Task 1: Web Vulnerability Lab

Web app used for the lab: DVWA

Vulnerabilities exploited: Stored XSS and SQL Injection

Vulnerability: XSS (stored)

Possible Attack Scenerio: Stored XSS can be used to obtain cookie information on the unsuspecting victim computer.

Business Impact: Medium - Most organizations already recommend in security trainings to run untrusted links in a virtual machine with a fresh browser session so this should not affect the organization that much.

Threat Impact: High, especially when analyst is on undercover assignment on the darknet some VPN providers do not obsfucate possibly private details in cookies so it may expose the analyst's real life location in real time.

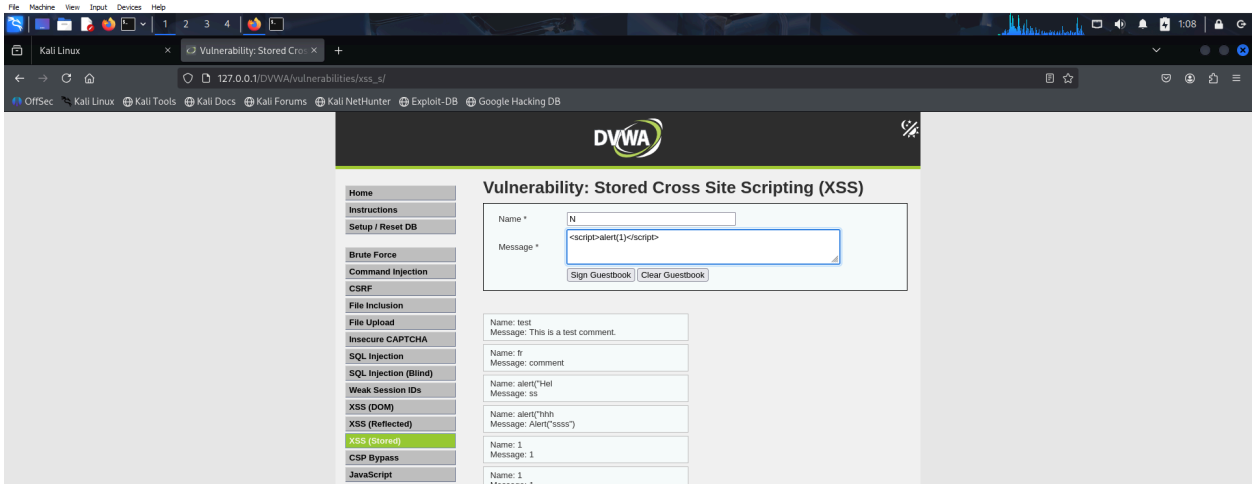
Risk Impact: High, clicking on a phishing site loaded with malware might cause further data exfil.

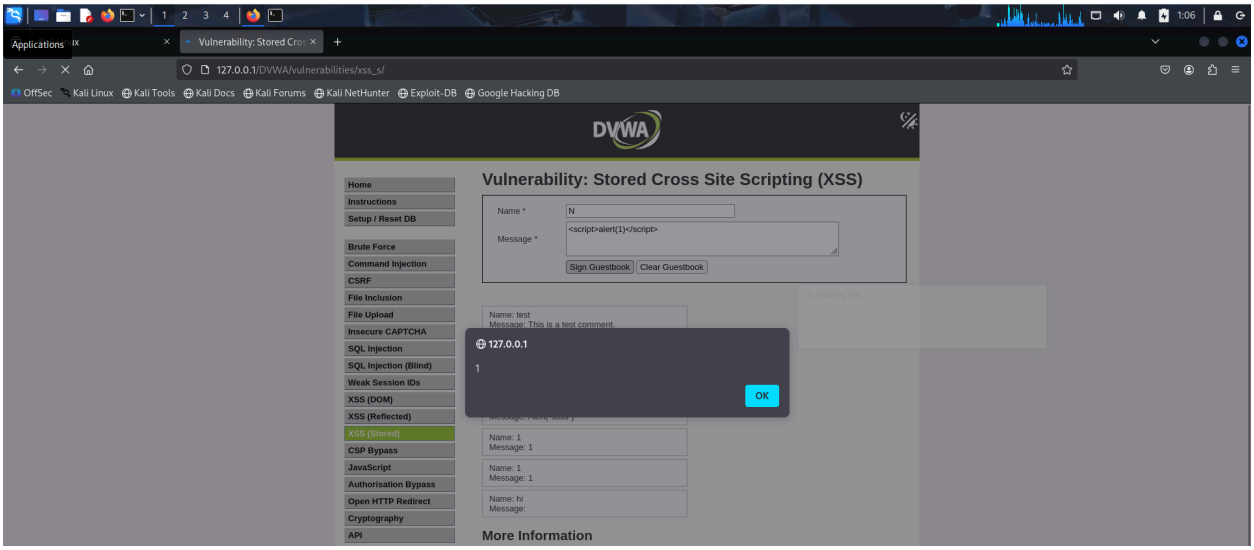
Reproduction steps:

1. Go to the "Stored (XSS)" lab
2. Type in any input for the "Name" field
3. Type in the following in in the "Message" field

```
<script>alert(1)</script>
```

Screenshots:





Vulnerability: SQL Injection

Possible Attack Scenario: SQL injection can be used to try to obtain unauthorized credentials to a webserver.

Business Impact: High - I do not think any security training in the organization can account for this. Also this can cause reputation damage to the organization.

Threat Impact: High, unauthorized access can lead to further data exfiltration

Risk Impact: High customer information can be affected.

Steps:

1. Go to the SQL Injection tab
2. In the ID filed input ‘1 OR ‘2’=’2’#
    a. Note the # symbol is to force Mysql to ignore the rest of the entire line after the #
3. Then afterwards enter the following query: ‘Union Select user, password from users#
    a. One can see that a list of users and passwords are displayed
    b. If you have a GPU, I believe one can try to brute force the hashes using hashcat

Screenshots: