

Tutorial No. 7

Title: Understanding and Performing an XSS Attack



(A Constituent College of Somaiya Vidyavihar University)

Roll No.: 16010423076

Tutorial No.: 7

Aim: Understanding and Performing an XSS Attack

Resources : Linux OS or a Linux Virtual Machine (hosted on any platform), DVWA

Theory:**What is XSS?**

Cross-Site Scripting (XSS) is a security vulnerability found in web applications. It occurs when an attacker injects malicious scripts into content that gets delivered to other users. The browser then executes these scripts as if they were trusted, leading to various security risks.

What is XSS Attack?

An XSS attack typically targets a user interacting with a vulnerable website. The attacker injects malicious code (often JavaScript) into web pages, which then gets executed on the user's browser. This can lead to:

- **Session Hijacking:** Stealing cookies or session tokens.
- **Phishing:** Redirecting users to malicious sites.
- **Data Theft:** Gaining access to sensitive data.
- **Defacement:** Altering the website's content.
- **Browser Exploitation:** Gaining control over the user's browser.

Discuss types of XSS in detail.**Stored XSS (Persistent XSS):**

- The malicious script is permanently stored on the target server (e.g., in a database).

(A Constituent College of Somaiya Vidyavihar University)

- When a user visits the infected page, the script runs in their browser.
- Example: A comment section where the attacker posts a script instead of a normal comment.

Reflected XSS (Non-Persistent XSS):

- The malicious script is reflected off a web server, typically via a URL parameter.
- The script executes when a victim clicks a crafted link.
- Example: A search page displaying user input without sanitization.

DOM-Based XSS:

- The vulnerability exists in the client-side scripts rather than the server.
- The script manipulates the DOM, leading to unexpected execution.
- Example: A JavaScript snippet that dynamically updates the webpage based on user input.

[Important: Note that you don't want to try this out on a regular website. Very high chances that you will be blocked. So be careful and always practice only on DVWA]

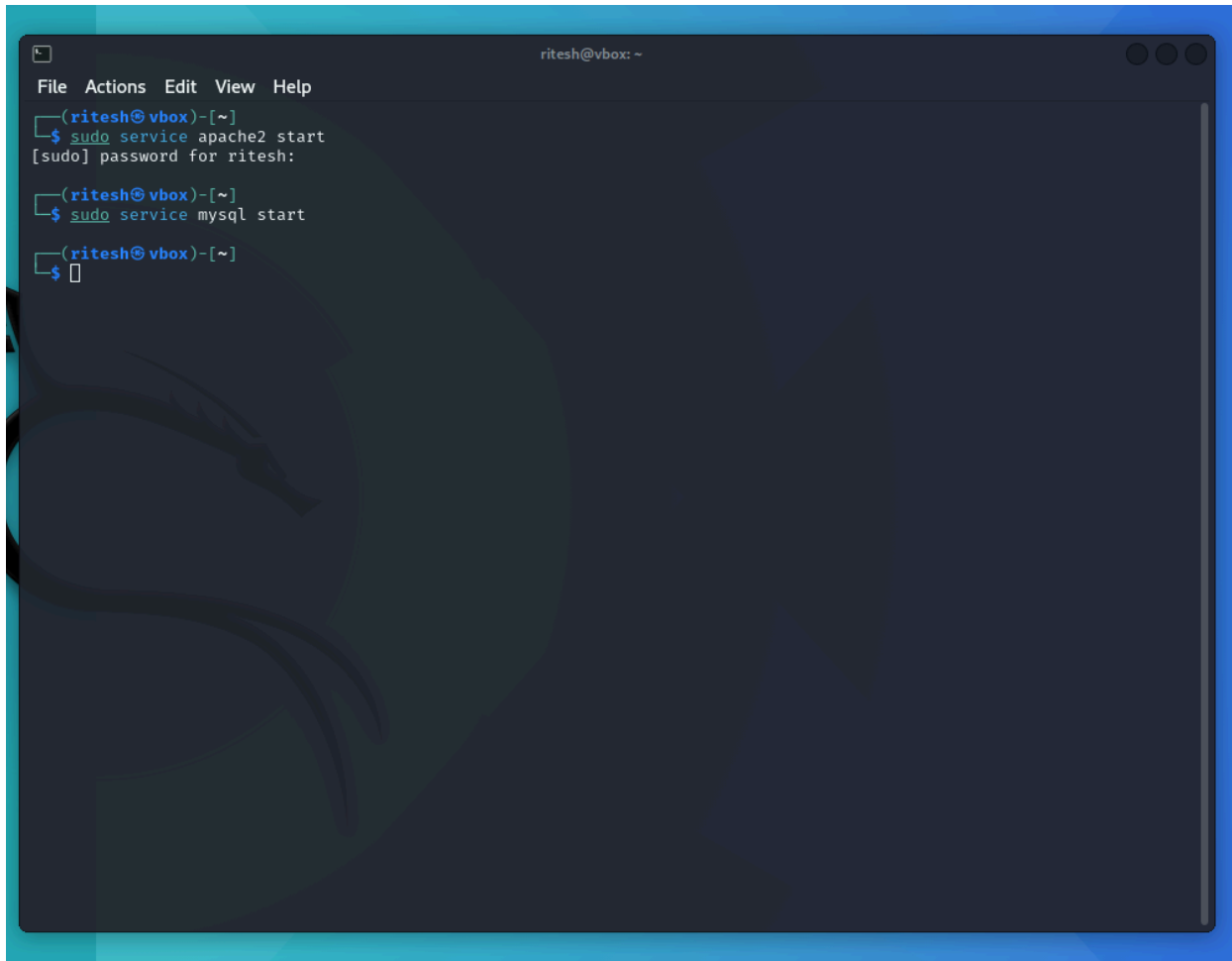
Hands-On Demonstration on DVWA (Damn Vulnerable Web Application)

Steps :

Start your web server and database:

```
sudo service apache2 start
```

```
sudo service mysql start
```

A screenshot of a terminal window titled 'ritesh@vbox: ~'. The terminal shows the execution of two commands: 'sudo service apache2 start' and 'sudo service mysql start'. The first command prompts for a password, which is entered. The second command is also entered. The terminal output shows the status of the services being started. The terminal window has a dark background with a blue border. The title bar shows 'ritesh@vbox: ~' and standard window controls. The menu bar includes 'File', 'Actions', 'Edit', 'View', and 'Help'. The prompt is '(ritesh@vbox)-[~]'. The commands are entered as '\$ sudo service apache2 start' and '\$ sudo service mysql start'. The output for the first command is '[sudo] password for ritesh:' followed by a blank line. The output for the second command is '[sudo] password for ritesh:' followed by a blank line. The prompt returns to '\$' after each command.

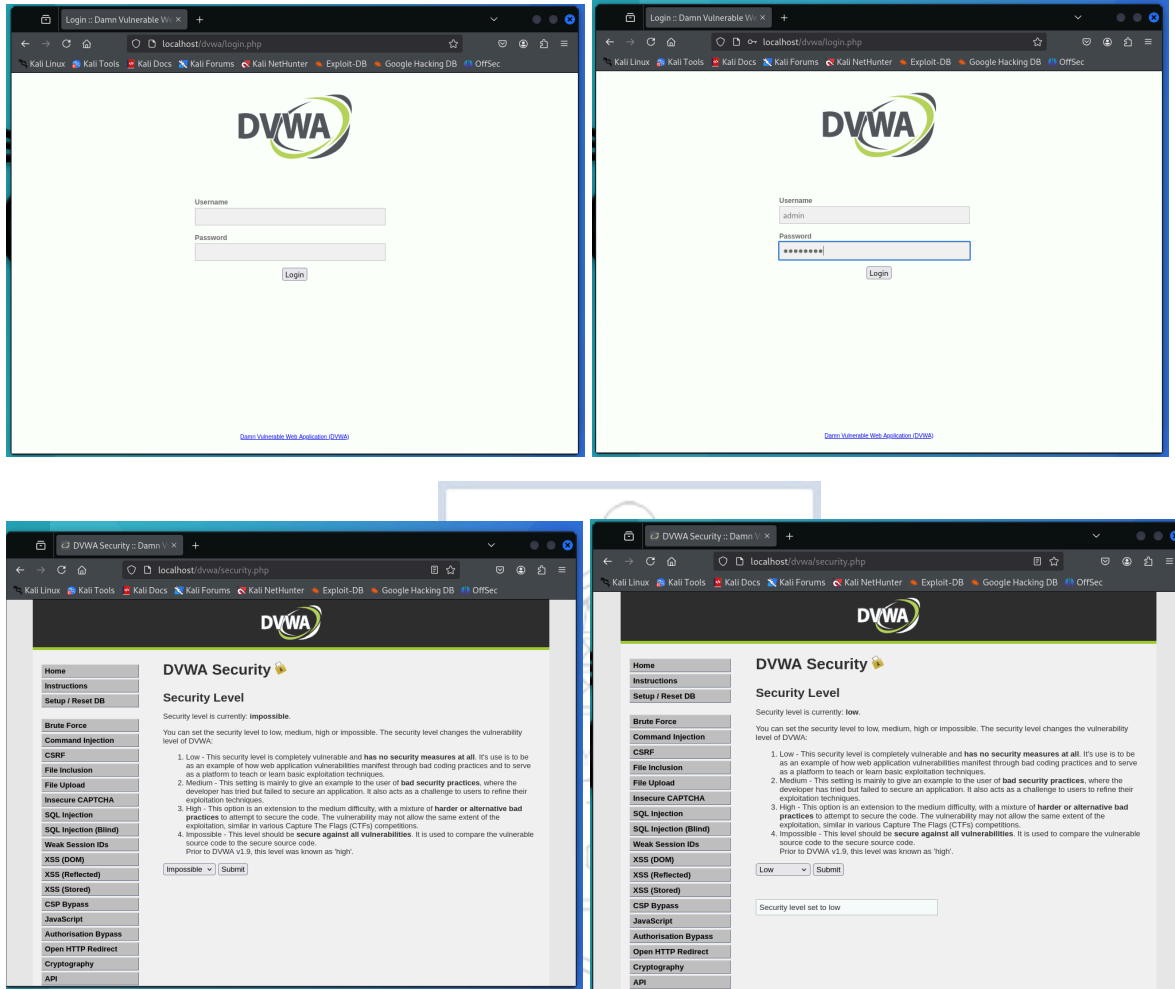
Navigate to DVWA in your browser:

<http://localhost/dvwa>

Login using : admin / password

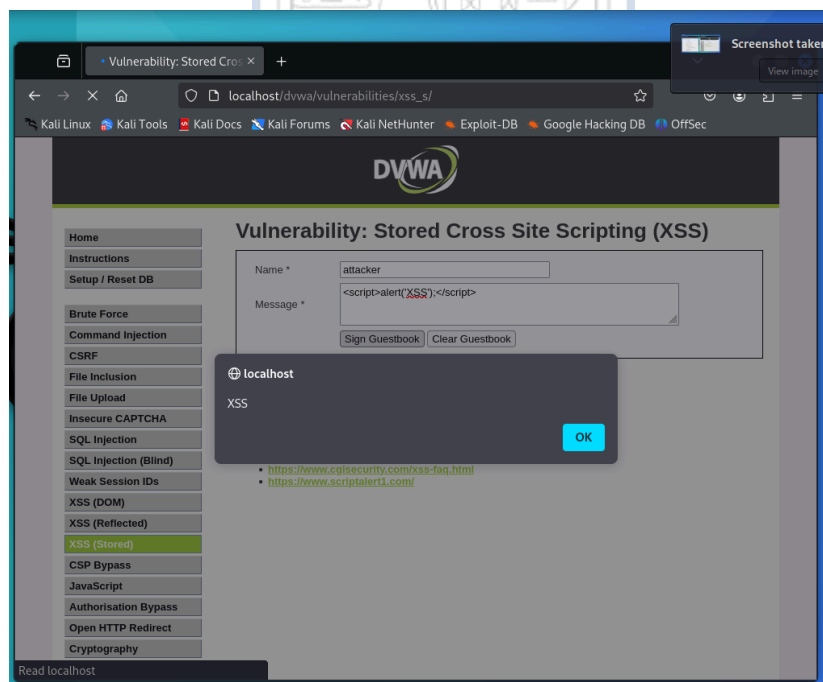
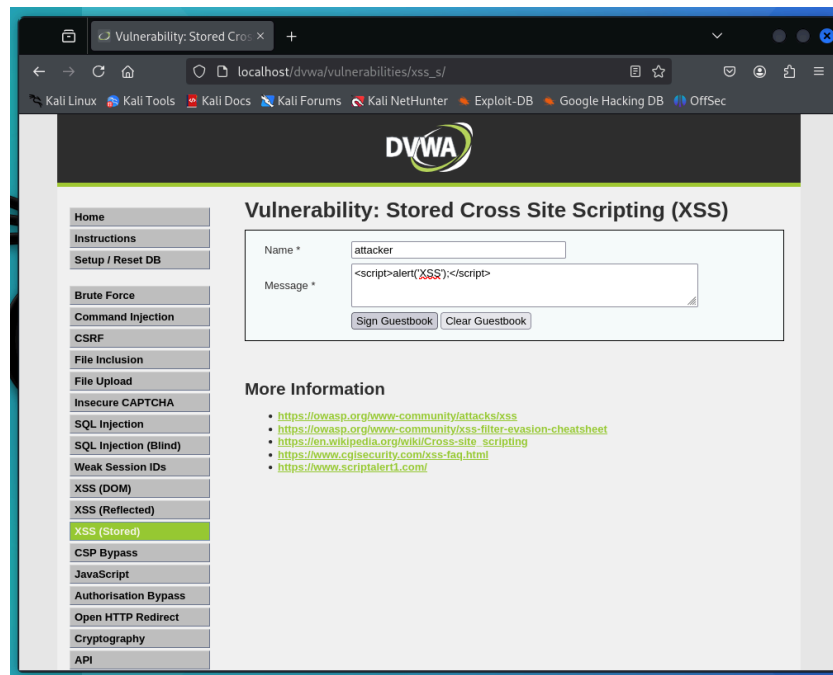
Set difficulty to low

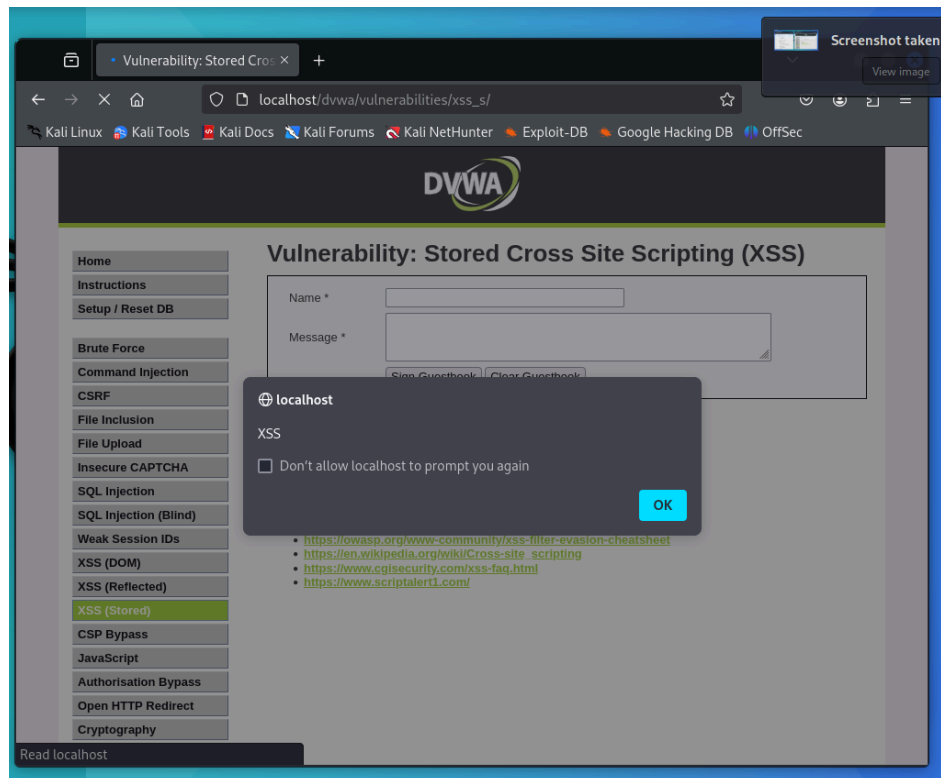
(A Constituent College of Somaiya Vidyavihar University)



1. Stored XSS

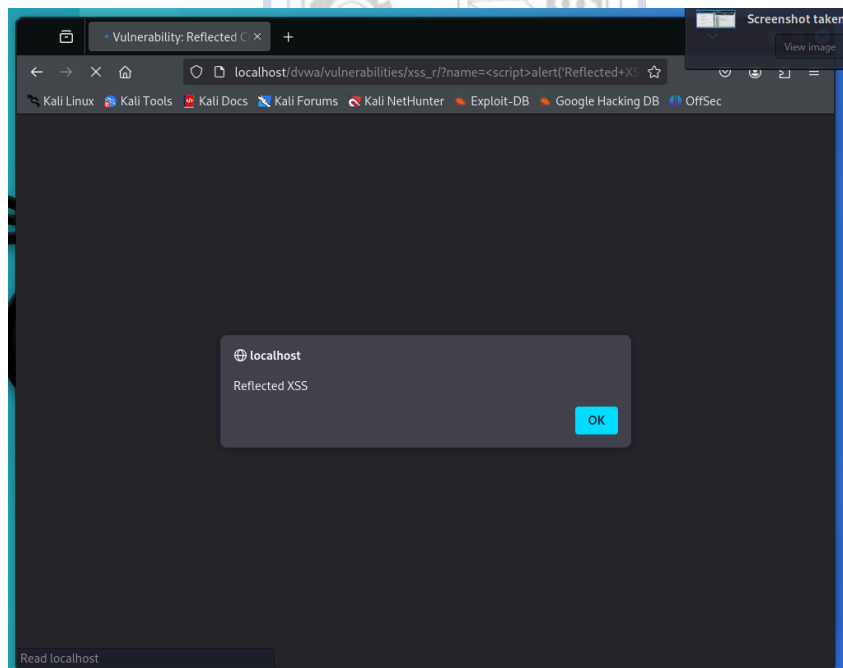
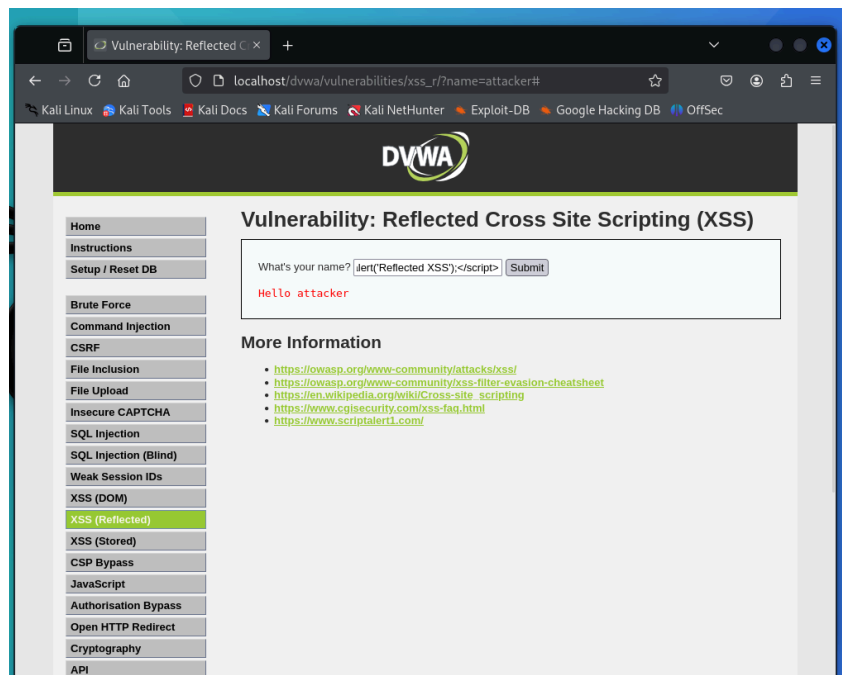
```
<script>alert('XSS');</script>
```





2. Reflected XSS

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

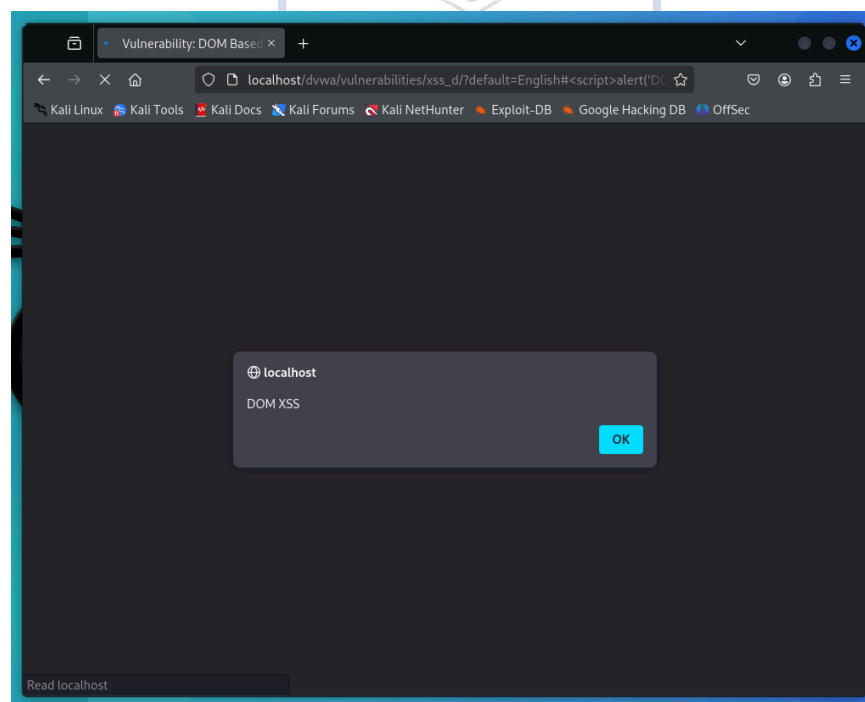
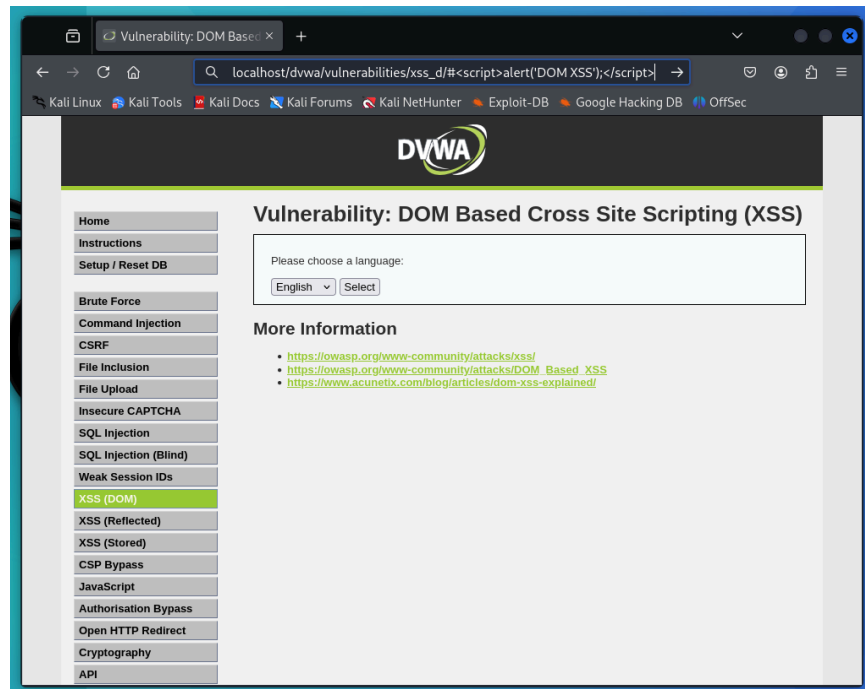


(A Constituent College of Somaiya Vidyavihar University)

3. DOM-Based XSS

Add this to the url and reload :

?default#<script>alert('DOM XSS');</script>



(A Constituent College of Somaiya Vidyavihar University)

Conclusion :

From this tutorial, I learned about Cross-Site Scripting (XSS), a security vulnerability that occurs when an attacker injects malicious scripts into web applications. I explored the three main types of XSS attacks: Stored, Reflected, and DOM-Based XSS. Stored XSS involves scripts being permanently stored on the server, Reflected XSS happens when scripts are reflected off the server, and DOM-Based XSS occurs directly on the client side through DOM manipulation. Additionally, I practiced performing these attacks safely on the Damn Vulnerable Web Application (DVWA), gaining hands-on experience with how each XSS type works and how attackers can exploit web application vulnerabilities.



(A Constituent College of Somaiya Vidyavihar University)