DVWA — XSS (Reflected) (low)

Security Micro-Scan

Client: DVWA Lab
Date: 2025-09-26
Author: Braxton Beck (Ben-Frank17)
Severity: Medium — Reflected XSS allows attacker JavaScript to run in victim context.

Summary

The Reflected XSS module reflects user input into the HTML response without proper output encoding. An attacker can inject JavaScript that executes in other users' browsers.

PoC

Payload: `<script>alert(1)</script>`
Steps

1. Login to DVWA and set Security = **low**.
2. Navigate to **Vulnerabilities** → **XSS (Reflected)**.
3. Submit the payload in the input field.
4. A browser alert appears confirming script execution.

Evidence

- Screenshot: `dvwa_xss_reflected.png`

Impact

Reflected XSS can steal session tokens, perform actions on behalf of a user, or deliver further payloads for phishing or credential theft.

Remediation

- Output-encode user-supplied data before rendering in HTML.
- Use Content Security Policy (CSP) to limit script execution.
- Sanitize inputs and validate expected types.

Retest

Verify payloads are rendered as escaped text and that no script executes in a fresh browser session.