ASSIGNMENT 7

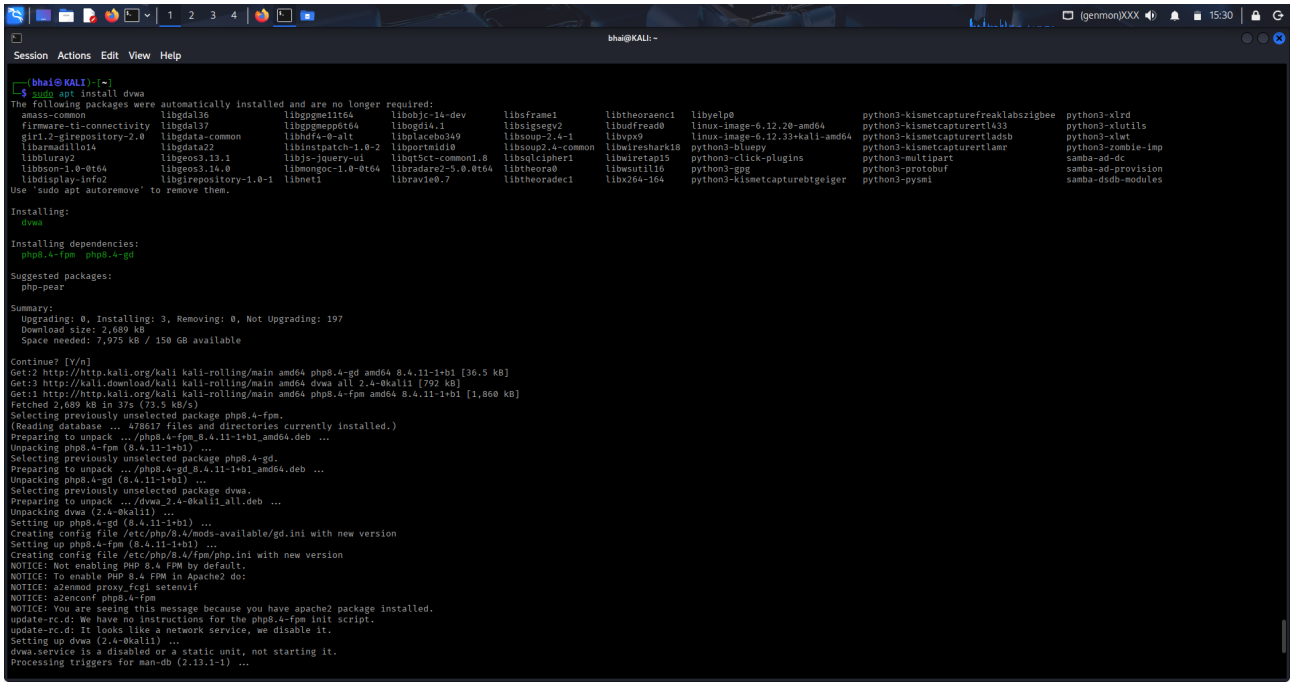
DVWA Installation + Vulnerability Discovery

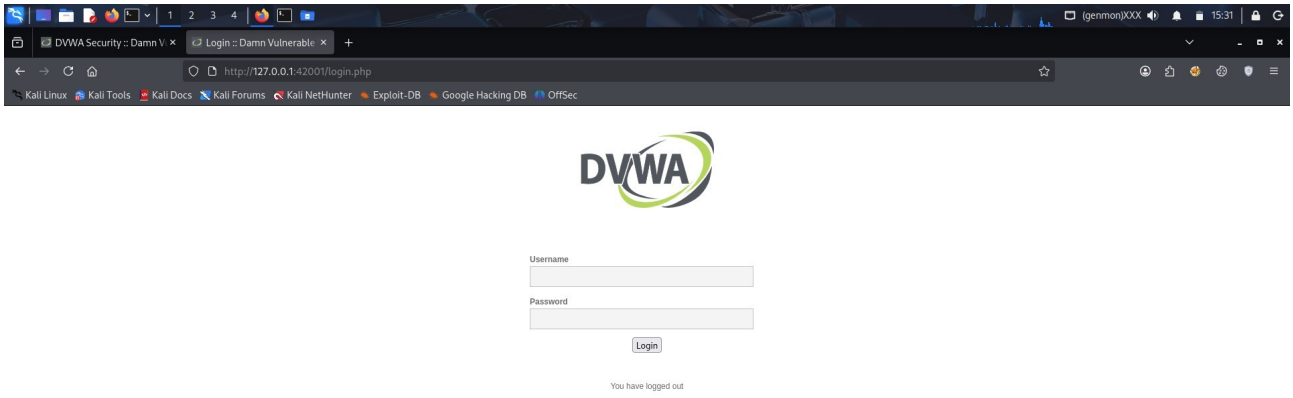
Step 1 - DVWA Installation

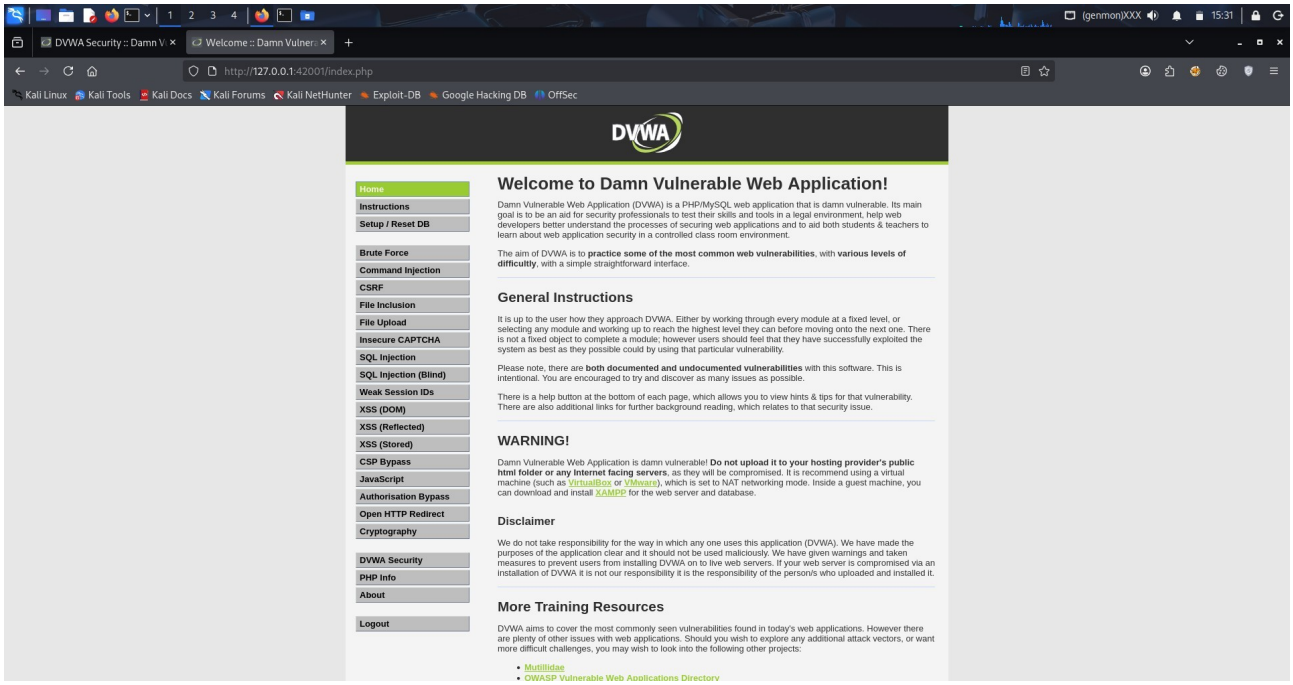
Installed DVWA on Kali using apt and started service.

Commands:

```
sudo apt update
sudo apt install dvwa
sudo dvwa-start
```

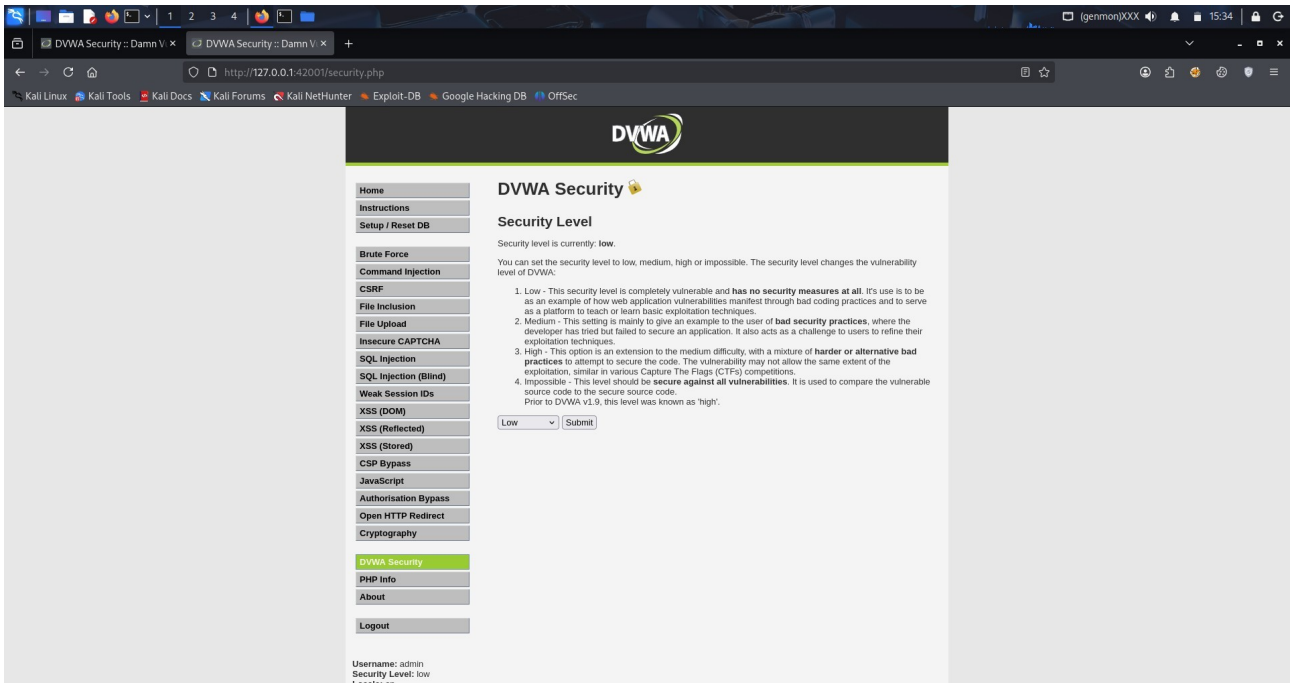






Step 2 - Security Levels

Changed DVWA security to Low → Medium → High and tested again.



Step 3 - Vulnerability Tests

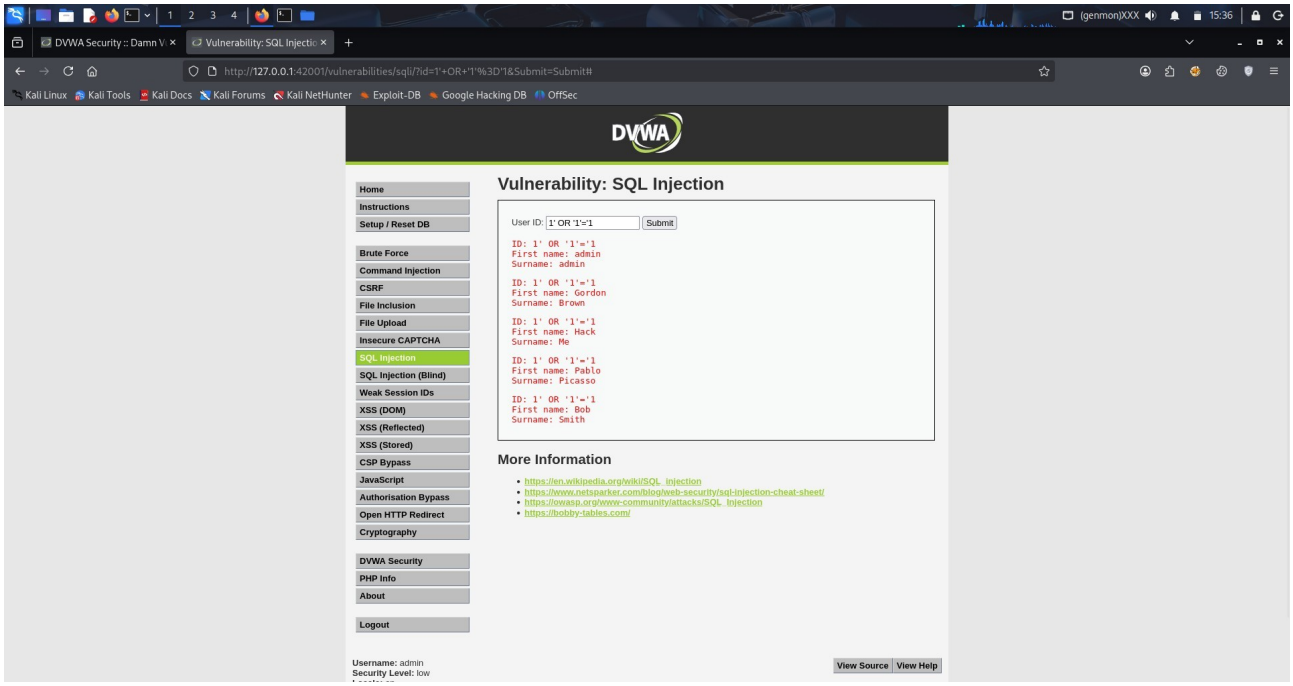
---

1. SQL Injection

Performed basic SQL injection to bypass login and extract DB info.

Payloads:

```
1' OR '1'='1
```



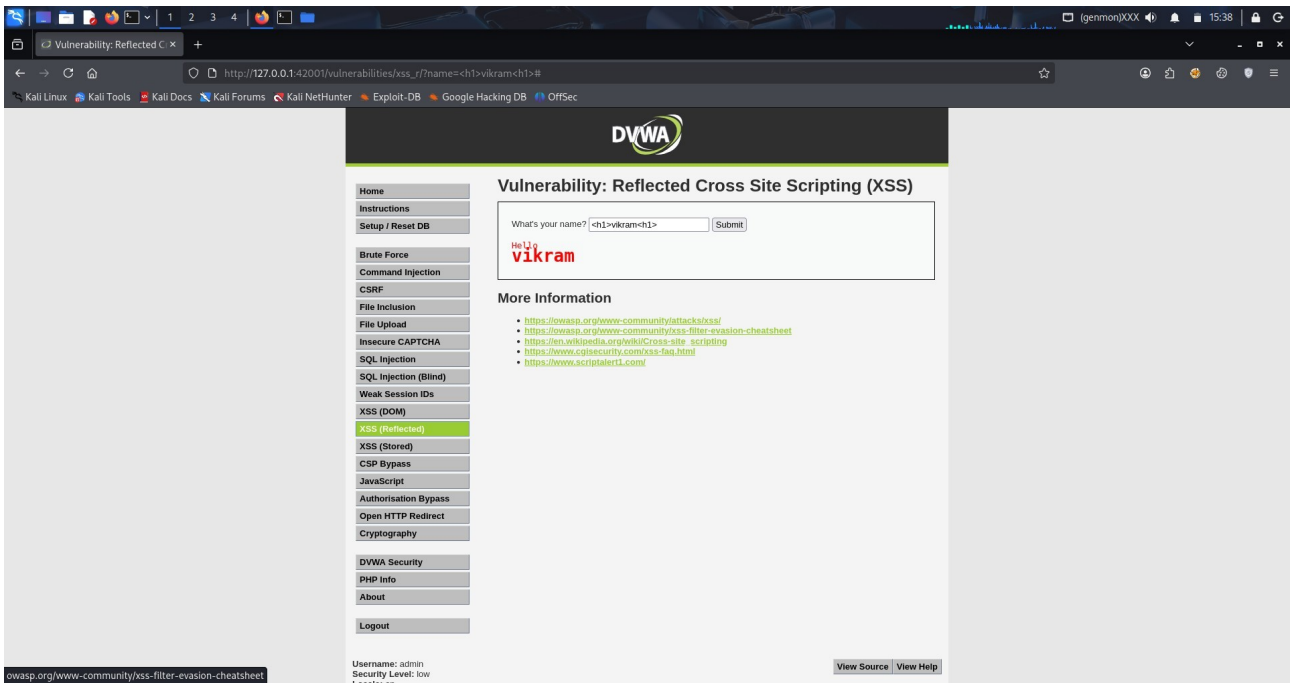
---

2. Cross-Site Scripting (XSS)

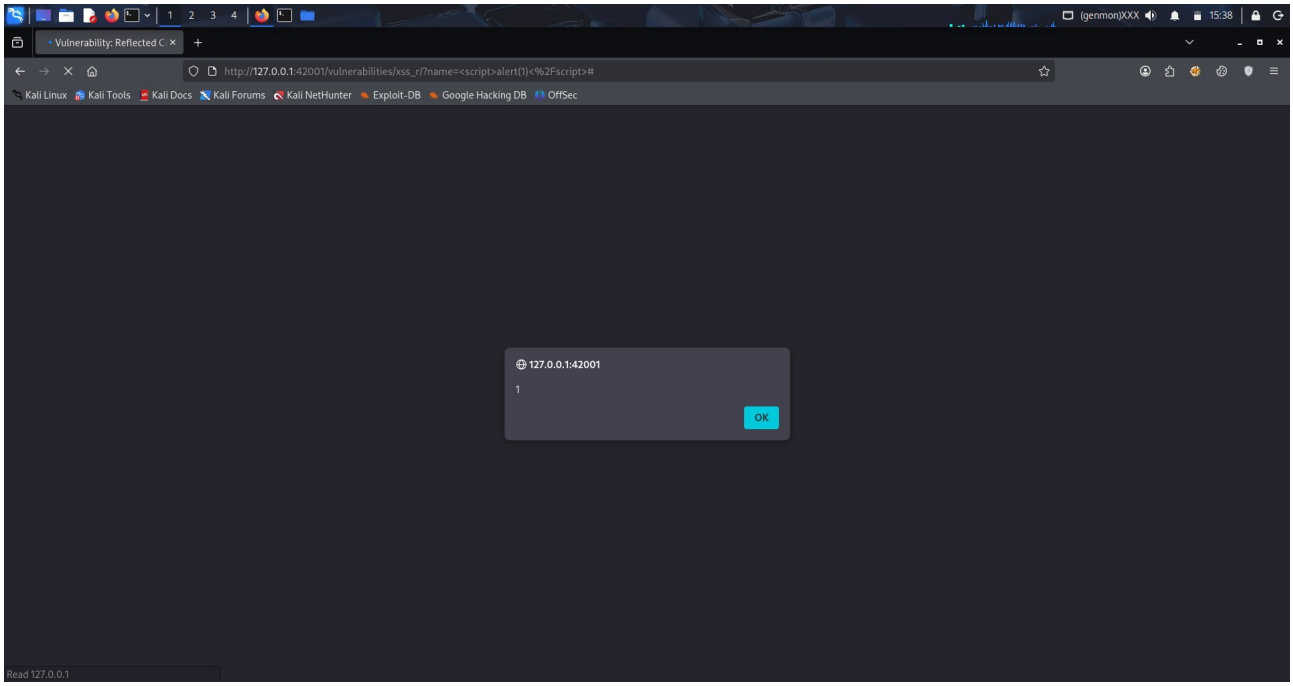
Injected JavaScript to confirm reflected and stored XSS.

Payloads:

```
<h1>vikram<h1>
```




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



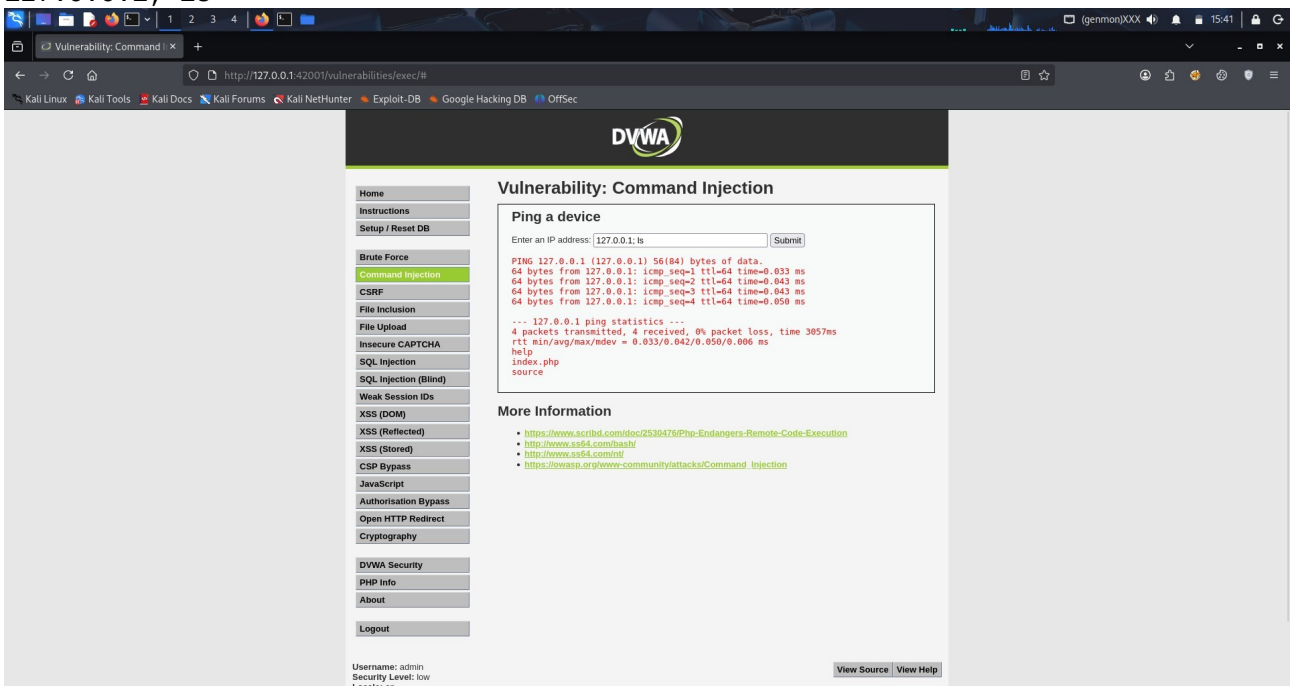
---

3. Command Injection

Executed system commands via vulnerable parameter.

Payloads:

```
127.0.0.1; ls
```



---

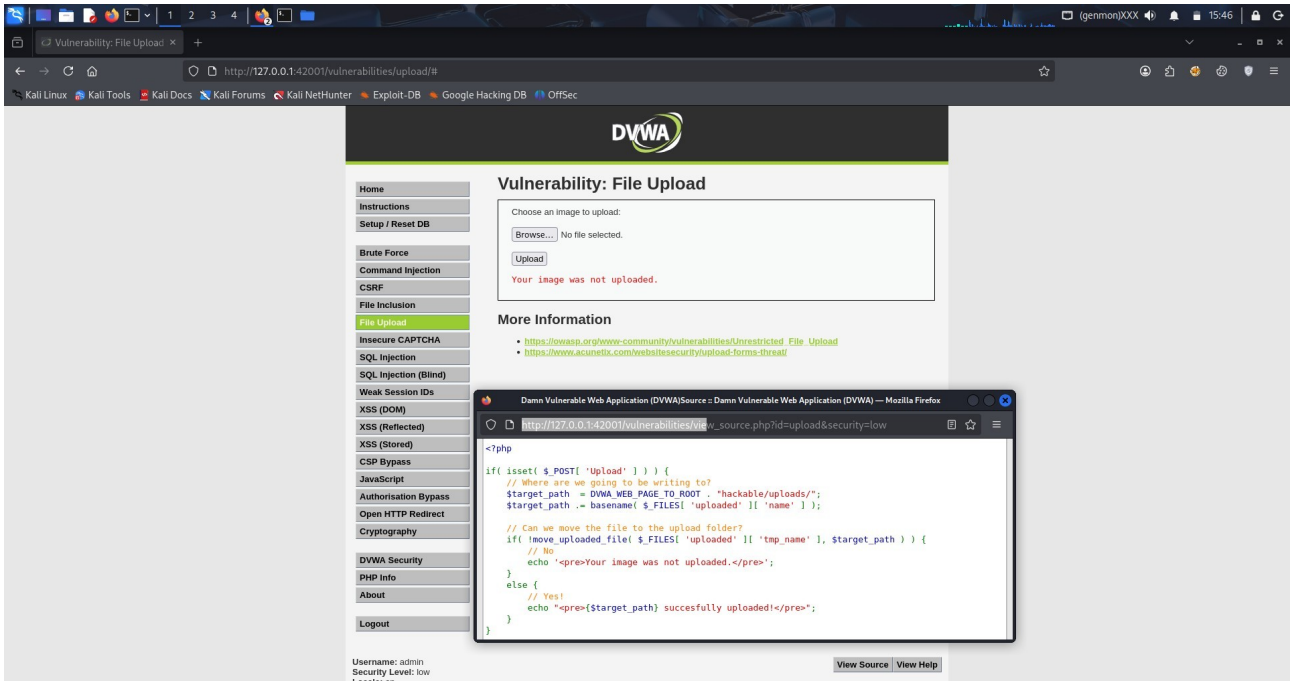
4. File Upload Vulnerability

Uploaded test PHP file by bypassing file extension filters.

Payload:

```
<?php echo "test"; ?>
```

Rename as: `shell.php.jpg`



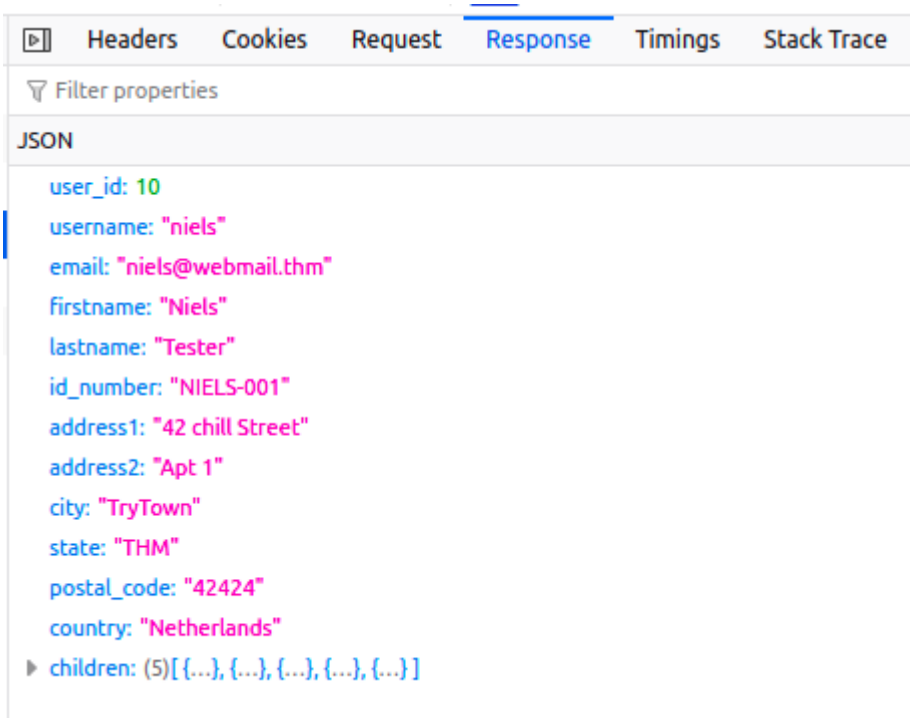
---

5. IDOR (Insecure Direct Object Reference)

Accessed other user info by modifying ID value.(performed on THM)

URL Test:

`?id=10`



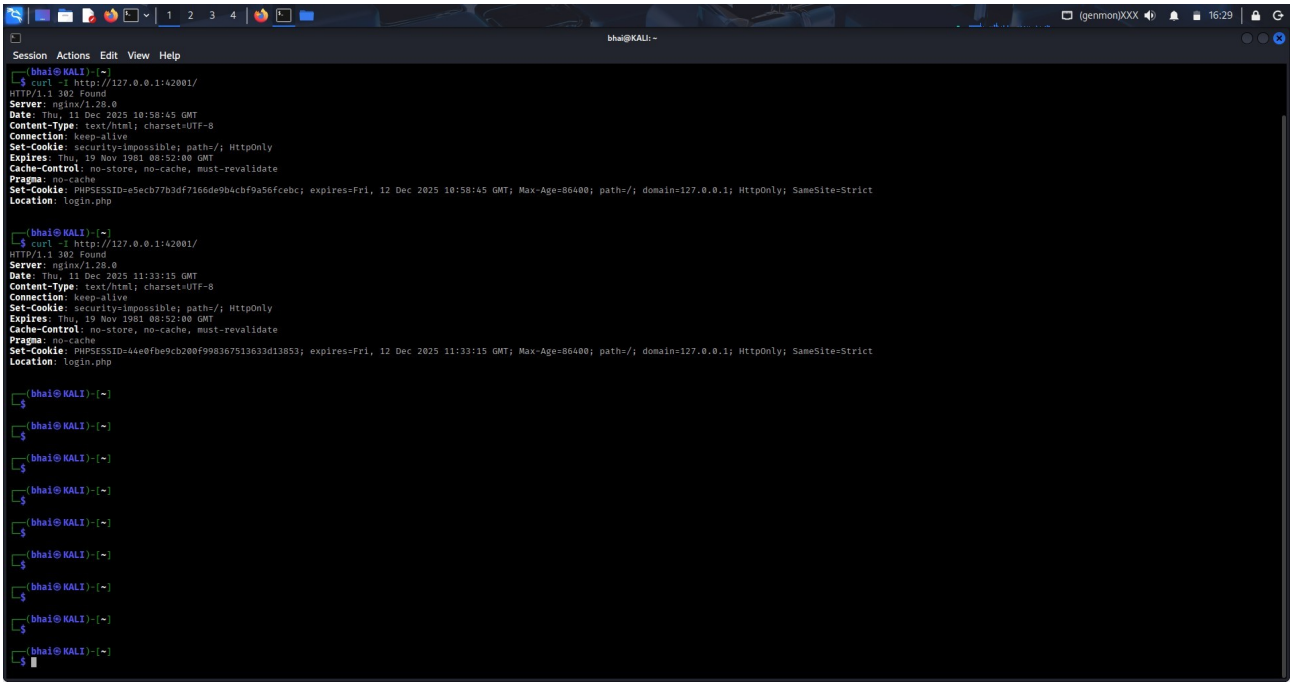
---

6. Security Misconfigurations / Headers

Checked missing security headers using curl.

Command:

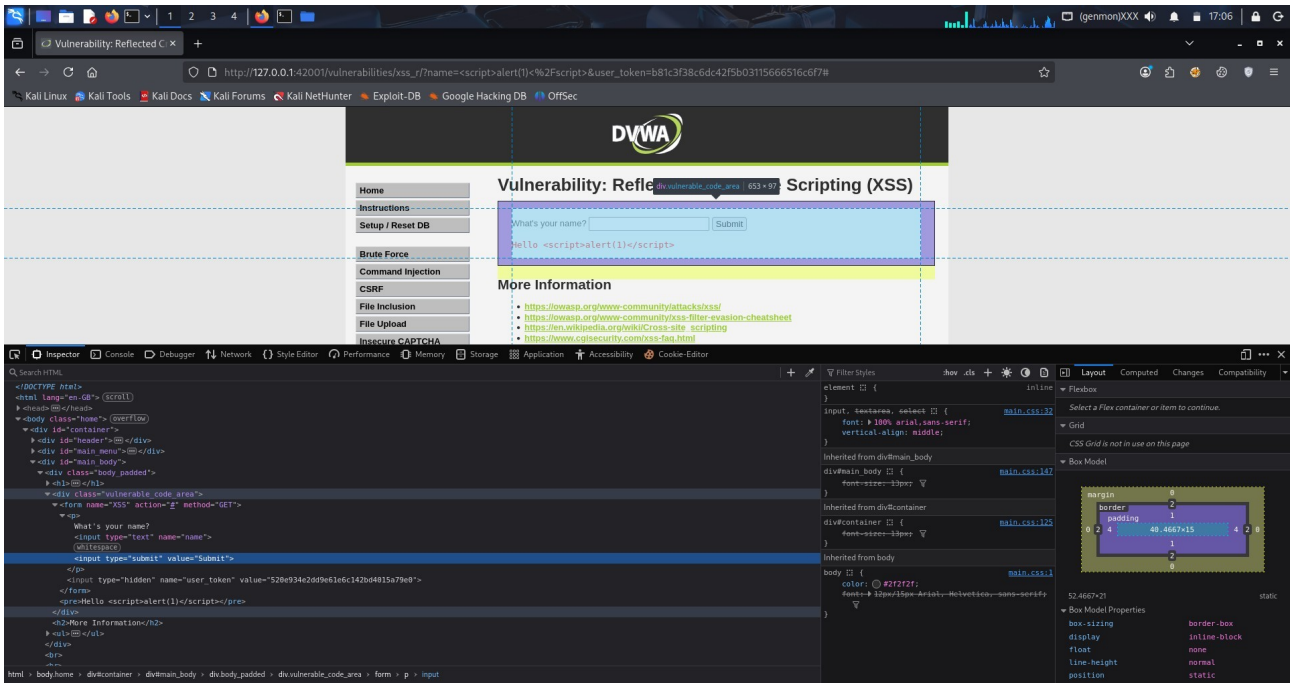
```
curl -I http://localhost/dvwa
```



---

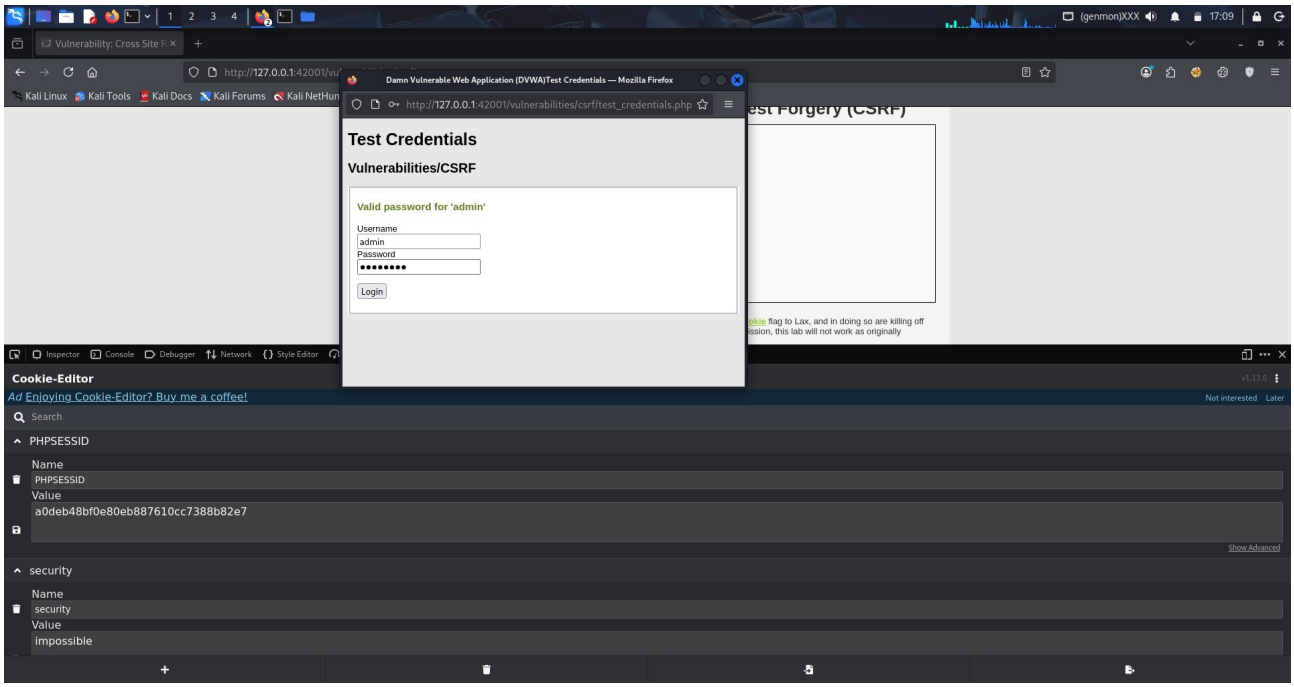
7. Sensitive Info in Source / JS

Viewed page source to identify exposed info.



8. Session Management Issues

Verified insecure cookies and missing flags.



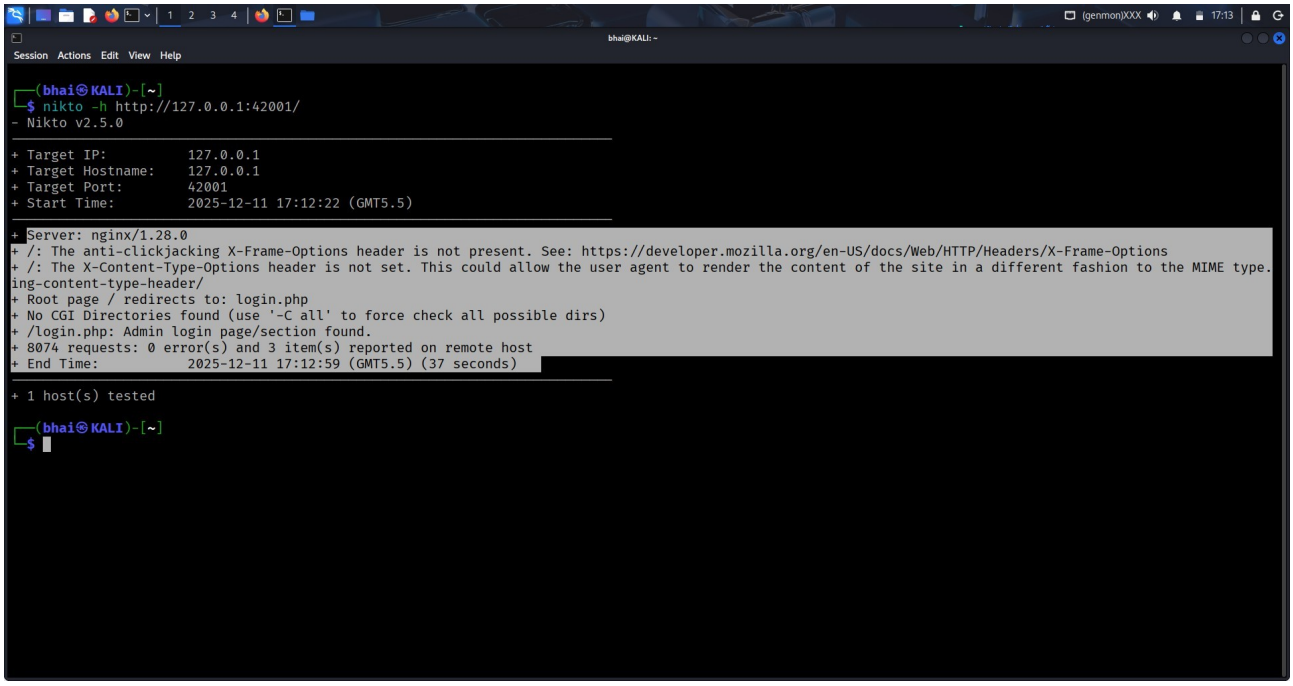
Step 4 - Light Automation

Nikto Scan

Scanned server for misconfigurations.

Command:

```
nikto -h http://localhost/dvwa
```

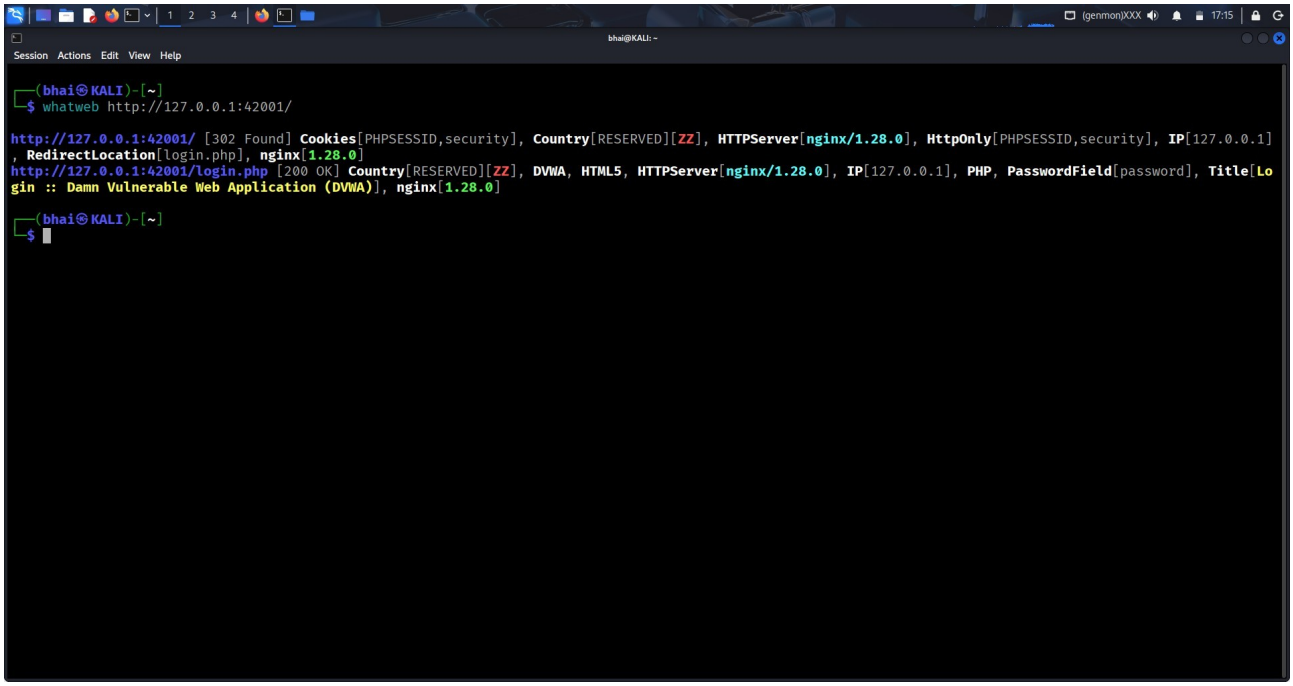


WhatWeb Fingerprinting

Identified technologies running on DVWA.

Command:

```
whatweb http://localhost/dvwa
```

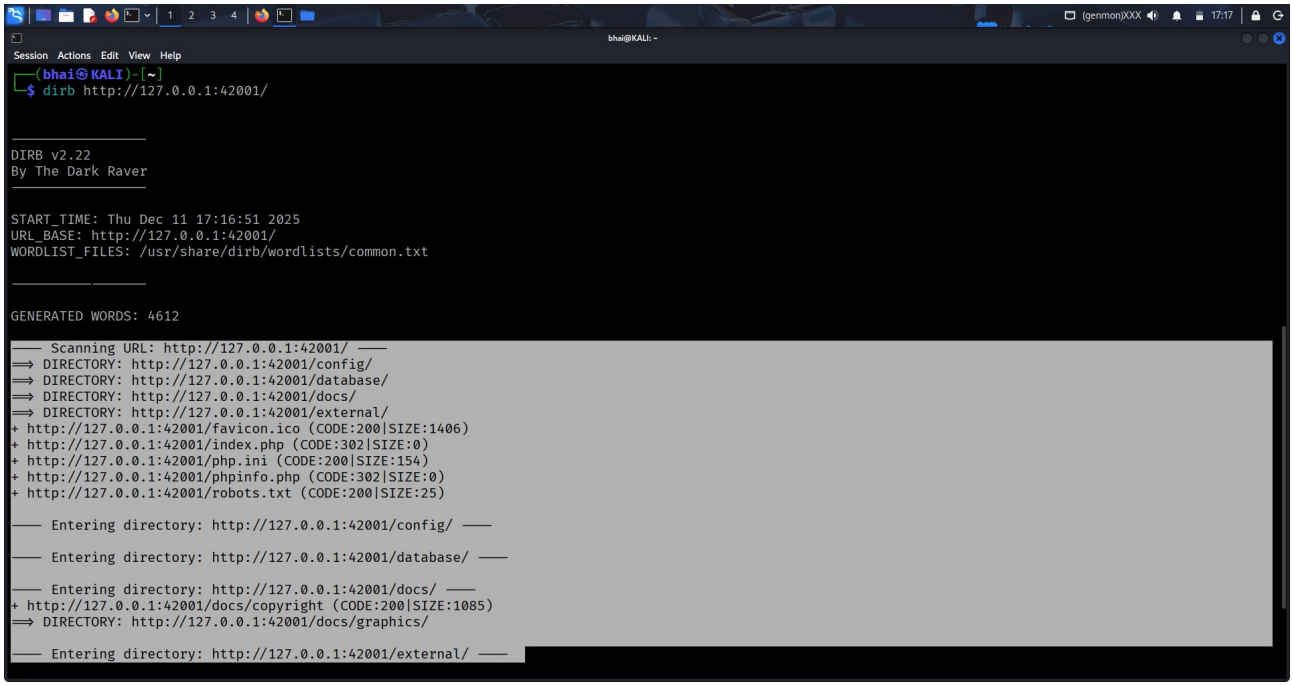


DIRB Directory Scan

Enumerated hidden directories and files.

Command:

```
dirb http://localhost/dvwa
```

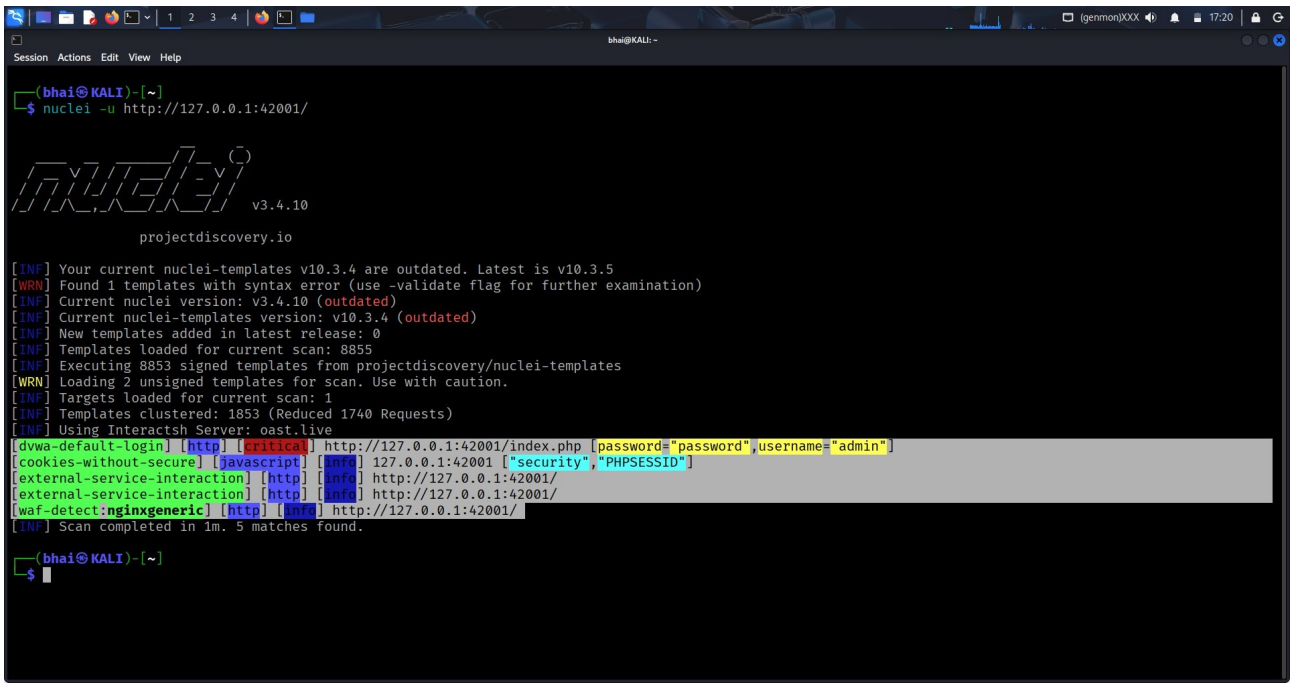


Nuclei Scan

Ran templates for common misconfigurations.

Command:

```
nuclei -u http://localhost/dvwa
```


bhai@KALI: ~
Session Actions Edit View Help
(bhai㉿KALI)-[~]
$ nuclei -u http://127.0.0.1:42001/
v3.4.10
projectdiscovery.io
[INF] Your current nuclei-templates v10.3.4 are outdated. Latest is v10.3.5
[WRN] Found 1 templates with syntax error (use -validate flag for further examination)
[INF] Current nuclei version: v3.4.10 (outdated)
[INF] Current nuclei-templates version: v10.3.4 (outdated)
[INF] New templates added in latest release: 0
[INF] Templates loaded for current scan: 8855
[INF] Executing 8853 signed templates from projectdiscovery/nuclei-templates
[WRN] Loading 2 unsigned templates for scan. Use with caution.
[INF] Targets loaded for current scan: 1
[INF] Templates clustered: 1853 (Reduced 1740 Requests)
[INF] Using Interactsh Server: oast.live
[dvwa-default-login] [http] [critical] http://127.0.0.1:42001/index.php [password="password",username="admin"]
[cookies-without-secure] [javascript] [info] 127.0.0.1:42001 ["security","PHPSESSID"]
[external-service-interaction] [http] [info] http://127.0.0.1:42001/
[external-service-interaction] [http] [info] http://127.0.0.1:42001/
[waf-detect:nginxgeneric] [http] [info] http://127.0.0.1:42001/
[INF] Scan completed in 1m. 5 matches found.
(bhai㉿KALI)-[~]
$