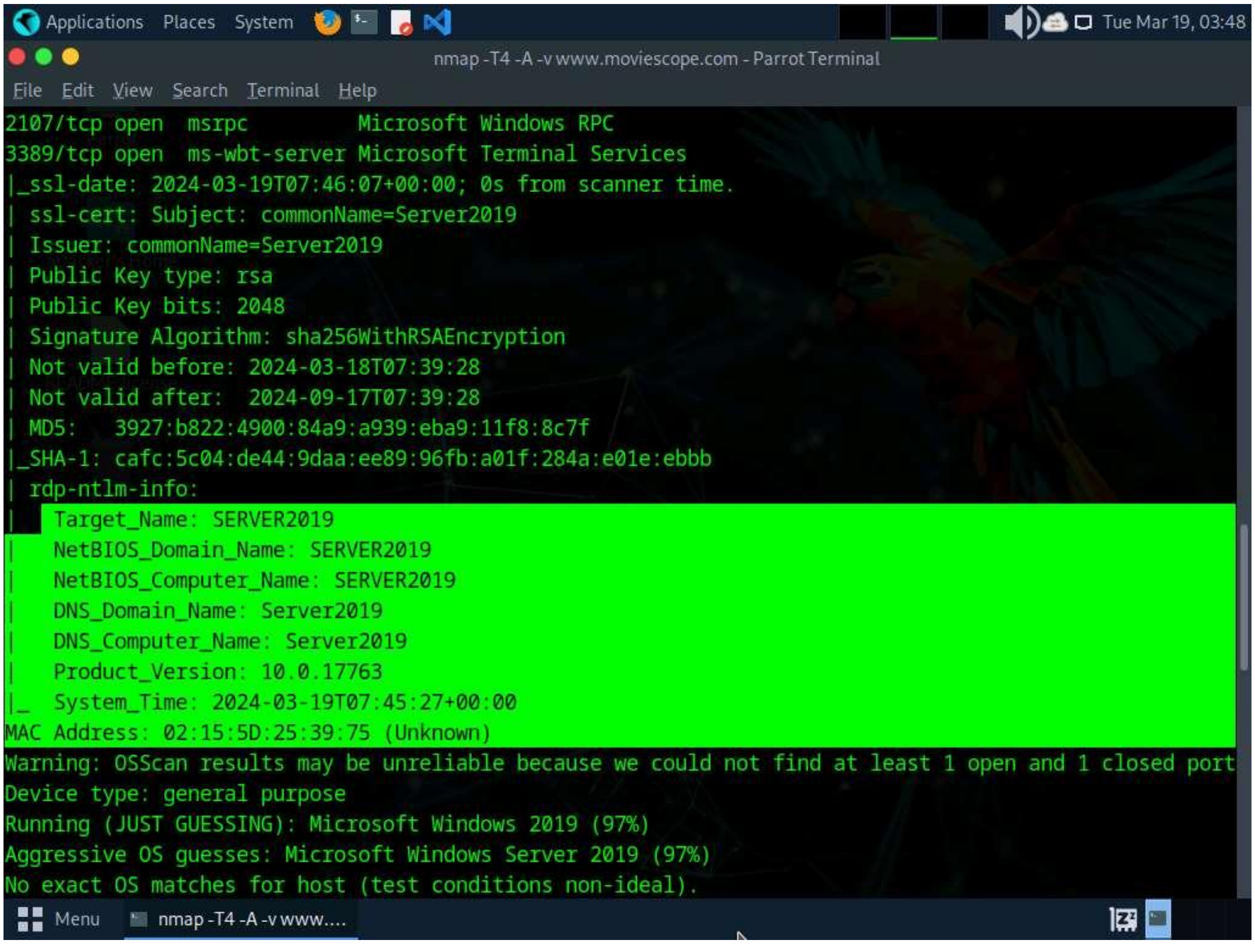
```
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #cd
┌─[root@parrot]─[~]
└──╼ #nmap -T4 -A -v www.moviescope.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-19 03:44 EDT
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 03:44
Completed NSE at 03:44, 0.00s elapsed
Initiating NSE at 03:44
Completed NSE at 03:44, 0.00s elapsed
Initiating NSE at 03:44
Completed NSE at 03:44, 0.00s elapsed
Initiating ARP Ping Scan at 03:44
Scanning www.moviescope.com (10.10.1.19) [1 port]
Completed ARP Ping Scan at 03:44, 0.09s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 03:44
Scanning www.moviescope.com (10.10.1.19) [1000 ports]
Discovered open port 80/tcp on 10.10.1.19
Discovered open port 135/tcp on 10.10.1.19
Discovered open port 139/tcp on 10.10.1.19
Discovered open port 3389/tcp on 10.10.1.19
Discovered open port 445/tcp on 10.10.1.19
```

9. The result appears, displaying the open ports and services running on the machine hosting the target website.


Applications Places System
Tue Mar 19, 03:48
nmap -T4 -A -v www.moviescope.com - Parrot Terminal
File Edit View Search Terminal Help
Menu
nmap -T4 -A -v www....

```
|_ This server supports the following commands: HELO EHLO STARTTLS RCPT DATA RSET MAIL QUIT HELP AUTH
 TURN ETRN BDAT VRFY
80/tcp   open  http          Microsoft IIS httpd 10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-favicon: Unknown favicon MD5: 1FAD49E61DC317546884FBA6EDF0A4B3
|_http-title: Login - MovieScope
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
1801/tcp open  msmq?
2103/tcp open  msrpc         Microsoft Windows RPC
2105/tcp open  msrpc         Microsoft Windows RPC
2107/tcp open  msrpc         Microsoft Windows RPC
3389/tcp open  ms-wbt-server Microsoft Terminal Services
|_ssl-date: 2024-03-19T07:46:07+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=Server2019
| Issuer: commonName=Server2019
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2024-03-18T07:39:28
| Not valid after:  2024-09-17T07:39:28
| MD5:   3927:b822:4900:84a9:a939:eba9:11f8:8c7f
```

10. Scroll down to see the complete results. You can observe that the target machine name, NetBIOS name, DNS name, MAC address, OS, and other information is displayed, as shown in the screenshot.



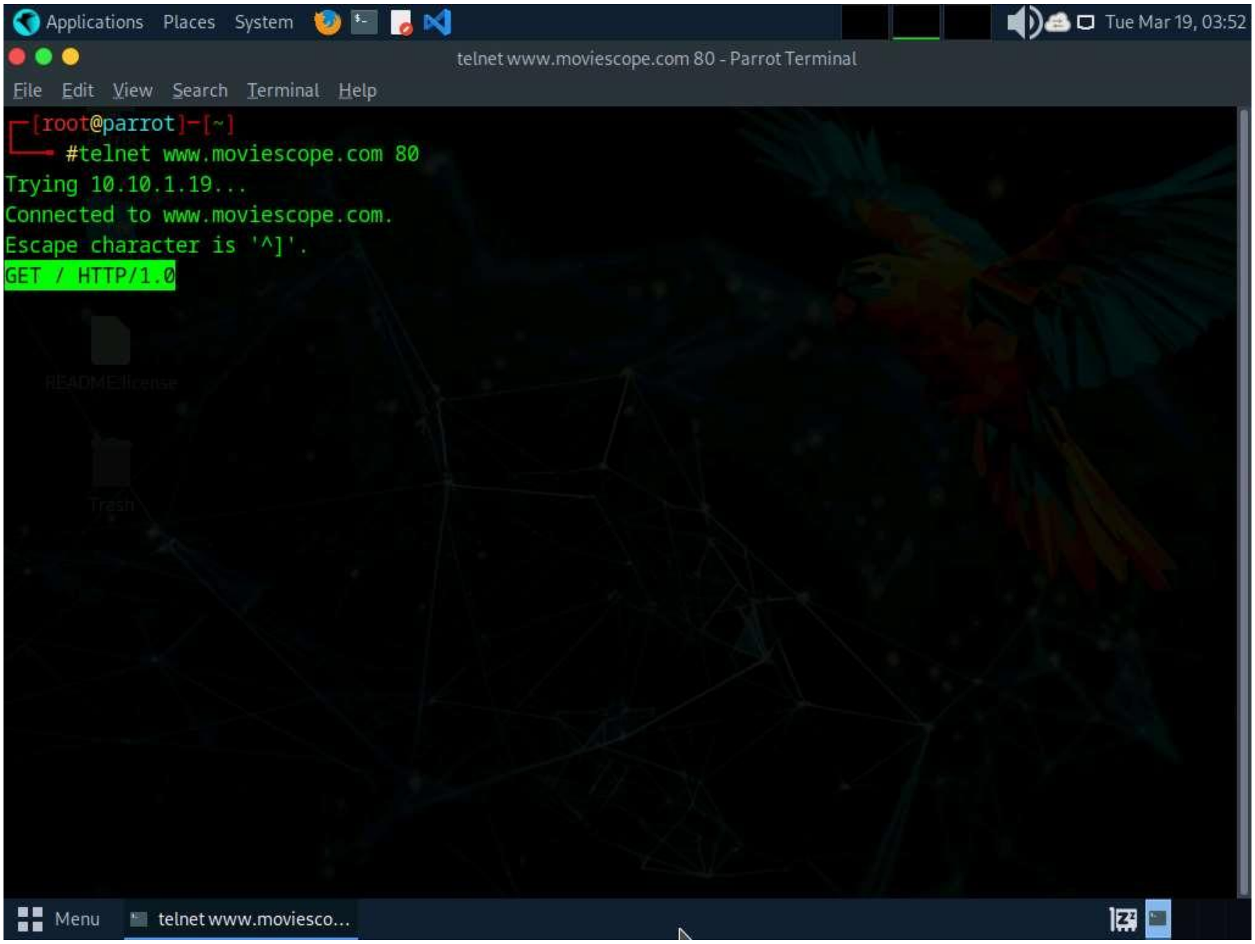
```
2107/tcp open  msrpc         Microsoft Windows RPC
3389/tcp open  ms-wbt-server Microsoft Terminal Services
|_ssl-date: 2024-03-19T07:46:07+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=Server2019
| Issuer: commonName=Server2019
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2024-03-18T07:39:28
| Not valid after:  2024-09-17T07:39:28
| MD5:   3927:b822:4900:84a9:a939:eba9:11f8:8c7f
|_SHA-1: cafc:5c04:de44:9daa:ee89:96fb:a01f:284a:e01e:ebbb
| rdp-ntlm-info:
|   Target_Name: SERVER2019
|   NetBIOS_Domain_Name: SERVER2019
|   NetBIOS_Computer_Name: SERVER2019
|   DNS_Domain_Name: Server2019
|   DNS_Computer_Name: Server2019
|   Product_Version: 10.0.17763
|_  System_Time: 2024-03-19T07:45:27+00:00
MAC Address: 02:15:5D:25:39:75 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2019 (97%)
Aggressive OS guesses: Microsoft Windows Server 2019 (97%)
No exact OS matches for host (test conditions non-ideal).
```

11. Now, perform banner grabbing to identify the make, model, and version of the target web server software.

12. In the terminal window, run command **telnet www.moviescope.com 80** to establish a telnet connection with the target machine.

Port 80 is the port number assigned to the commonly used Internet communication protocol, Hypertext Transfer Protocol (HTTP).

13. The **Trying 10.10.1.19…** message appears; type **GET / HTTP/1.0** and press **Enter** two times.



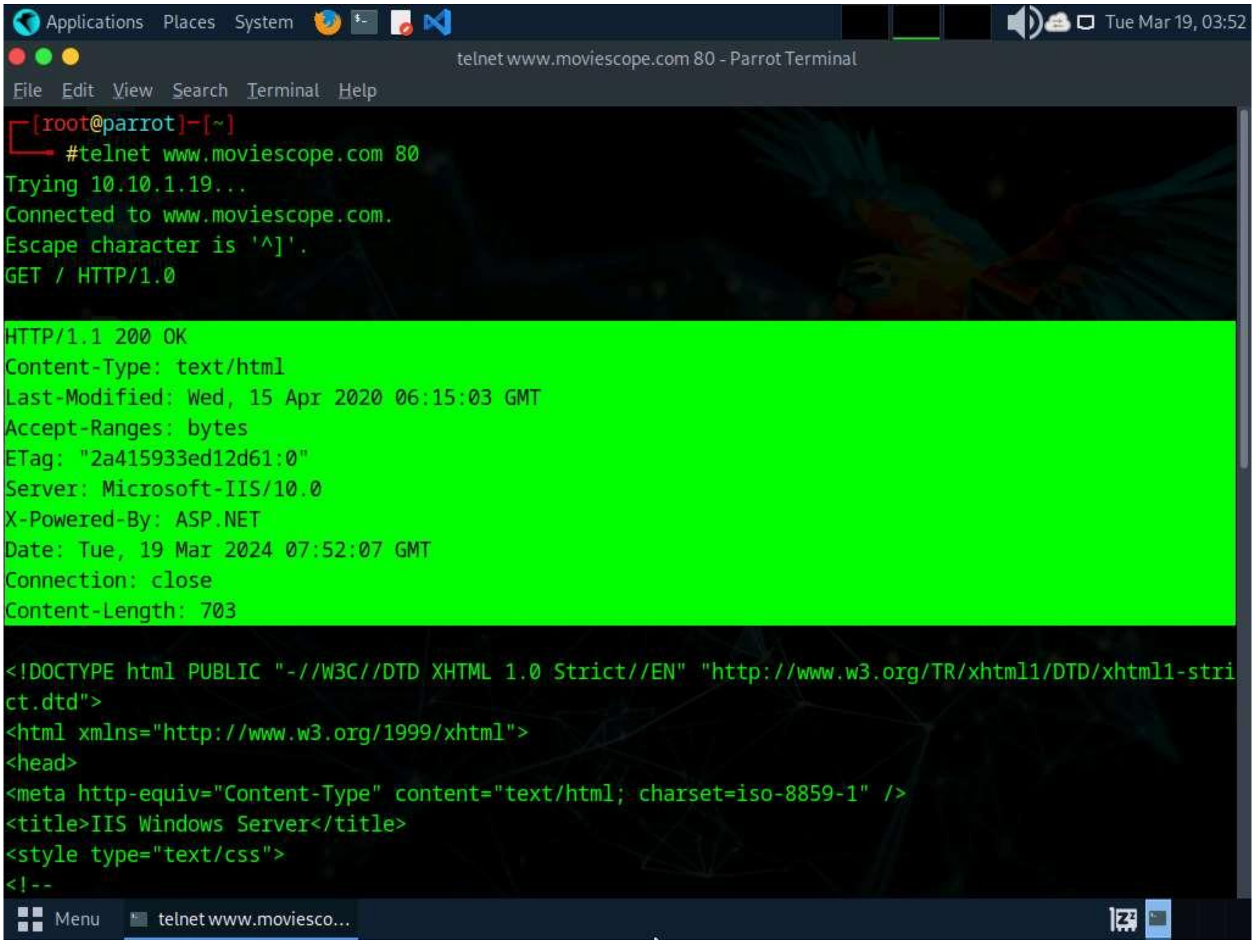
```
┌─[root@parrot]─[~]
└──╼ #telnet www.moviescope.com 80
Trying 10.10.1.19...
Connected to www.moviescope.com.
Escape character is '^]'.
GET / HTTP/1.0
```

14. The result appears, displaying information related to the server name and its version, technology used.

15. Here, the server is identified as **Microsoft-IIS/10.0** and the technology used is **ASP.NET**.

In real-time, an attacker can specify either the IP address of a target machine or the URL of a website. In both cases, the attacker obtains the banner information of the respective target. In other words, if the attacker entered an IP address, they receive the banner information of the target machine; if they enter the URL of a website, they receive the banner information of the respective web server that hosts the website.

more...


Applications Places System
Tue Mar 19, 03:52
telnet www.moviescope.com 80 - Parrot Terminal
File Edit View Search Terminal Help
Menu
telnet www.moviesco...

```
┌─[root@parrot]─[~]
└──╼ #telnet www.moviescope.com 80
Trying 10.10.1.19...
Connected to www.moviescope.com.
Escape character is '^]'.
GET / HTTP/1.0

HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Wed, 15 Apr 2020 06:15:03 GMT
Accept-Ranges: bytes
ETag: "2a415933ed12d61:0"
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Tue, 19 Mar 2024 07:52:07 GMT
Connection: close
Content-Length: 703

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-stri
ct.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS Windows Server</title>
<style type="text/css">
<!--
```

16. This concludes the demonstration of how to perform web application reconnaissance (Whois lookup, DNS interrogation, port and services discovery, banner grabbing, and firewall detection).

17. Close all open windows and document all acquired information.

Question 14.1.1.1

Perform a port and service discovery scan using Nmap on the website www.moviescope.com. Enter the IP address of the machine hosting www.moviescope.com.

Question 14.1.1.2

Perform a scan using Nmap on the website www.moviescope.com. Enter the name of the DNS server hosting the domain name for www.moviescope.com.

Question 14.1.1.3

Perform banner grabbing using Telnet on the website www.moviescope.com to identify the make, model, and version of the target web-server software. Identify the server-side application used to develop the web pages.

Task 2: Perform Web Spidering using OWASP ZAP

OWASP Zed Attack Proxy (ZAP) is an integrated penetration testing tool for finding vulnerabilities in web applications. It offers automated scanners as well as a set of tools that allow you to find security vulnerabilities manually. ZAP provides functionality for a range of skill levels—from developers to testers new to security testing, to security testing specialists.

Here, we will perform web spidering on the target website using OWASP ZAP.

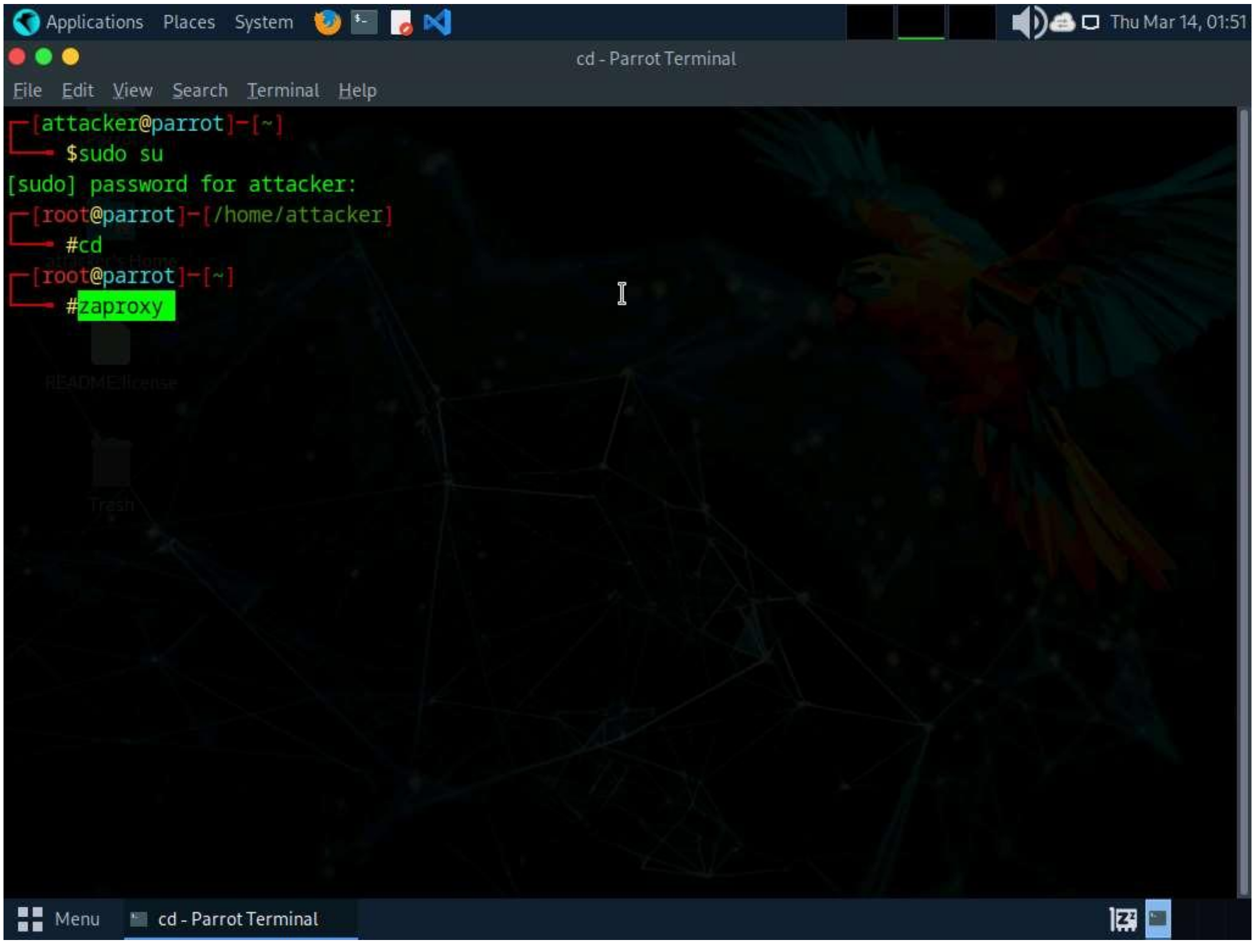
In this task, the target website (**www.moviescope.com**) is hosted by the victim machine (**Windows Server 2019**). Here, the host machine is the **Parrot Security** machine.

1. In the **Parrot Security** machine, open a **Terminal** window and execute **sudo su** to run the programs as a root user (When prompted, enter the password **toor**).

The password that you type will not be visible.

2. Now, run **cd** command to jump to the root directory.

3. In the **Terminal** window, type **zaproxy** and press **Enter** to launch OWASP ZAP.



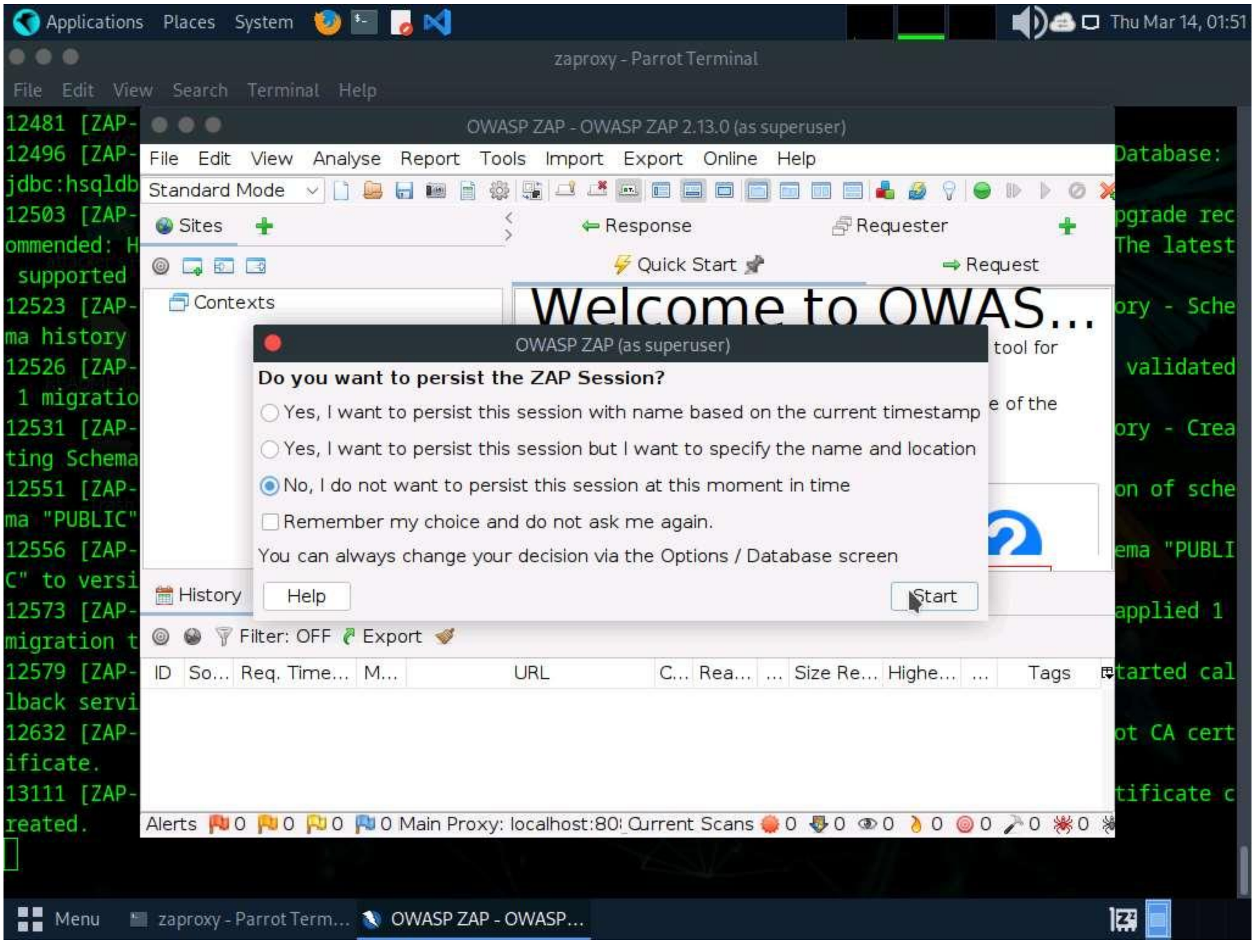
Applications Places System
Thu Mar 14, 01:51
cd - Parrot Terminal
File Edit View Search Terminal Help
Menu
cd - Parrot Terminal

```
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #cd
┌─[root@parrot]─[~]
└──╼ #zaproxy
```

4. The **OWASP ZAP** initializing window appears; wait for it to complete.

5. After completing initialization, a prompt that reads **Do you want to persist the ZAP Session?** appears; select the **No, I do not want to persist this session at this moment in time** radio button and click **Start**.

If a **Manage Add-ons** window appears, click the **Close** button.



Applications Places System
Thu Mar 14, 01:51
zaproxy - Parrot Terminal
File Edit View Search Terminal Help
OWASP ZAP - OWASP ZAP 2.13.0 (as superuser)
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Contexts
Response
Requester
Quick Start
Request
Welcome to OWAS...
History
Filter: OFF
Export
ID So... Req. Time... M... URL C... Rea... ... Size Re... Highe... ... Tags
Alerts 0 0 0 0 Main Proxy: localhost:80 Current Scans 0 0 0 0 0 0 0
Menu
zaproxy - Parrot Term...
OWASP ZAP - OWASP...
Help
Start

OWASP ZAP (as superuser)

Do you want to persist the ZAP Session?

○ Yes, I want to persist this session with name based on the current timestamp

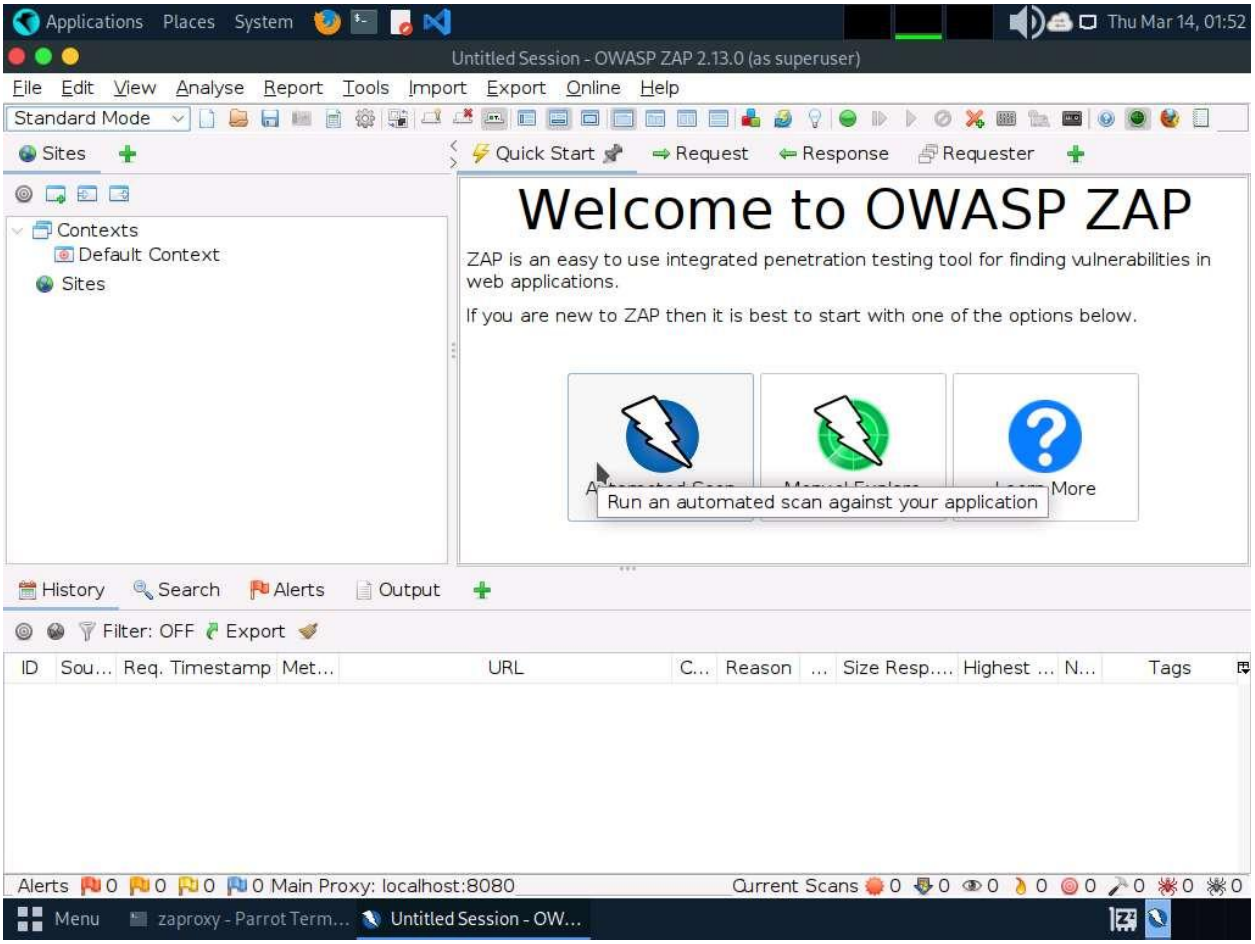
○ Yes, I want to persist this session but I want to specify the name and location

● No, I do not want to persist this session at this moment in time

□ Remember my choice and do not ask me again.

You can always change your decision via the Options / Database screen

6. The **OWASP ZAP** main window appears. Under the **Quick Start** tab, click the **Automated Scan** option under **Welcome to OWASP ZAP**.



Untitled Session - OWASP ZAP 2.13.0 (as superuser)

Welcome to OWASP ZAP

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

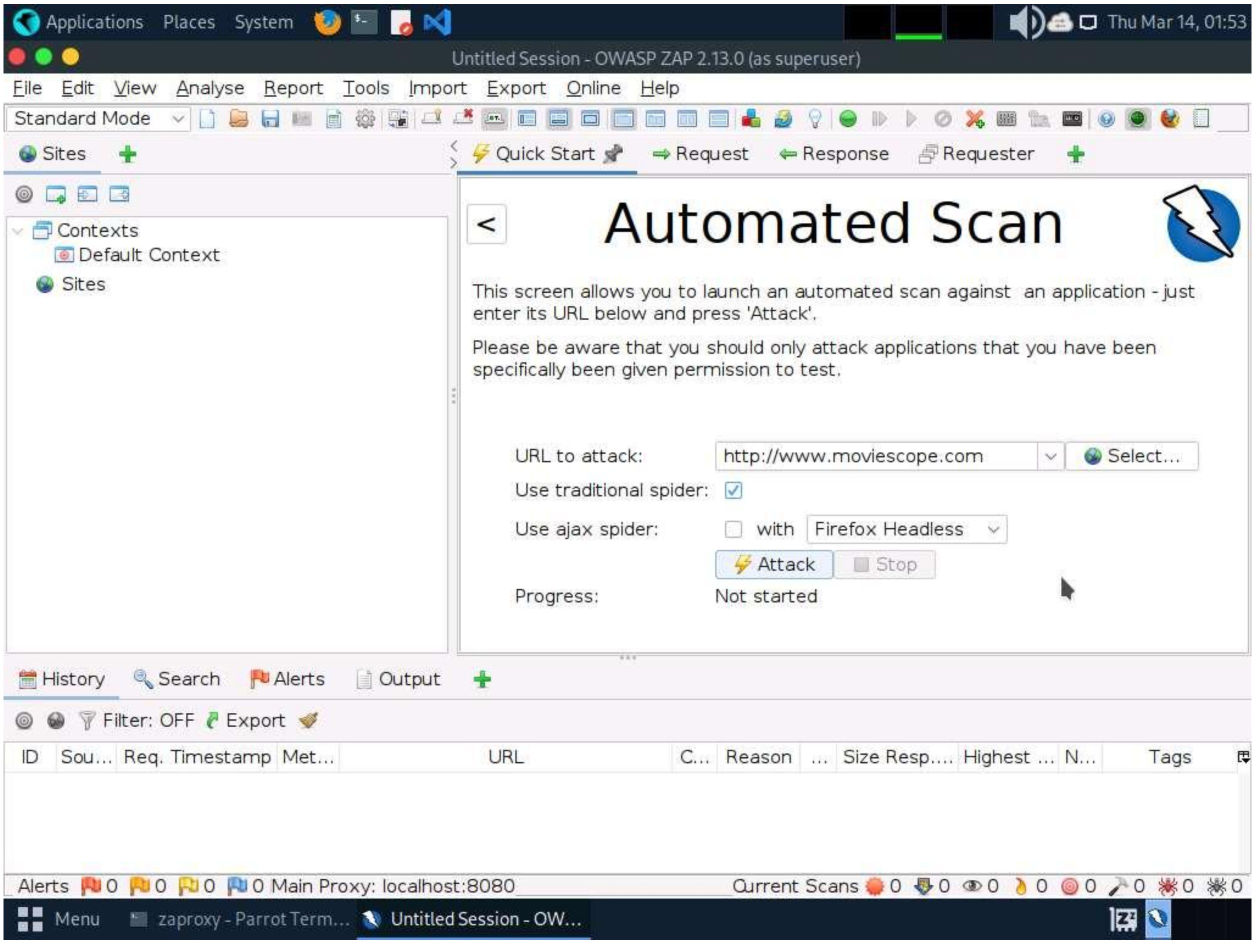
If you are new to ZAP then it is best to start with one of the options below.

Run an automated scan against your application

Alerts 0 0 0 0 Main Proxy: localhost:8080

Current Scans 0 0 0 0 0 0 0 0

7. The **Automated Scan** wizard appears; enter the target website under the **URL to attack** field (here, **www.moviescope.com**). Leave the other settings to default and click the **Attack** button.



Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

URL to attack: http://www.moviescope.com Select…

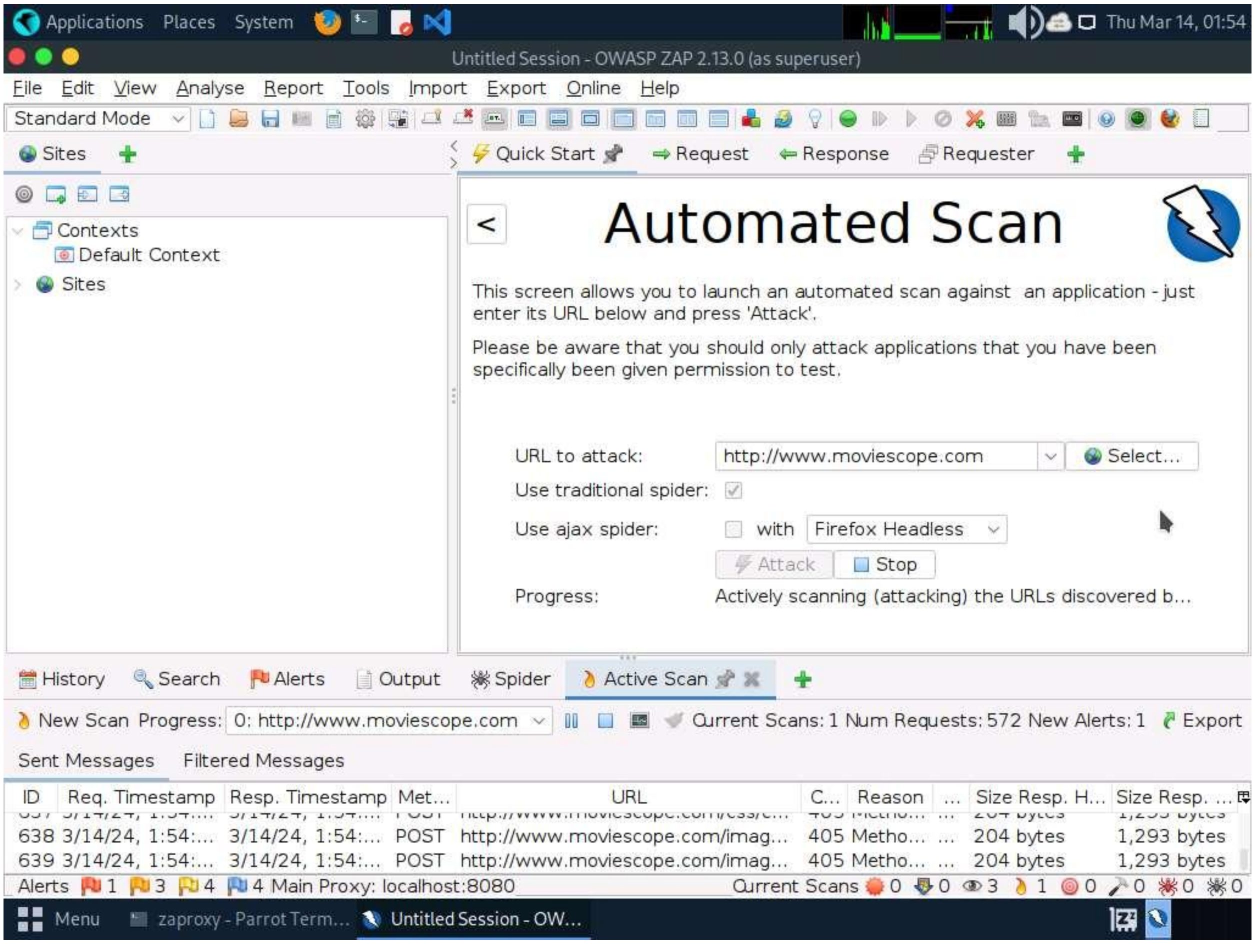
Use traditional spider: ☑

Use ajax spider: □ with Firefox Headless

Attack Stop

Progress: Not started

8. **OWASP ZAP** starts scanning the target website. You can observe various URLs under the **Spider** tab.



Untitled Session - OWASP ZAP 2.13.0 (as superuser)

Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

URL to attack: http://www.moviescope.com

Use traditional spider: ☑

Use ajax spider: □ with Firefox Headless

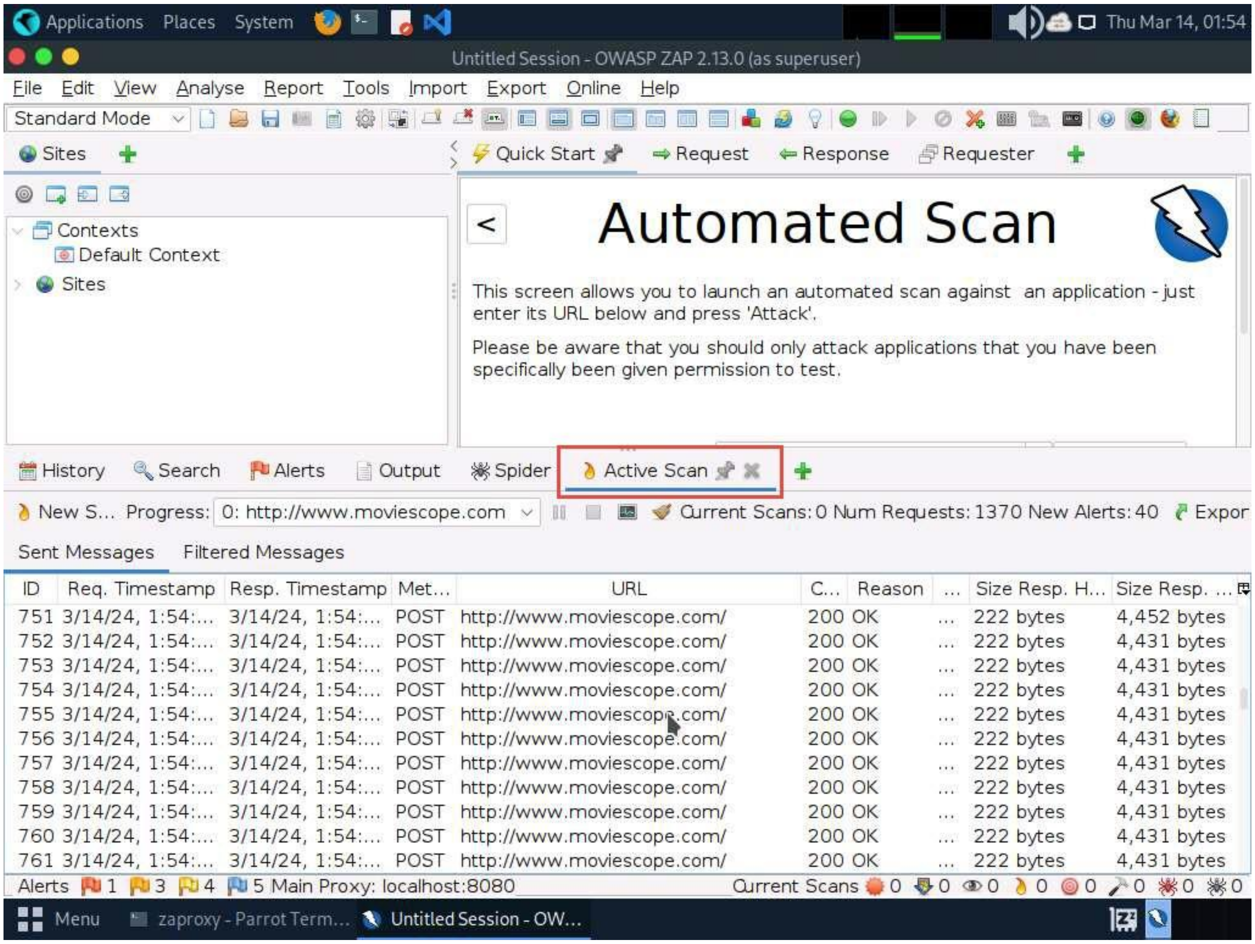
Progress: Actively scanning (attacking) the URLs discovered b...

New Scan Progress: 0: http://www.moviescope.com Current Scans: 1 Num Requests: 572 New Alerts: 1 Export

ID	Req. Timestamp	Resp. Timestamp	Met...	URL	C...	Reason	...	Size Resp. H...	Size Resp. ...
637	3/14/24, 1:54:...	3/14/24, 1:54:...	POST	http://www.moviescope.com/css/c...	405	Metho...	...	204 bytes	1,293 bytes
638	3/14/24, 1:54:...	3/14/24, 1:54:...	POST	http://www.moviescope.com/imag...	405	Metho...	...	204 bytes	1,293 bytes
639	3/14/24, 1:54:...	3/14/24, 1:54:...	POST	http://www.moviescope.com/imag...	405	Metho...	...	204 bytes	1,293 bytes

Alerts 1 3 4 4 Main Proxy: localhost:8080 Current Scans 0 0 3 1 0 0 0 0

9. After performing web spidering, **OWASP ZAP** performs active scanning. Navigate to the **Active Scan** tab to observe the various scanned links.



Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

New S... Progress: 0: http://www.moviescope.com Current Scans: 0 Num Requests: 1370 New Alerts: 40 Expor

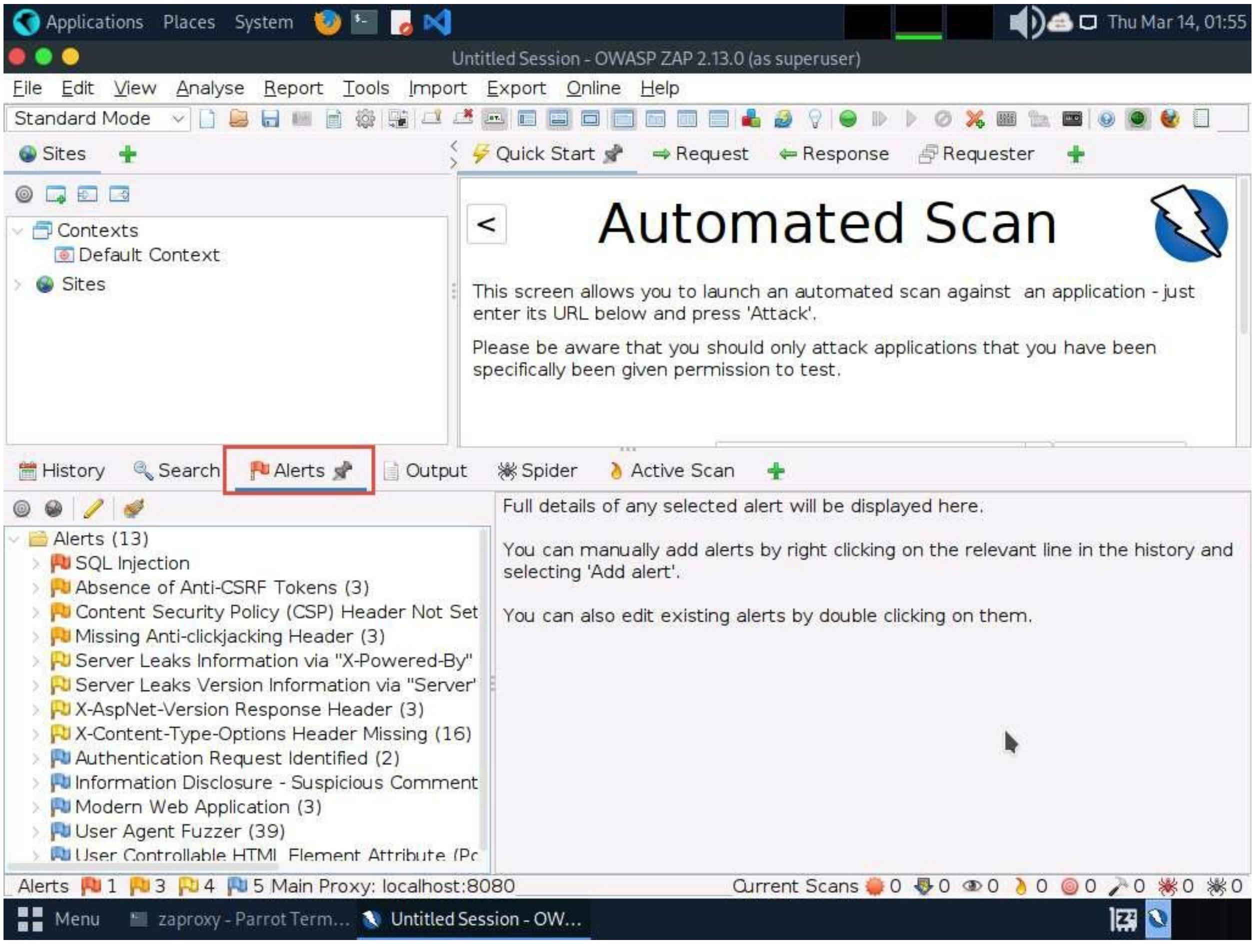
Sent Messages   Filtered Messages

ID	Req. Timestamp	Resp. Timestamp	Met...	URL	C...	Reason	...	Size Resp. H...	Size Resp. ...
751	3/14/24, 1:54:...	3/14/24, 1:54:...	POST	http://www.moviescope.com/	200	OK	...	222 bytes	4,452 bytes
752	3/14/24, 1:54:...	3/14/24, 1:54:...	POST	http://www.moviescope.com/	200	OK	...	222 bytes	4,431 bytes
753	3/14/24, 1:54:...	3/14/24, 1:54:...	POST	http://www.moviescope.com/	200	OK	...	222 bytes	4,431 bytes
754	3/14/24, 1:54:...	3/14/24, 1:54:...	POST	http://www.moviescope.com/	200	OK	...	222 bytes	4,431 bytes
755	3/14/24, 1:54:...	3/14/24, 1:54:...	POST	http://www.moviescope.com/	200	OK	...	222 bytes	4,431 bytes
756	3/14/24, 1:54:...	3/14/24, 1:54:...	POST	http://www.moviescope.com/	200	OK	...	222 bytes	4,431 bytes
757	3/14/24, 1:54:...	3/14/24, 1:54:...	POST	http://www.moviescope.com/	200	OK	...	222 bytes	4,431 bytes
758	3/14/24, 1:54:...	3/14/24, 1:54:...	POST	http://www.moviescope.com/	200	OK	...	222 bytes	4,431 bytes
759	3/14/24, 1:54:...	3/14/24, 1:54:...	POST	http://www.moviescope.com/	200	OK	...	222 bytes	4,431 bytes
760	3/14/24, 1:54:...	3/14/24, 1:54:...	POST	http://www.moviescope.com/	200	OK	...	222 bytes	4,431 bytes
761	3/14/24, 1:54:...	3/14/24, 1:54:...	POST	http://www.moviescope.com/	200	OK	...	222 bytes	4,431 bytes

Alerts 1 3 4 5 Main Proxy: localhost:8080   Current Scans 0 0 0 0 0 0 0 0

10. After completing the active scan, the results appear under the **Alerts** tab, displaying the various vulnerabilities and issues associated with the target website, as shown in the screenshot.

In this task, the objective being web spidering, we will focus on the information obtained while performing web spidering.



Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

Alerts (13)
- SQL Injection
- Absence of Anti-CSRF Tokens (3)
- Content Security Policy (CSP) Header Not Set
- Missing Anti-clickjacking Header (3)
- Server Leaks Information via "X-Powered-By"
- Server Leaks Version Information via "Server"
- X-AspNet-Version Response Header (3)
- X-Content-Type-Options Header Missing (16)
- Authentication Request Identified (2)
- Information Disclosure - Suspicious Comment
- Modern Web Application (3)
- User Agent Fuzzer (39)
- User Controllable HTML Element Attribute (Pc

Full details of any selected alert will be displayed here.

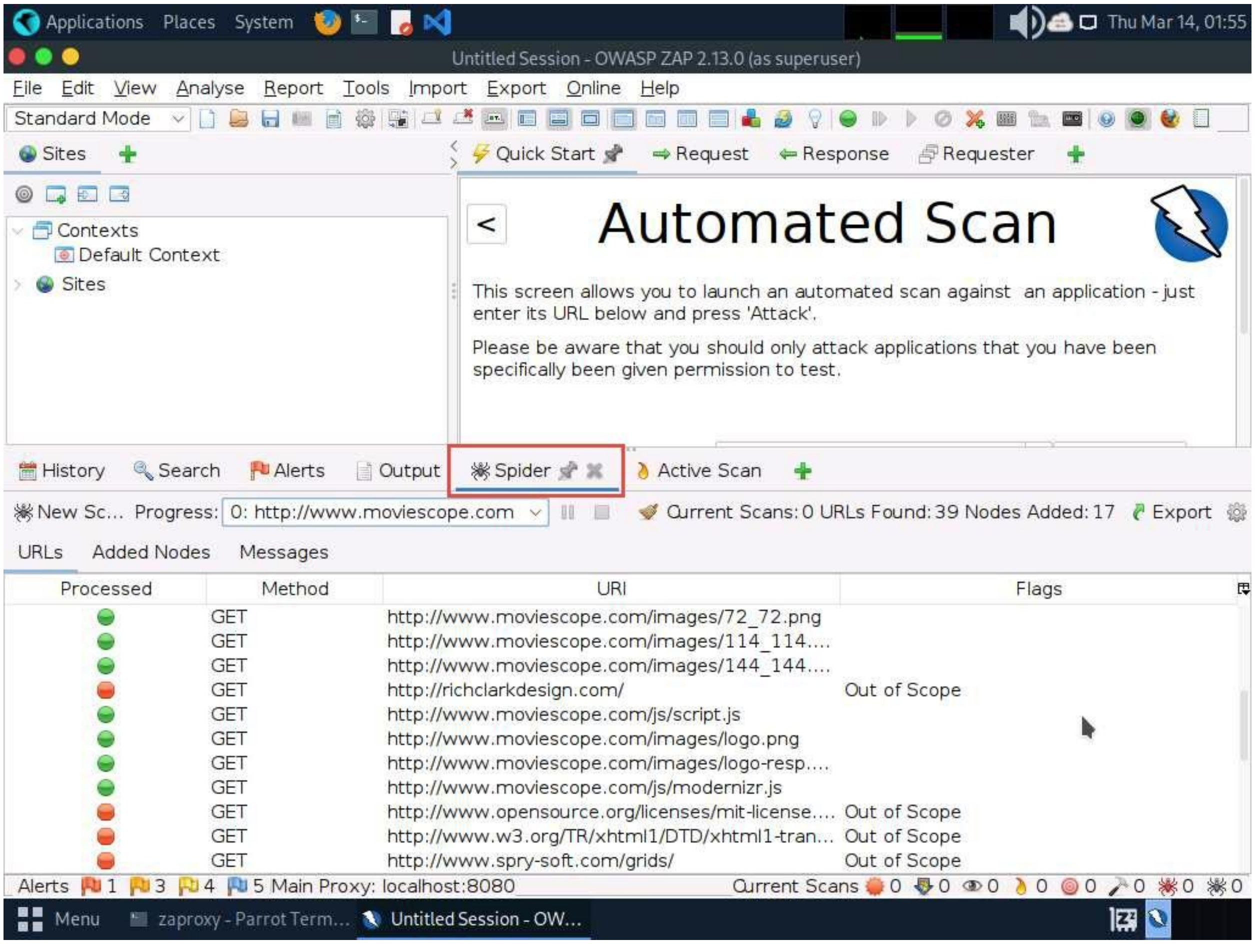
You can manually add alerts by right clicking on the relevant line in the history and selecting 'Add alert'.

You can also edit existing alerts by double clicking on them.

Alerts 1 3 4 5 Main Proxy: localhost:8080 Current Scans 0 0 0 0 0 0 0 0

11. Now, click on the **Spider** tab from the lower section of the window to view the web spidering information. By default, the **URLs** tab appears under the **Spider** tab.

12. The **URLs** tab contains various links for hidden content and functionality associated with the target website (**www.moviescope.com**).



Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

Progress: 0: http://www.moviescope.com

Current Scans: 0 URLs Found: 39 Nodes Added: 17

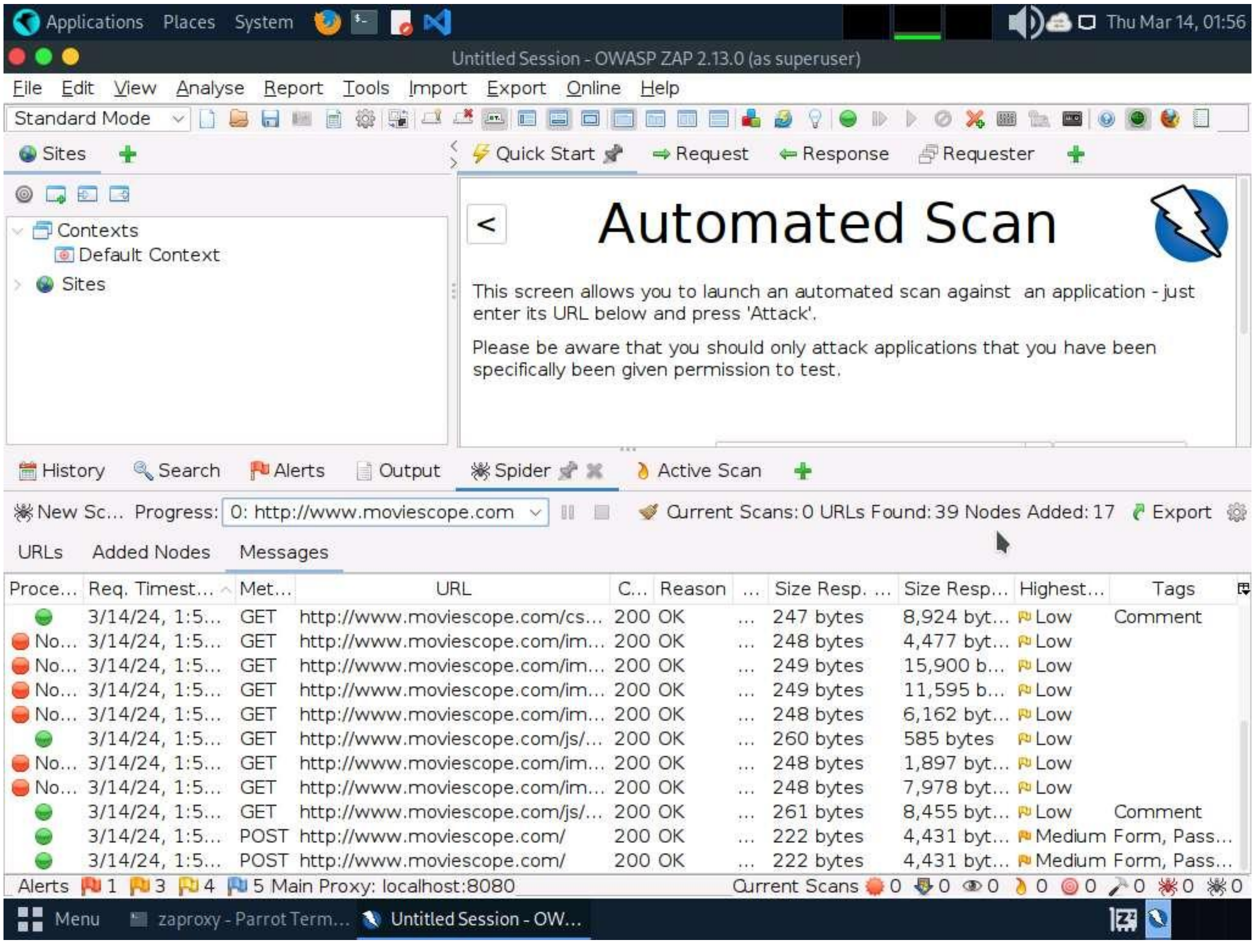
Processed	Method	URI	Flags
●	GET	http://www.moviescope.com/images/72_72.png	
●	GET	http://www.moviescope.com/images/114_114....	
●	GET	http://www.moviescope.com/images/144_144....	
●	GET	http://richclarkdesign.com/	Out of Scope
●	GET	http://www.moviescope.com/js/script.js	
●	GET	http://www.moviescope.com/images/logo.png	
●	GET	http://www.moviescope.com/images/logo-resp....	
●	GET	http://www.moviescope.com/js/modernizr.js	
●	GET	http://www.opensource.org/licenses/mit-license....	Out of Scope
●	GET	http://www.w3.org/TR/xhtml1/DTD/xhtml1-tran...	Out of Scope
●	GET	http://www.spry-soft.com/grids/	Out of Scope

Alerts 1 3 4 5 Main Proxy: localhost:8080 Current Scans 0 0 0 0 0 0 0 0

13. Now, navigate to the **Messages** tab under the **Spider** tab to view more detailed information regarding the URLs obtained while performing the web spidering, as shown in the screenshot.

In real-time, attackers perform web spidering or crawling to discover hidden content and functionality, which is not reachable from the main visible content, to exploit user privileges within the application. It also allows attackers to recover backup copies of live files, configuration and log files containing sensitive data, backup archives containing snapshots of files within the web root, and new functionality that is not linked to the main application.

more...



Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

Progress: 0: http://www.moviescope.com   Current Scans: 0 URLs Found: 39 Nodes Added: 17

Proce...	Req. Timest...	Met...	URL	C...	Reason	...	Size Resp. ...	Size Resp...	Highest...	Tags
●	3/14/24, 1:5...	GET	http://www.moviescope.com/cs...	200	OK	...	247 bytes	8,924 byt...	Low	Comment
● No...	3/14/24, 1:5...	GET	http://www.moviescope.com/im...	200	OK	...	248 bytes	4,477 byt...	Low	
● No...	3/14/24, 1:5...	GET	http://www.moviescope.com/im...	200	OK	...	249 bytes	15,900 b...	Low	
● No...	3/14/24, 1:5...	GET	http://www.moviescope.com/im...	200	OK	...	249 bytes	11,595 b...	Low	
● No...	3/14/24, 1:5...	GET	http://www.moviescope.com/im...	200	OK	...	248 bytes	6,162 byt...	Low	
●	3/14/24, 1:5...	GET	http://www.moviescope.com/js/...	200	OK	...	260 bytes	585 bytes	Low	
● No...	3/14/24, 1:5...	GET	http://www.moviescope.com/im...	200	OK	...	248 bytes	1,897 byt...	Low	
● No...	3/14/24, 1:5...	GET	http://www.moviescope.com/im...	200	OK	...	248 bytes	7,978 byt...	Low	
●	3/14/24, 1:5...	GET	http://www.moviescope.com/js/...	200	OK	...	261 bytes	8,455 byt...	Low	Comment
●	3/14/24, 1:5...	POST	http://www.moviescope.com/	200	OK	...	222 bytes	4,431 byt...	Medium	Form, Pass...
●	3/14/24, 1:5...	POST	http://www.moviescope.com/	200	OK	...	222 bytes	4,431 byt...	Medium	Form, Pass...

Alerts 1 3 4 5 Main Proxy: localhost:8080   Current Scans 0 0 0 0 0 0 0 0

14. This concludes the demonstration of how to perform web spidering on a target website using OWASP ZAP.

15. Close all open windows and document all acquired information.

Question 14.1.2.1

Perform web spidering on the www.moviescope.com website using OWASP ZAP. Enter the name of the tab on the OWASP ZAP application that allows you to view detailed information regarding the URLs obtained while performing web spidering.

Task 3: Perform Web Application Vulnerability Scanning using SmartScanner

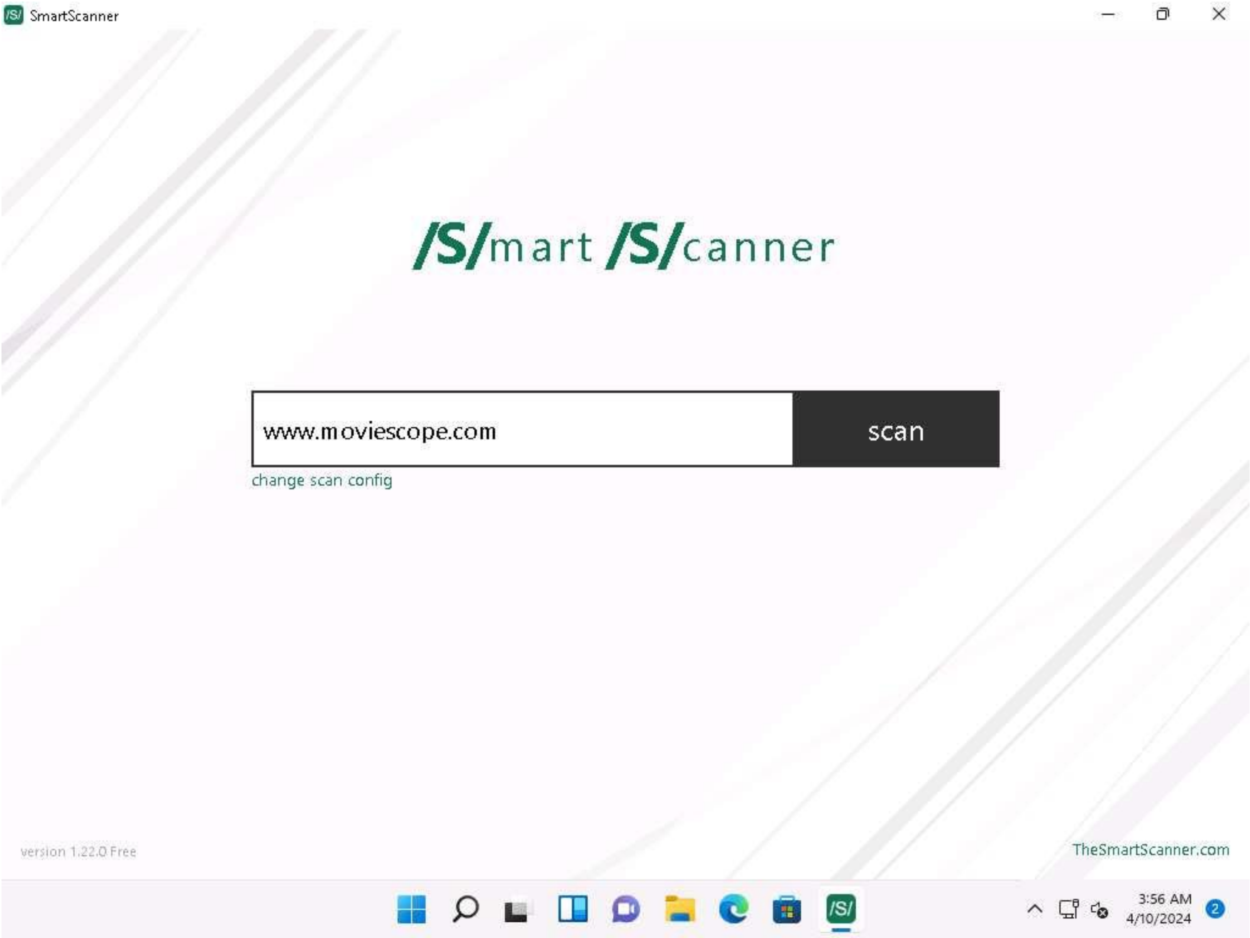
SmartScanner leverages machine learning (ML) and artificial intelligence (AI) techniques to adapt its methodologies to the behavior of the target. This integration allows SmartScanner to minimize false positives. It uses AI for identifying vulnerable pages, detecting 404 custom pages, identifying input vectors, fingerprinting the target and calculating the security risk.

Here, we will discover vulnerabilities in the target web application using SmartScanner.

1. Click Windows 11 to switch to the **Windows 11** machine, click Ctrl+Alt+Delete to activate the machine and login using **Admin/Pa$$w0rd**.

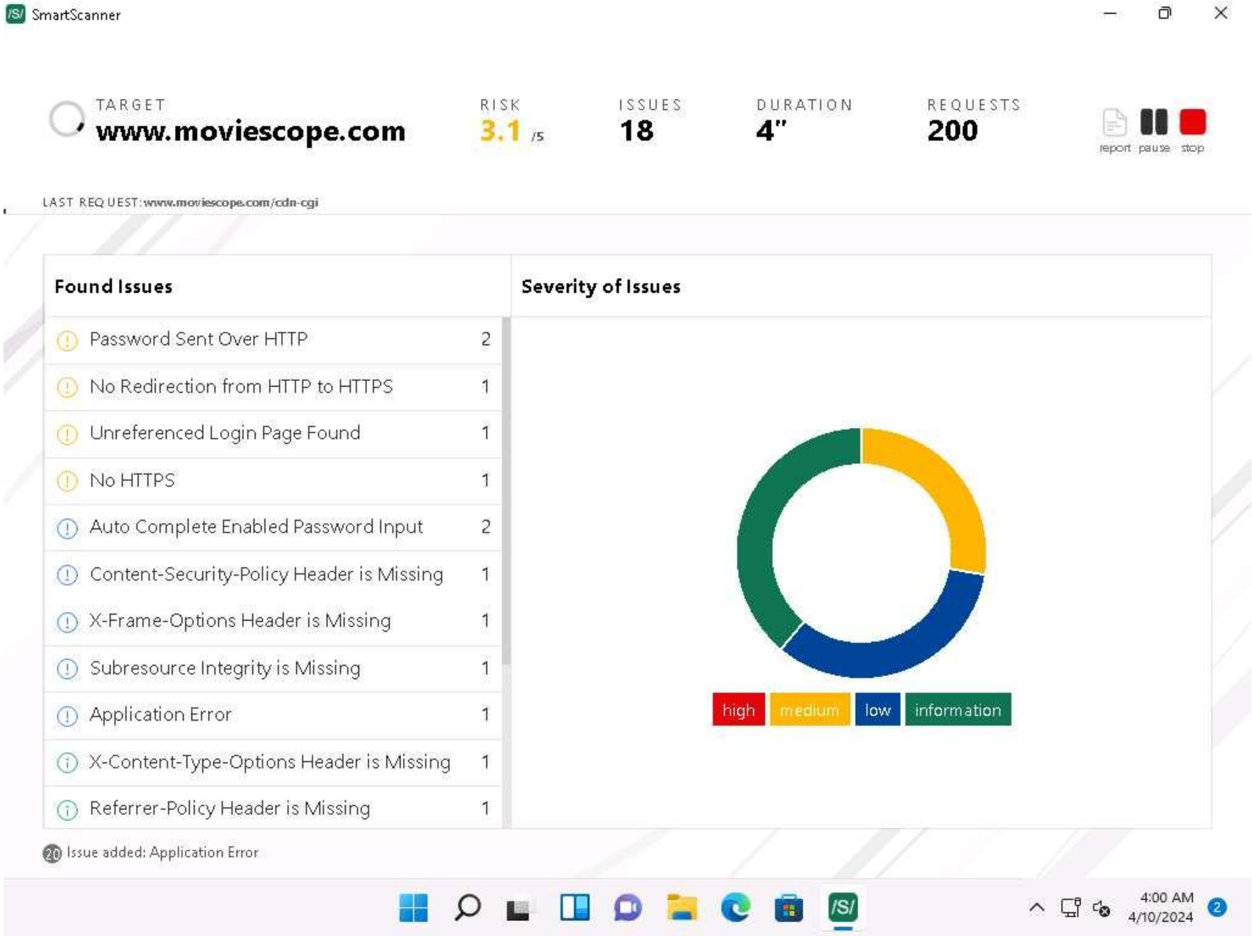
2. Click **Search** icon (🔍) on the **Desktop**. Search **smartscanner** in the search field, the **SmartScanner** appears in the results, click **Open** to launch it.

3. **SmartScanner** window appears. In the **enter site address to scan** field, enter **www.moviescope.com** and click **scan** button.



www.moviescope.com

4. The tool starts scanning the target website for vulnerabilities.



TARGET www.moviescope.com

RISK 3.1 /5

ISSUES 18

DURATION 4"

REQUESTS 200

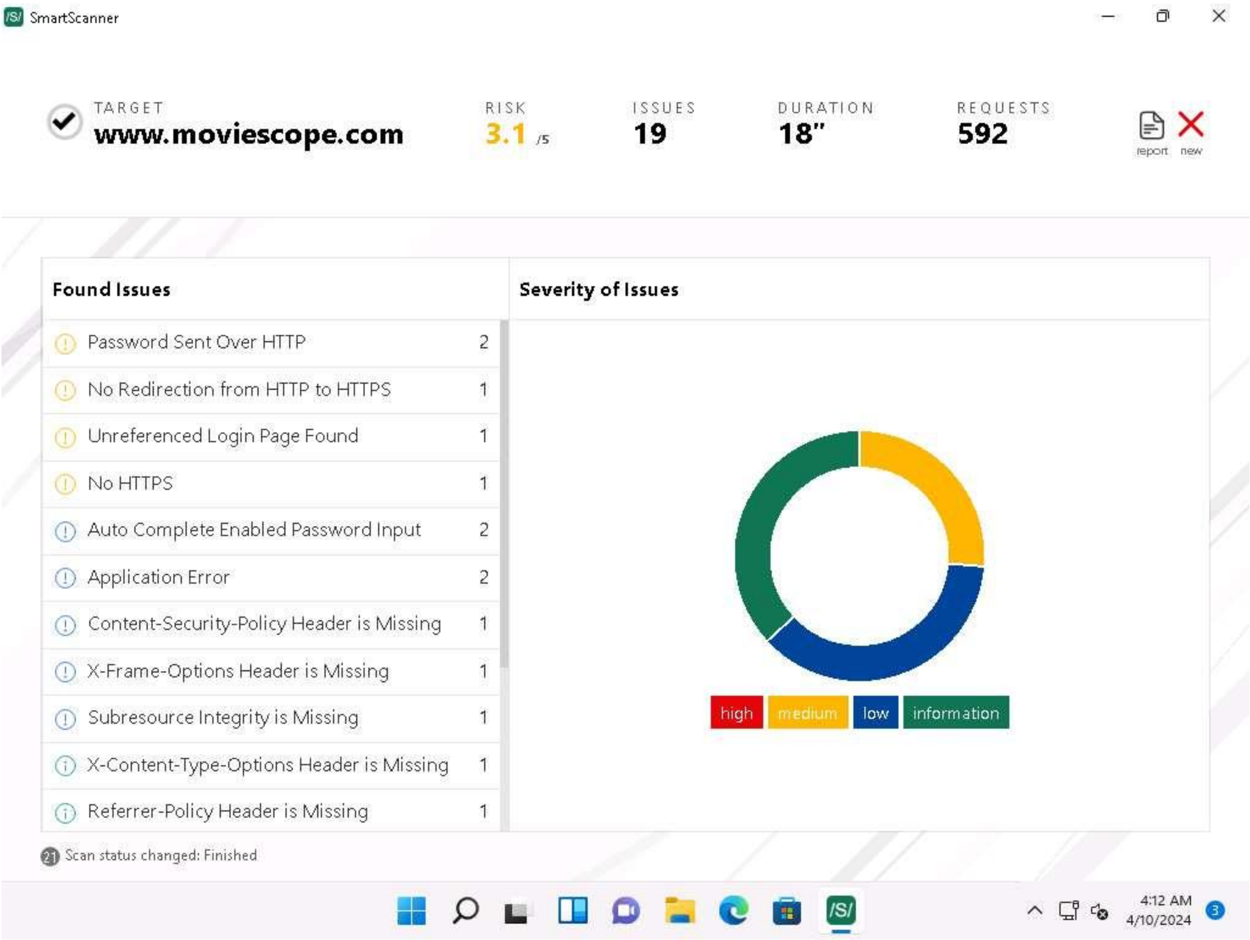
LAST REQUEST: www.moviescope.com/cdn-cgi

Found Issues	
Password Sent Over HTTP	2
No Redirection from HTTP to HTTPS	1
Unreferenced Login Page Found	1
No HTTPS	1
Auto Complete Enabled Password Input	2
Content-Security-Policy Header is Missing	1
X-Frame-Options Header is Missing	1
Subresource Integrity is Missing	1
Application Error	1
X-Content-Type-Options Header is Missing	1
Referrer-Policy Header is Missing	1

Severity of Issues

20 Issue added: Application Error

5. Once the tool completes scanning, it will display the issues that are found under **Found Issues** section and **Severity of Issues**.



TARGET www.moviescope.com

RISK 3.1 /5

ISSUES 19

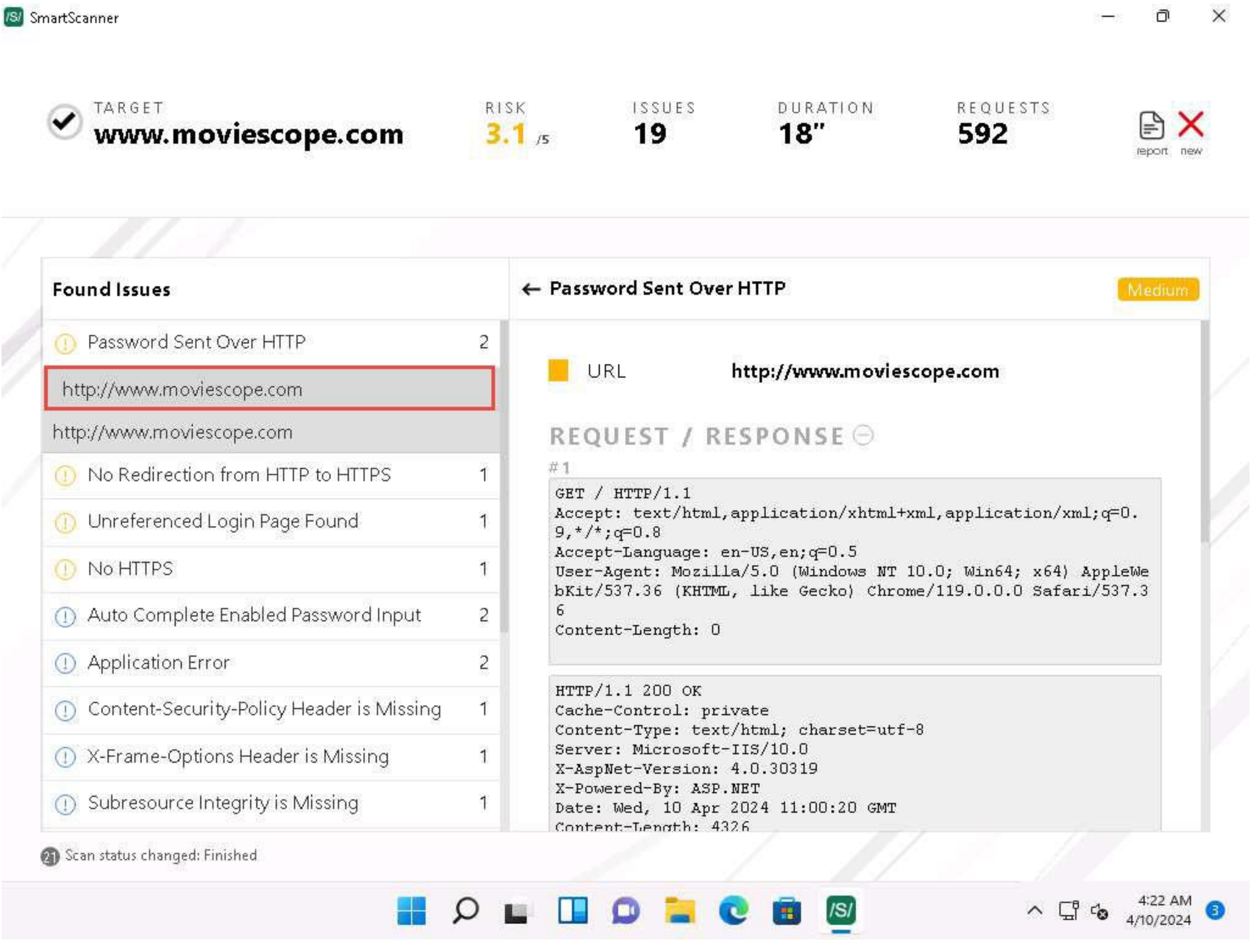
DURATION 18"

REQUESTS 592

Found Issues	
Password Sent Over HTTP	2
No Redirection from HTTP to HTTPS	1
Unreferenced Login Page Found	1
No HTTPS	1
Auto Complete Enabled Password Input	2
Application Error	2
Content-Security-Policy Header is Missing	1
X-Frame-Options Header is Missing	1
Subresource Integrity is Missing	1
X-Content-Type-Options Header is Missing	1
Referrer-Policy Header is Missing	1

21 Scan status changed: Finished

6. Now, expand **Password Sent Over HTTP** and click on first **http://www.moviescope.com** link from the left pane to view the details of the vulnerability.



TARGET www.moviescope.com

RISK 3.1 /5

ISSUES 19

DURATION 18"

REQUESTS 592

Found Issues

Password Sent Over HTTP	2
http://www.moviescope.com	
http://www.moviescope.com	
No Redirection from HTTP to HTTPS	1
Unreferenced Login Page Found	1
No HTTPS	1
Auto Complete Enabled Password Input	2
Application Error	2
Content-Security-Policy Header is Missing	1
X-Frame-Options Header is Missing	1
Subresource Integrity is Missing	1

← Password Sent Over HTTP Medium

URL http://www.moviescope.com

REQUEST / RESPONSE

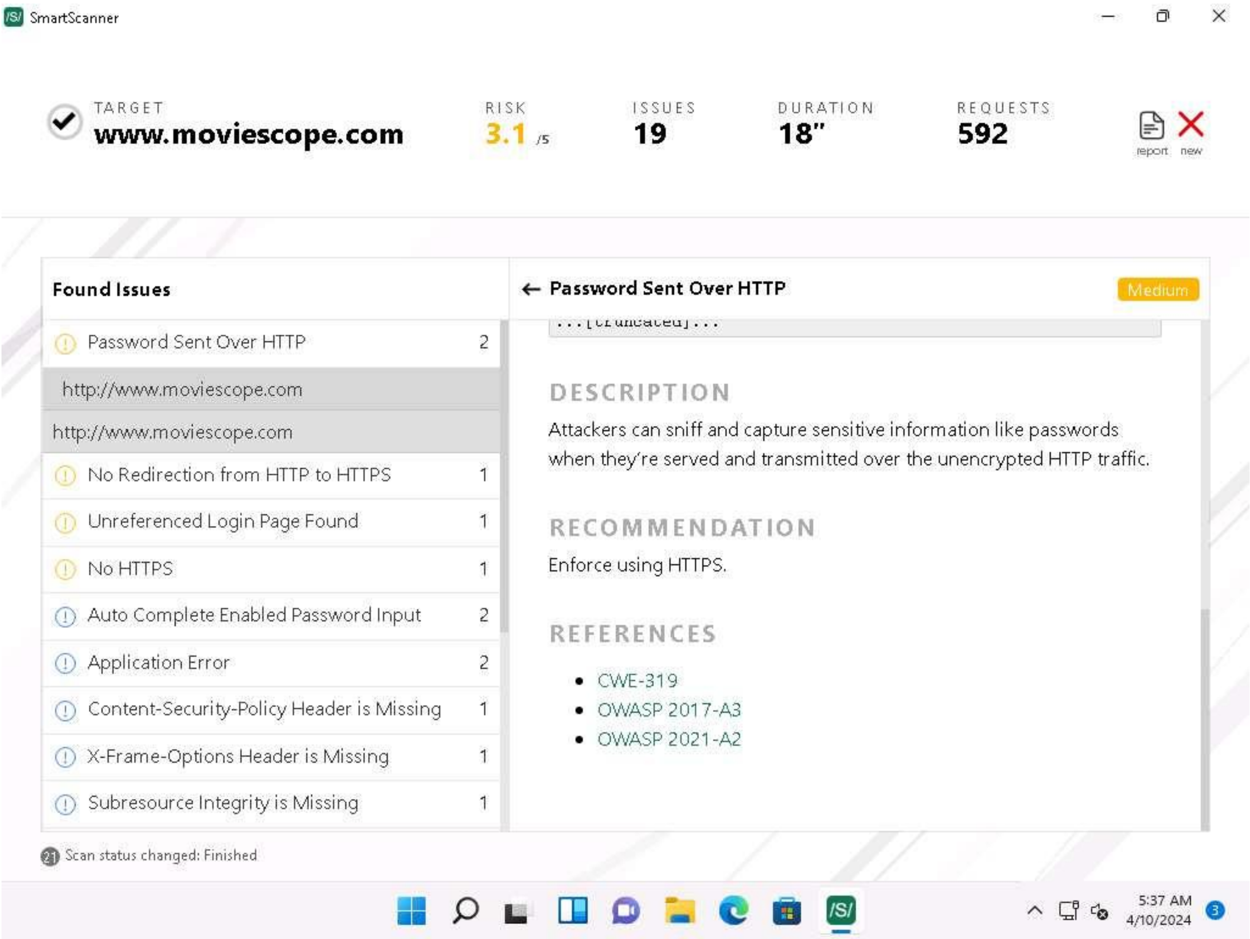
#1

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.
9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWe
bKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.3
6
Content-Length: 0
```

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/10.0
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 10 Apr 2024 11:00:20 GMT
Content-Length: 4326
```

21 Scan status changed: Finished

7. In the right pane, scroll down to the **DESCRIPTION** part. We can observe that this website contains a vulnerability, which could be exploited by attackers to intercept sensitive information like passwords during transmission over unencrypted HTTP traffic.



TARGET **www.moviescope.com**

RISK **3.1** /5

ISSUES **19**

DURATION **18"**

REQUESTS **592**

Found Issues

Password Sent Over HTTP	2
http://www.moviescope.com	
http://www.moviescope.com	
No Redirection from HTTP to HTTPS	1
Unreferenced Login Page Found	1
No HTTPS	1
Auto Complete Enabled Password Input	2
Application Error	2
Content-Security-Policy Header is Missing	1
X-Frame-Options Header is Missing	1
Subresource Integrity is Missing	1

← **Password Sent Over HTTP** Medium

```
...[truncated]...
```

DESCRIPTION

Attackers can sniff and capture sensitive information like passwords when they're served and transmitted over the unencrypted HTTP traffic.

RECOMMENDATION

Enforce using HTTPS.

REFERENCES

- CWE-319
- OWASP 2017-A3
- OWASP 2021-A2

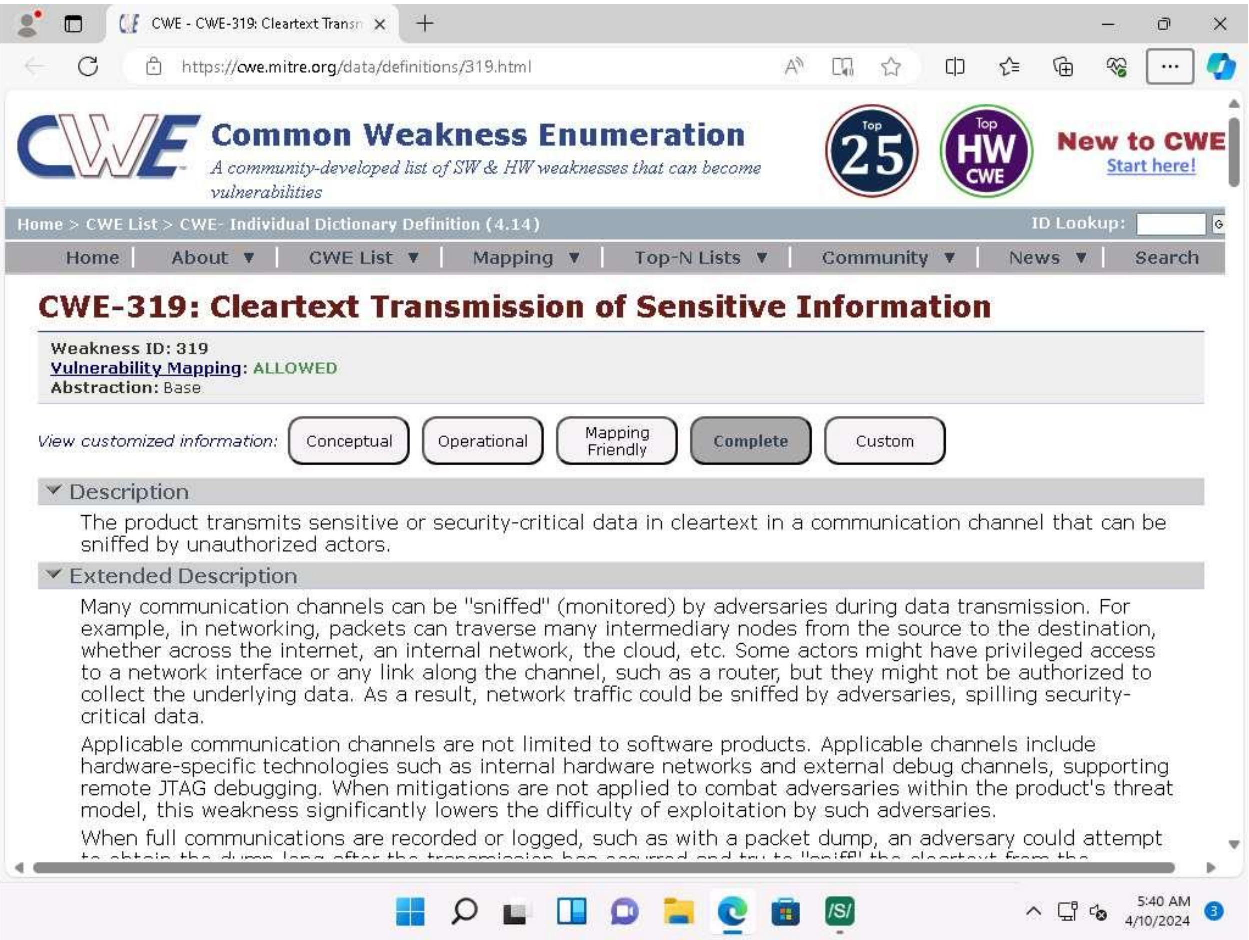
21 Scan status changed: Finished

5:37 AM
4/10/2024

8. You can also go through the **RECOMMENDATION** section to check for the recommended actions to patch the vulnerability.

9. Now, under **REFERENCES** section, press **Ctrl** and click on **CWE-319** hyperlink .

10. A CWE website appears in **Microsoft Edge** web browser, displaying the details of **CWE-319 ClearText Transmission of Sensitive Information**.



CWE - CWE-319: Cleartext Transn
https://cwe.mitre.org/data/definitions/319.html
Common Weakness Enumeration
A community-developed list of SW & HW weaknesses that can become vulnerabilities
Top 25
Top HW CWE
New to CWE
Start here!
Home > CWE List > CWE- Individual Dictionary Definition (4.14)
ID Lookup:
Home
About ▼
CWE List ▼
Mapping ▼
Top-N Lists ▼
Community ▼
News ▼
Search
View customized information:
Conceptual
Operational
Mapping Friendly
Complete
Custom
5:40 AM
4/10/2024

CWE-319: Cleartext Transmission of Sensitive Information

Weakness ID: 319
Vulnerability Mapping: ALLOWED
Abstraction: Base

Description

The product transmits sensitive or security-critical data in cleartext in a communication channel that can be sniffed by unauthorized actors.

Extended Description

Many communication channels can be "sniffed" (monitored) by adversaries during data transmission. For example, in networking, packets can traverse many intermediary nodes from the source to the destination, whether across the internet, an internal network, the cloud, etc. Some actors might have privileged access to a network interface or any link along the channel, such as a router, but they might not be authorized to collect the underlying data. As a result, network traffic could be sniffed by adversaries, spilling security-critical data.

Applicable communication channels are not limited to software products. Applicable channels include hardware-specific technologies such as internal hardware networks and external debug channels, supporting remote JTAG debugging. When mitigations are not applied to combat adversaries within the product's threat model, this weakness significantly lowers the difficulty of exploitation by such adversaries.

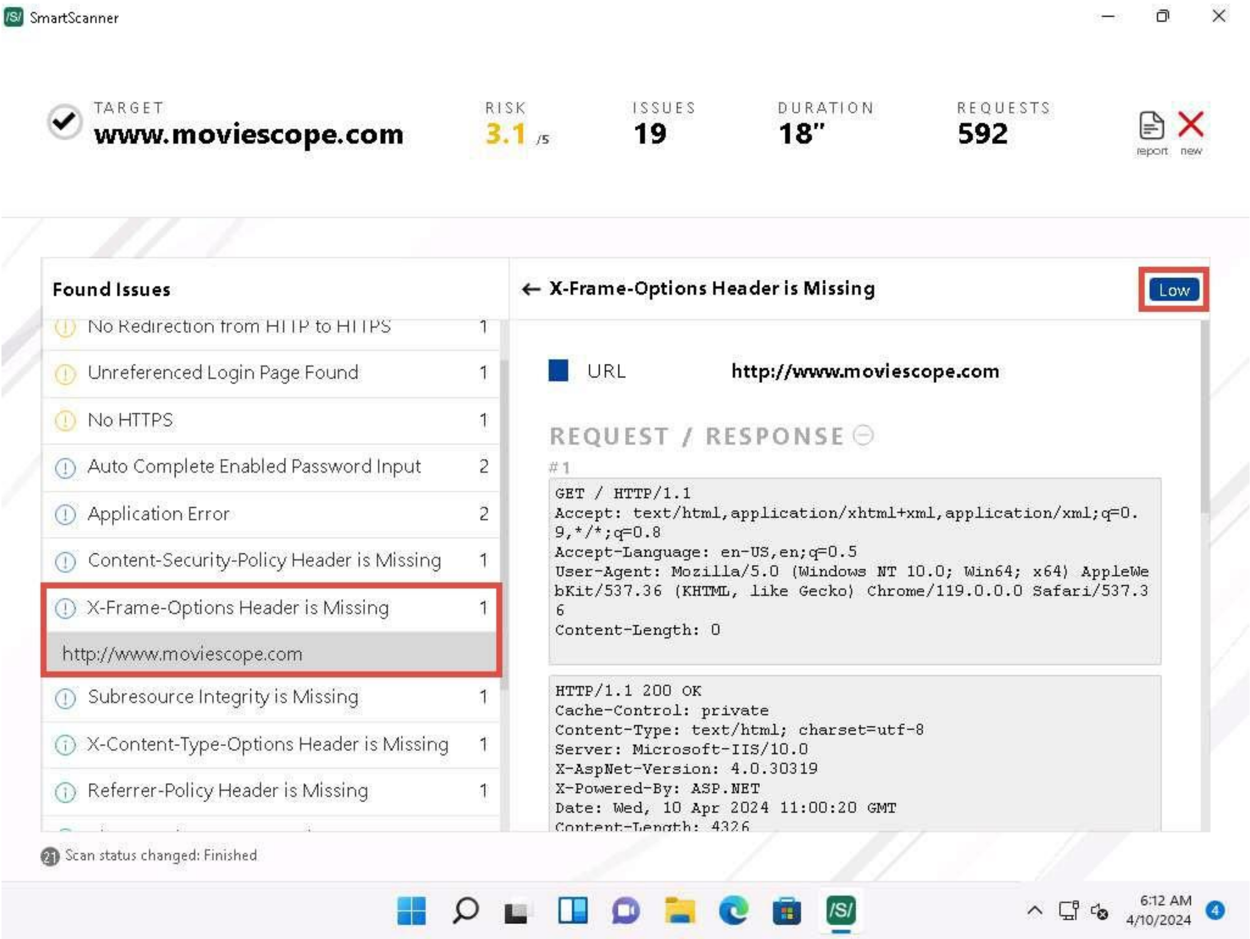
When full communications are recorded or logged, such as with a packet dump, an adversary could attempt

11. In the CWE page, we can see that the attackers can gather sensitive information such as passwords etc. by sniffing the network, if the information is transmitted in cleartext format.

We have already performed a lab about **Password Sniffing using Wireshark** in **Module 08: Sniffing**.

12. Close the browser window and switch to the SmartScanner window.

13. Similarly, click the **http://www.moviescope.com** link available under **X-Frame-Options Header is Missing** node which is termed as **Low** severity.



TARGET www.moviescope.com RISK 3.1 /5 ISSUES 19 DURATION 18" REQUESTS 592

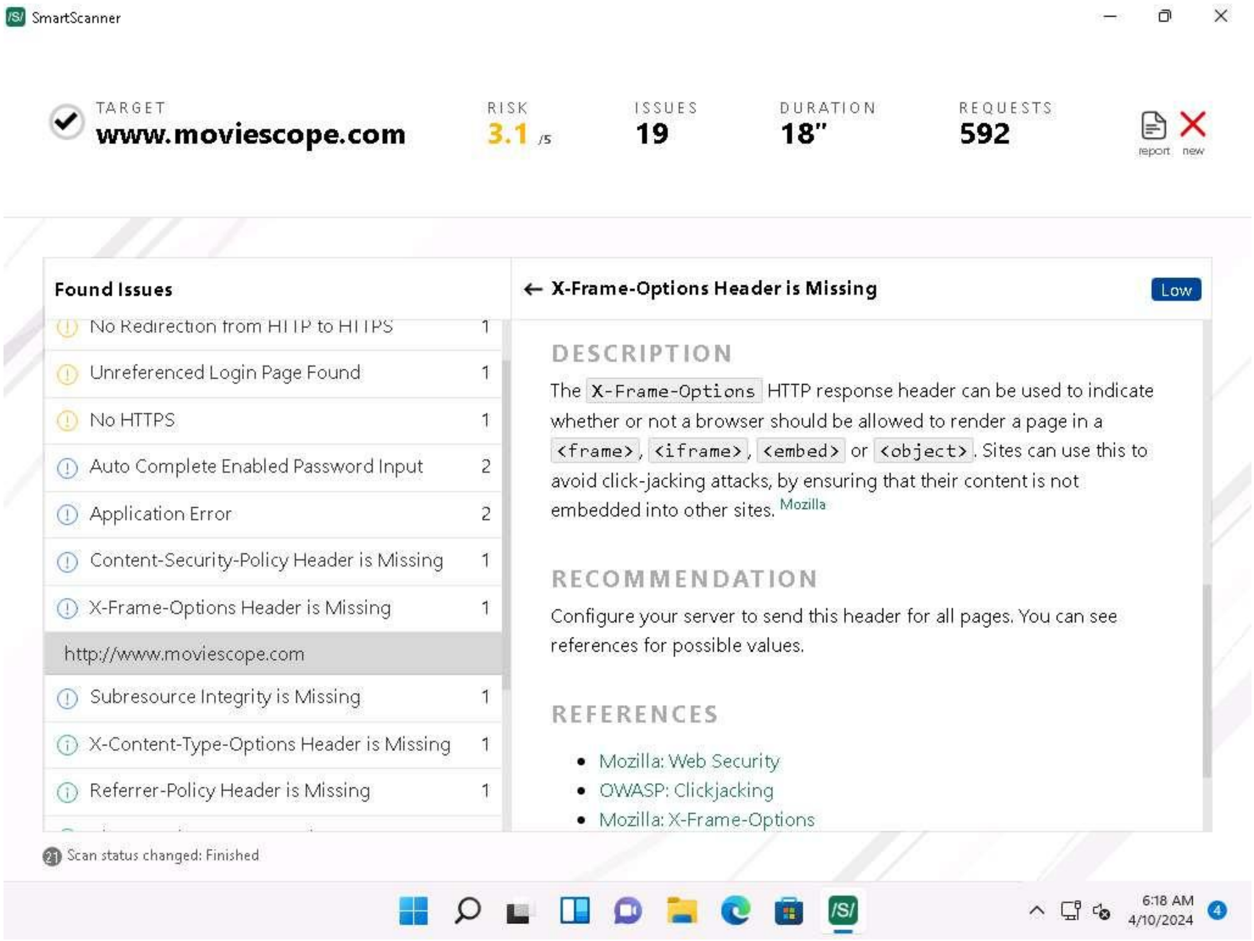
No Redirection from HTTP to HTTPS	1
Unreferenced Login Page Found	1
No HTTPS	1
Auto Complete Enabled Password Input	2
Application Error	2
Content-Security-Policy Header is Missing	1
X-Frame-Options Header is Missing	1
http://www.moviescope.com	
Subresource Integrity is Missing	1
X-Content-Type-Options Header is Missing	1
Referrer-Policy Header is Missing	1

URL http://www.moviescope.com

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.
9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWe
bKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.3
6
Content-Length: 0
```

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/10.0
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 10 Apr 2024 11:00:20 GMT
Content-Length: 4326
```

14. Scroll down to the **DESCRIPTION** here, we can observe that the **X-Frame-Options Header is Missing** which will make this site vulnerable to click-jacking.


SmartScanner

TARGET
www.moviescope.com

RISK 3.1 /5

ISSUES 19

DURATION 18"

REQUESTS 592

Found Issues

No Redirection from HTTP to HTTPS	1
Unreferenced Login Page Found	1
No HTTPS	1
Auto Complete Enabled Password Input	2
Application Error	2
Content-Security-Policy Header is Missing	1
X-Frame-Options Header is Missing	1
http://www.moviescope.com	
Subresource Integrity is Missing	1
X-Content-Type-Options Header is Missing	1
Referrer-Policy Header is Missing	1

← **X-Frame-Options Header is Missing** Low

DESCRIPTION

The `X-Frame-Options` HTTP response header can be used to indicate whether or not a browser should be allowed to render a page in a `<frame>`, `<iframe>`, `<embed>` or `<object>`. Sites can use this to avoid click-jacking attacks, by ensuring that their content is not embedded into other sites. Mozilla

RECOMMENDATION

Configure your server to send this header for all pages. You can see references for possible values.

REFERENCES

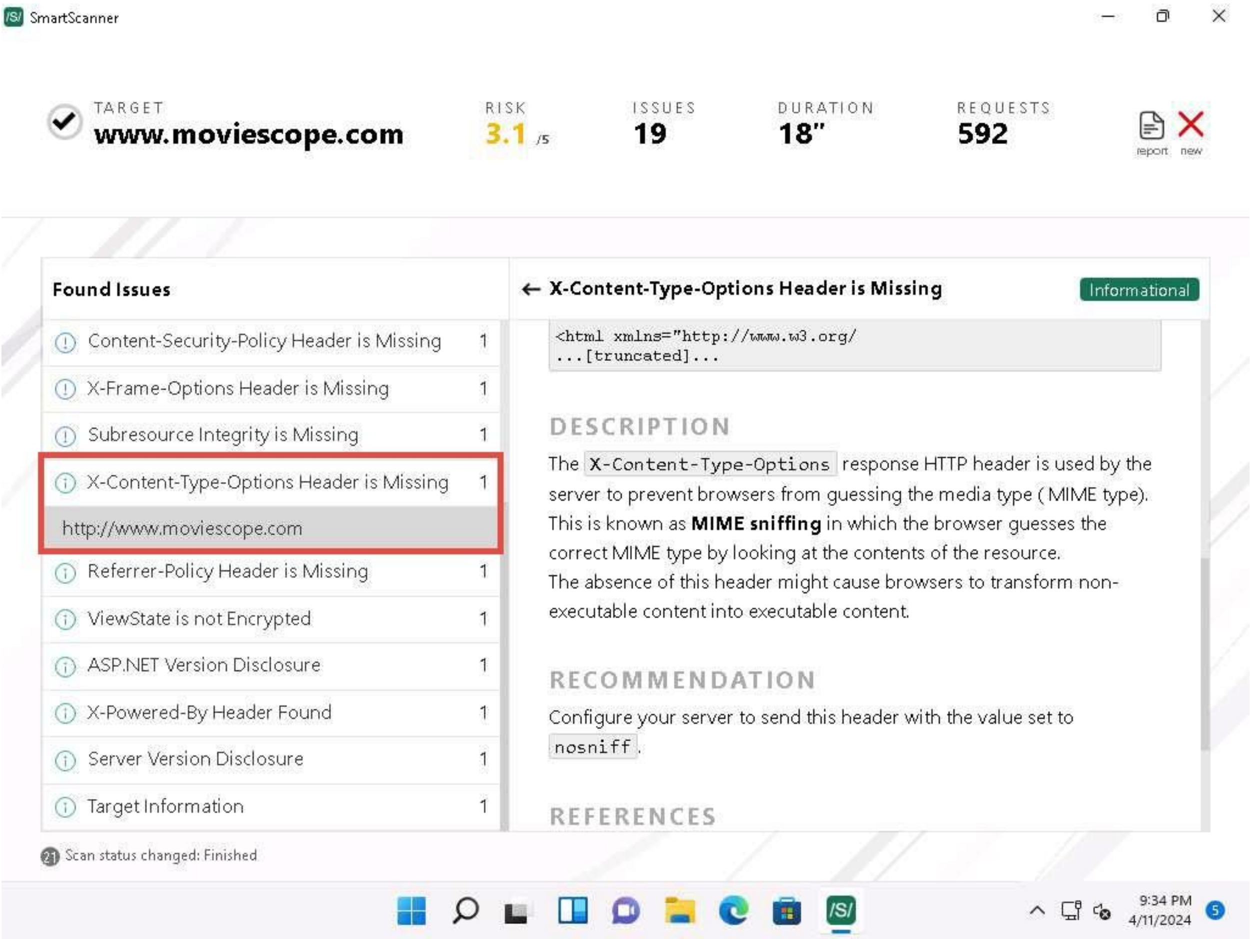
- Mozilla: Web Security
- OWASP: Clickjacking
- Mozilla: X-Frame-Options

Scan status changed: Finished

15. Similarly, you can view the **RECOMMENDATION** section and click on the reference link under **REFERENCES** section.

16. Now, expand **X-Content-Type-Options Header is Missing** node and click on **http://www.moviescope.com** link to view its contents.

17. Under **DESCRIPTION** section we can observe that the browsers can perform **MIME sniffing** which can cause the browsers to transform non-executable content into executable content.



TARGET
www.moviescope.com

RISK 3.1 /5 | ISSUES 19 | DURATION 18" | REQUESTS 592

Found Issues

Content-Security-Policy Header is Missing	1
X-Frame-Options Header is Missing	1
Subresource Integrity is Missing	1
X-Content-Type-Options Header is Missing	1
http://www.moviescope.com	
Referrer-Policy Header is Missing	1
ViewState is not Encrypted	1
ASP.NET Version Disclosure	1
X-Powered-By Header Found	1
Server Version Disclosure	1
Target Information	1

← **X-Content-Type-Options Header is Missing** Informational

```
<html xmlns="http://www.w3.org/
...[truncated]...
```

DESCRIPTION

The `X-Content-Type-Options` response HTTP header is used by the server to prevent browsers from guessing the media type (MIME type). This is known as **MIME sniffing** in which the browser guesses the correct MIME type by looking at the contents of the resource.
The absence of this header might cause browsers to transform non-executable content into executable content.

RECOMMENDATION

Configure your server to send this header with the value set to `nosniff`.

REFERENCES

21 Scan status changed: Finished

18. Similarly, you can view the the **RECOMMENDATION** section and click on the reference link under **REFERENCES** section.

19. You can also click on any other vulnerability to view its detailed information.

20. This concludes the demonstration of discovering vulnerabilities in a target website scanning using SmartScanner.

21. You can also use other web application vulnerability scanning tools such as **WPScan Vulnerability Database** (https://wpscan.com), **Codename SCNR** (https://ecsypno.com), **AppSpider** (https://www.rapid7.com), **Uniscan** (https://github.com) and **N-Stalker** (https://www.nstalker.com).

22. Close all open windows and document all acquired information.

Question 14.1.3.1

On the windows 11 machine use SmartScanner tool to perform vulnerability scan on www.moviescope.com and analyse the report. Enter the CWE ID that is connected to No redirects from HTTP to HTTPS vulnerability that is found on the target website while scanning.