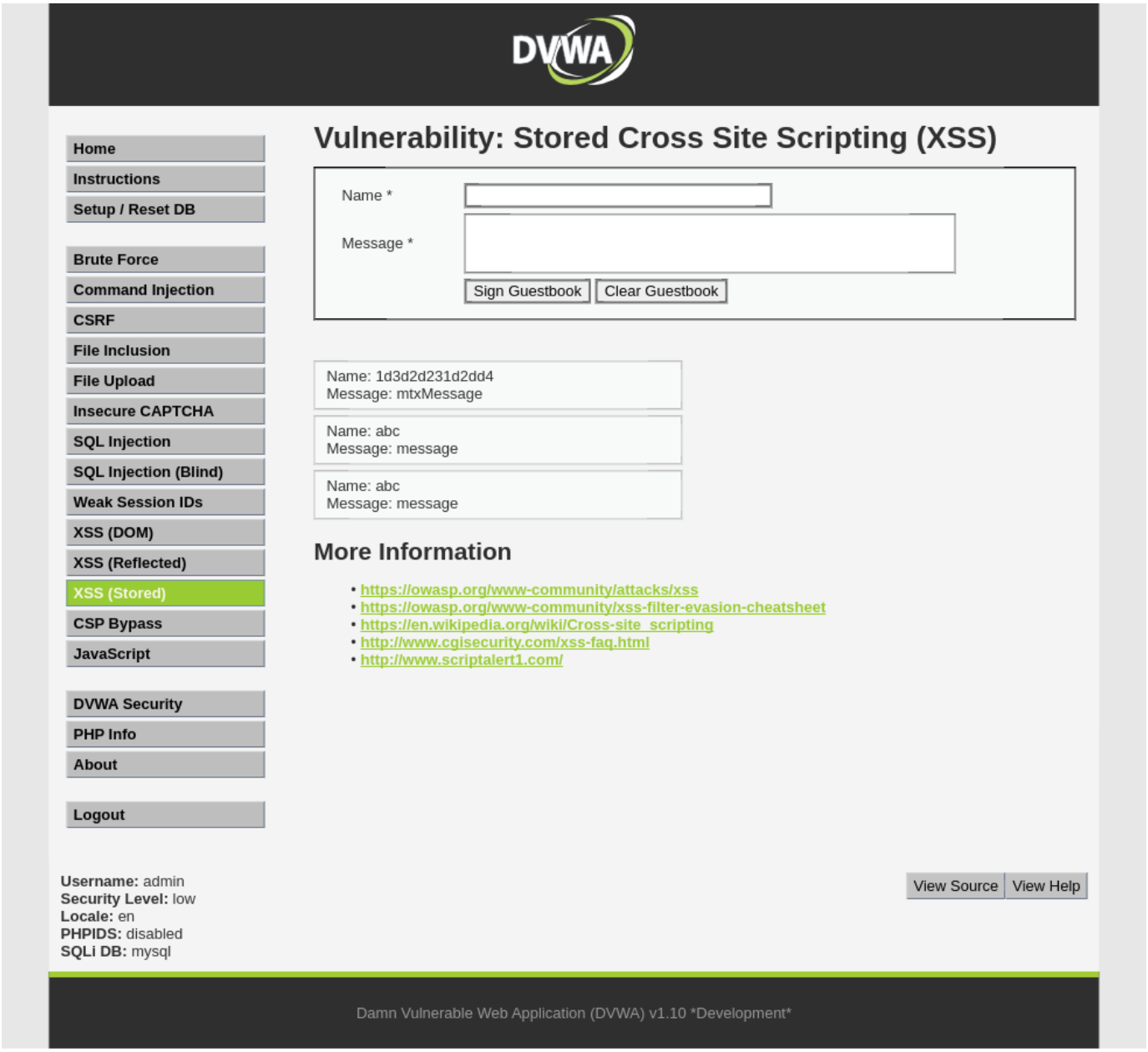
XSS Exploiter Report

Label	JS Payload	Options	Requests received
sample-report	https://app.pentest-tools.com/xss-payload/AIMvGHTNO4/	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
PHPSESSID=sd09h5nep6880ghokclffnbku6; security=low	`http://dvwa.pentest-ground.com/vulnerabilities/xss_s/`	Image 1	username@test.compassword123	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36	Tue March 28, 2023 05:57:29 pm (GMT +3)

Image 1


DVWA
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
DVWA Security
PHP Info
About
Logout
Vulnerability: Stored Cross Site Scripting (XSS)
Name *
Message *
Sign Guestbook
Clear Guestbook
Name: 1d3d2d231d2dd4
Message: mtxMessage
Name: abc
Message: message
Name: abc
Message: 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: admin
Security Level: low
Locale: en
PHPIDS: disabled
SQLi DB: mysql
View Source
View Help
Damn Vulnerable Web Application (DVWA) v1.10 *Development*