Web Application Exploit SQLi

Stefano Di Prospero (NetRaiders)

Traccia Giorno 1:

Utilizzando le tecniche viste nelle lezione teoriche, sfruttare la vulnerabilità SQL injection presente sulla Web Application DVWA per recuperare in chiaro la password dell'utente Gordon Brown (ricordatevi che una volta trovate le password, c'è bisogno di un ulteriore step per recuperare la password in chiaro). NB: non usare tool automatici come sqlmap. È ammesso l'uso di repeater burp suite.

Requisiti laboratorio Giorno 1:

Livello difficoltà DVWA: LOW

IP Kali Linux: 192.168.66.110/24

IP Metasploitable: 192.168.66.120/24

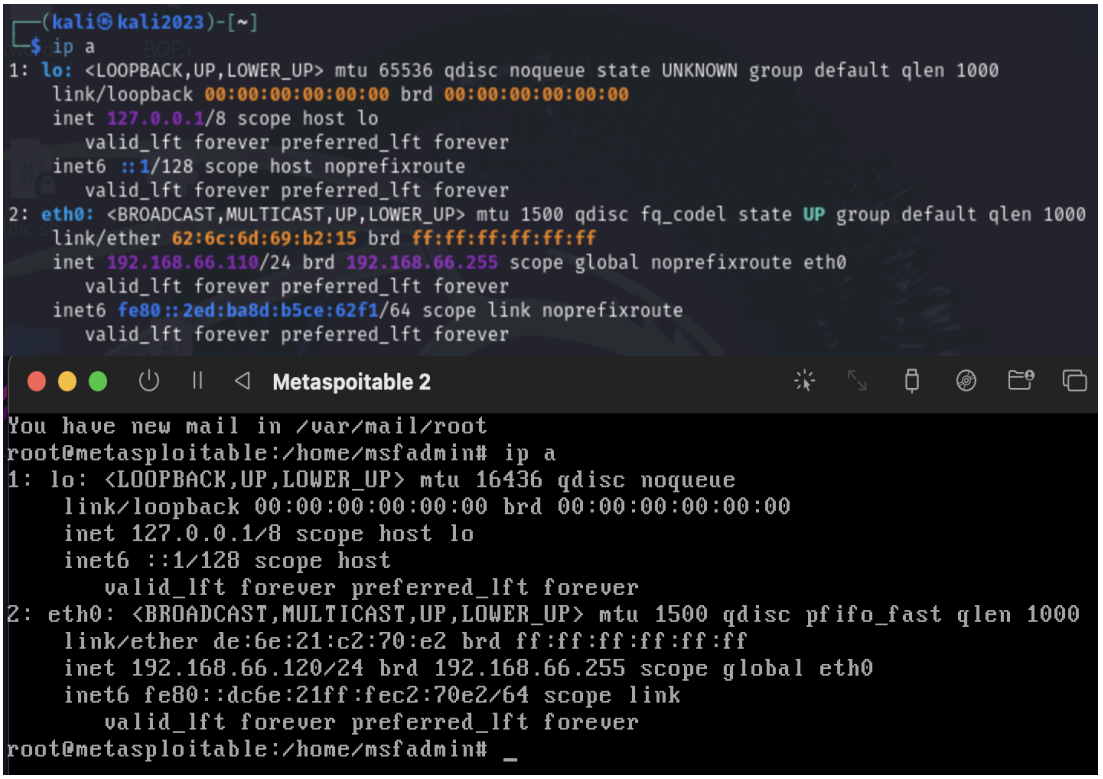
Bonus:

-Replicare tutto a livello medium.

-Verificare se è possibile inserire un utente tramite SQL injection.

-Recuperare informazioni vitali da altri db collegati.

-Creare una guida illustrata per spiegare ad un utente medio come replicare questo attacco (usare termini accattivanti in stile punk).



IP KALI

IP META

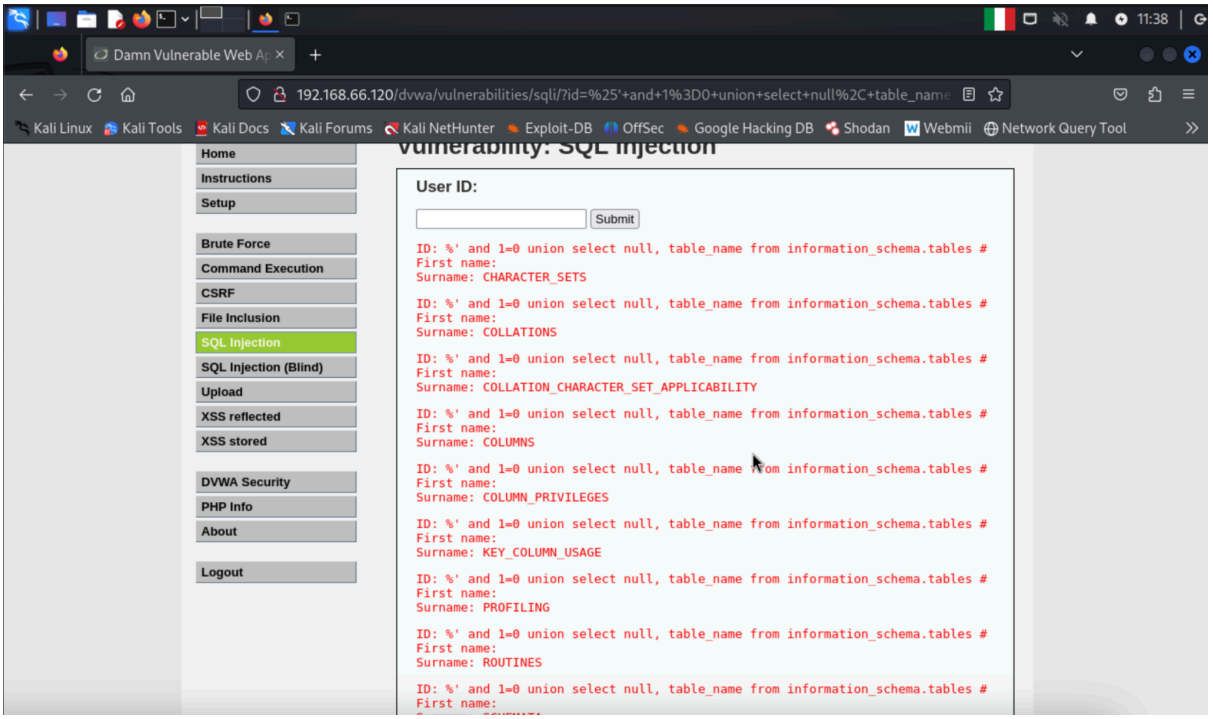
Risoluzione della traccia:

Per prima cosa ci connettiamo, tramite il browser firefox presente sulla macchina KALI, all'indirizzo IP di metasploitable, ovvero 192.168.66.120.

Dopo aver effettuato l'accesso tramite 'admin' e 'password', andremo ad impostare la sicurezza su "LOW" nella sezione DVWA Security.

Ora possiamo iniziare la SQL injection.

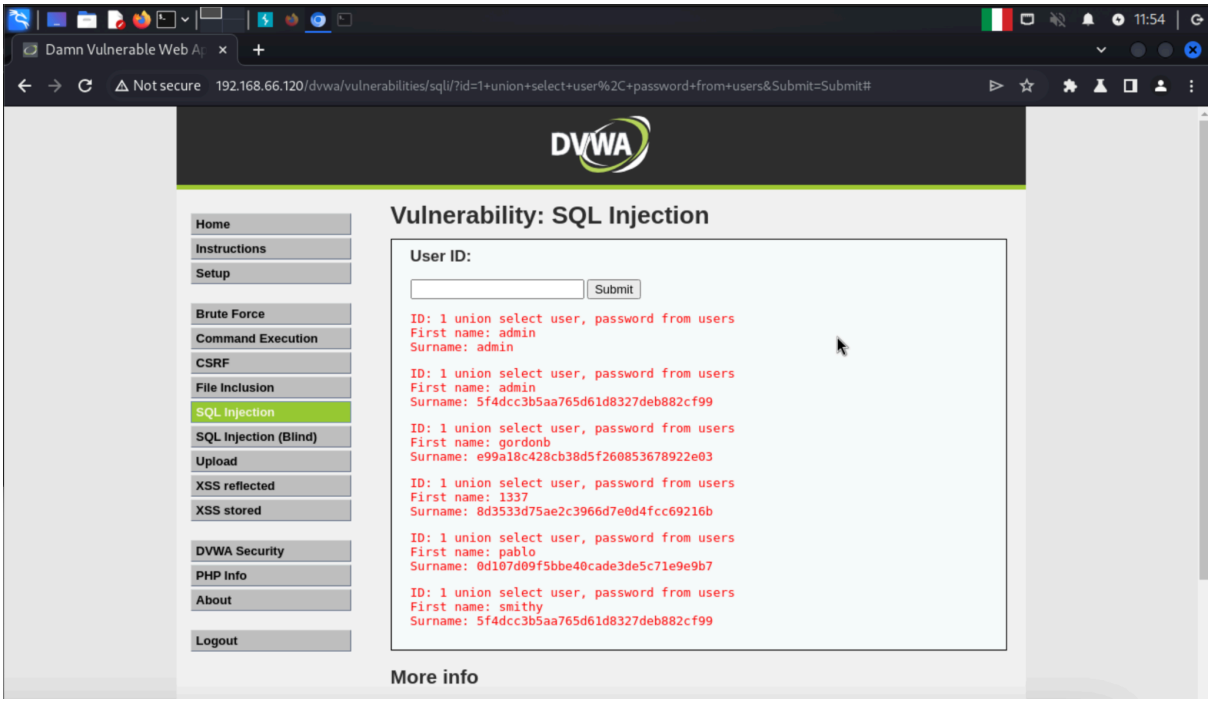
Per far si che ciò che scriveremo sia efficace andremo ad utilizzare vari modi di scrittura in modo da indurre il database a fornire dati utili.



Per prima cosa andiamo a cercare le tabelle presenti e per farlo tramite la funzione *UNION SELECT* è possibile far restituire i nomi utilizzati. In questo modo possiamo aver presenti varie tabelle e le loro informazioni.

" %' and 1=0 union select null, table_name from information_schema.tables # "

Ne abbiamo trovata una che riguarda gli user e con un altro comando di *UNION SELECT* andiamo a farci restituire le informazioni presenti dentro il *DataBase* e possibilmente anche una possibile password associata.



“ 1 union select user, password from users ”

Come richiesto dalla traccia prendiamo come nostro obiettivo ‘ *gordonb* ‘

Come possiamo notare c’è anche una serie di caratteri. Questi rappresentano l’*hash* della password che a breve andremo a *decifrare*. Questo perché quando una viene inserita una password essa viene poi *cifrata* in modo da rendere difficile la visualizzazione da parte di un malintenzionato.

Per trovare la password copieremo in un file di testo l’hash della password che utilizzeremo poi con un tool di decriptazione chiamato ***John the Ripper***.
Quest’ultimo funziona tramite quelle che sono delle liste che contengono password conosciute e le andremo ad incrociare con il file di testo creato in precedenza.

```
┌──(kali㉿kali2023)-[~]
└─$ john -format=raw-md5 -wordlist=/usr/share/wordlists/rockyou.txt /home/kali/Desktop/pswg
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 ASIMD 4x2])
No password hashes left to crack (see FAQ)
```

Questa rappresenta l'utilizzo del tool a cui abbiamo dato una lista chiamata '*rockyou.txt*' contenente le varie password e '*pswg*' che è il file da noi creato contenente l'hash dell'utente *'gordonb'*

```
┌──(kali㉿kali2023)-[~]
└─$ john --show --format=raw-md5 /home/kali/Desktop/pswg
Gordonb:abc123

1 password hash cracked, 0 left
```

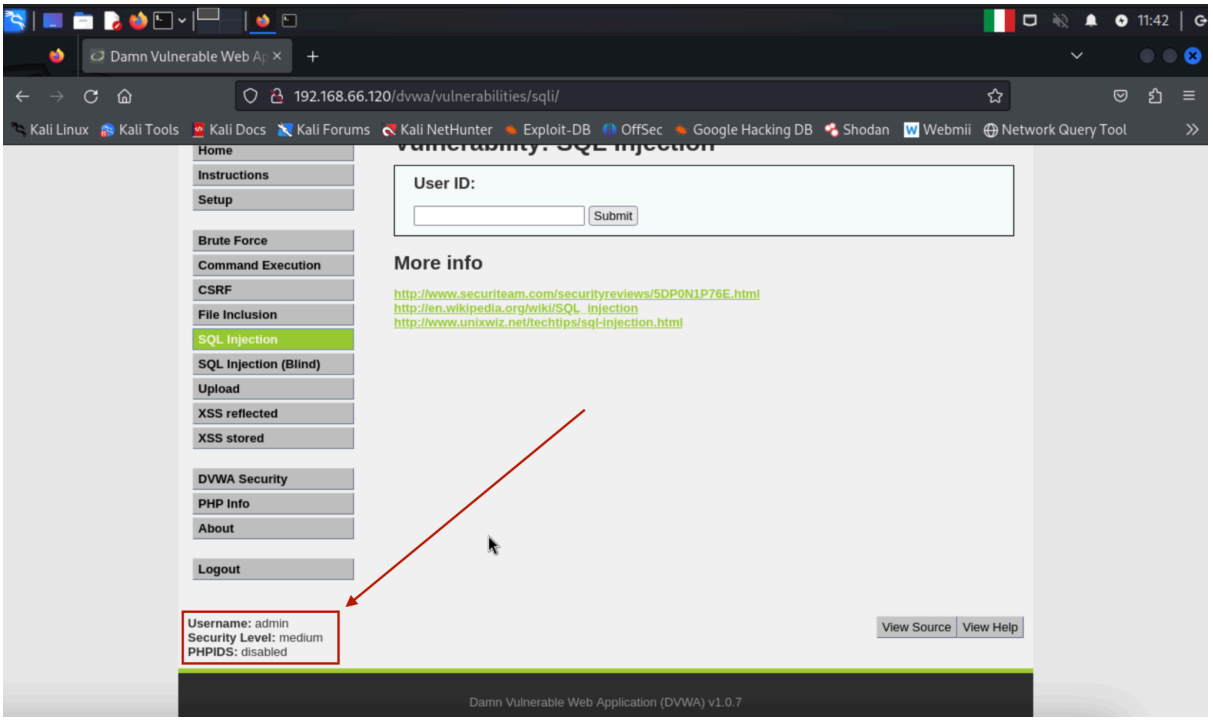
Ed ecco la password decifrata:

" abc123 "

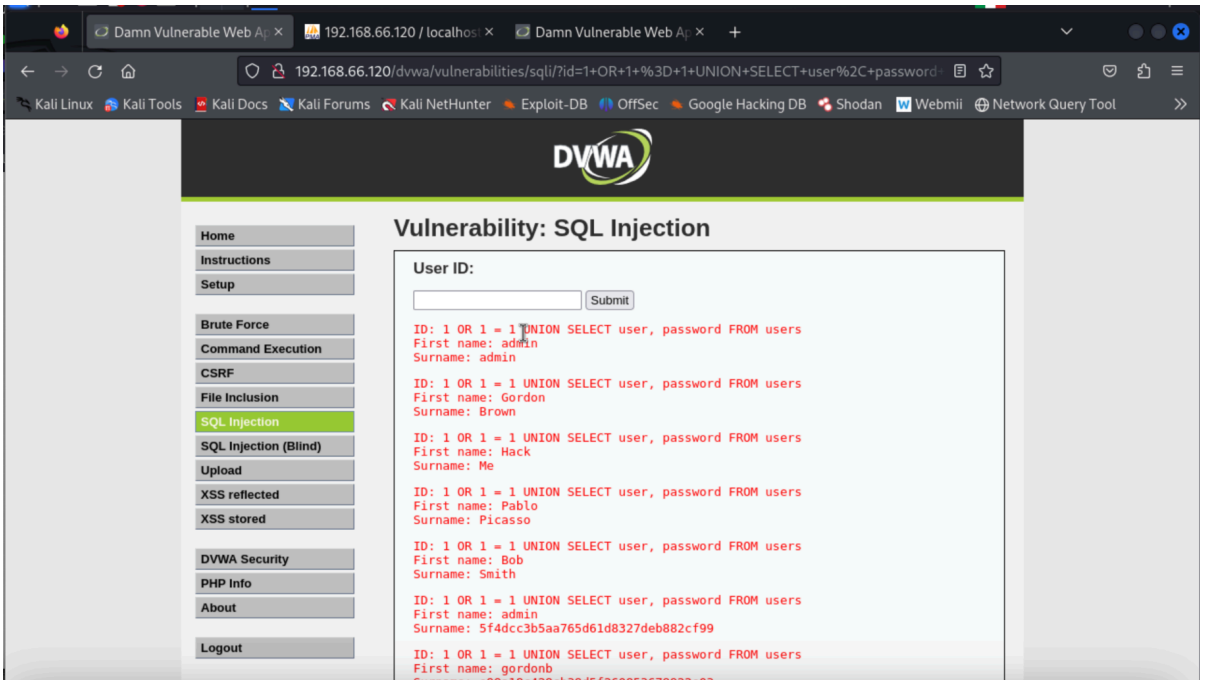
BONUS

Sicurezza *Medium*

Andiamo ad impostare la sicurezza a medio.



Ora conoscendo già i vari nomi delle tabelle etc… grazie alle iniezioni della sicurezza bassa, andiamo a provare una variante della UNION SELECT per farci restituire utente e password.

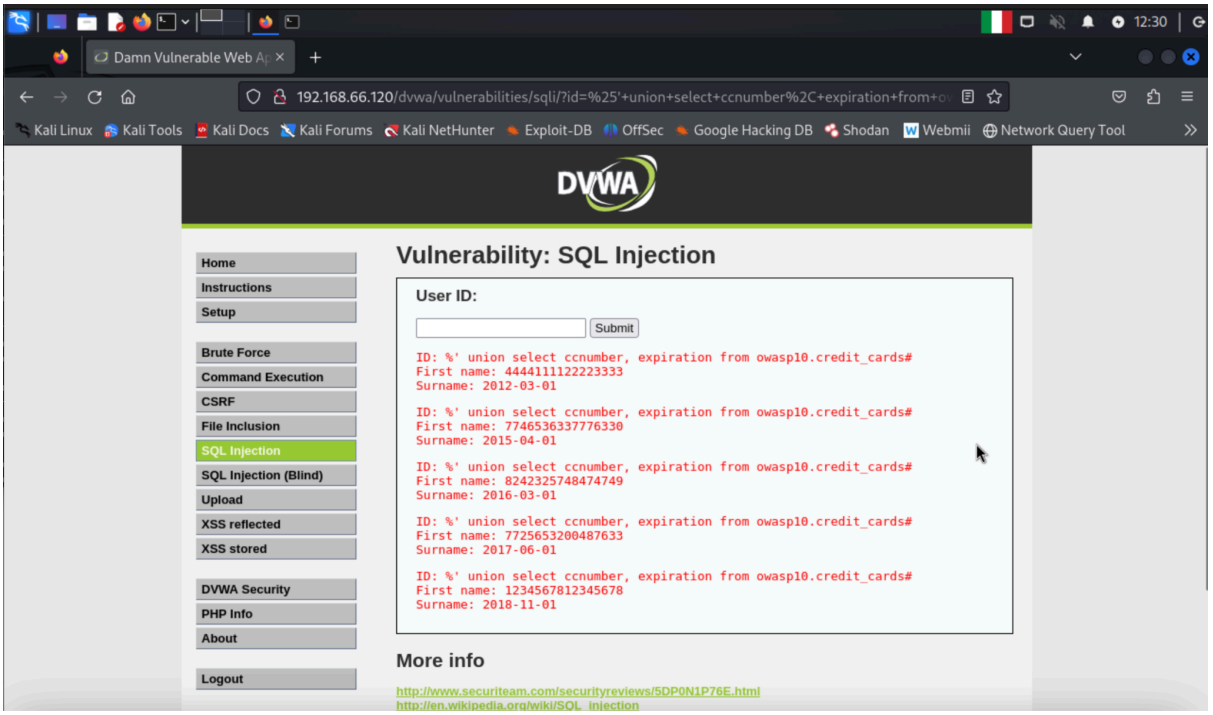


Ecco qui che anche nel livello medio abbiamo trovato un modo per farci veder utenti e password

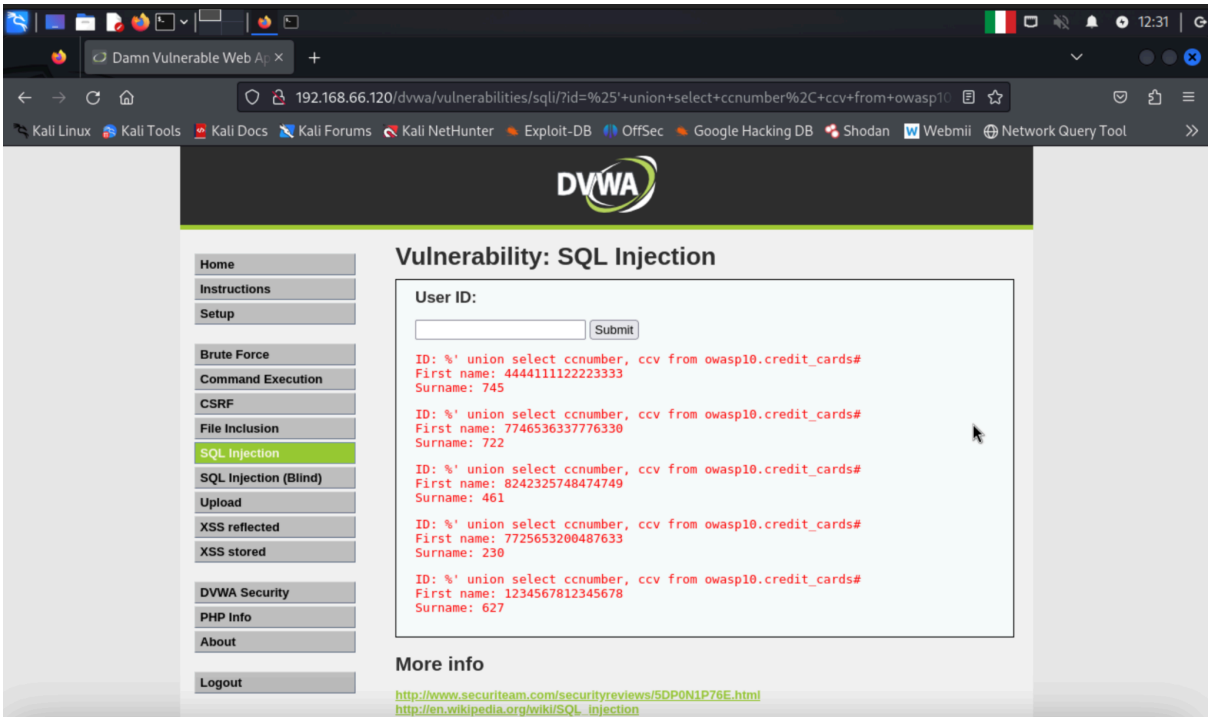
“ 1 or 1=1 UNION SELECT user, password FROM users ”

Informazioni aggiuntive da altre tabelle

Dando un’occhiata si è notata la presenza di dati sensibili che restituiscono le carte di credito degli utenti.



da qui possiamo vedere il numero delle carte di credito e la loro scadenza.



qui invece abbiamo ricavato il cvv.
Abbiamo utilizzato lo stesso metodo utilizzato in precedenza per ricavare questi dati.