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 :

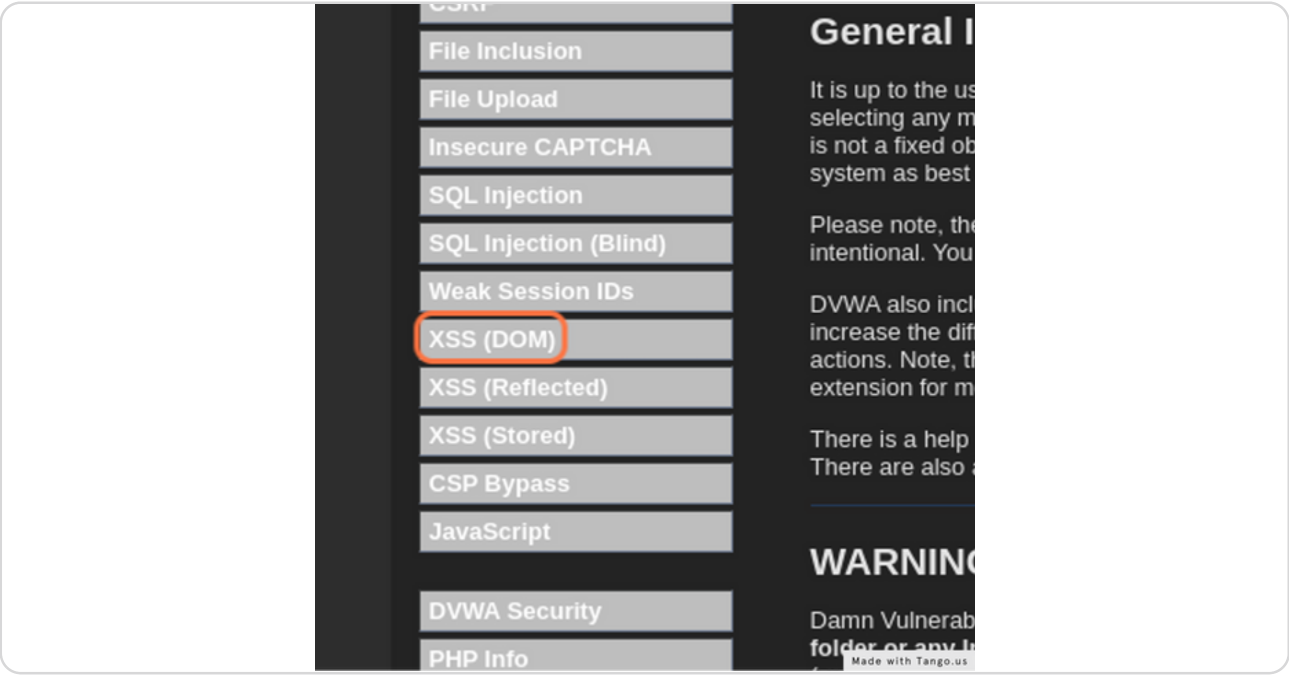
Validation and sanitization of user input
Filtering and escaping

Occurrence

DOM Based XSS

STEP 1

Click on XSS (DOM)



General I

It is up to the us
selecting any m
is not a fixed ob
system as best

Please note, the
intentional. You

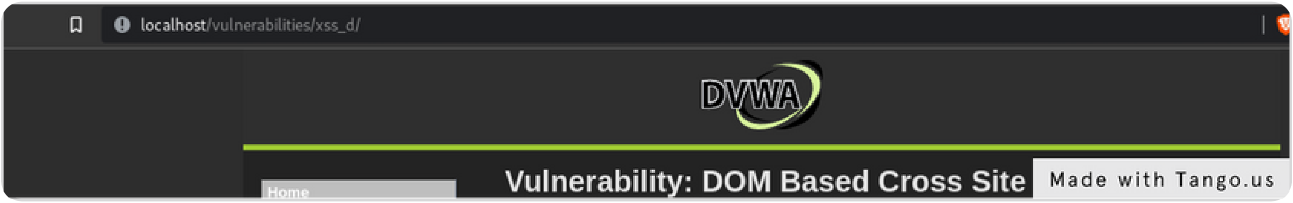
DVWA also incl
increase the dif
actions. Note, t
extension for m

There is a help
There are also

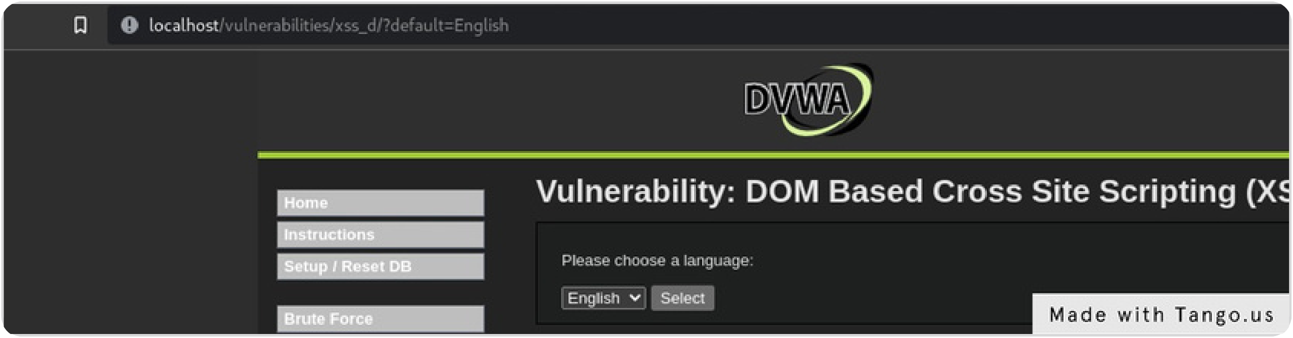
WARNIN

Damn Vulnerab
folder or any I

STEP 2



Vulnerability: DOM Based Cross Site



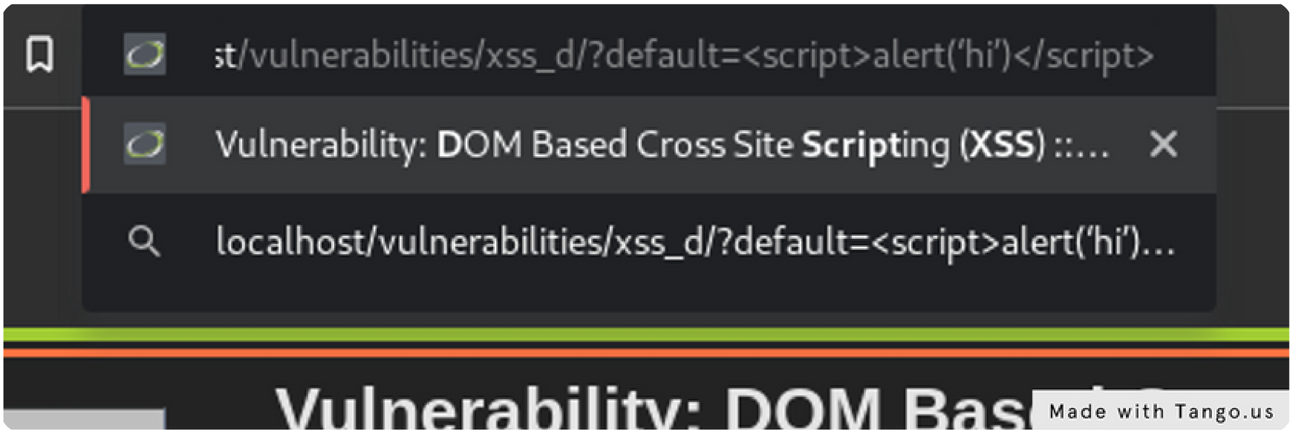
localhost/vulnerabilities/xss_d/?default=English

Vulnerability: DOM Based Cross Site Scripting (XS

Please choose a language:

English Select

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



st/vulnerabilities/xss_d/?default=<script>alert(‘hi’)</script>

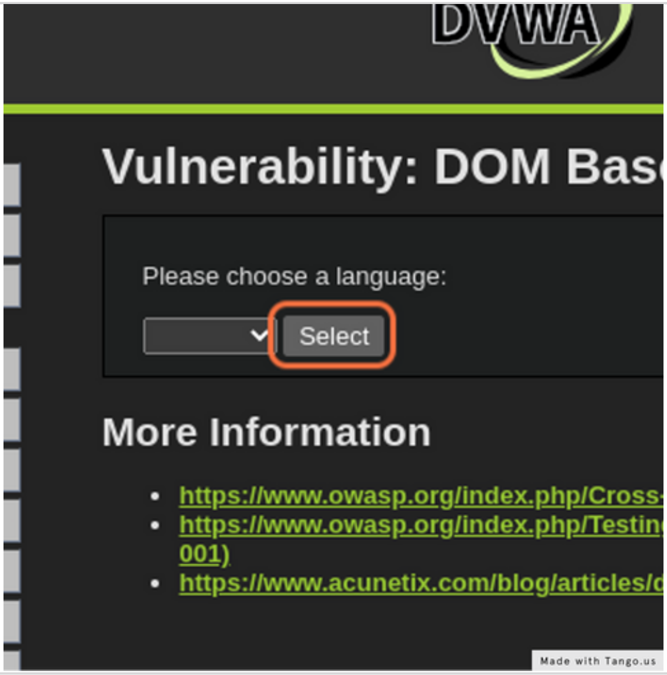
Vulnerability: DOM Based Cross Site Scripting (XSS) ::...

localhost/vulnerabilities/xss_d/?default=<script>alert(‘hi’)...

Vulnerability: DOM Bas

STEP 3

Click on Select



DVWA

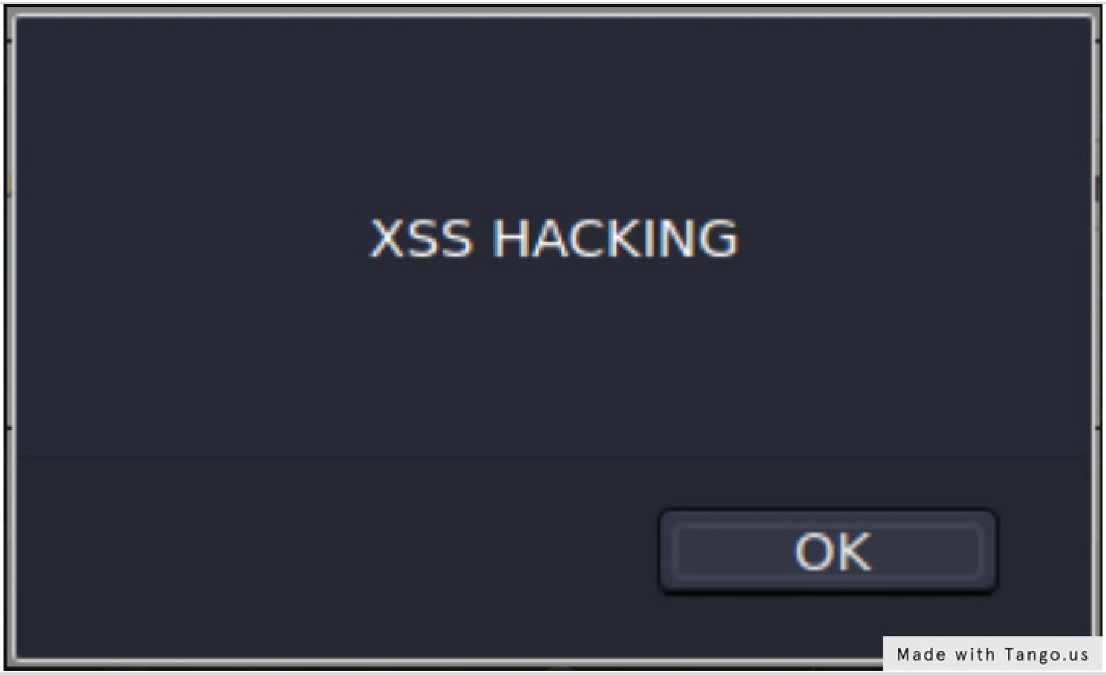
Vulnerability: DOM Bas

Please choose a language:

More Information

- https://www.owasp.org/index.php/Cross-
- https://www.owasp.org/index.php/Testin 001)
- https://www.acunetix.com/blog/articles/c

An alert pops up



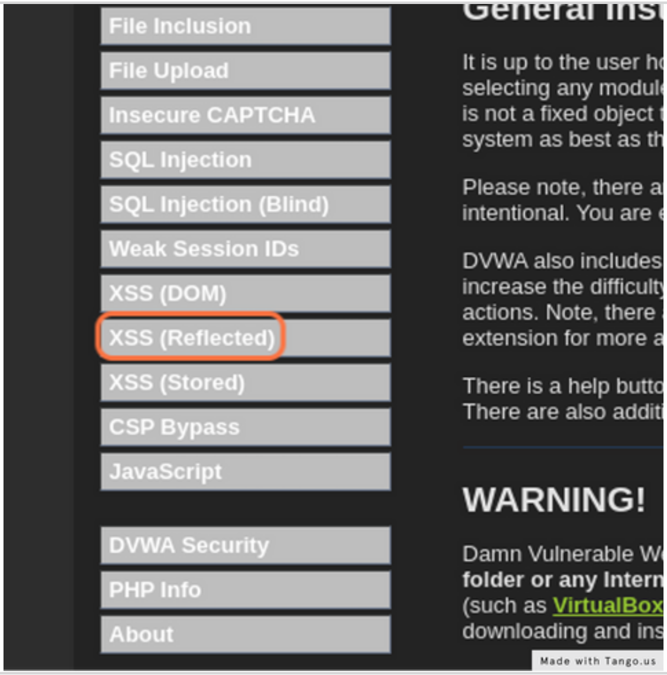
XSS HACKING

Occurrence

Reflected XSS

STEP 1

Click on XSS (Reflected)



General Inst

It is up to the user h
selecting any modul
is not a fixed object
system as best as th

Please note, there a
intentional. You are

DVWA also includes
increase the difficult
actions. Note, there
extension for more a

There is a help butto
There are also additi

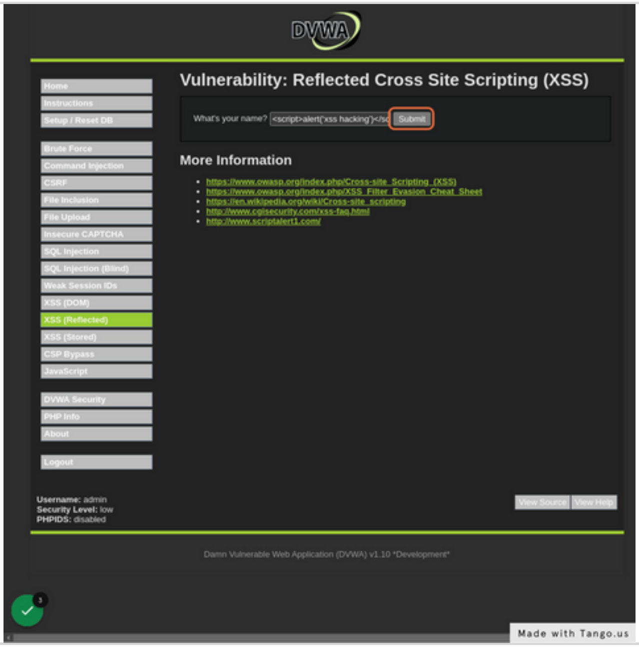
WARNING!

Damn Vulnerable W
folder or any Intern
(such as VirtualBox
downloading and ins

STEP 2

Click on Submit

Payload: <script>alert(‘stored hack’)</script>



Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name? <script>alert('xss hacking')</sc

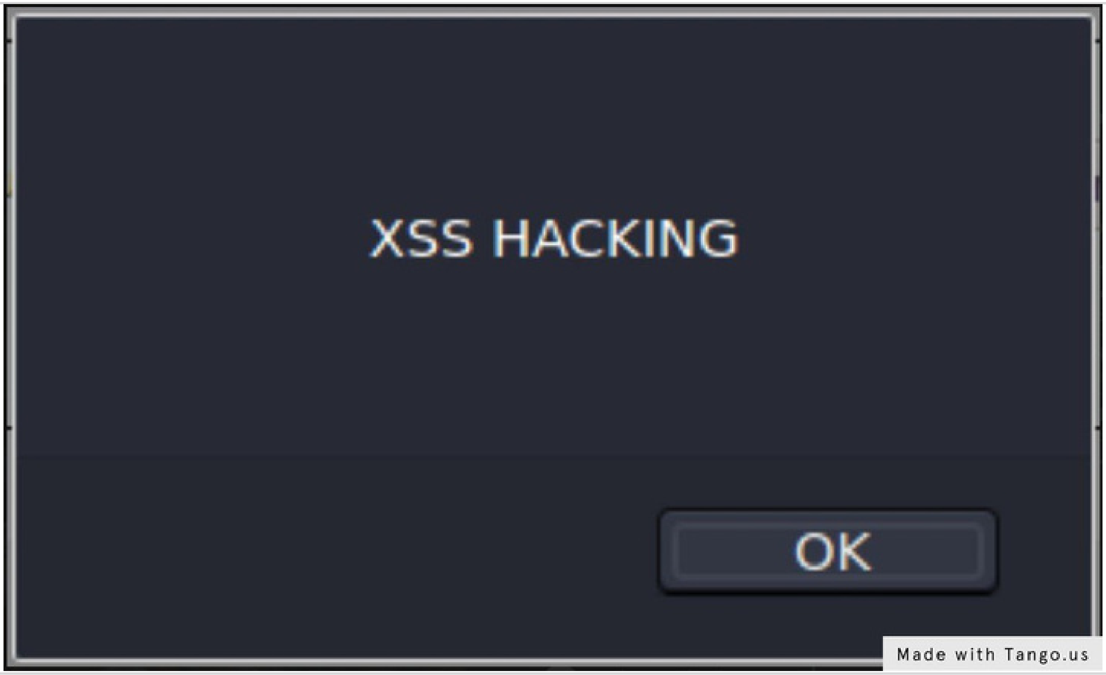
More Information

- 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/

Username: admin
Security Level: low
PHPIDS: disabled

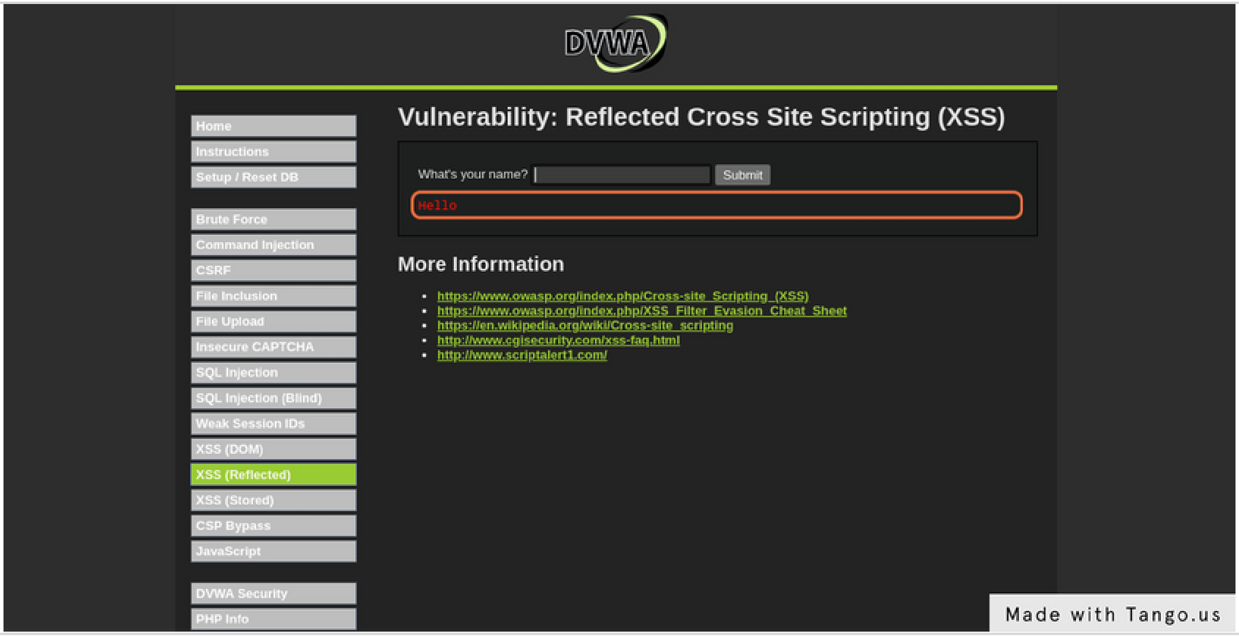
Damn Vulnerable Web Application (DVWA) v1.10 *Development*

STEP 3



XSS HACKING

STEP 4



Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name? Submit

Hello

More Information

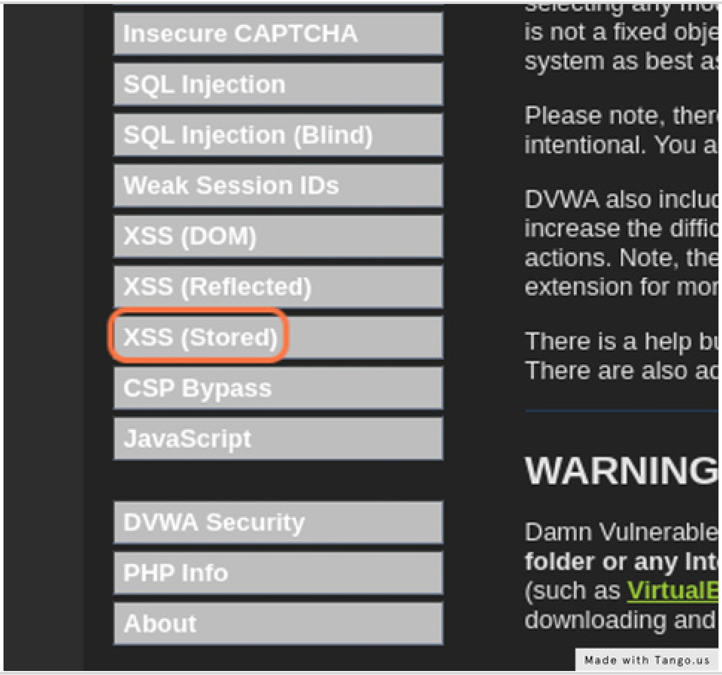
- https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
- https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet
- https://en.wikipedia.org/wiki/Cross-site_scripting
- http://www.cgisecurity.com/xss-faq.html
- http://www.scriptalert1.com/

Occurrence

Stored XSS

STEP 1

Click on XSS (Stored)



selecting any mo
is not a fixed obje
system as best a

Please note, ther
intentional. You a

DVWA also inclu
increase the diffi
actions. Note, the
extension for mor

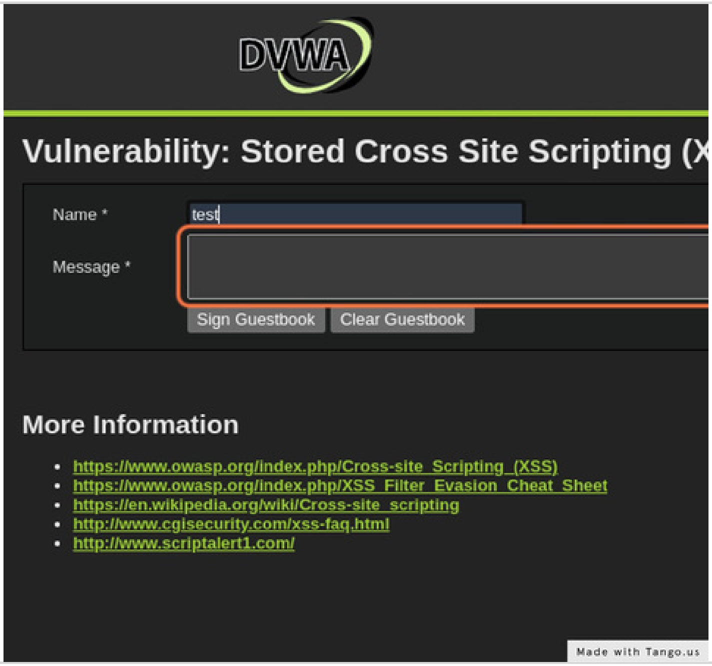
There is a help b
There are also ac

WARNING

Damn Vulnerable
folder or any Int
(such as VirtualB
downloading and

STEP 2

Type "test" for Name



Vulnerability: Stored Cross Site Scripting (X

Name * test

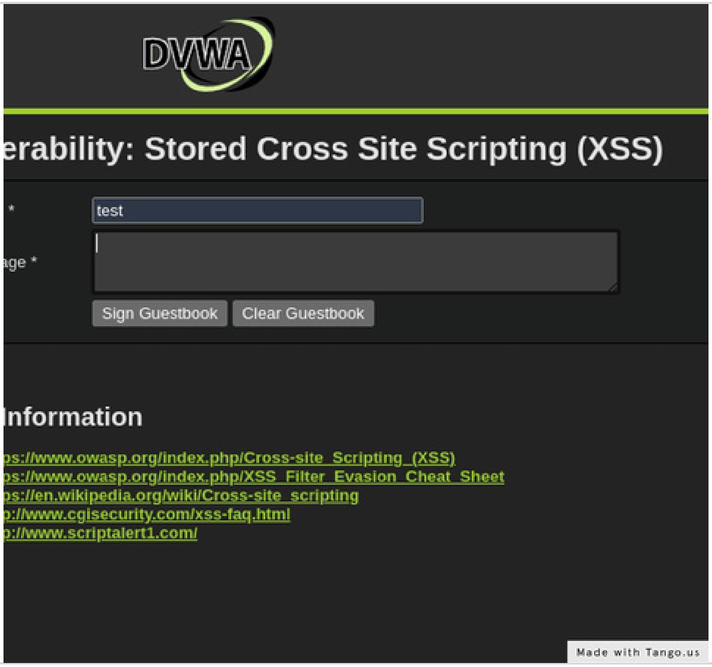
Message *

More Information

- 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/

STEP 3

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



erability: Stored Cross Site Scripting (XSS)

* test

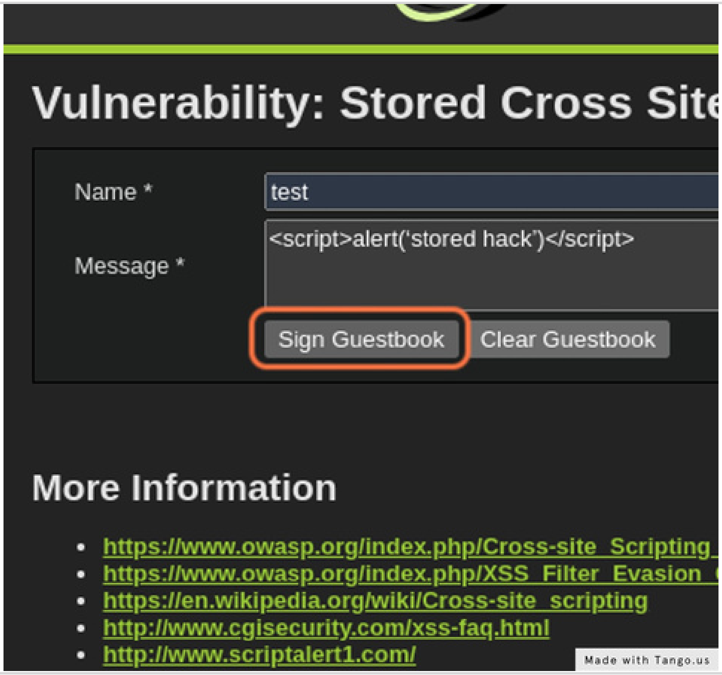
age *

Information

ps://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
ps://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet
ps://en.wikipedia.org/wiki/Cross-site_scripting
p://www.cgisecurity.com/xss-faq.html
p://www.scriptalert1.com/

STEP 4

Click on Sign Guestbook



Vulnerability: Stored Cross Site

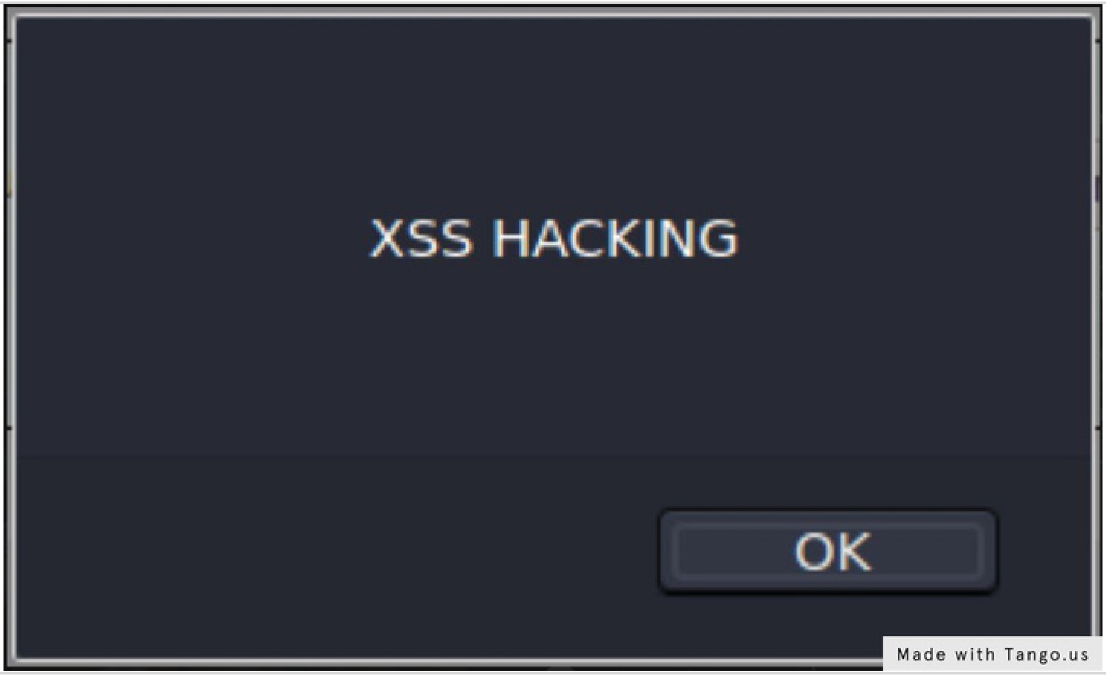
Name * test

Message * <script>alert('stored hack')</script>

More Information

- https://www.owasp.org/index.php/Cross-site_Scripting_
- https://www.owasp.org/index.php/XSS_Filter_Evasion_
- https://en.wikipedia.org/wiki/Cross-site_scripting
- http://www.cgisecurity.com/xss-faq.html
- http://www.scriptalert1.com/

STEP 5



XSS HACKING