

Assignment 2

COMP421B



may 20th, 2025

FARAZ WAQAR (251707570)

Section: B



# Introduction:

In this assignment, I explored different types of Cross-Site Scripting (XSS) attacks using a platform called DVWA (Damn Vulnerable Web Application). The tasks were designed to show how attackers can exploit weak spots in web applications. I performed the following:

* Reflected XSS
* Cookie stealing via XSS
* Stored XSS

These tasks helped me understand how these attacks work and why it’s important to secure web applications properly.

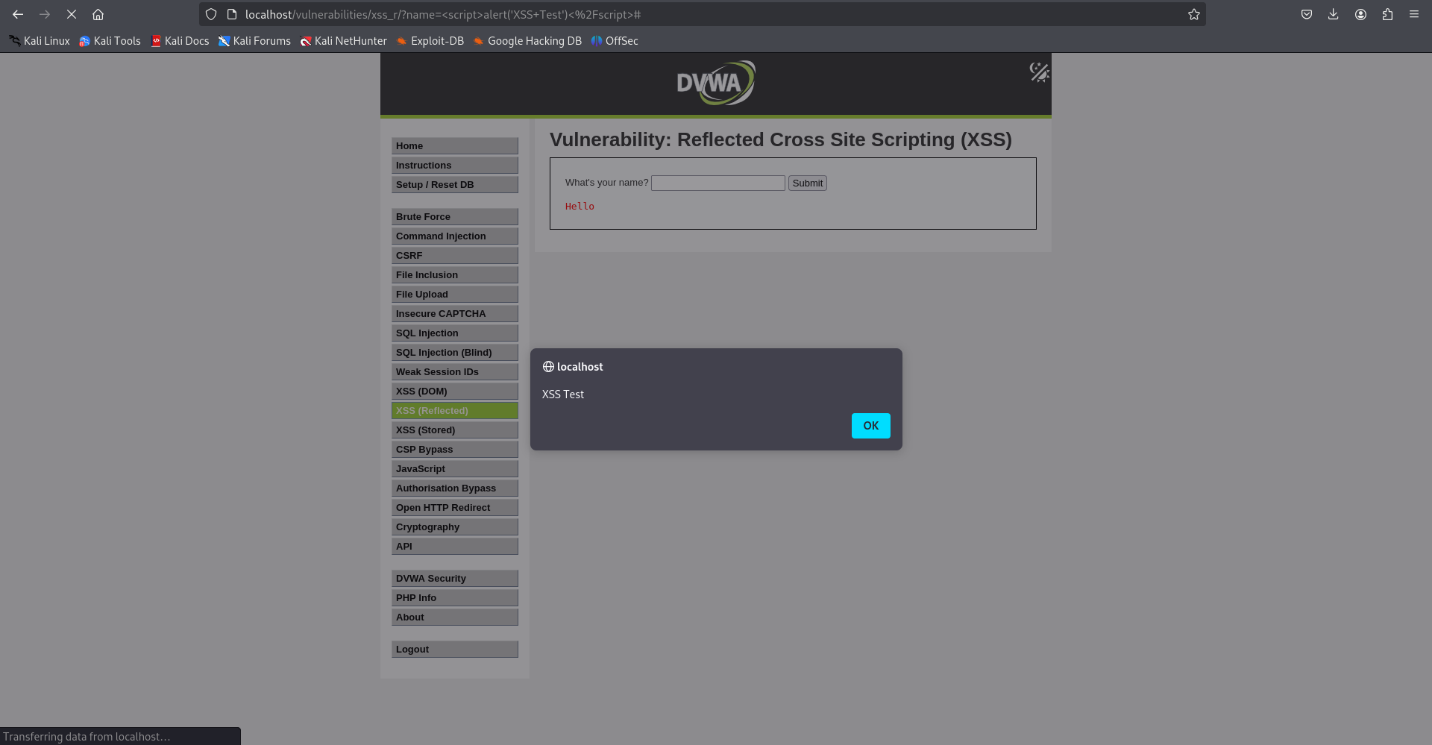
# Task Details and Observations

## Task 1: Reflected XSS

What I did:  
I opened the Reflected XSS page in DVWA and entered the following script:

**<script>alert('XSS Test')</script>**

What happened:  
A popup appeared showing the message “XSS Test”, which confirmed that the script ran in the browser. This means the site is vulnerable to reflected XSS.

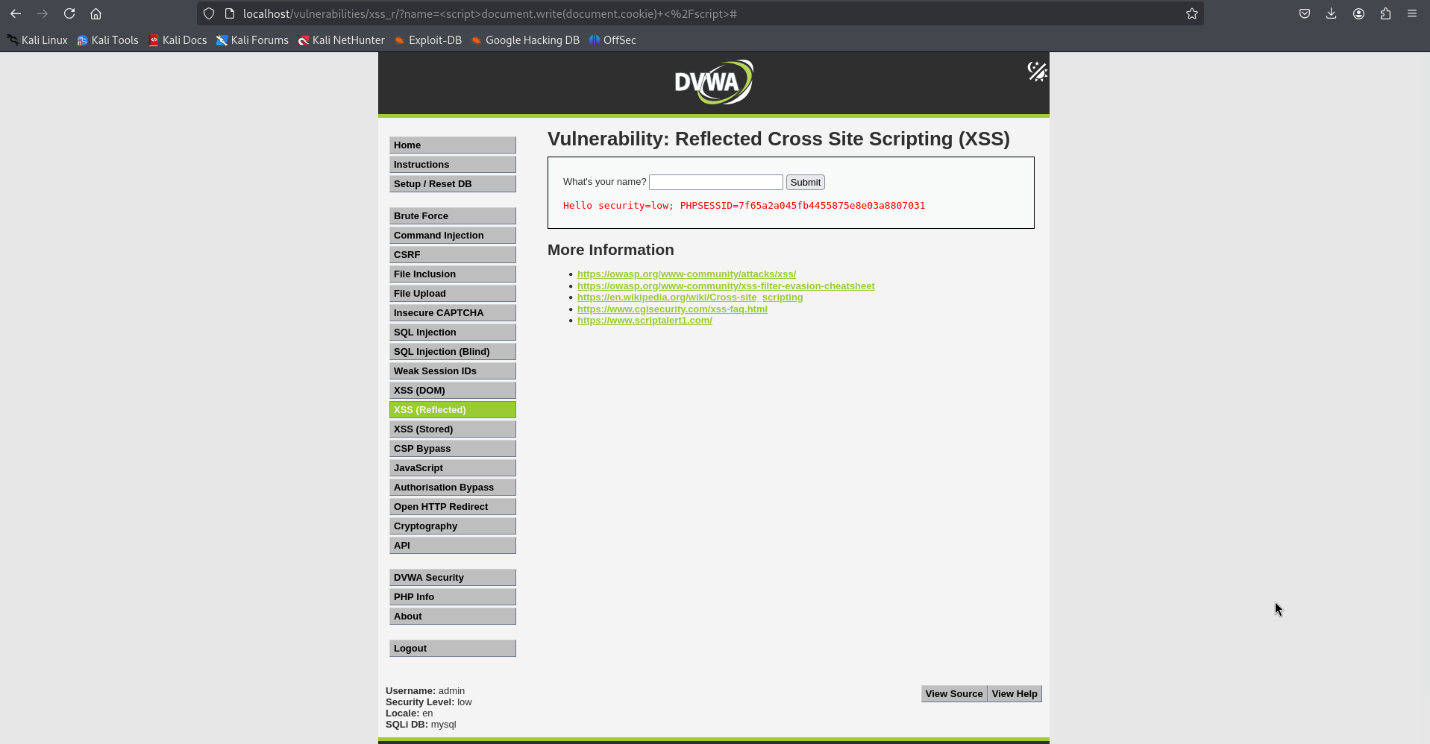


## Task 2: Stealing Cookies

What I did:  
On the same page, I entered this script to display the browser’s cookie:

**<script>document.write(document.cookie)</script>**

What happened:  
The browser displayed the session cookie on the page. This showed how an attacker could steal a user’s cookie using XSS and possibly take control of their session.

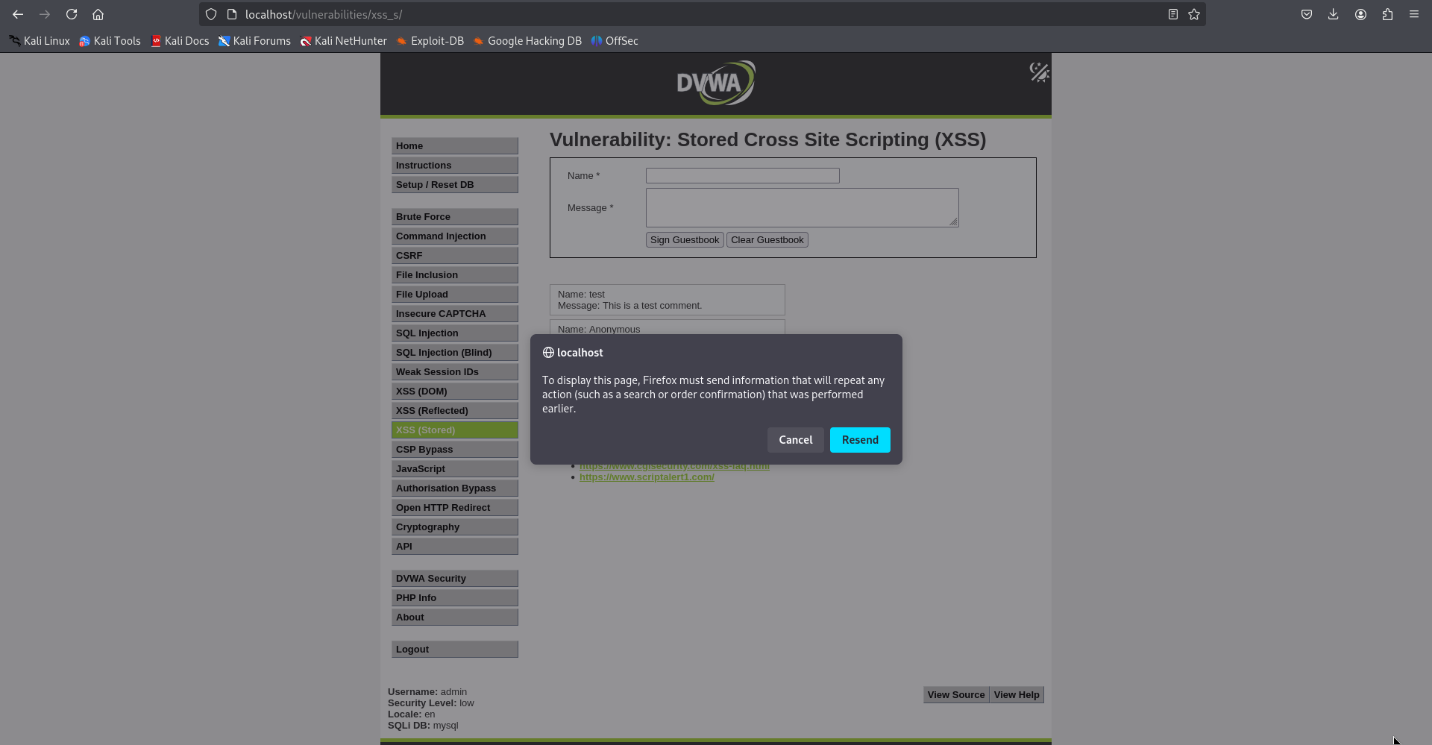


## Task 3: Stored XSS

What I did:  
I went to the Stored XSS page in DVWA and posted a comment with this script:

**<script>alert('Stored XSS')</script>**

What happened:  
After posting the comment, every time I refreshed or visited the page, the popup showed again. This proved the script was stored and triggered for anyone who views the page, which is a stored XSS attack.



# What I Learned:

XSS is dangerous:  
These attacks can be used to steal data, hijack sessions, or trick users into doing things they didn’t mean to.

Always filter input:  
Websites should clean or validate all user input to prevent malicious scripts from being executed.

Stored XSS is more serious than reflected XSS:  
Reflected XSS affects one user at a time, while stored XSS can impact every user who loads the affected page.

Security settings are important:  
Setting DVWA to a low security level made it easier to test, but also showed how important it is to configure applications securely in real life.

# Conclusion:

This assignment helped me understand XSS attacks in a practical way. I saw how easy it is to break into insecure web apps and learned how developers can protect their sites. It was interesting to think like an attacker and also learn how to defend against these kinds of attacks.

# GitHub Link: