

Damn Vulnerable Web Application (DVWA)

Cross Site Scripting (XSS)

Description:

A server is vulnerable to cross shell scripting which occurs when a malicious hacker is able to introduce undesired commands into legitimate client side code executed by a browser. Types of cross shell scripting are: reflected xss, stored xss and dom based xss.

Solution :

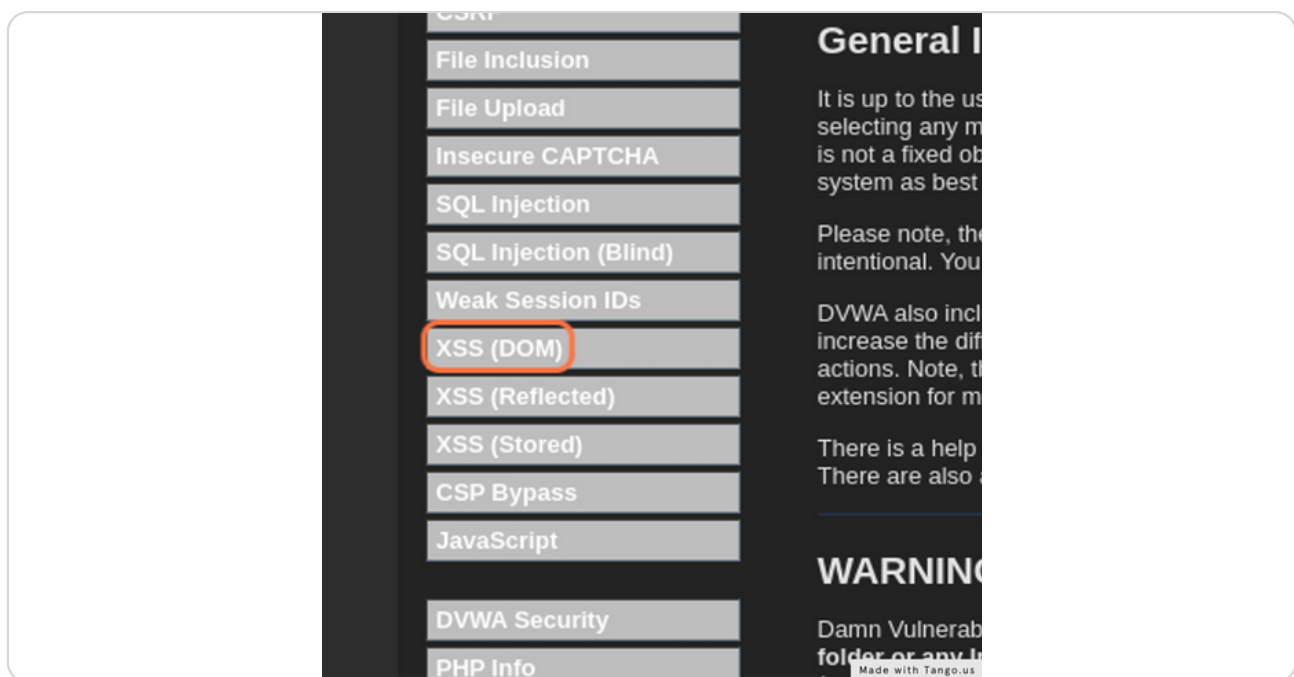
Validation and sanitization of user input
Filtering and escaping

Occurrence

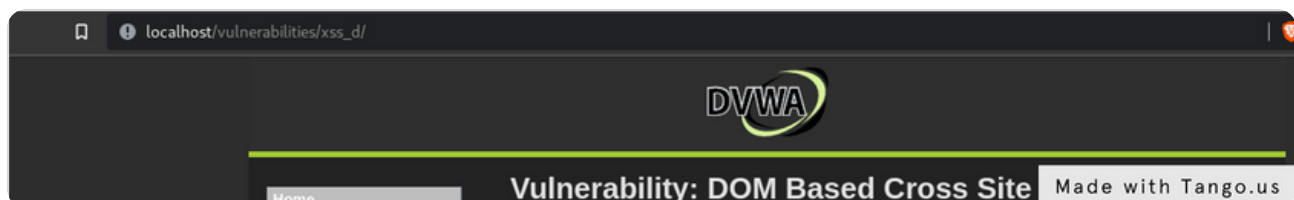
DOM Based XSS

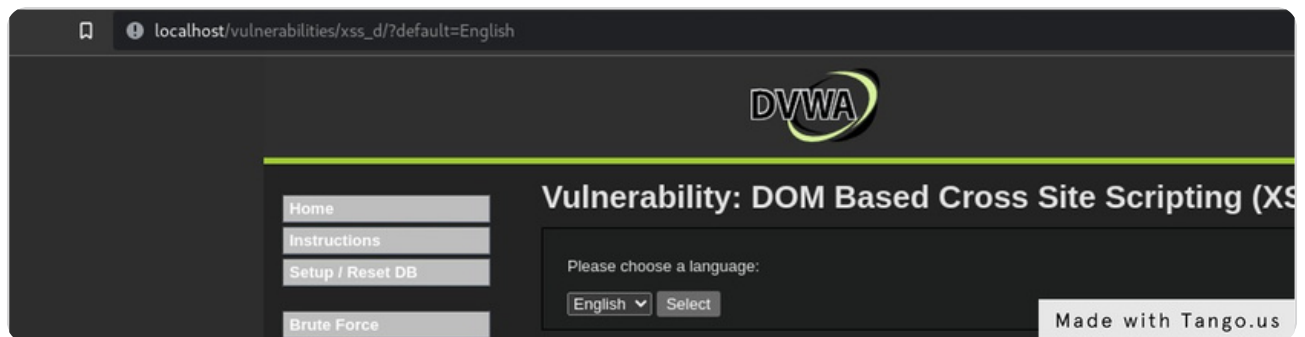
STEP 1

Click on XSS (DOM)

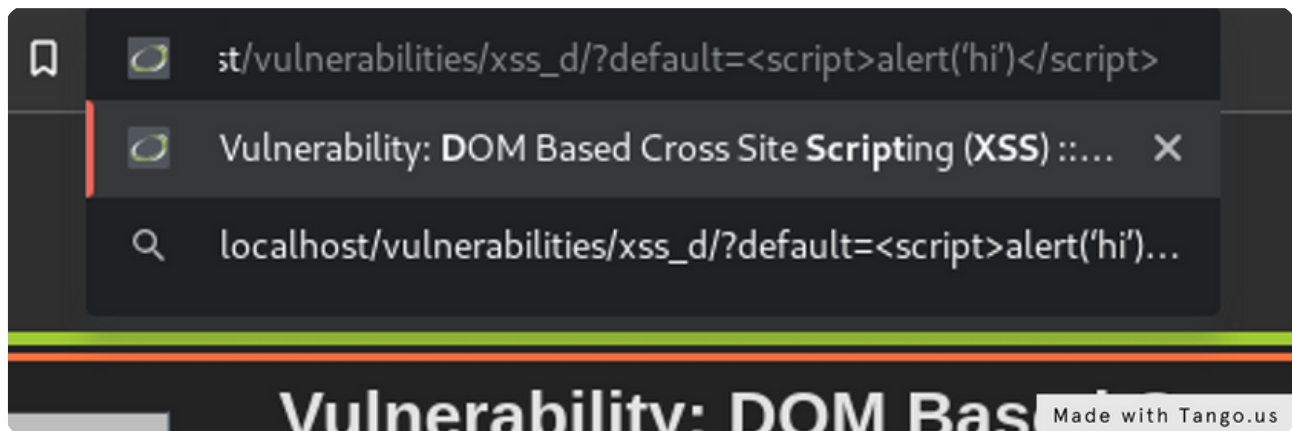


STEP 2



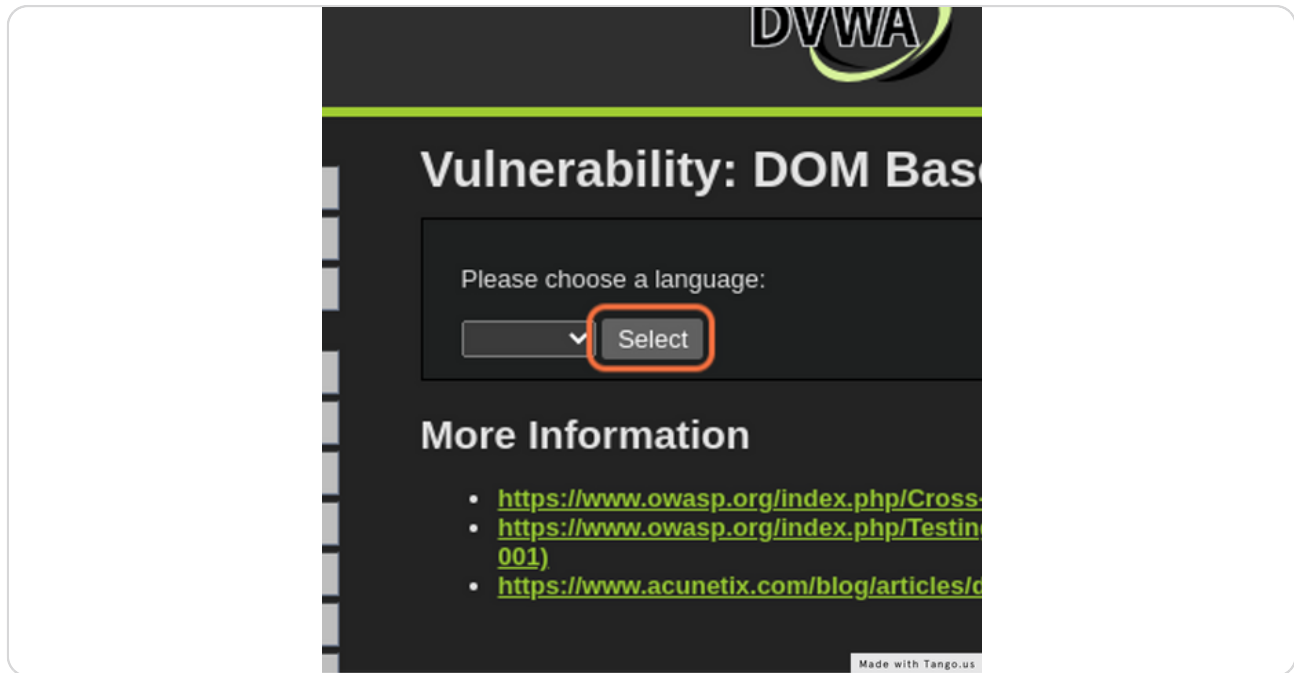


Change url to
localhost/vulnerability/xss_d/?default=<script>alert('xss hacking')</script>

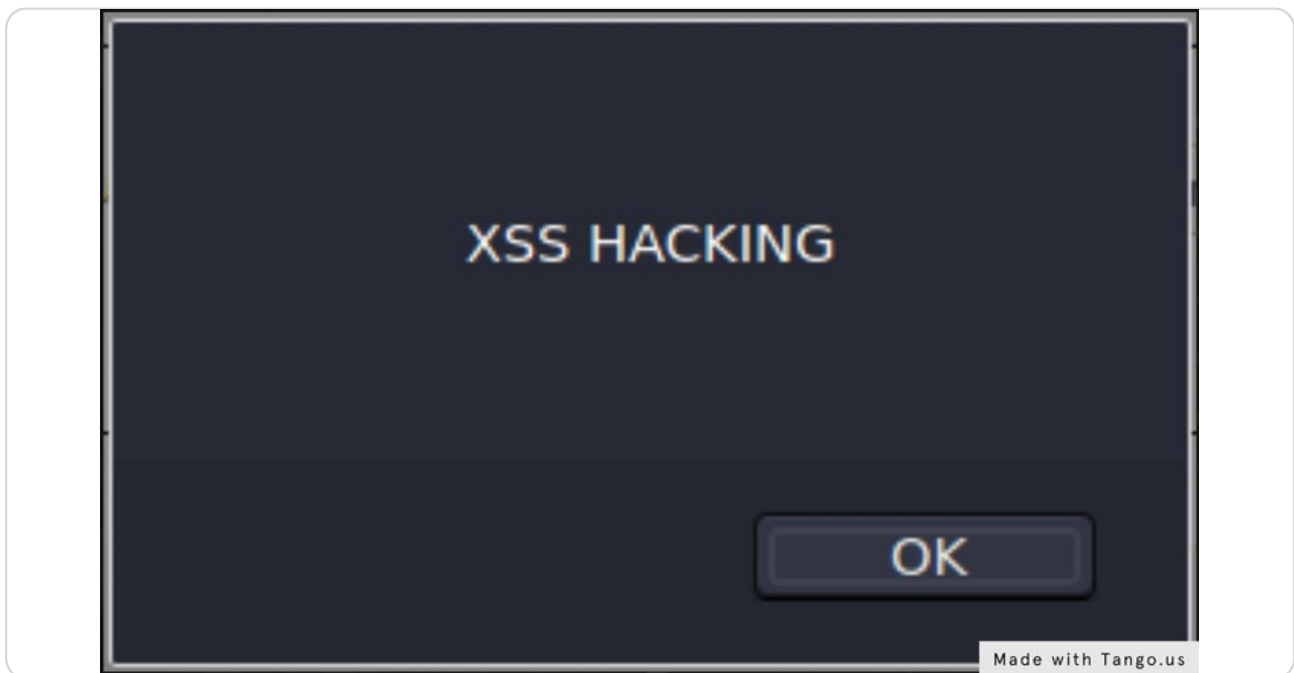


STEP 3

Click on Select



An alert pops up

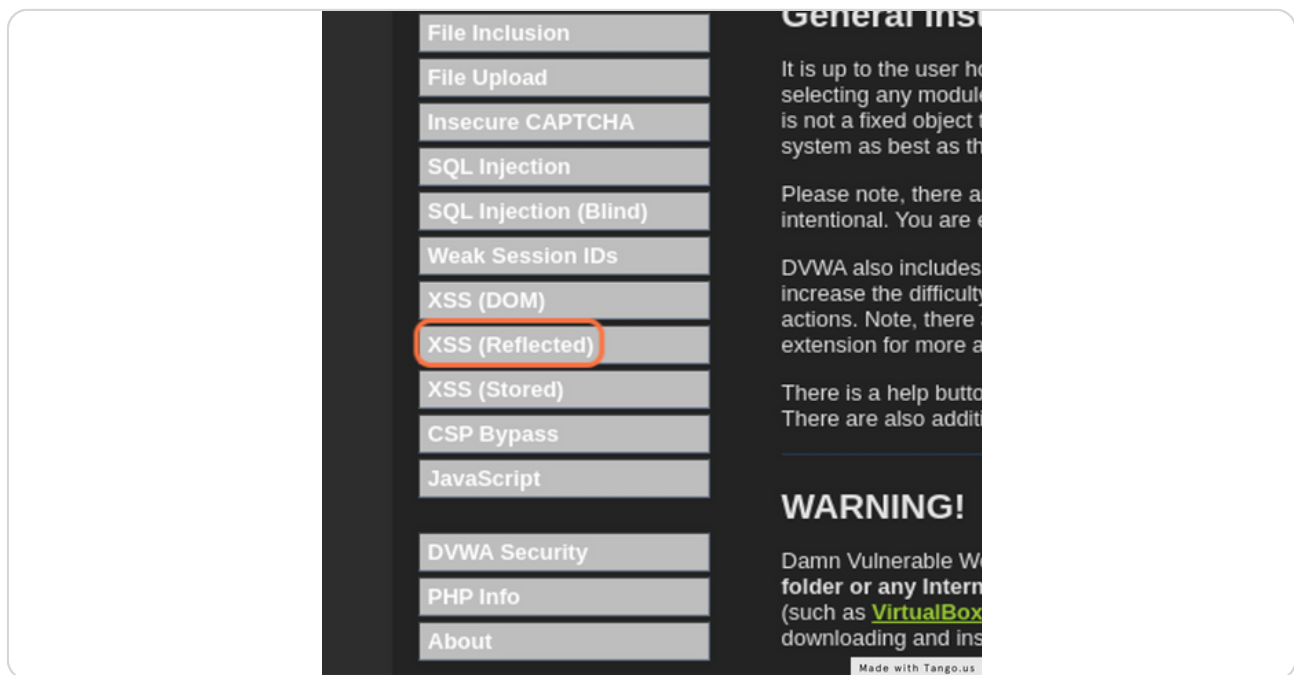


Occurrence

Reflected XSS

STEP 1

Click on XSS (Reflected)



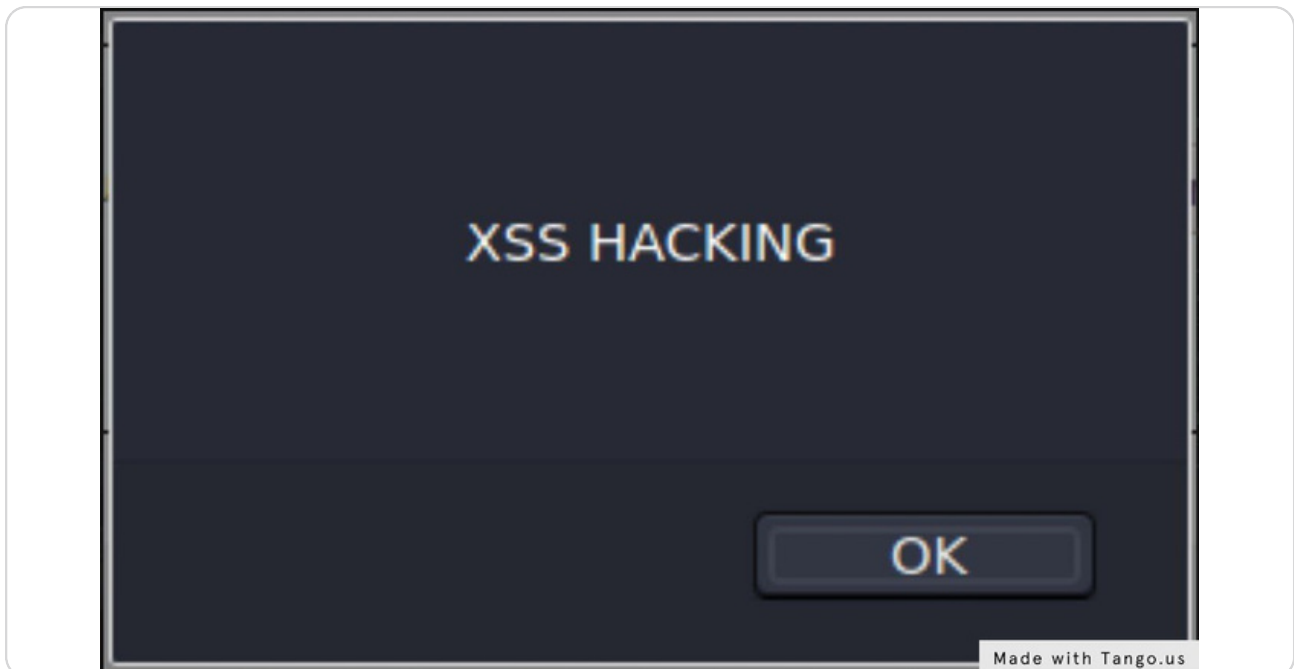
STEP 2

Click on Submit


Payload: `<script>alert('stored hack')</script>`



STEP 3



STEP 4



[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](#)

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

More Information

- [https://www.owasp.org/index.php/Cross-site_Scripting_\(XSS\)](https://www.owasp.org/index.php/Cross-site_Scripting_(XSS))
- https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet
- https://en.wikipedia.org/wiki/Cross-site_scripting
- <http://www.cgisecurity.com/xss-faq.html>
- <http://www.scriptalert1.com/>

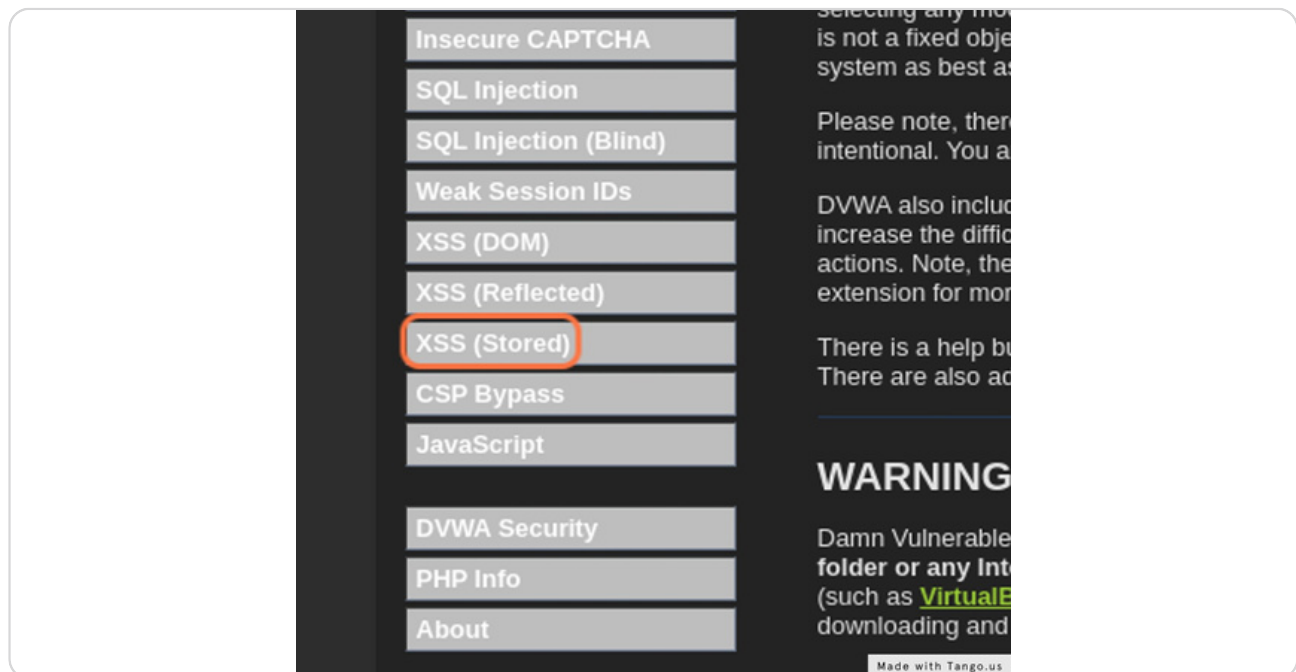
Made with Tango.us

Occurrence

Stored XSS

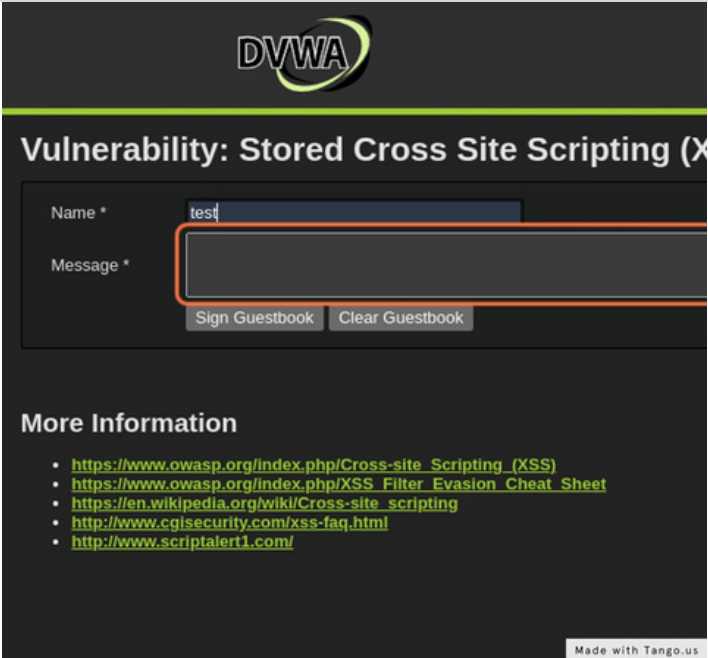
STEP 1

Click on XSS (Stored)



STEP 2

Type "test" for Name



The screenshot shows the DVWA (Damn Vulnerable Web Application) interface for the 'Stored Cross Site Scripting (XSS)' vulnerability. The 'Name' field contains the text 'test'. The 'Message' field is empty. Below the fields are two buttons: 'Sign Guestbook' and 'Clear Guestbook'. Under the 'More Information' section, there are five links to external resources. A small 'Made with Tango.us' watermark is visible in the bottom right corner.

Vulnerability: Stored Cross Site Scripting (XSS)

Name * test

Message *

Sign Guestbook Clear Guestbook

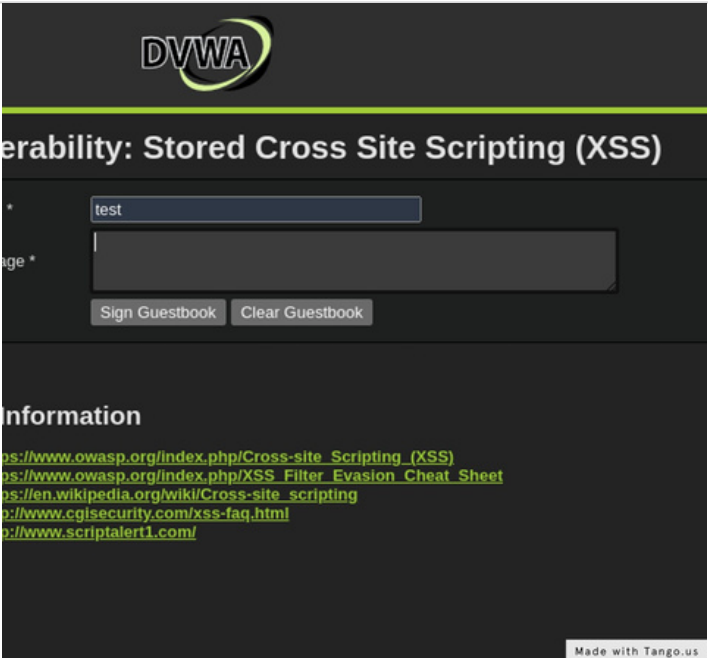
More Information

- [https://www.owasp.org/index.php/Cross-site_Scripting_\(XSS\)](https://www.owasp.org/index.php/Cross-site_Scripting_(XSS))
- https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet
- https://en.wikipedia.org/wiki/Cross-site_scripting
- <http://www.cgisecurity.com/xss-faq.html>
- <http://www.scriptalert1.com/>

Made with Tango.us

STEP 3

Type "<script>alert('XSS HACKING')</script>" into text area



The screenshot shows the DVWA interface for the 'Stored Cross Site Scripting (XSS)' vulnerability. The 'Name' field contains the text 'test'. The 'Message' field contains the payload '<script>alert('XSS HACKING')</script>'. Below the fields are two buttons: 'Sign Guestbook' and 'Clear Guestbook'. Under the 'More Information' section, there are five links to external resources. A small 'Made with Tango.us' watermark is visible in the bottom right corner.

Vulnerability: Stored Cross Site Scripting (XSS)

Name * test

Message * <script>alert('XSS HACKING')</script>

Sign Guestbook Clear Guestbook

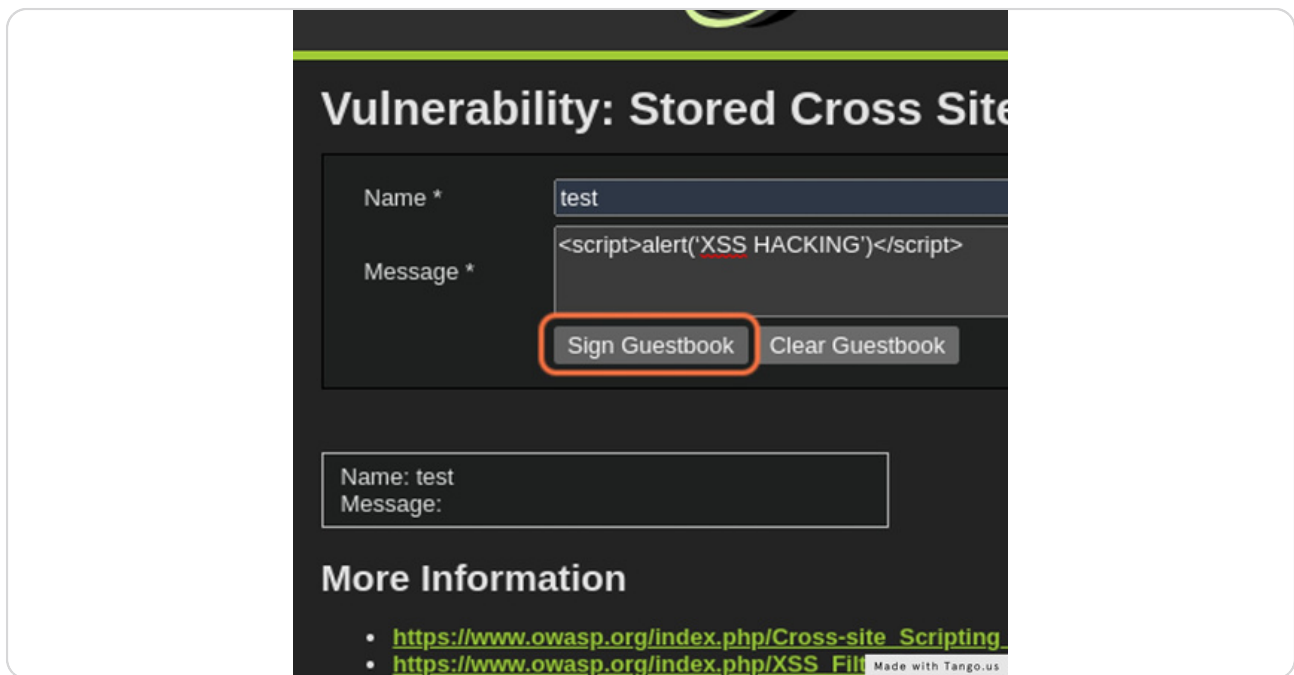
More Information

- [https://www.owasp.org/index.php/Cross-site_Scripting_\(XSS\)](https://www.owasp.org/index.php/Cross-site_Scripting_(XSS))
- https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet
- https://en.wikipedia.org/wiki/Cross-site_scripting
- <http://www.cgisecurity.com/xss-faq.html>
- <http://www.scriptalert1.com/>

Made with Tango.us

STEP 4

Click on Sign Guestbook



Vulnerability: Stored Cross Site

Name *

Message *

Name: test
Message:

More Information

- https://www.owasp.org/index.php/Cross-site_Scripting
- https://www.owasp.org/index.php/XSS_Fill

Made with Tango.us

STEP 5

