

XSS-AutoPwn Report

Target: http://localhost:8080/vulnerabilities/xss_r/

Payload: <script>alert('XSS-AutoPwn')</script>

Status: **VULNERABLE**

The screenshot shows the DVWA application interface. On the left, a vertical menu bar lists various security vulnerabilities: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection, SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected) (which is highlighted in green), XSS (Stored), CSP Bypass, JavaScript, DVWA Security, PHP Info, and About. The main content area has a dark header with the DVWA logo. Below the header, a red banner displays the text "XSS-AutoPwn EXPLOITED!". The main content area title is "Vulnerability: Reflected Cross Site Scripting (XSS)". It contains a form field labeled "What's your name?" with a placeholder value "Hello" and a "Submit" button. The "Hello" text is displayed in red, indicating it was injected by the exploit.

Fix: Sanitize user input with HTML escaping