Shaheed Sukhdev College of Business Studies

University of Delhi

Post Graduate Diploma in Cyber Security and Law

Sakshi Garg • Roll no-23726 • Semester-1

Lab Setup

1. Burp Suite

It is a proxy tool for analysing requests and analysing responses. It is the most widely used software for web application penetration testing. It has several features by which we can perform scanning, manual scanning, etc. This tool comes as Community Edition(for students, learners) and Paid Professional Version(for industry experts)
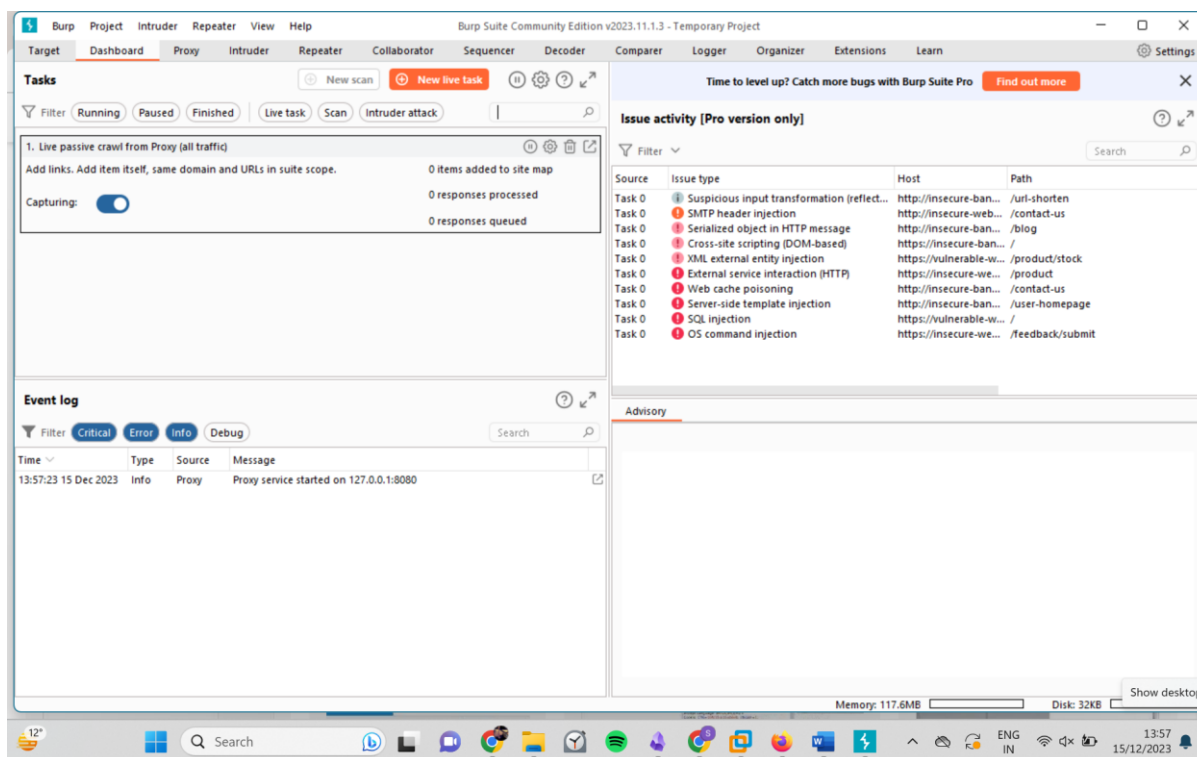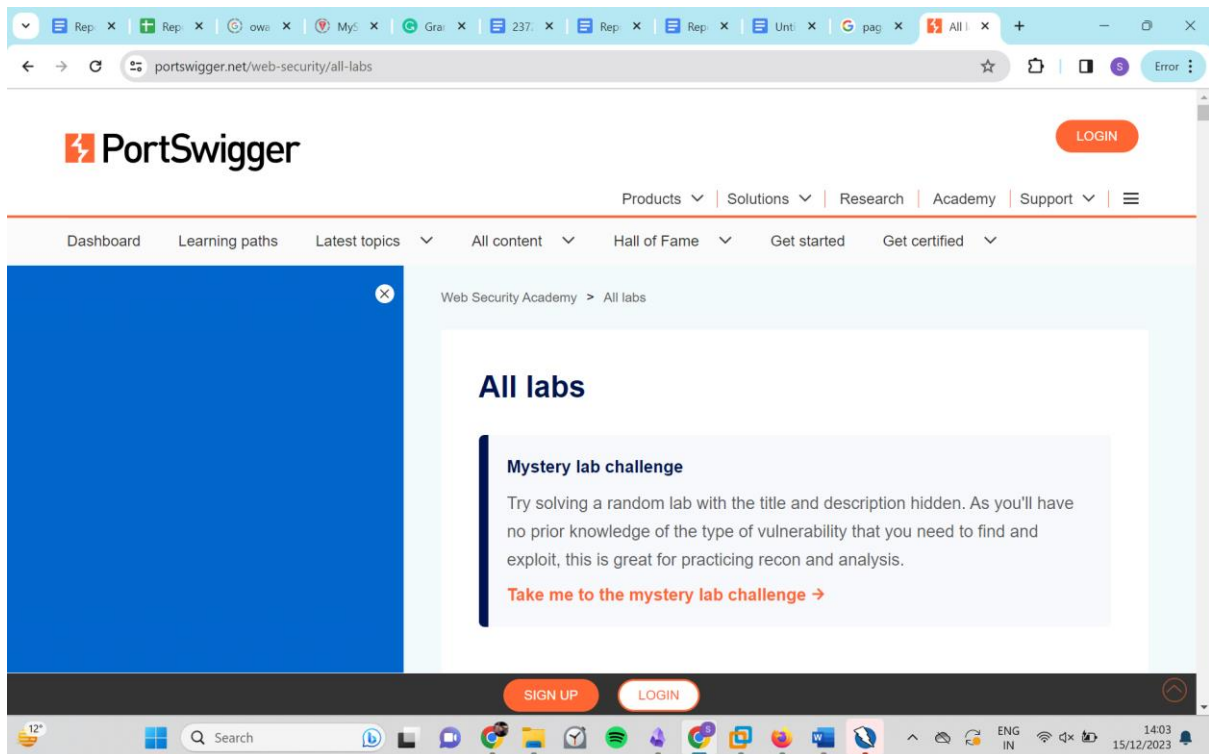

2. ZAP Proxy

It is a open source tool used for scanning and manual scanning for web applications. It is usually used for vulnerability assessment by the industry(VA)
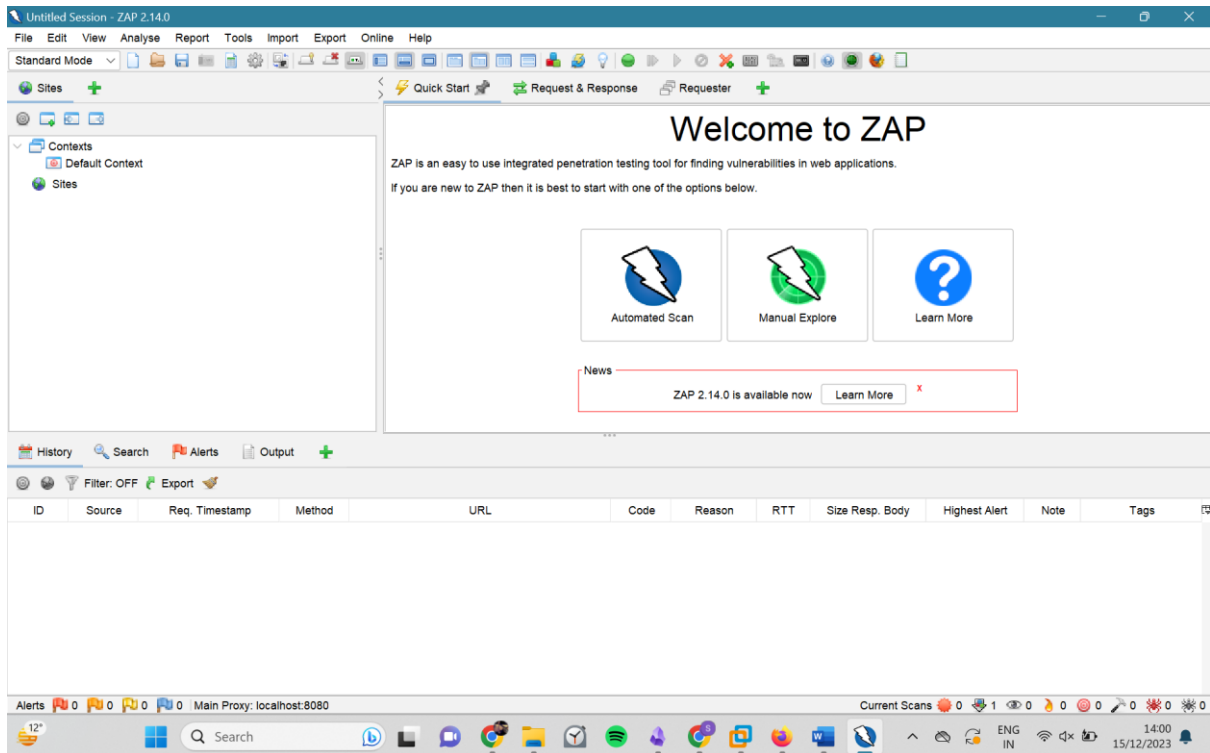
3. Port Swigger Lab

It is the world's first lab which has explained attacks deeply, used for finding more bugs.

It is used for website penetration testing practice, mobile applications, concepts, etc.

4. NMAP

Nmap is one of the core tools used by network administrators to map their networks. The program can be used to find live hosts on a network, perform port scanning, ping sweeps, OS detection, and version detection.

```
root@wks01:/home/vivek# nmap --top-ports 10 192.168.1.1

Starting Nmap 5.00 ( http://nmap.org ) at 2012-11-27 03:30 IST
Interesting ports on 192.168.1.1:
PORT       STATE   SERVICE
21/tcp     closed  ftp
22/tcp     open    ssh
23/tcp     closed  telnet
25/tcp     closed  smtp
80/tcp     open    http
110/tcp    closed  pop3
139/tcp    closed  netbios-ssn
443/tcp    closed  https
445/tcp    closed  microsoft-ds
3389/tcp   closed  ms-term-serv
MAC Address: BC:AE:C5:C3:16:93 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.58 seconds
```