Vulnerability Assessment Report

Target: DVWA (Damn Vulnerable Web Application)

Date: October 17 2026

Author: Sahil Punia

Description: XSS vulnerabilities allow attackers to inject client-side scripts into web pages viewed by other users. This can lead to session hijacking, defacement, or redirection to malicious sites.

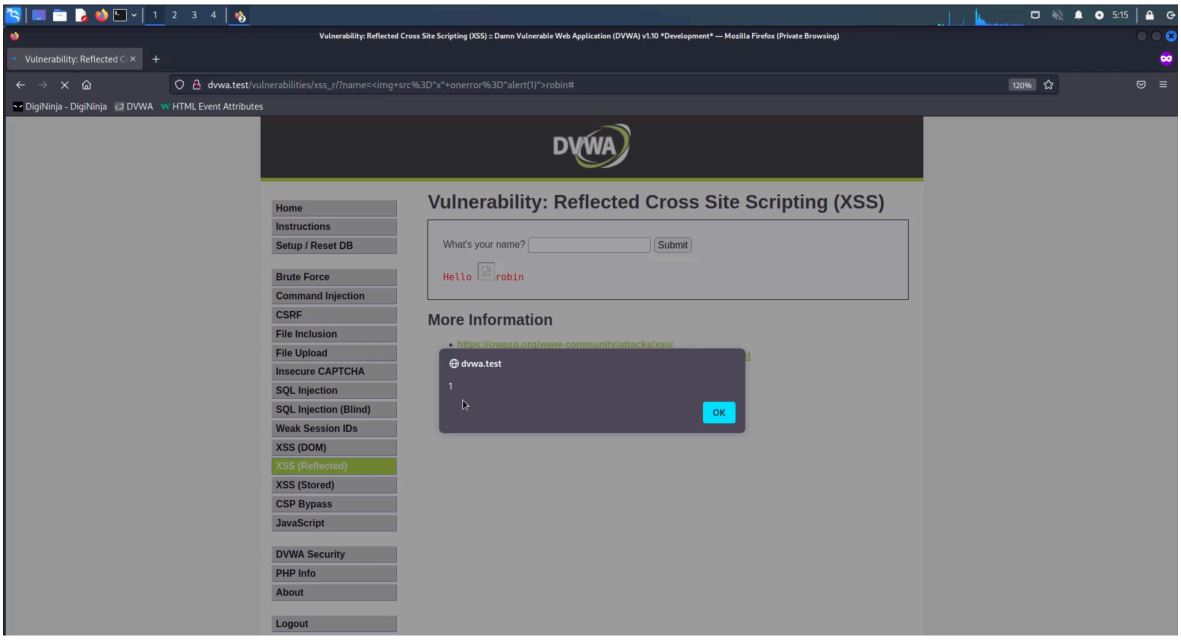
Vulnerable Endpoint: `http://dvwa.test/vulnerabilities/xss_r/`

Proof of Concept (PoC):

> **Reflected XSS Payload:** `<script>alert(‘1');</script>`

Reproduction Steps:

1. Navigate to the XSS (Reflected) page in DVWA.
2. Enter the reflected XSS payload into the input field.
3. Observe the JavaScript alert box.
4. The alert box will appear immediately, and for subsequent visitors to that page.



Vulnerability: Reflected Cross Site Scripting (XSS) :: Damn Vulnerable Web Application (DVWA) v1.10 *Development* — Mozilla Firefox (Private Browsing)

dvwa.test/vulnerabilities/xss_r/?name=<img+src%3D"x"+onerror%3D"alert(1)">robin#

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name? [ ] Submit

Hello robin

More Information

dvwa.test

1

OK

Impact :

The impact of XSS is often underestimated, but it is one of the most dangerous web vulnerabilities because it targets the **users** of the application rather than the server itself.

1. Session Hijacking (Account Takeover)

This is the most common high-impact result. An attacker can use JavaScript to steal a user’s session cookies (`document.cookie`).

payload: <script>alert(document.cookie);</script>

- **Consequence:** The attacker can bypass login credentials and completely take over the victim's account by importing the stolen session token into their own browser.

2. Unauthorized Actions (CSRF via XSS)

If an XSS vulnerability exists, an attacker can force the victim's browser to perform actions on their behalf while they are logged in.

- **Examples:** Changing the account password, updating the email address, or making unauthorized purchases/transfers without the user ever knowing.