CSYE 6225 - SU 19
PENETRATION TESTING

Overview:
Penetration testing was done on various end-points points of the AWS hosted web application to identify security vulnerabilities that can be exploited harmfully.
The Debian-based Kali Linux distribution is a common base for most penetration testing systems and hence the tools developed on it were used to identify possible attack vectors.
The following Kali Linux tools were used to test and identify attack vectors:

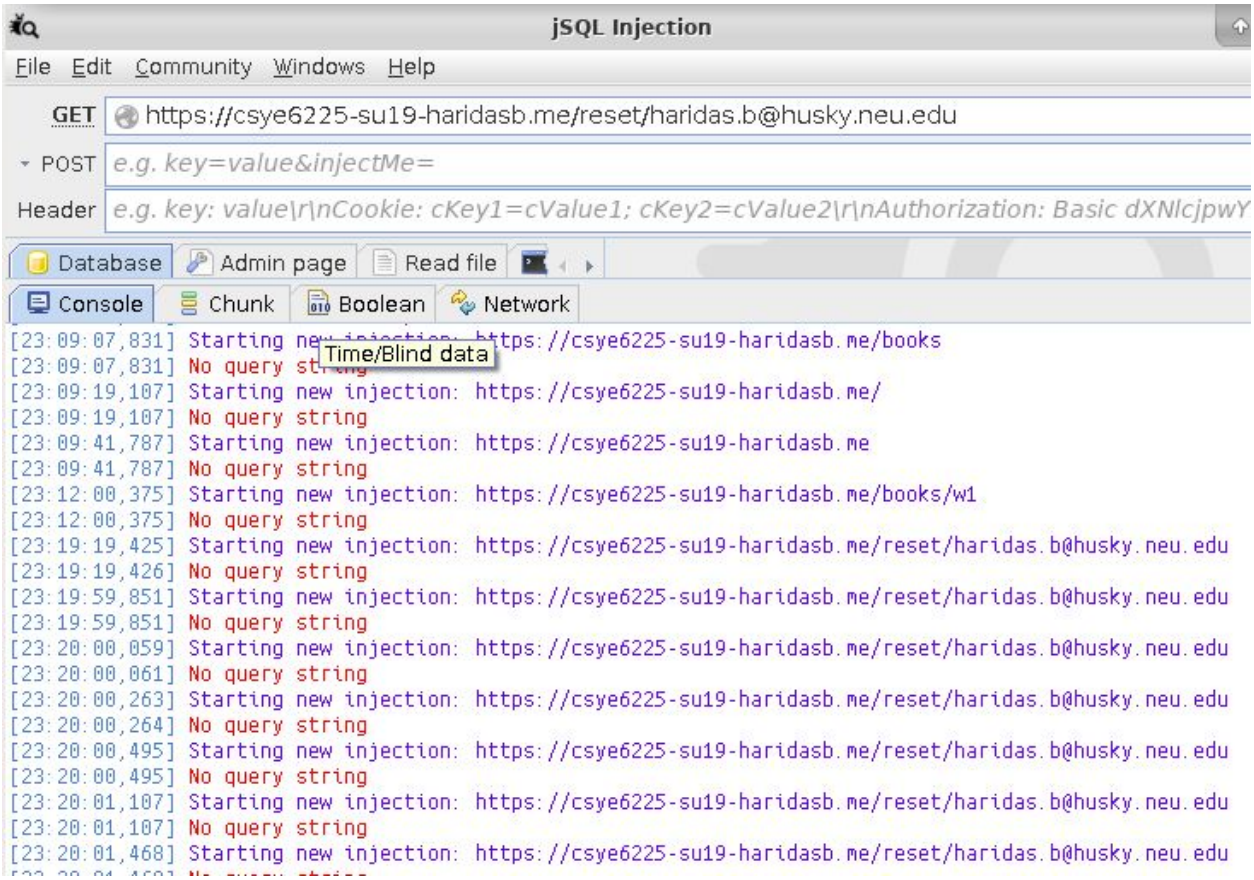
1. JSQL Injection

Attack Vector to be identified - SQL Injection

Reason for selection - SQL injection is widely used for backend database manipulation to access information that was not intended to be displayed.
It was important to test the ability of the Spring Boot application hosted on AWS Resources against any SQL queries returned or possible SQL injections made.

JSQL injection package was used to find database information from the remote server.

Result - No query results were returned from the server indicating no possibilities of a direct database injection to the server.



2. NMAP

Attack Vector to be identified - Passive Eavesdropping, DOS

Reason for selection - The scripts for nmap cover categories such as -S (safe - performs general network security scan that's less likely to alarm remote administrators) and -V (Vuln - finds vulnerabilities on the target) which are useful for a potential hacker in gaining a basic understanding of the network.

Result - Ports other than 443, 8080 and 80 were not recognised and filtered out .

```
root@kali:~/w3af# nmap -sS csye6225-su19-haridasb.me -D 10.0.0.1,10.0.0.2,10.
0.0.4
Starting Nmap 7.70 ( https://nmap.org ) at 2019-08-08 22:55 EDT
Nmap scan report for csye6225-su19-haridasb.me (3.216.175.210)
Host is up (0.030s latency).
Other addresses for csye6225-su19-haridasb.me (not scanned): 3.224.45.94
rDNS record for 3.216.175.210: ec2-3-216-175-210.compute-1.amazonaws.com
Not shown: 997 filtered ports
PORT     STATE  SERVICE
80/tcp   closed http
443/tcp  open   https
8080/tcp closed http-proxy

Nmap done: 1 IP address (1 host up) scanned in 96.37 seconds
```

HACKER TARGET SCANNERS

```
Starting Nmap 7.70 ( https://nmap.org ) at 2019-08-10 04:10 UTC
Nmap scan report for csye6225-su19-haridasb.me (54.174.153.76)
Host is up (0.0082s latency).
Other addresses for csye6225-su19-haridasb.me (not scanned): 3.223.75.36
rDNS record for 54.174.153.76: ec2-54-174-153-76.compute-1.amazonaws.com

PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
80/tcp   closed   http
110/tcp  filtered pop3
143/tcp  filtered imap
443/tcp  open     https
3389/tcp filtered ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 1.33 seconds
```

DOS script was unable to identify subnet masks

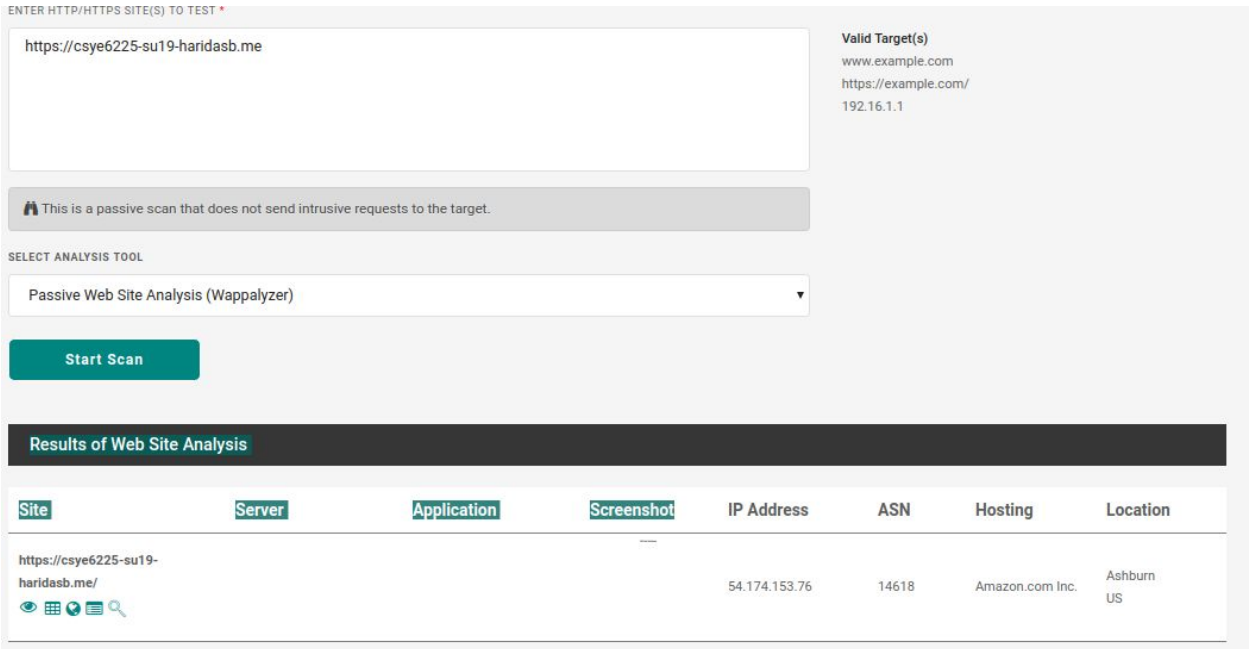
```
root@kali:~# nmap -v --script dos https://csye6225-su19-haridasb.me
Starting Nmap 7.70 ( https://nmap.org ) at 2019-08-10 00:02 EDT
NSE: Loaded 11 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 00:02
Completed NSE at 00:02, 10.01s elapsed
Unable to split netmask from target expression: "https://csye6225-su19-harida
sb.me"
NSE: Script Post-scanning.
Initiating NSE at 00:02
Completed NSE at 00:02, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
```

3. WhatWeb

Attack Vector to be identified - Security vulnerabilities

Reason for selection-
WhatWeb plugins identify version numbers, email addresses, account IDs, web framework modules, SQL errors etc. A typical WhatWeb plugin has about 15 tests, which include checking the favicon, default installation files, login pages, and checking for “/wp-content/” within relative links.
They examine the web server HTTP Headers and the HTML source of a web page to determine technologies in use.

Results -



The application server was identified to be Java based when /books endpoint was hit.