

VULNERABILITA' XSS e SQL

Con l'esercizio di oggi abbiamo tentato di prendere il controllo della macchina :
metasploit 192.168.50.101

Dopo esserci assicurati che le due macchine parlassero tra di loro, abbiamo configurato la sicurezza DVWA a low ed abbiamo iniziato ad eseguire quanto segue.

Dal menu ci siamo spostati sulla pagina **XSS reflected** ed abbiamo modificato il codice in maniera temporanea.

Questi gli elenchi di codici eseguiti con le loro immagini al seguito:

<i> Massimiliano in corsivo

** Massimiliano in grassetto**

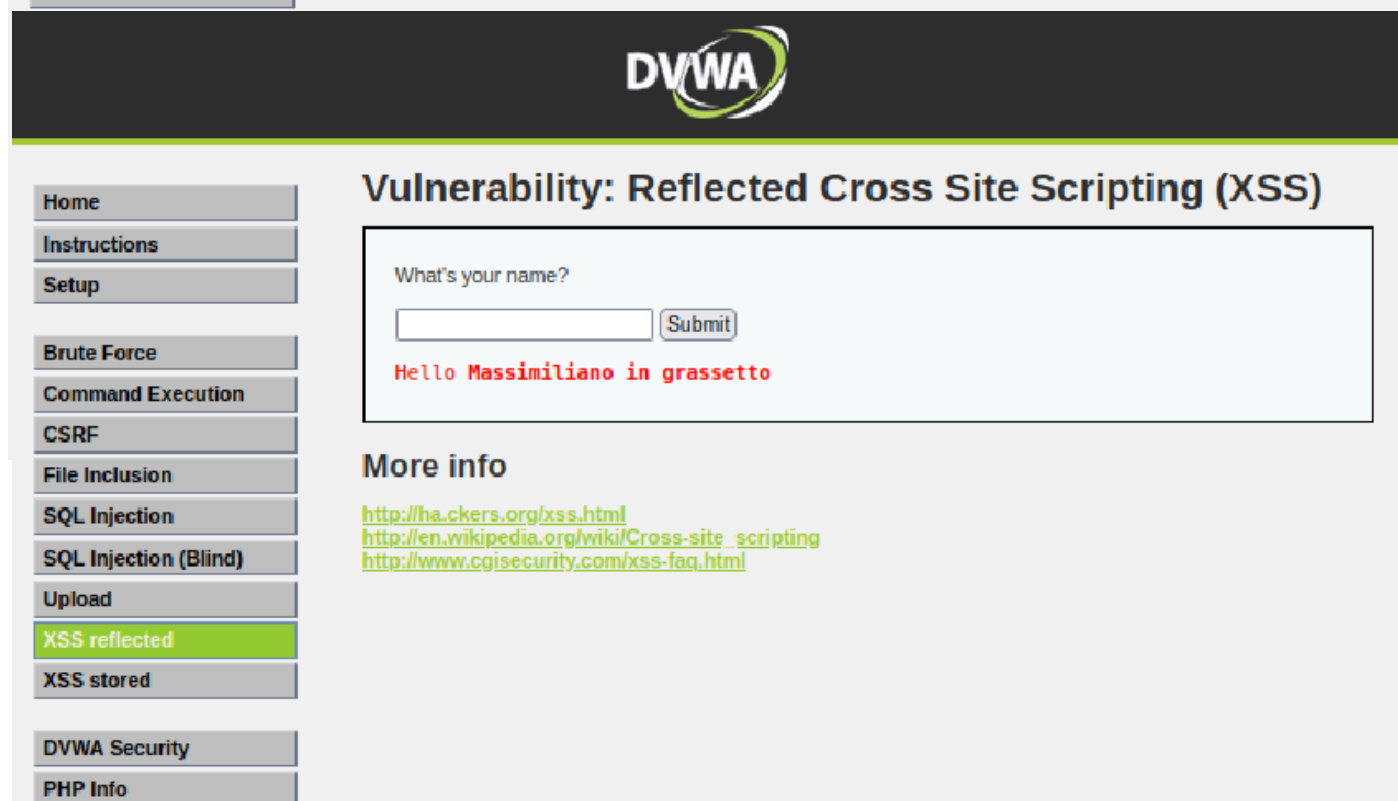
<div> Massimiliano a capo come elemento blocco

<blockquote> la citazione di Massimiliano (potete notare una tabulazione differente del testo)

<h1> MASSIMILIANO HA UN TITOLO



The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. The top header is dark grey with the DVWA logo. On the left is a navigation menu with buttons for Home, Instructions, Setup, Brute Force, Command Execution, CSRF, and File Inclusion. The main content area is titled 'Vulnerability: Reflected Cross Site Scripting (XSS)'. It contains a form with the label 'What's your name?' and a 'Submit' button. Below the form, the output is displayed in red text: 'Hello Massimiliano in corsivo'. A 'More info' link is visible below the output.



This screenshot is similar to the one above, showing the DVWA XSS page. However, the navigation menu on the left is more extensive, including buttons for SQL Injection, SQL Injection (Blind), Upload, XSS reflected (which is highlighted in green), XSS stored, DVWA Security, and PHP Info. The main content area shows the same 'Vulnerability: Reflected Cross Site Scripting (XSS)' form. The output below the form is 'Hello Massimiliano in grassetto' in red text. Below the output, there are three links: <http://hackers.org/xss.html>, http://en.wikipedia.org/wiki/Cross-site_scripting, and <http://www.cgisecurity.com/xss-faq.html>.

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

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

Submit

Hello
Massimiliano a capo

More info

<http://ha.ckers.org/xss.html>
http://en.wikipedia.org/wiki/Cross-site_scripting
<http://www.cgisecurity.com/xss-faq.html>

- 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
la citazione di Massimiliano

More info

<http://ha.ckers.org/xss.html>
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: Reflected Cross Site Scripting (XSS)

What's your name?

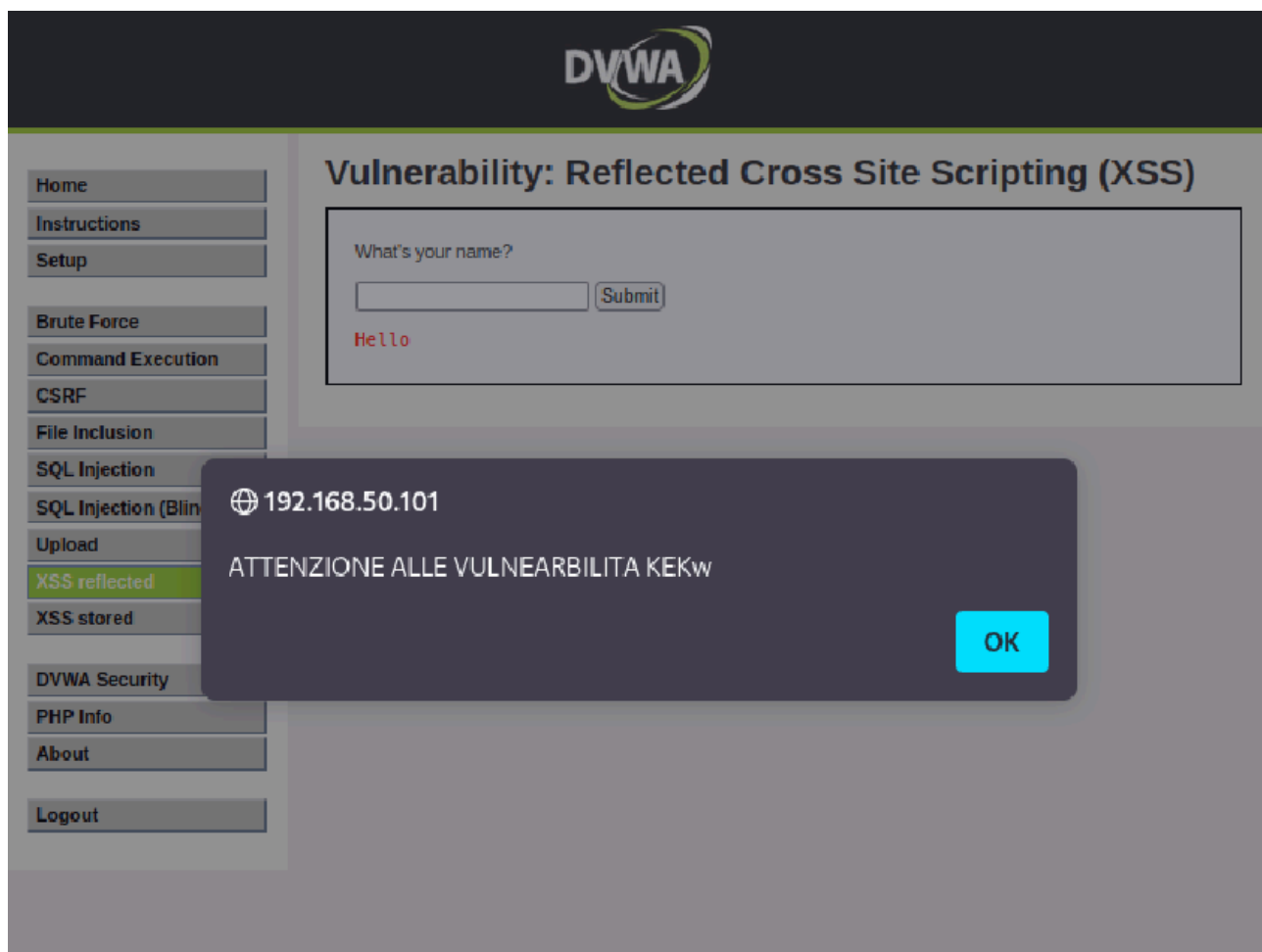
Submit

Hello
Massimiliano ha un titolo

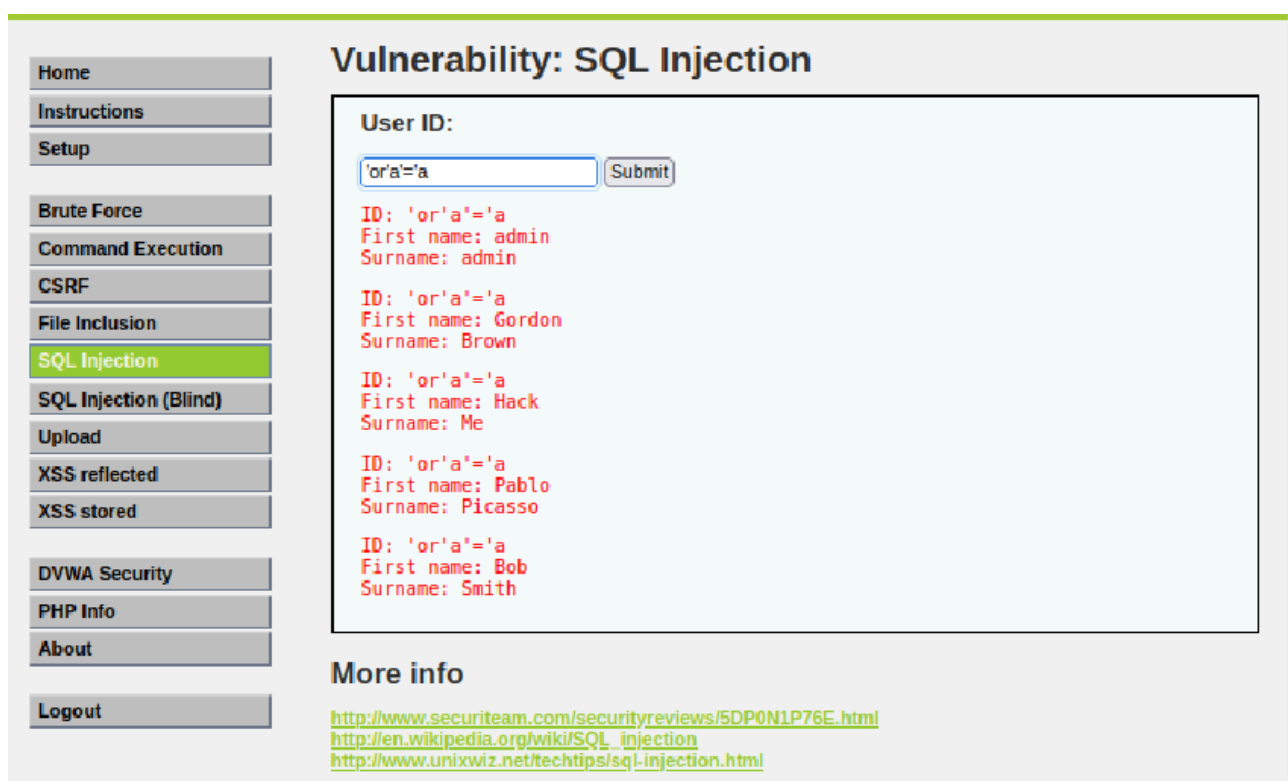
More info

<http://ha.ckers.org/xss.html>
http://en.wikipedia.org/wiki/Cross-site_scripting
<http://www.cgisecurity.com/xss-faq.html>

In seguito abbiamo attivato un alert come da figura qui sotto



Dopodiché abbiamo sfruttato la vulnerabilità **SQL Injection**, prima elencando il database degli ID presenti sulla macchina metasploit, inserendo il seguente comando 'or' a'='a



ed in seguito andando a svuotare i campi, con il comando ' UNION SELECT null, null ', dove i comandi null rappresentano l'input di svuotamento campi. Si noti che ad ogni null corrispondono degli attributi, quindi se la nostra tabella è composta da un attributo first name ed da un attributo Surname, per poter avere un empty result per entrambi dobbiamo inserire in fase di input due "null".

Vulnerability: SQL Injection

User ID:

Submit

```
ID: ' ' UNION SELECT user () ; ' UNION SELECT null, null ' ;  
First name:  
Surname:
```

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>

http://en.wikipedia.org/wiki/SQL_injection

<http://www.unixwiz.net/techtips/sql-injection.html>