# Tutorial SQL Injection DVWA – MEDIUM

Analizzando il codice php relativo alle operazioni che la DVWA livello medium compie per eseguire la query sql, notiamo come la stringa in ingresso venga sanificata mediante la funzione *mysql\_real\_escape\_string()*. Questa funzione, da documentazione, aggiunge un carattere **‘\’** davanti ai caratteri **\x00, \n, \r, \, ', "**e**\x1a**.

Immagine che contiene testo, schermata, Carattere

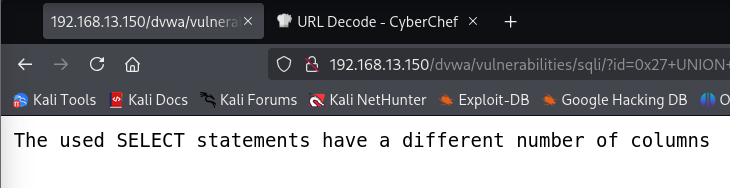
Il contenuto generato dall'IA potrebbe non essere corretto.Per bypassare la sanificazione dell’input sostituiamo i parametri inseriti come input, e quindi racchiusi tra apici, con il loro controvalore in esadecimale utilizzando la funzione in python riportata di seguito o un qualsiasi tool online come CyberChef.

Nostro obiettivo è restituire a schermo dati contenuti nel database. Utilizziamo l’operatore UNION utilizzato per combinare il risultato della prima query, quella inserita nel sorgente della pagina, con una seconda inserita da noi nel campo input.

[query\_1] UNION [query\_2]

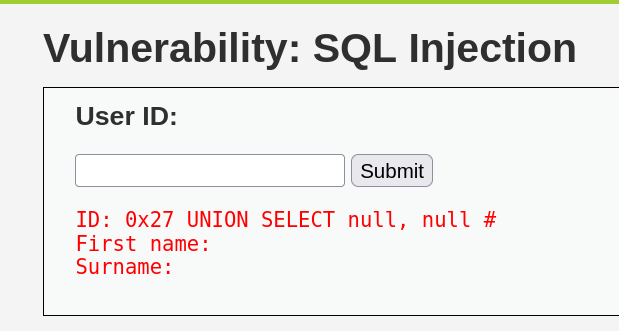
Come requisito fondamentale, le query unite dall’operatore UNION devono restituire lo stesso numero di colonne. Il numero di colonne, e quindi del numero di parametri da inserire dopo l’operatore SELECT, si trova per tentativi, partendo dall’inserire un solo parametro ed aumentandone il numero di volta in volta finché la pagina non restituirà più errore.

**Tentativo con un parametro:**

0x27 UNION SELECT null #

**Tentativo con due parametri:**

0x27 UNION SELECT null, null #

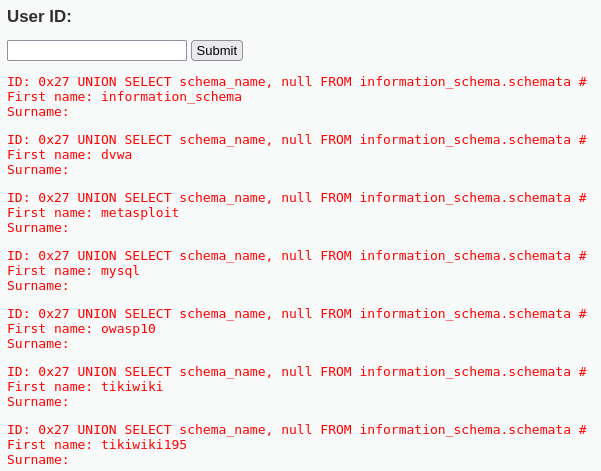


La query nel codice sorgente della pagina restituisce due colonne.

Per visualizzare informazioni vitali dai database presenti abbiamo bisogno di conoscere i nomi dei database presenti. Per portare a termine questo obiettivo utilizziamo le informazioni contenute nella tabella [schemata nel database information-schema](https://dev.mysql.com/doc/refman/8.4/en/information-schema-schemata-table.html).

Query 1:

0x27 UNION SELECT schema\_name, null FROM information\_schema.schemata #



Tra la lista dei nomi elencati notiamo la presenza del database mysql. Andiamo a vedere che tabelle contiene tramite la query:

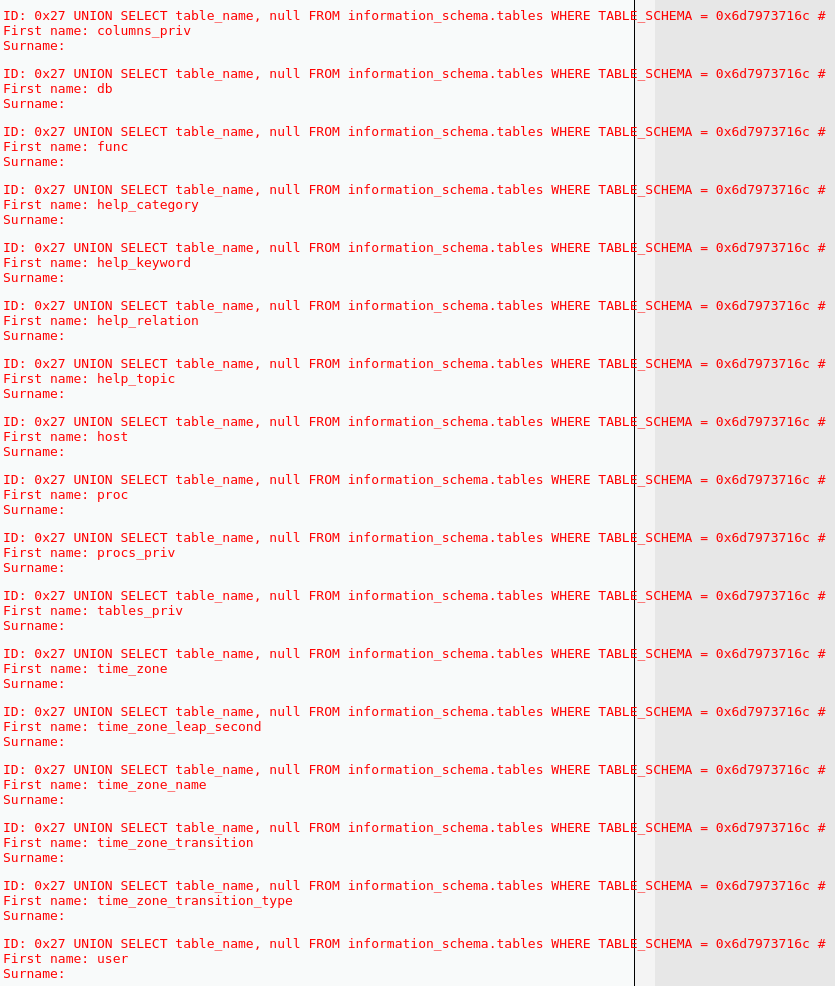
Query 2:

0x27

UNION

SELECT table\_name, table\_schema

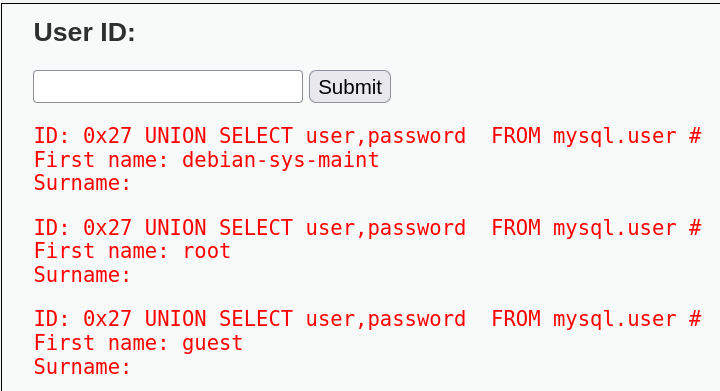
FROM information\_schema.tables

WHERE table\_schema = 0x6d7973716c #

La tabella user nel database mysql potrebbe contenere dati importanti sugli utenti e sui loro privilegi. Andiamo a stampare gli utenti e le relative password contenuti nella tabella user:

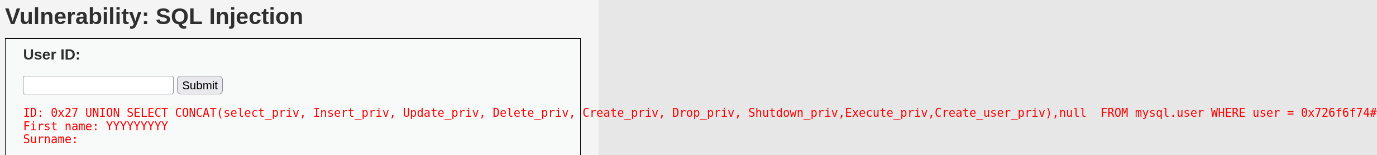
Query 3:

0x27 UNION SELECT user, password FROM mysql.user #



Dell’utente root visualizziamo alcuni dei suoi privilegi e nello specifico:

* Select\_priv
* Insert\_priv
* Update\_priv
* Delete\_priv
* Create\_priv
* Drop\_priv
* Shutdown\_priv
* Execute\_priv
* Create\_user\_priv

Query 4:

L’utente root ha tutti i privilegi precedentemente elencati.

## Conclusioni

Mediante l’utilizzo dell’SQL Injection siamo andati sempre più a fondo all’interno dei database presenti nella DVWA andando a scoprire che l’account dell’utente root, che ha tutti i privilegi, non è protetto da alcuna password.

Da shell è possibile connettersi al database mediante il seguente comando:

MySQL -h <IP\_META> -u root -p --skip-ssl

E operare su sul database.

