


XSS Exploiter Report

Label	JS Payload	Options	Requests received
sample-report	https://app.pentest-tools.com/xss-payload/FcxqExhVJG/	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
security=low; PHPSESSID=8393a79c339432095c7a61f26d8e500d	https://pentest-ground.com:4280/vulnerabilities/xss_s/	Image 1	testadmin@password password1234test	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:125.0) Gecko/20100101 Firefox/125.0	Tue April 30, 2024 03:01:58 pm (GMT +3)

Image 1



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 (Reflected)

XSS (Stored)

CSP Bypass

JavaScript

Open HTTP Redirect

DVWA Security

PHP Info

About

Logout

Name *

Message *

Name: test

Message:

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.cgisecurity.com/xss-faq.html>
- <http://www.scriptalert1.com/>

Username: Unknown

Security Level: low

Locale: en

SQLi DB: mysql

Damn Vulnerable Web Application (DVWA)