

ASSIGNMENT 6

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
```

```
bhai@KALI:~$ sudo apt install dvwa
The following packages were automatically installed and are no longer required:
  amass-common libgdal36 libgpgme11t64 libbobjc-14-dev libsfame1 libtheoraenc1 libyelp0 python3-kismetcapturefreaklabszigbee python3-xlrd
  firmware-ti-connectivity libgdal37 libgpgmepp6t64 libhogdi4.1 libsigsegv2 libudfread0 linux-image-6.12.20-amd64 python3-kismetcapturefreaklabszigbee python3-xlrd
  gnl2-girepository-2.0 libgdata-common libhdf4-0-alt libpixman-1-0 libsoup-2.4-1 libvpx9 linux-image-6.12.33-kali-amd64 python3-kismetcapturefreaklabszigbee python3-xlrd
  libarmadillo4 libgdata22 libinstpatch-1.0-2 libportmidi0 libsoup2.4-common libwireless18 python3-bluepy python3-kismetcapturefreaklabszigbee python3-xlrd
  libbluray2 libgeo3.11.1 libjs-jquery-ui libqt5ct-common1.8 libqt5ct-common1.8 libqt5ct-common1.8 libqt5ct-common1.8 libqt5ct-common1.8 python3-click-plugins python3-kismetcapturefreaklabszigbee python3-xlrd
  libbson-1.0-0t64 libgeo3.14-0 libmongoc-1.0-0t64 libtheoradec1 libtheoradec1 libtheoradec1 libtheoradec1 libtheoradec1 python3-gpg python3-kismetcapturefreaklabszigbee python3-xlrd
  libdisplay-info2 libgirepository1.0-1 libnet1 libravie0.7 libtheoradec1 libtheoradec1 libtheoradec1 libtheoradec1 libtheoradec1 python3-gpg python3-kismetcapturefreaklabszigbee python3-xlrd
Use 'sudo apt autoremove' to remove them.

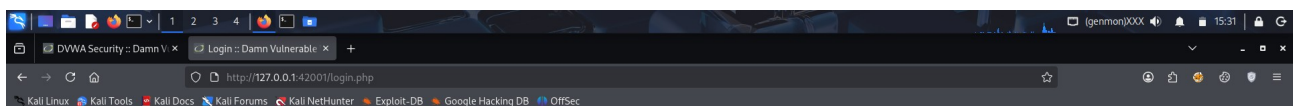
Installing:
  dvwa

Installing dependencies:
  php8.4-fpm php8.4-gd

Suggested packages:
  php-pear

Summary:
  Upgrading: 0, Installing: 3, Removing: 0, Not Upgrading: 197
  Download size: 2,489 kB
  Space needed: 7,975 kB / 150 GB available

Continue? [Y/n]
Get:2 http://http.kali.org/kali kali-rolling/main amd64 php8.4-gd amd64 8.4.11-1+b1 [36.5 kB]
Get:3 http://http.kali.org/kali kali-rolling/main amd64 dvwa all 2.4-0kali1 [792 kB]
Get:1 http://http.kali.org/kali kali-rolling/main amd64 php8.4-fpm amd64 8.4.11-1+b1 [1,860 kB]
Fetched 2,689 kB in 37s (72.5 kB/s)
Selecting previously unselected package php8.4-fpm.
(Reading database ... 478672 files and directories currently installed.)
Preparing to unpack .../php8.4-fpm_8.4.11-1+b1_amd64.deb ...
Unpacking php8.4-fpm (8.4.11-1+b1) ...
Selecting previously unselected package php8.4-gd.
Preparing to unpack .../php8.4-gd_8.4.11-1+b1_amd64.deb ...
Unpacking php8.4-gd (8.4.11-1+b1) ...
Selecting previously unselected package dvwa.
Preparing to unpack .../dvwa_2.4-0kali1_all.deb ...
Unpacking dvwa (2.4-0kali1) ...
Setting up php8.4-gd (8.4.11-1+b1) ...
Creating config file /etc/php/8.4/mods-available/gd.ini with new version
Setting up php8.4-fpm (8.4.11-1+b1) ...
Creating config file /etc/php/8.4/fpm/php.ini with new version
NOTICE: Not enabling PHP 8.4 FPM by default.
NOTICE: To enable PHP 8.4 FPM in Apache2 do:
NOTICE: a2enmod proxy_fcgi setenvif
NOTICE: a2enconf php8.4-fpm
NOTICE: You are seeing this message because you have apache2 package installed.
update-rc.d: We have no instructions for the php8.4-fpm init script.
update-rc.d: It looks like a network service, we disable it.
Setting up dvwa (2.4-0kali1) ...
dvwa.service is a disabled or a static unit, not starting it.
Processing triggers for man-db (2.12.1-1) ...
```

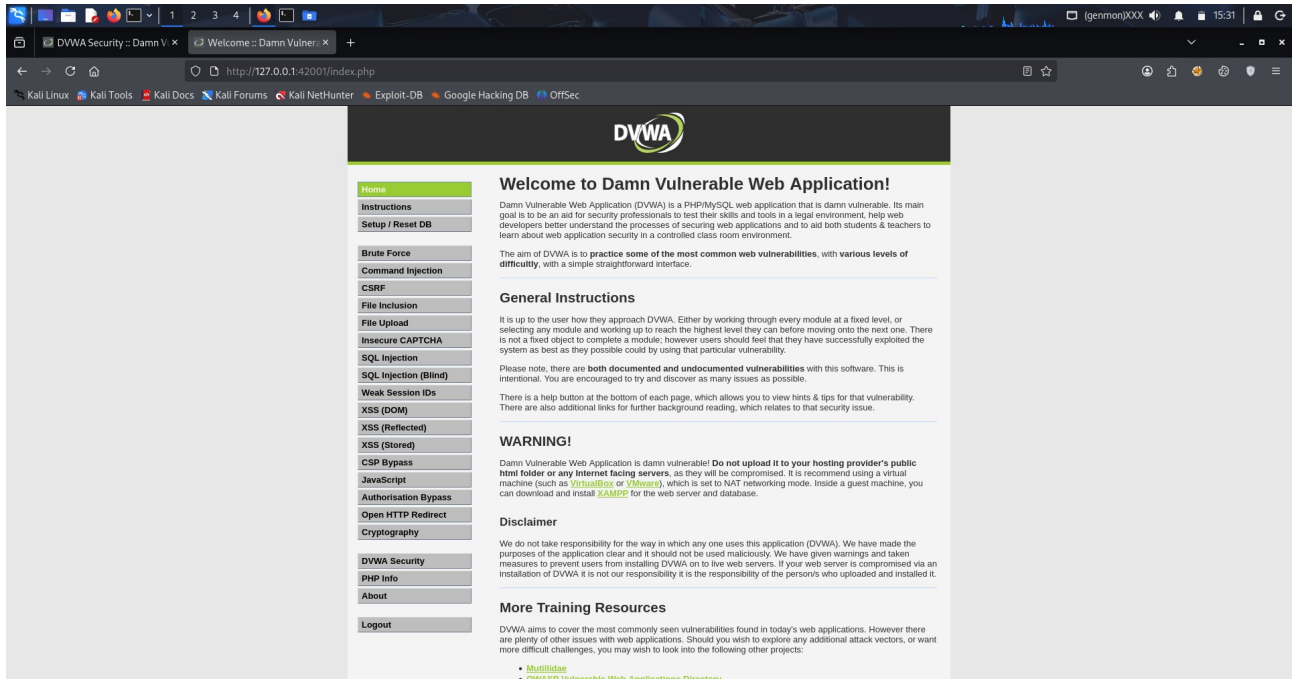


Username

Password

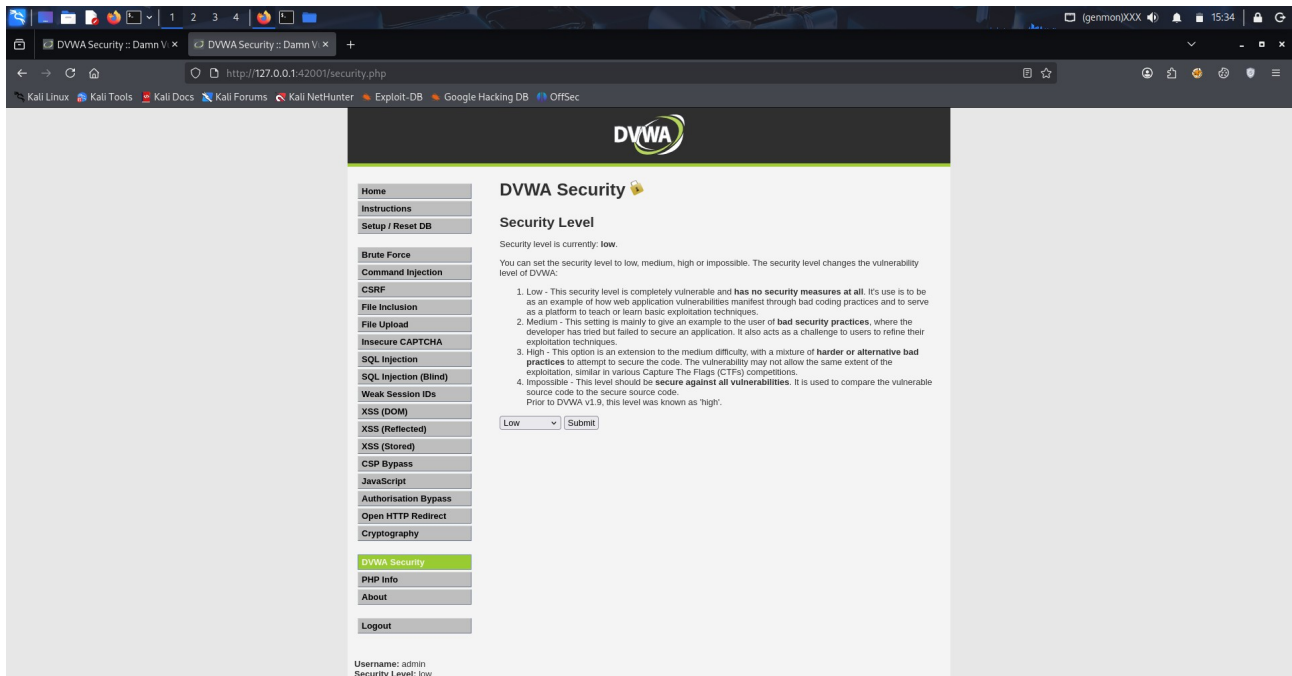
Login

You have logged out



Step 2 - Security Levels

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



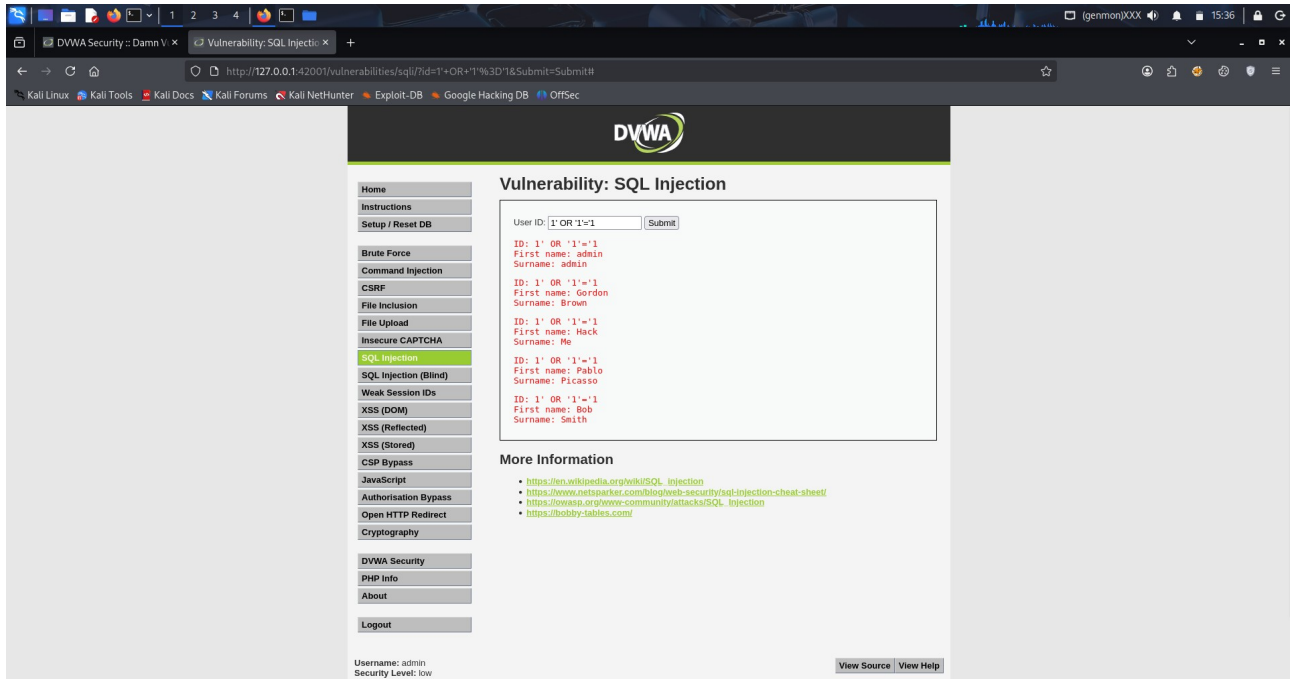
Step 3 - Vulnerability Tests

1. SQL Injection

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

Payloads:

1' OR '1'='1

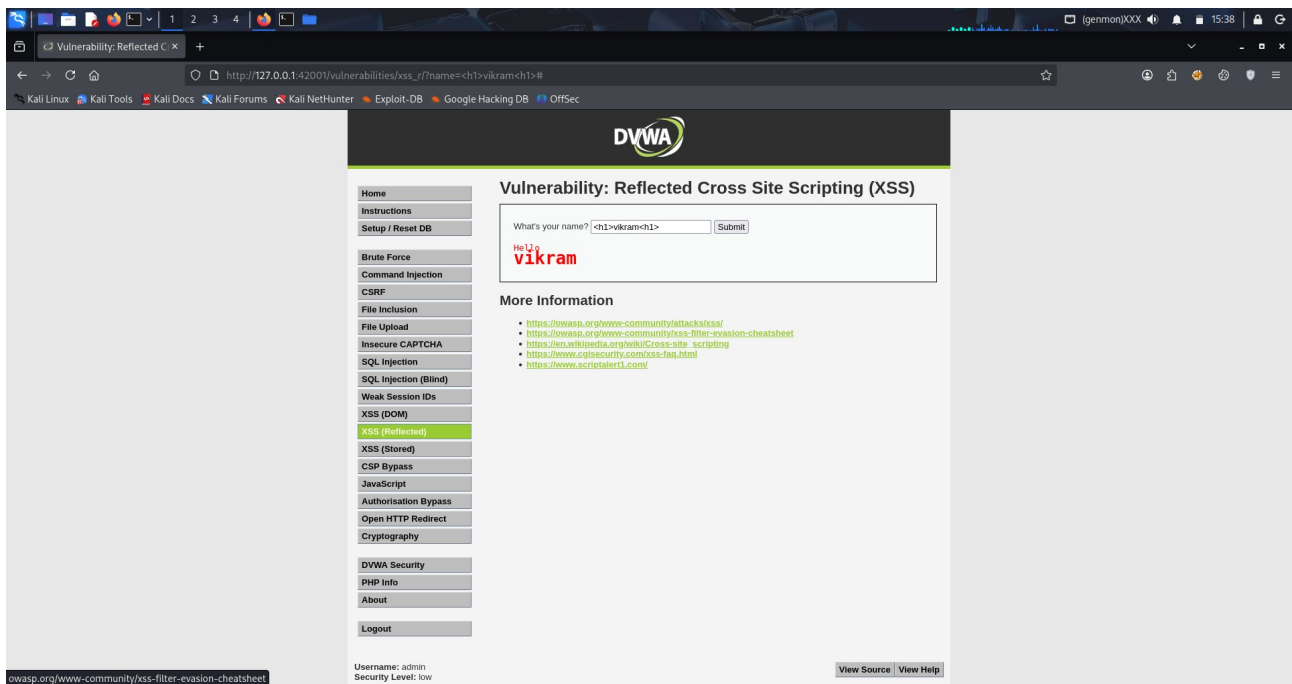


2. Cross-Site Scripting (XSS)

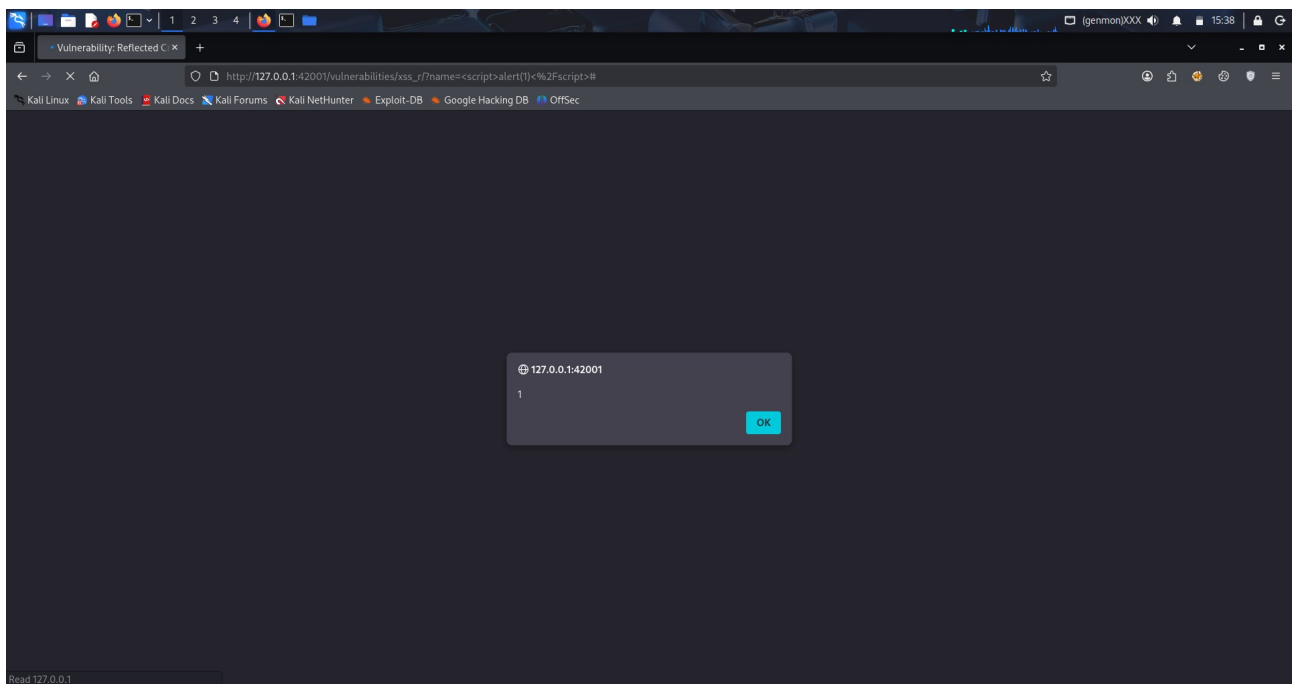
Injected JavaScript to confirm reflected and stored XSS.

Payloads:

<h1>vikram<h1>



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

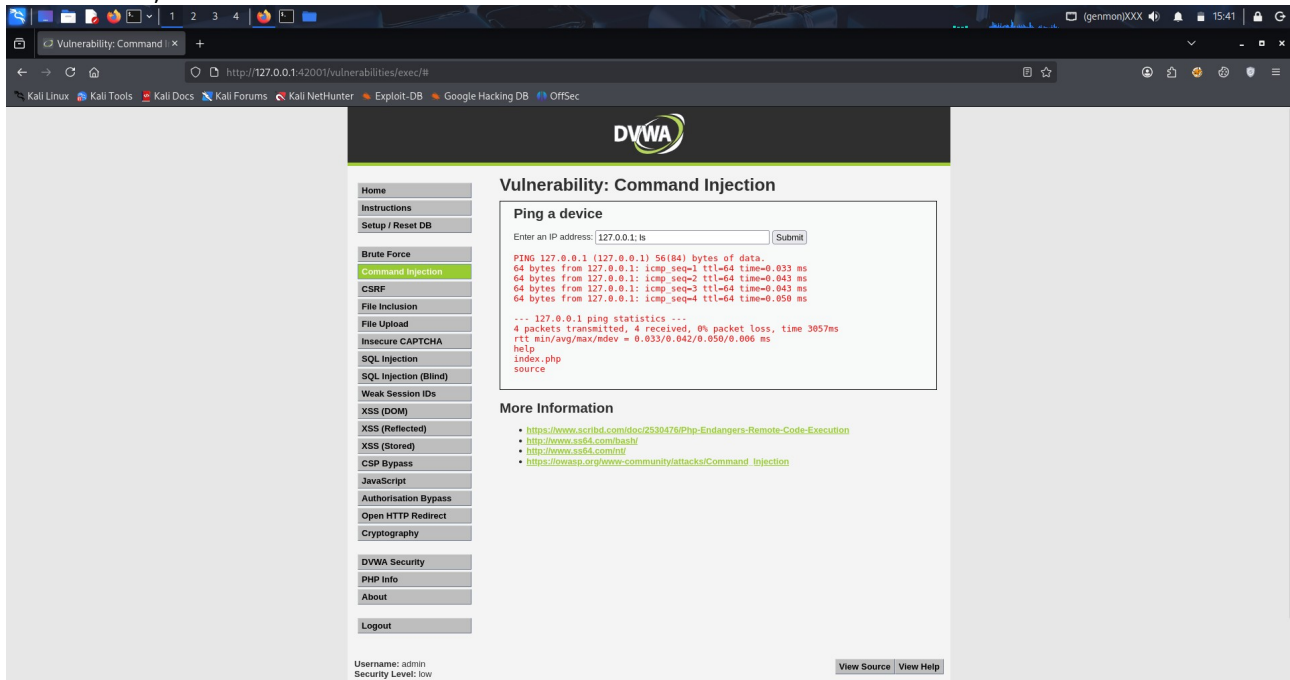


3. Command Injection

Executed system commands via vulnerable parameter.

Payloads:

127.0.0.1; ls



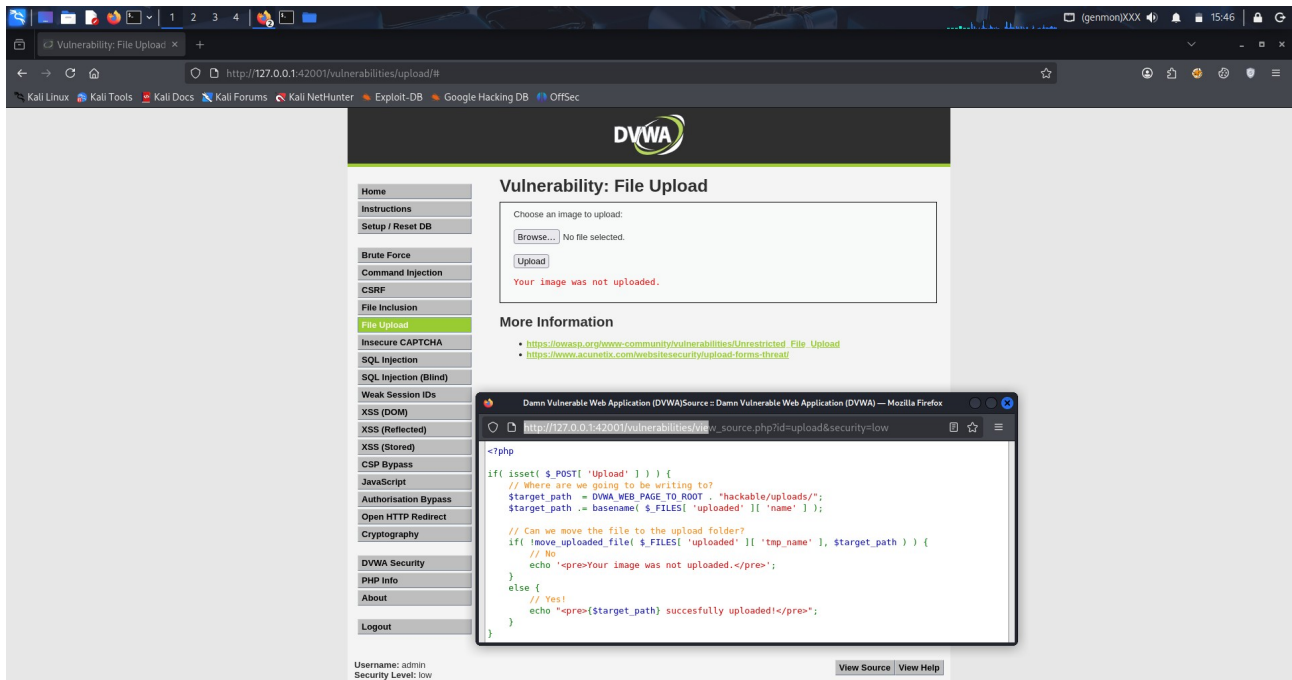
4. File Upload Vulnerability

Uploaded test PHP file by bypassing file extension filters.

Payload:

<?php echo "test"; ?>

Rename as: shell.php.jpg

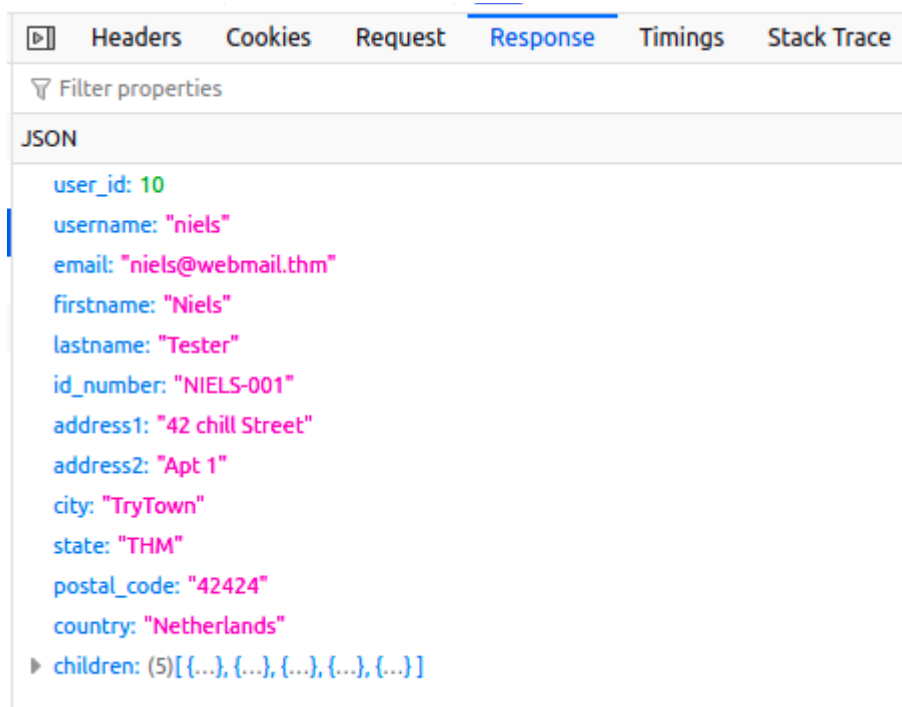


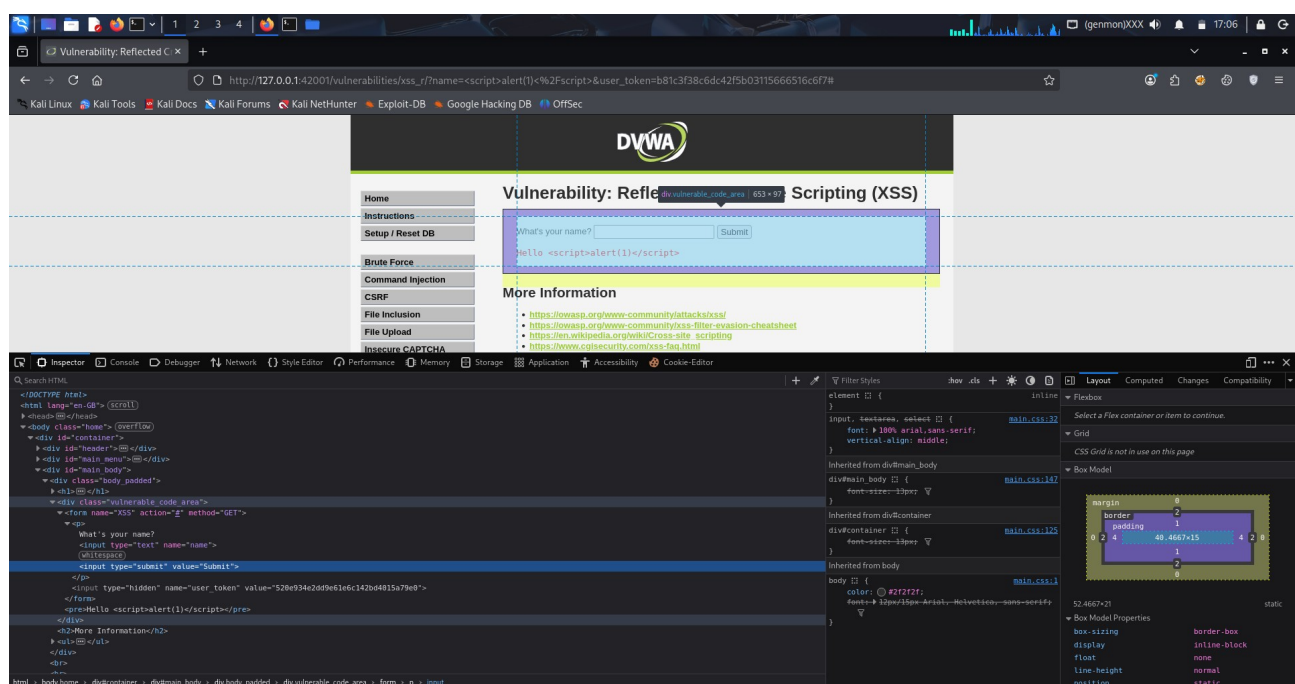
5. IDOR (Insecure Direct Object Reference)

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

URL Test:

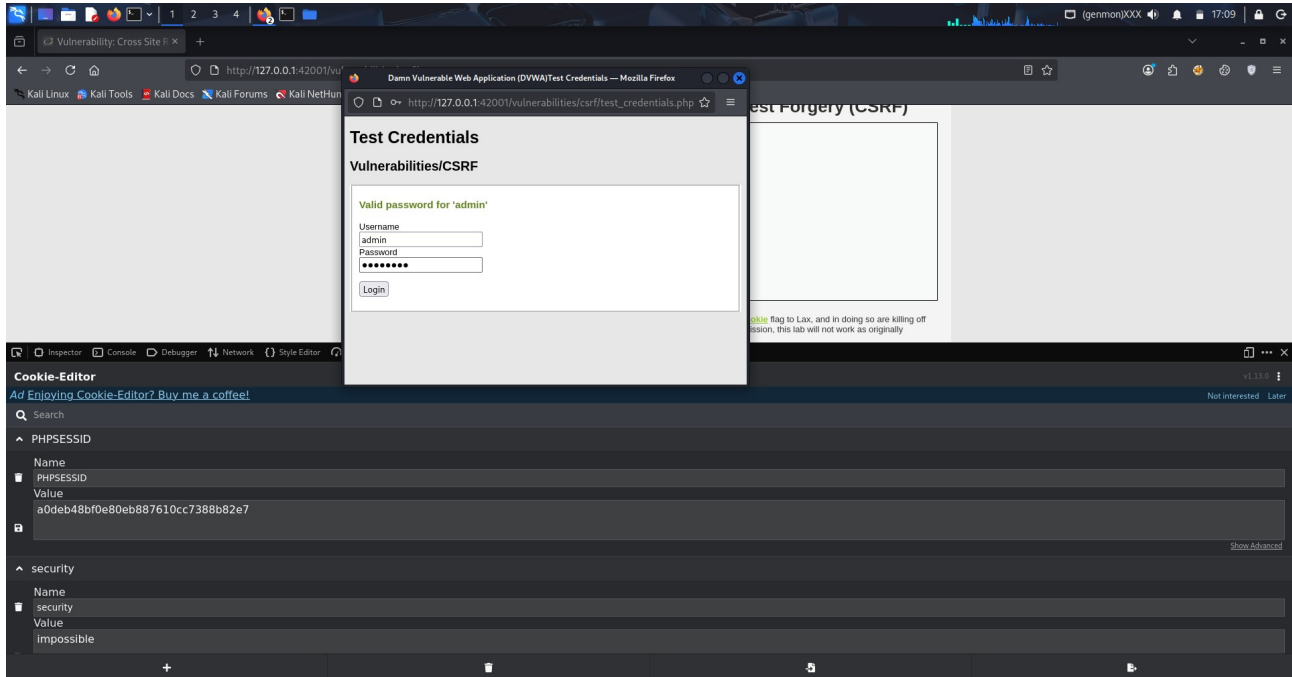
?id=10





8. Session Management Issues

Verified insecure cookies and missing flags.



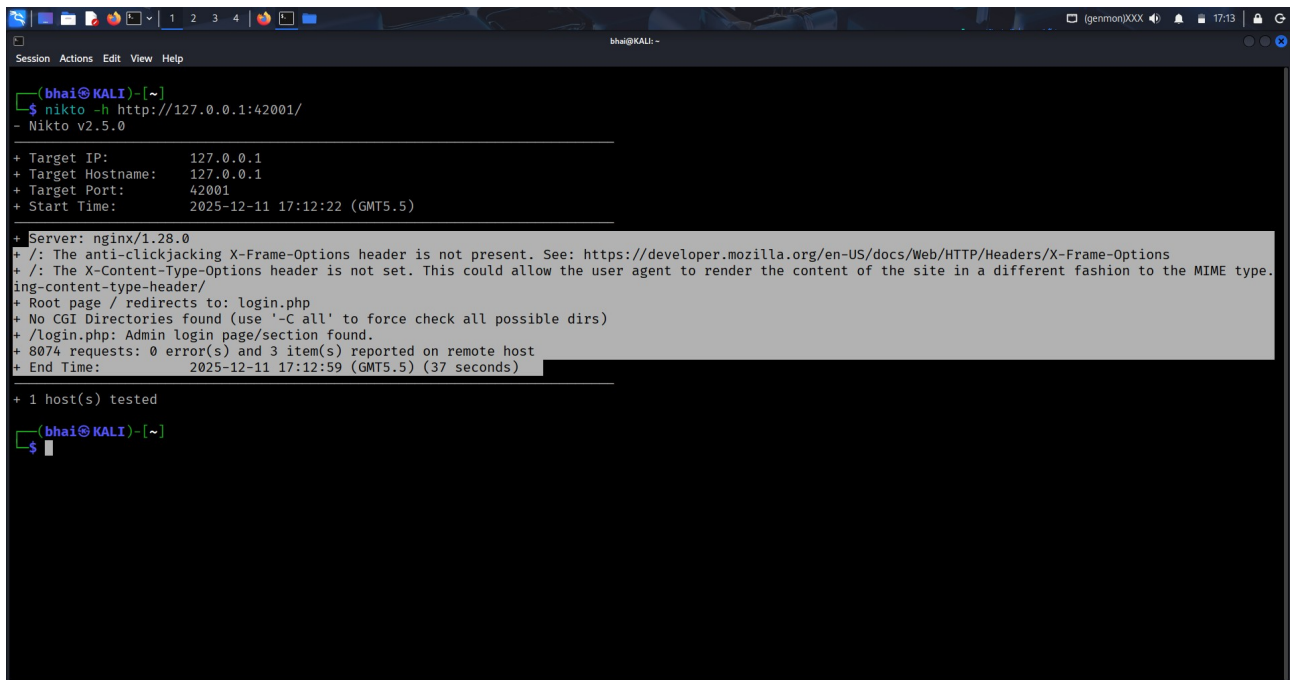
Step 4 - Light Automation

Nikto Scan

Scanned server for misconfigurations.

Command:


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



```
(bhai@KALI)-[~]
$ nikto -h http://127.0.0.1:42001/
- Nikto v2.5.0

+ Target IP: 127.0.0.1
+ Target Hostname: 127.0.0.1
+ Target Port: 42001
+ Start Time: 2025-12-11 17:12:22 (GMT5.5)

+ Server: nginx/1.28.0
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type.
+ Root page / redirects to: login.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /login.php: Admin login page/section found.
+ 8074 requests: 0 error(s) and 3 item(s) reported on remote host
+ End Time: 2025-12-11 17:12:59 (GMT5.5) (37 seconds)

+ 1 host(s) tested

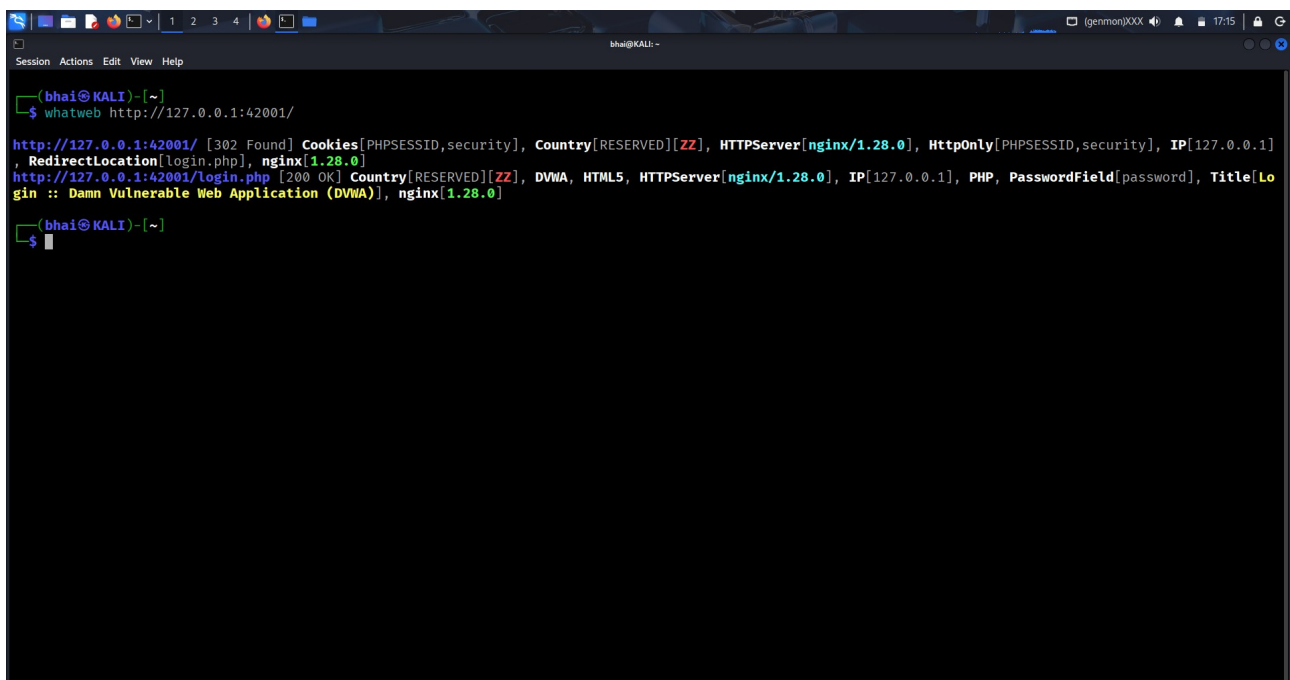
(bhai@KALI)-[~]
$
```

WhatWeb Fingerprinting

Identified technologies running on DVWA.

Command:

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



```
(bhai@KALI)-[~]
$ whatweb http://127.0.0.1:42001/

http://127.0.0.1:42001/ [302 Found] Cookies[PHPSESSID,security], Country[RESERVED][ZZ], HTTPServer[nginx/1.28.0], HttpOnly[PHPSESSID,security], IP[127.0.0.1], RedirectLocation[login.php], nginx[1.28.0]
http://127.0.0.1:42001/login.php [200 OK] Country[RESERVED][ZZ], DVWA, HTML5, HTTPServer[nginx/1.28.0], IP[127.0.0.1], PHP, PasswordField[password], Title[Login :: Damn Vulnerable Web Application (DVWA)], nginx[1.28.0]

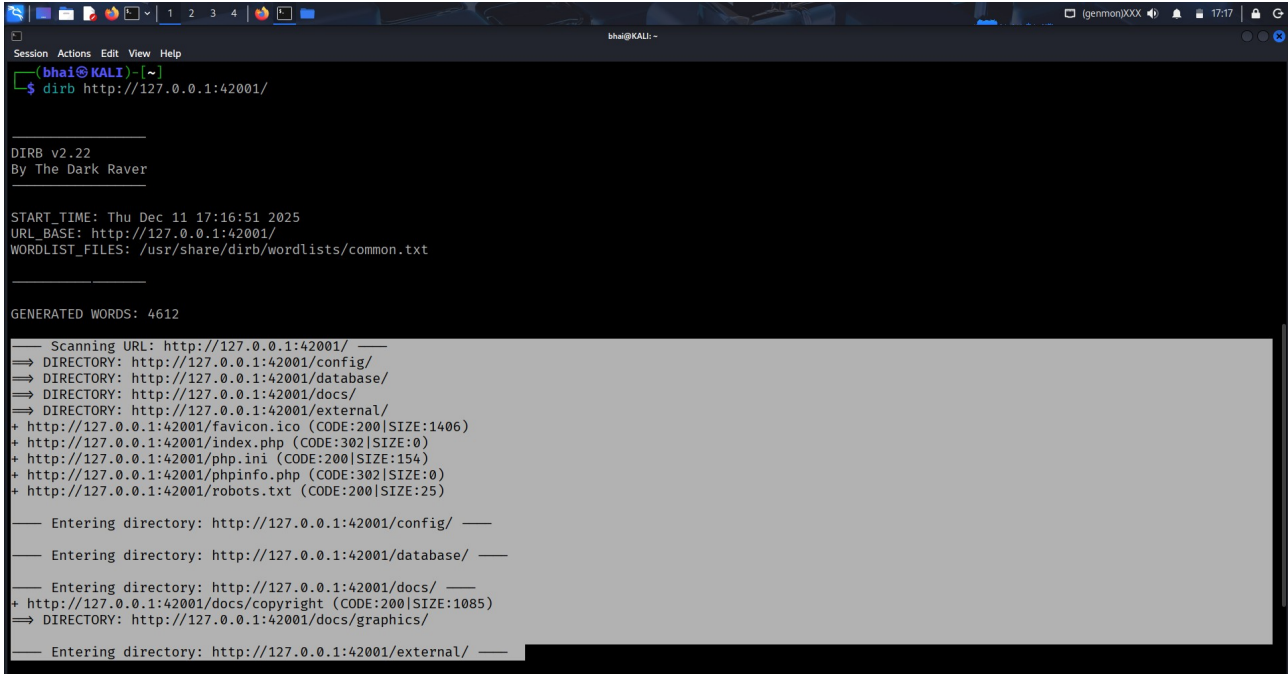
(bhai@KALI)-[~]
$
```

DIRB Directory Scan

Enumerated hidden directories and files.

Command:

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



```
Session Actions Edit View Help
bhai@KALI: ~
$ dirb http://127.0.0.1:42001/

DIRB v2.22
By The Dark Raver

START_TIME: Thu Dec 11 17:16:51 2025
URL_BASE: http://127.0.0.1:42001/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

--- Scanning URL: http://127.0.0.1:42001/ ---
=> DIRECTORY: http://127.0.0.1:42001/config/
=> DIRECTORY: http://127.0.0.1:42001/database/
=> DIRECTORY: http://127.0.0.1:42001/docs/
=> DIRECTORY: http://127.0.0.1:42001/external/
+ http://127.0.0.1:42001/favicon.ico (CODE:200|SIZE:1406)
+ http://127.0.0.1:42001/index.php (CODE:302|SIZE:0)
+ http://127.0.0.1:42001/php.ini (CODE:200|SIZE:154)
+ http://127.0.0.1:42001/phpinfo.php (CODE:302|SIZE:0)
+ http://127.0.0.1:42001/robots.txt (CODE:200|SIZE:25)

--- Entering directory: http://127.0.0.1:42001/config/ ---
--- Entering directory: http://127.0.0.1:42001/database/ ---
--- Entering directory: http://127.0.0.1:42001/docs/ ---
+ http://127.0.0.1:42001/docs/copyright (CODE:200|SIZE:1085)
=> DIRECTORY: http://127.0.0.1:42001/docs/graphics/
--- Entering directory: http://127.0.0.1:42001/external/ ---
```

Nuclei Scan

Ran templates for common misconfigurations.

Command:

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

```
Session Actions Edit View Help

(bhai@KALI)-[~]
$ nuclei -u http://127.0.0.1:42001/

nuclei 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)-[~]
$
```