Lab Experiment: Finding & Exploiting XSS Vulnerabilities using DVWA on Kali Linux

Aim

To identify and exploit **Cross-Site Scripting (XSS)** vulnerabilities in a vulnerable web application (DVWA) using Kali Linux.

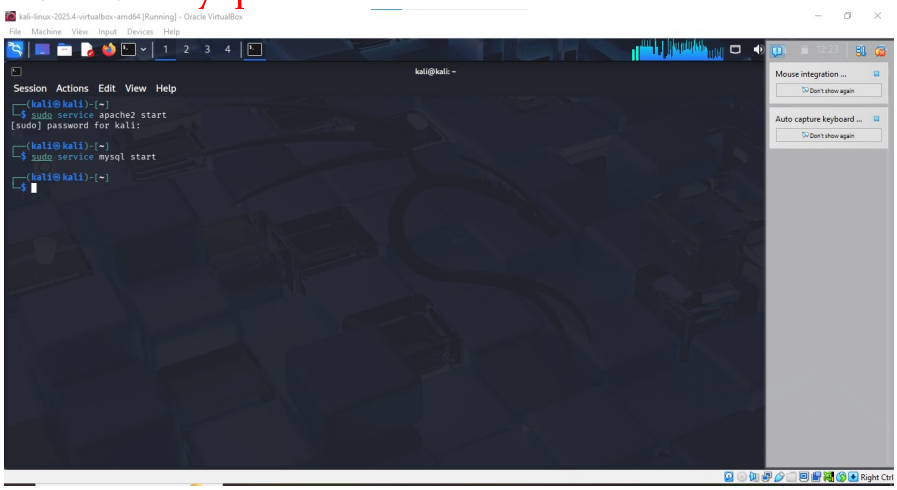
Requirements

- Kali Linux
- DVWA (Damn Vulnerable Web Application)
- Browser (Firefox/Chromium)
- Apache & MySQL running

Step 1: Start DVWA Services

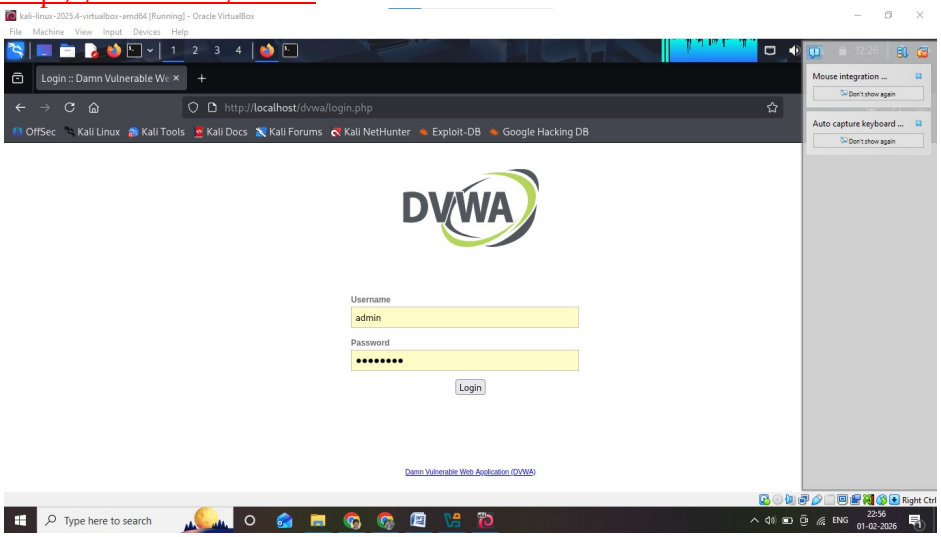
Open terminal:

```
sudo service apache2 start
sudo service mysql start
```



Open browser and go to:

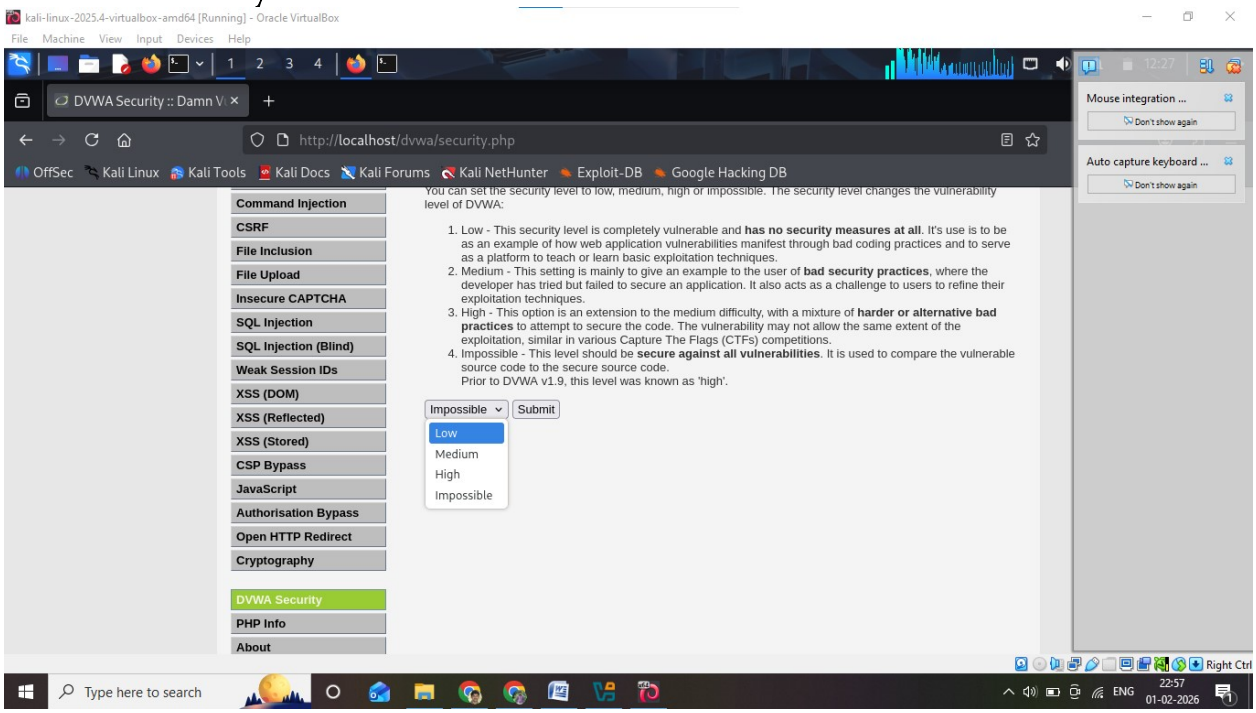
http://localhost/dvwa



Login:

- **Username:** admin
- **Password:** password

Click **DVWA Security** → set level to **Low** → Submit.



Step 2: Understanding XSS

XSS allows attackers to inject **JavaScript code** into a webpage that runs in another user's browser.

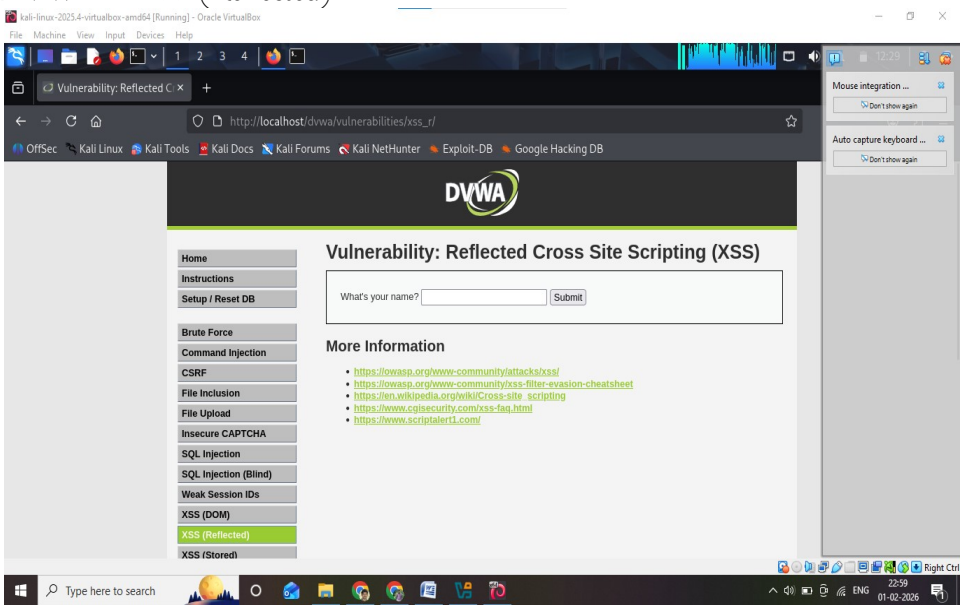
Types in DVWA:

- Reflected XSS
- Stored XSS
- DOM Based XSS

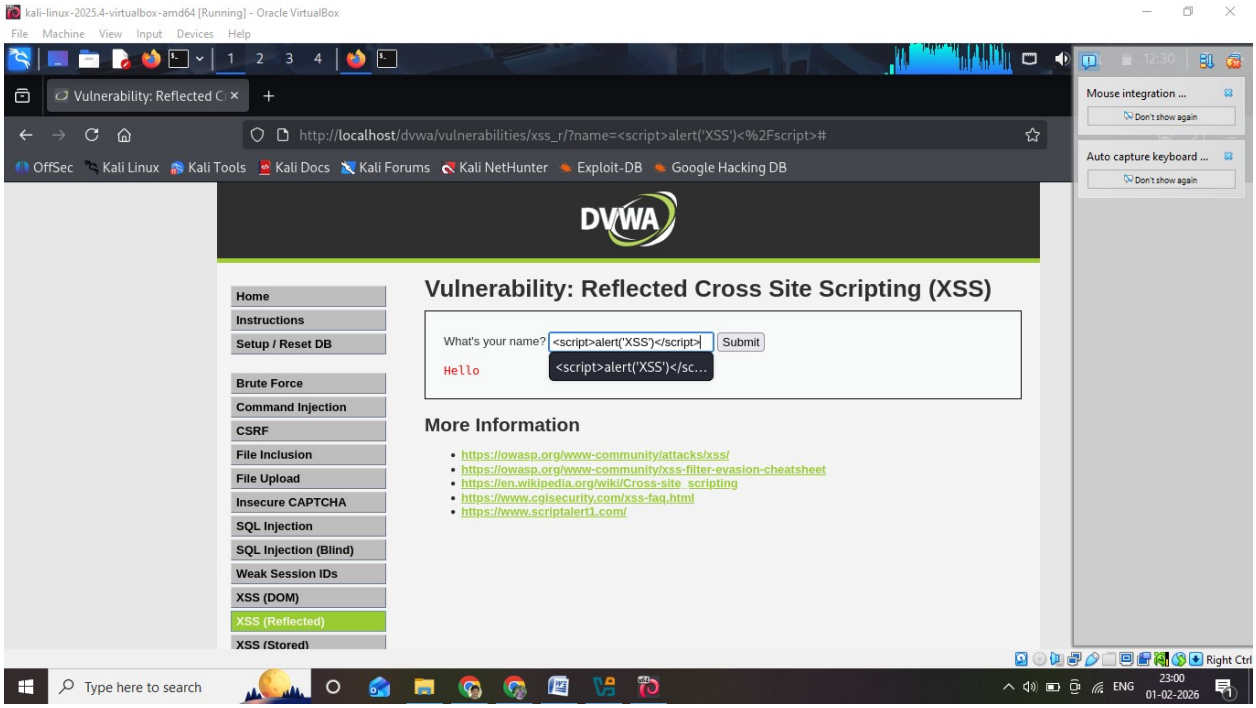
Step 3: Reflected XSS Test

Go to:

DVWA → XSS (Reflected)

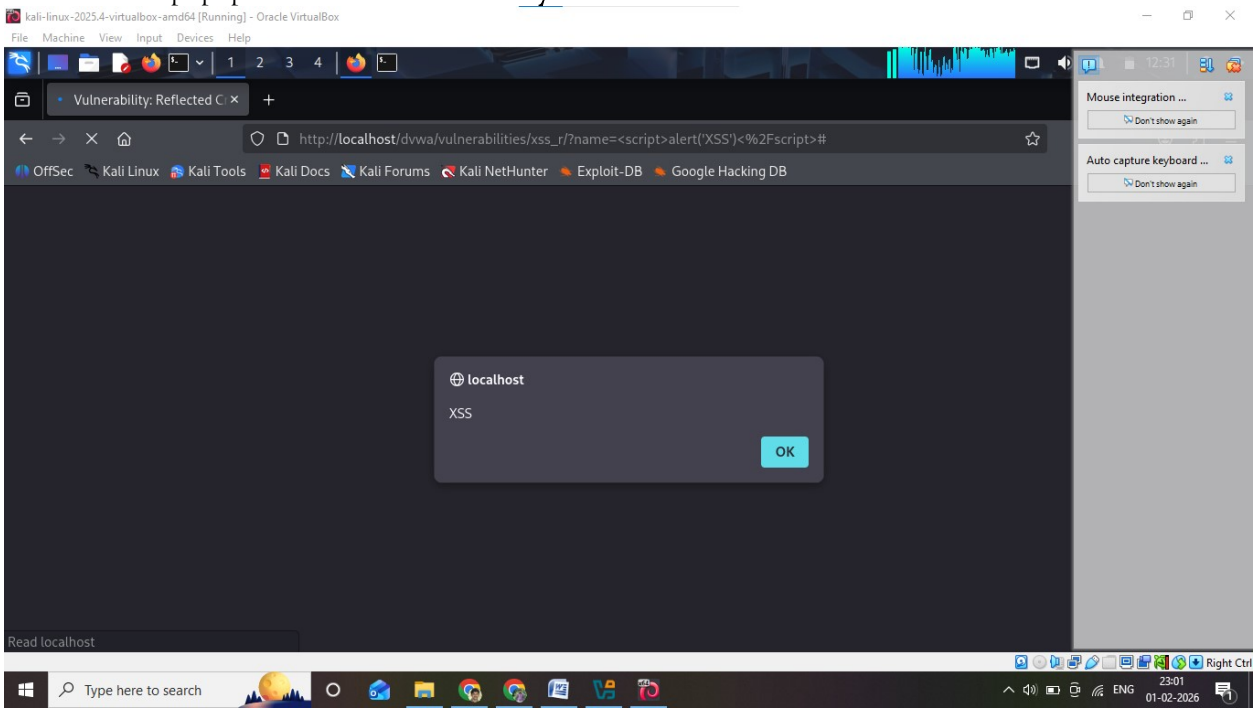


In the input box, type:
<script>alert('XSS')</script>
Click **Submit**.

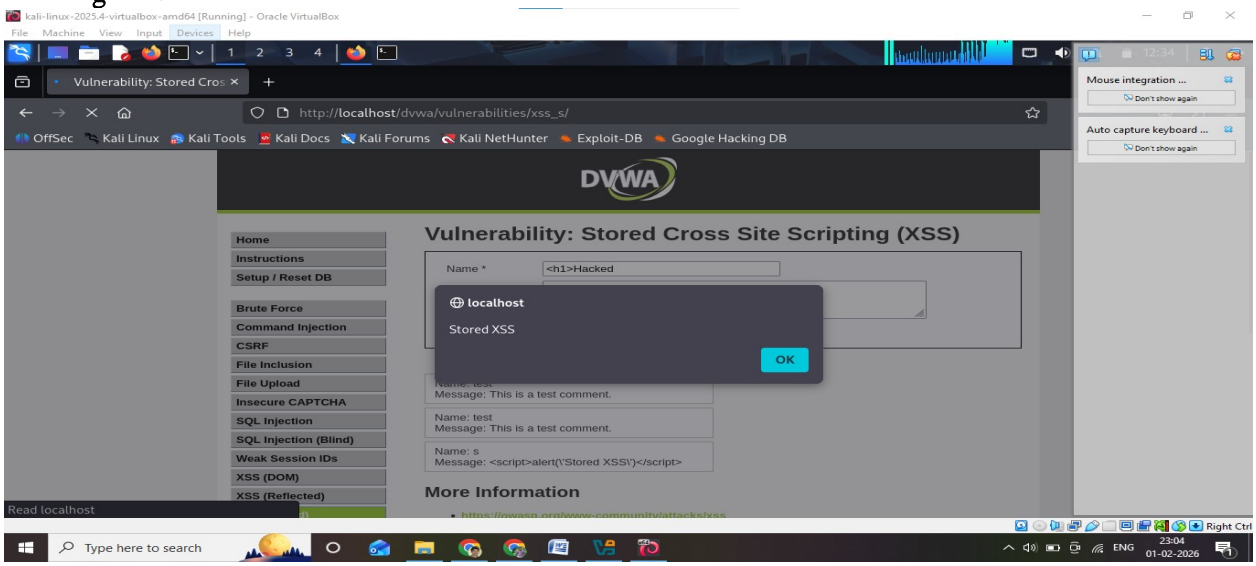


Output:

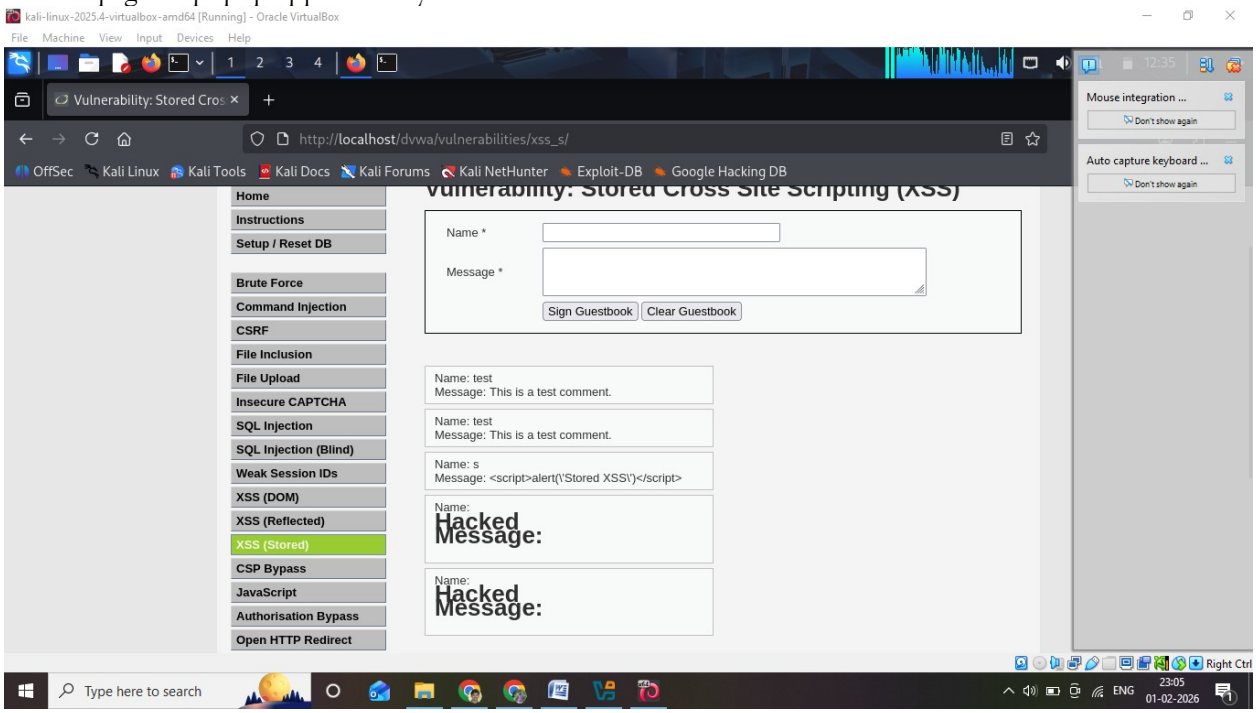
You will see a popup alert → **XSS vulnerability confirmed.**



Step 4: Stored XSS Test
Go to:
DVWA → XSS (Stored)
Fill the form:
Name:
<h1>Hacked</h1>
Message:
<script>alert('Stored XSS')</script>
Click **Sign Guestbook.**



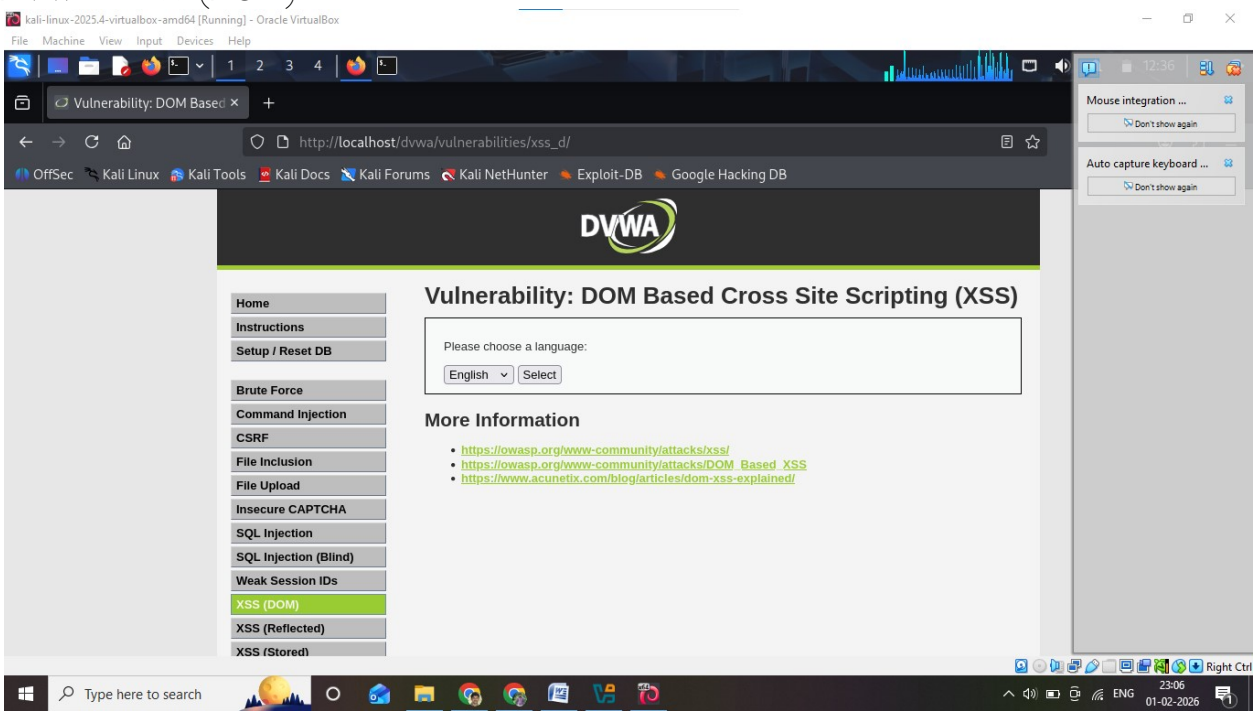
Refresh page → popup appears every time → **Stored XSS successful.**



Step 5: DOM Based XSS

Go to:

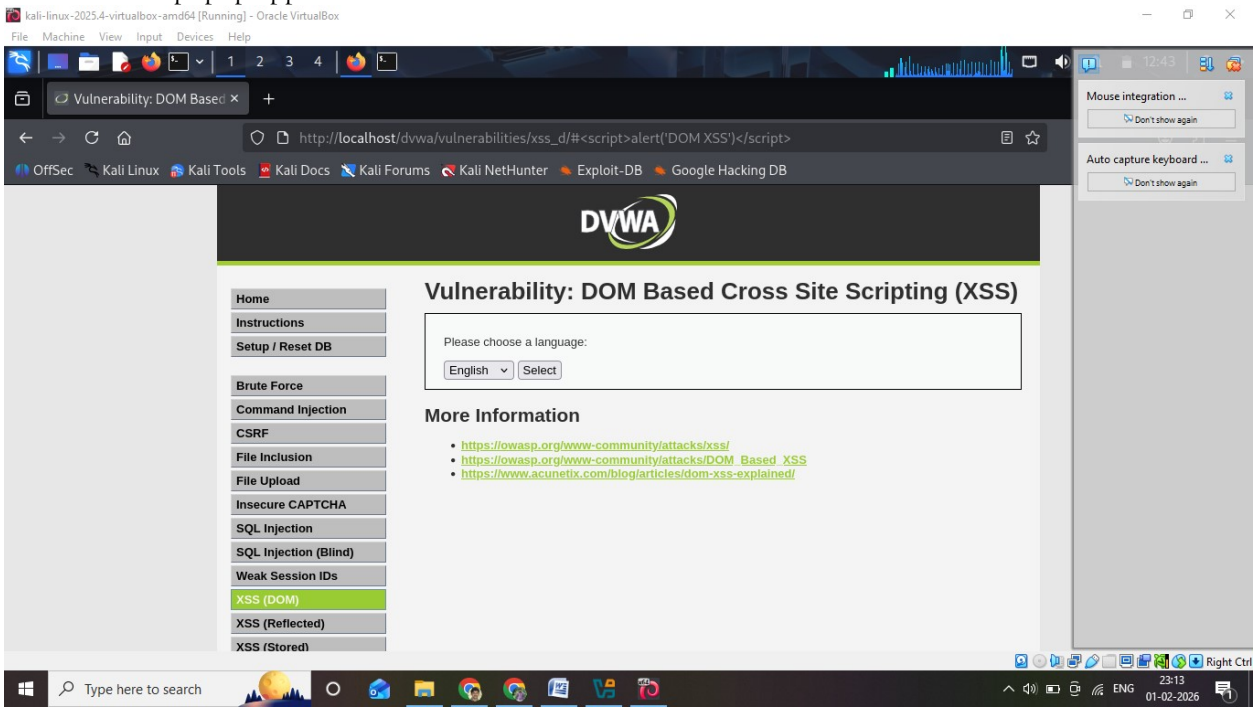
DVWA → XSS (DOM)



In the URL bar add:

#<script>alert('DOM XSS')</script>

Press Enter → popup appears.

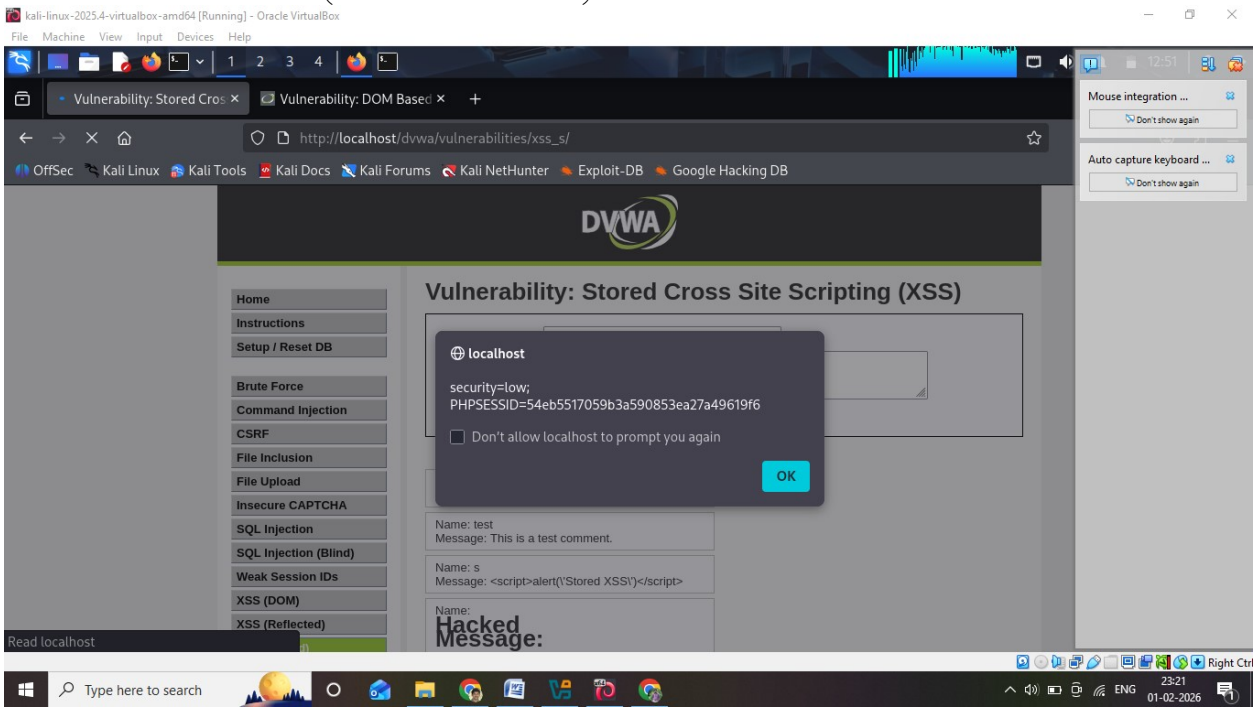


Step 6: Capture Cookie (Lab Demo)

In Stored XSS Message box:

<script>alert(document.cookie)</script>

This shows session cookies (demo of session theft).



Step 7: Change Security Level

Go to **DVWA Security** → set:

- Medium
- High

Repeat the same payloads → see how filtering blocks them.

Result

XSS vulnerabilities were successfully identified and exploited in DVWA.