DVWA - Stored Cross Site Scripting (XSS) Report

Objective

The objective of this task was to demonstrate Stored Cross Site Scripting (XSS) in DVWA under different security levels (Low and Medium). Stored XSS occurs when a malicious script is permanently stored on the target server and served to users whenever they access the stored data.

Low Security Level

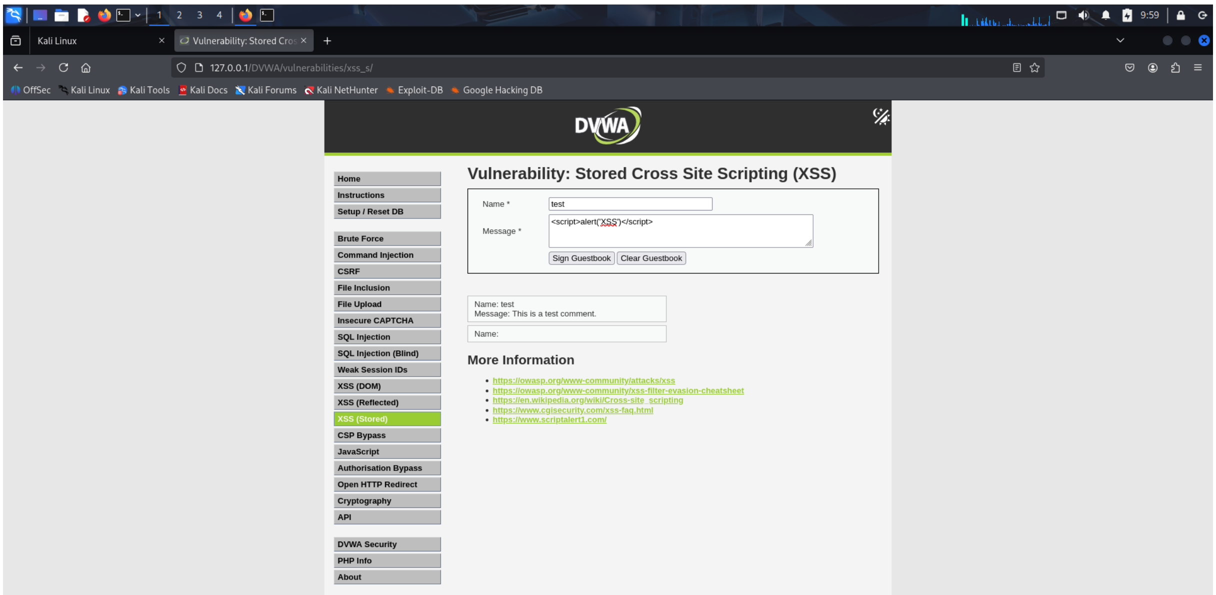
1. Navigate to 'XSS (Stored)' in DVWA.

2. Enter a test payload in the 'Message' field.

3. Payload used:

<script>alert('XSS')</script>

4. After submitting, the alert popup confirms the stored XSS execution.



Vulnerability: Stored Cross Site Scripting (XSS)

Name * test

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

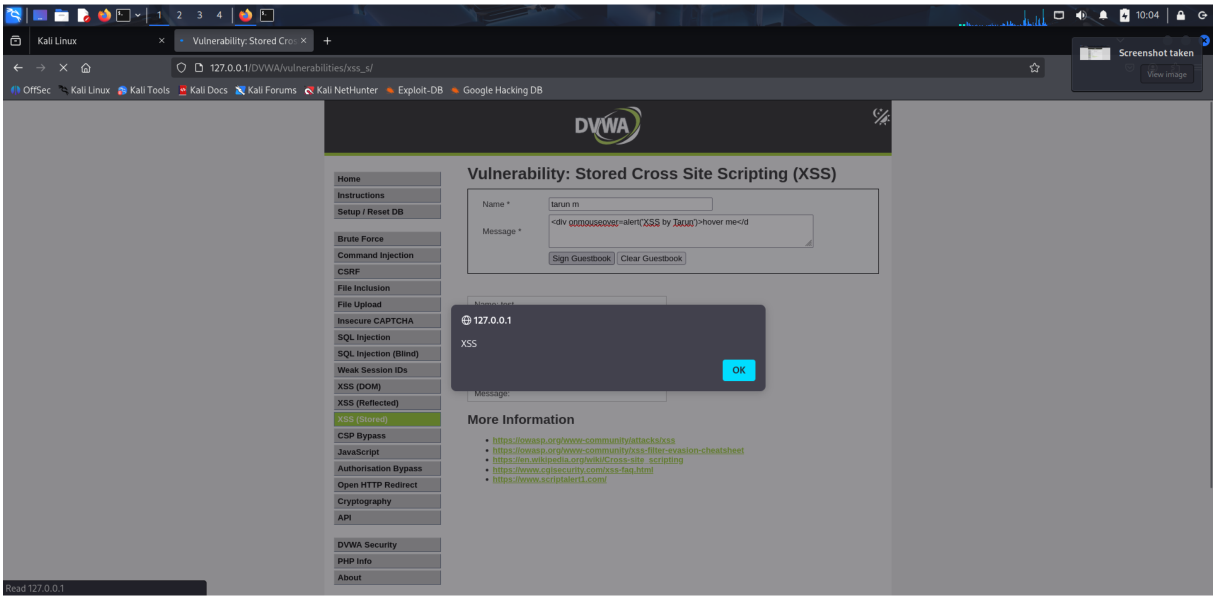
Name: test
Message: This is a test comment.

Name:

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
- https://www.cgisecurity.com/xss-faq.html
- https://www.scriptalert1.com/

Screenshot: Entering the XSS payload in Low Security mode.



Vulnerability: Stored Cross Site Scripting (XSS)

Name * tarun m

Message * <div onmouseover=alert('XSS by Tarun')>hover me</d

127.0.0.1

XSS

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
- https://www.cgisecurity.com/xss-faq.html
- https://www.scriptalert1.com/

DVWA - Stored Cross Site Scripting (XSS) Report

Screenshot: Alert popup triggered in Low Security mode.

Medium Security Level

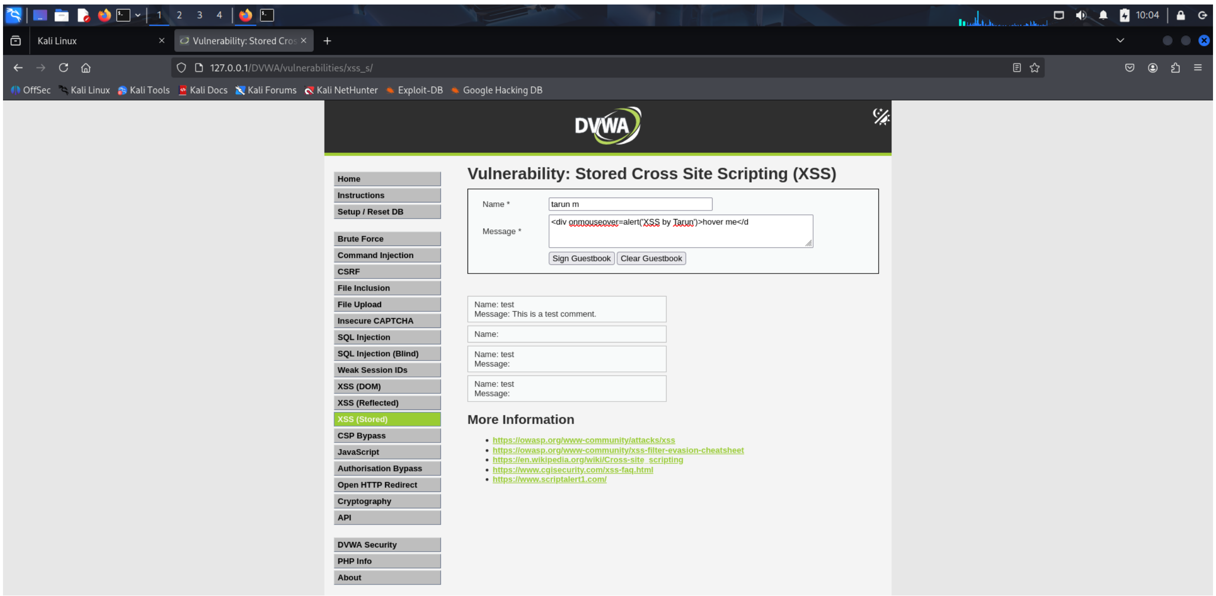
1. Navigate to 'XSS (Stored)' in DVWA with security set to Medium.

2. The application may apply basic filtering; therefore, a different payload was used.

3. Payload used:

<div onmouseover=alert('XSS by Tarun')>hover me</div>

4. The payload triggers when the user hovers over the text.



127.0.0.1/DVWA/vulnerabilities/xss_s/

Vulnerability: Stored Cross Site Scripting (XSS)

Name * tarun m

Message * <div onmouseover=alert('XSS by Tarun')>hover me</d

Name: test
Message: This is a test comment.

Name:

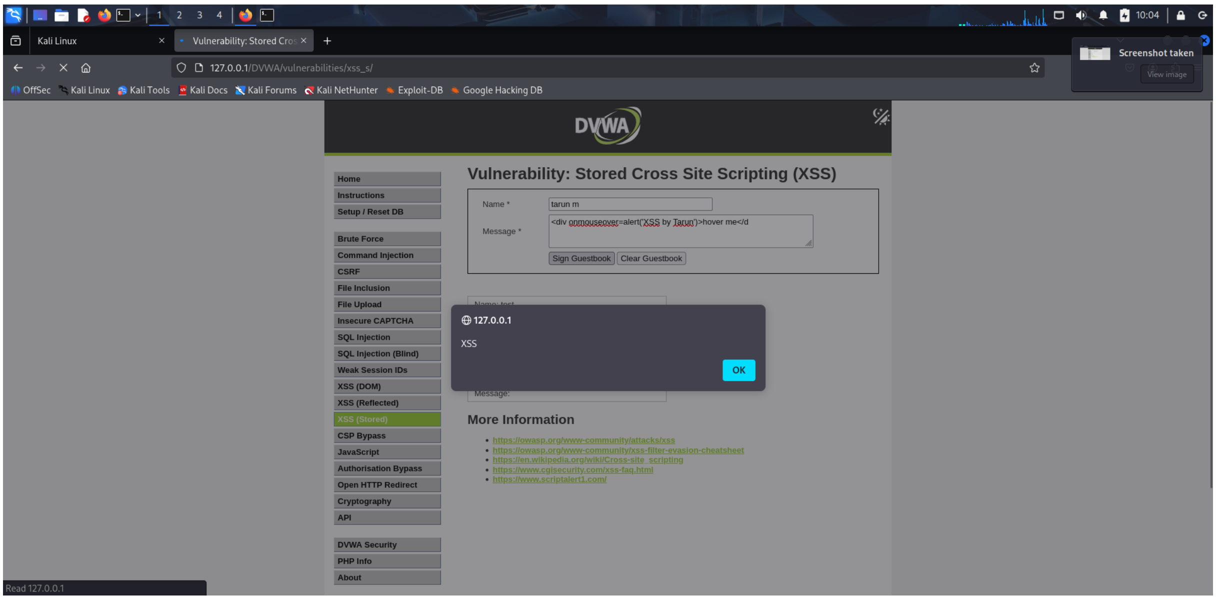
Name: test
Message:

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
- https://www.cgisecurity.com/xss-faq.html
- https://www.scriptalert1.com/

Screenshot: Entering the mouseover XSS payload in Medium Security mode.



127.0.0.1/DVWA/vulnerabilities/xss_s/

Vulnerability: Stored Cross Site Scripting (XSS)

Name * tarun m

Message * <div onmouseover=alert('XSS by Tarun')>hover me</d

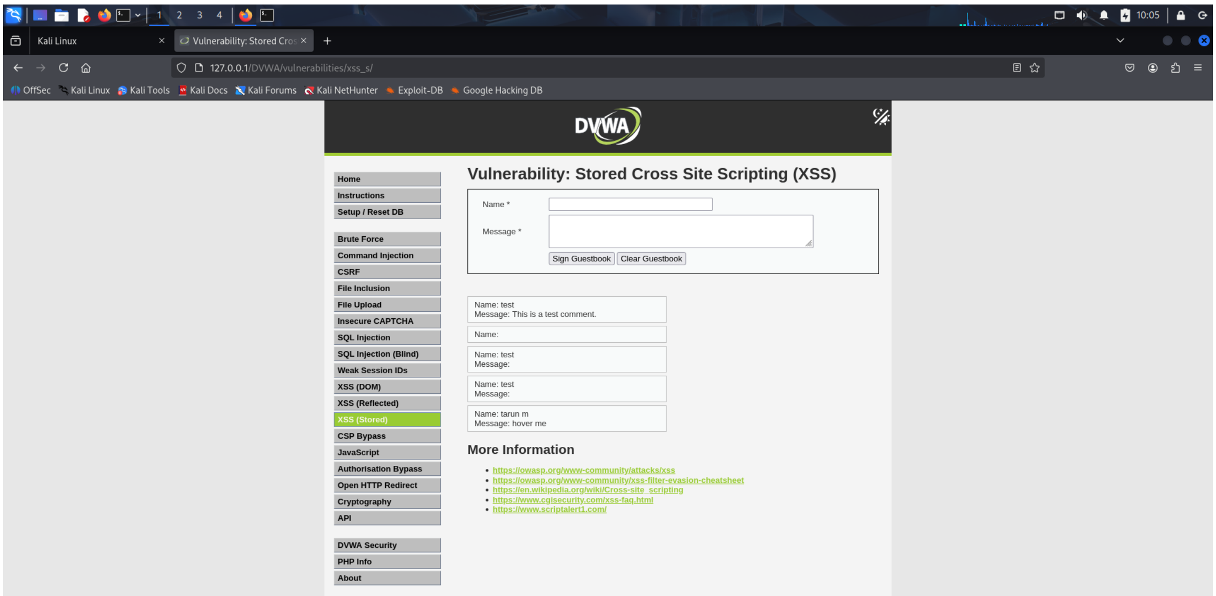
127.0.0.1

XSS

OK

Screenshot: Hovering over text triggers the XSS popup.

DVWA - Stored Cross Site Scripting (XSS) Report



Vulnerability: Stored Cross Site Scripting (XSS)

Name *

Message *

Name: test
Message: This is a test comment.

Name:

Name: test
Message:

Name: test
Message:

Name: tarun m
Message: hover me

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
- https://www.cgisecurity.com/xss-faq.html
- https://www.scriptalert1.com/

Screenshot: Stored payload visible on the page in Medium Security mode.