

# Task - 3

## DVWA Web Application Security

Name : Nikhitha Thagaram

Environment: DVWA (Low Security)

URL : <http://127.0.0.1/dvwa/>

### 1. SQL INJECTION (SQLi)

#### Objective

Test if DVWA login/ID parameter is vulnerable to SQL Injection.

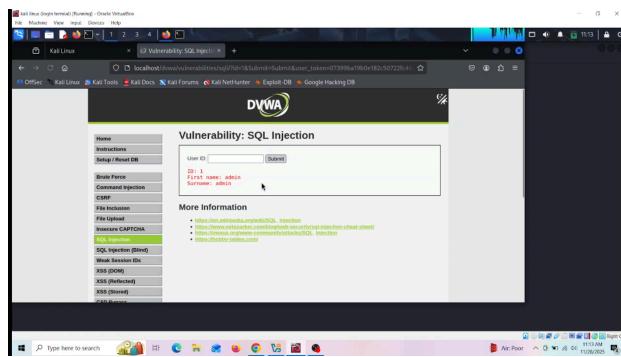
#### Steps

- Open DVWA → SQL Injection
- Enter the following payload in the ID field:
  - ‘1’ or 2 or 3....
- Click Submit

Observe the behavior/output

#### Result

- Application bypassed authentication
- Able to extract usernames & password hashes



### 2. CROSS-SITE SCRIPTING (XSS)

#### Objective

Perform Stored and Reflected XSS.

#### Steps – Stored XSS

- Go to DVWA → XSS (Stored)

Enter payload:

```
<script>alert('stored')</script>
```

- Click Sign Guestbook
- Refresh the page

## Steps – Reflected XSS

Go to DVWA → XSS (Reflected)

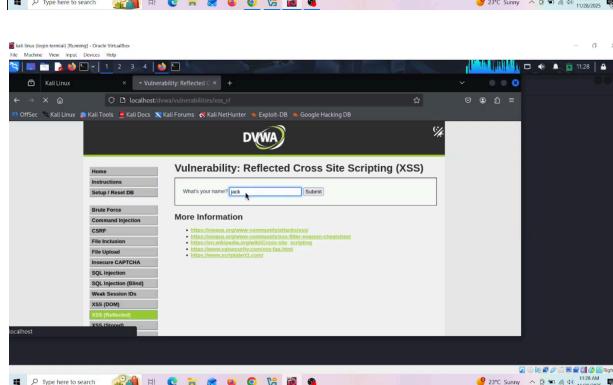
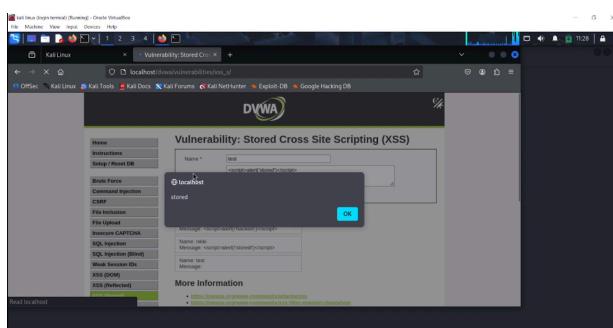
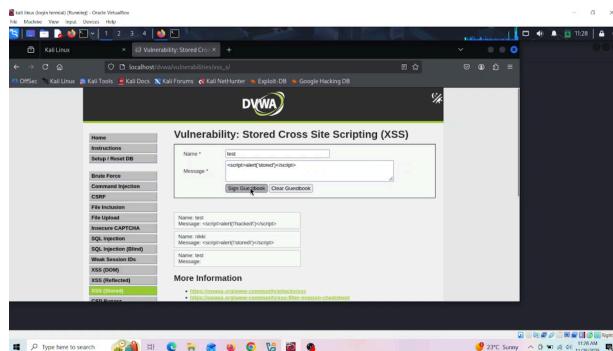
Enter:

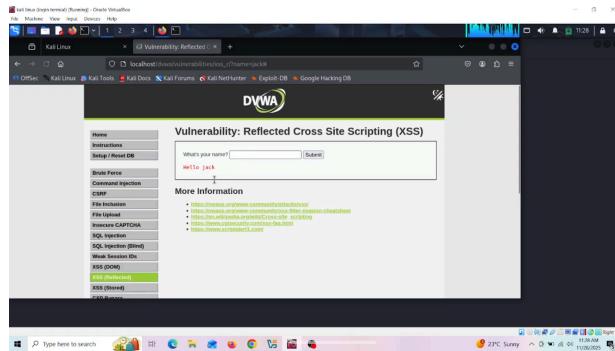
```
<script>alert('XSS')</script>
```

- submit

## Result

- Popup appears showing script executed
- Stored XSS persists in database





### 3. CROSS-SITE REQUEST FORGERY (CSRF)

#### Objective

Use a malicious external HTML page to change user password.

#### Steps

- Log into DVWA
- Open CSRF module

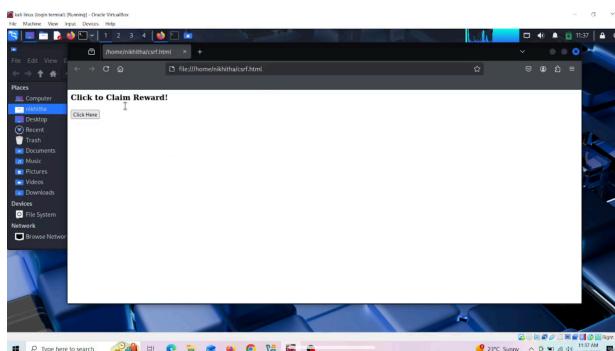
#### Create an external HTML file (csrf.html) with this code:

```
<form action="http://127.0.0.1/dvwa/vulnerabilities/csrf/" method="GET">  
  
<input type="hidden" name="password_new" value="hacked123">  
  
<input type="hidden" name="password_conf" value="hacked123">  
  
<input type="submit" value="Click Me">  
  
</form>
```

- While logged into DVWA, open csrf.html in browser
- Click Click Me

#### Result

Password changed without user's intention





## **5. BURP SUITE – INTRUDER (BRUTE FORCE)**

# Objective

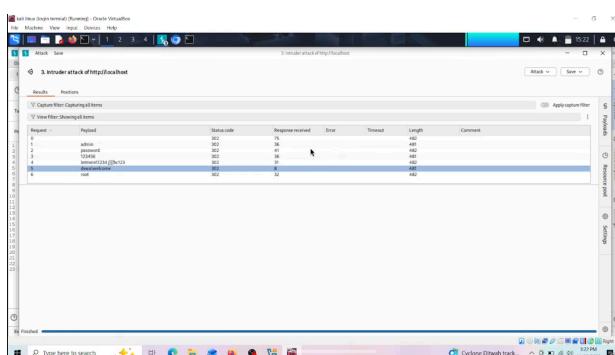
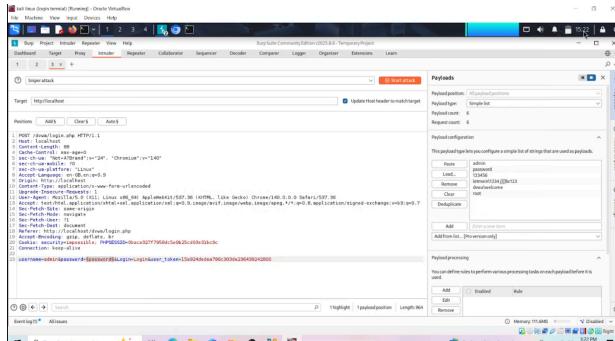
Use Burp Intruder to brute-force DVWA login using a demo wordlist.

## Steps

- Set browser to Burp proxy
  - Login to DVWA with wrong credentials
  - Burp → Proxy → Intercept ON
  - Capture request and Send to Intruder
  - Positions → set § around password field
  - Payloads → Load demo wordlist
  - Click Start Attack

## Result

Intruder identifies correct password by different Length or Status.



## 6. WEB SECURITY HEADERS

## Objective

Identify missing security headers and apply fixes.

## Steps

### Use command:

```
curl -I http://127.0.0.1/dvwa/
```

- Note missing headers

### Add these into Apache config:

Header set X-Frame-Options "DENY"

Header set X-Content-Type-Options "nosniff"

Header set X-XSS-Protection "1; mode=block"

Header set Content-Security-Policy "default-src 'self'"

## Result

Headers updated successfully.

