TRACCIA 1 :BWII

Web Application Exploit SQLi

Traccia Giorno 1: Utilizzando le tecniche viste nelle lezionI 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

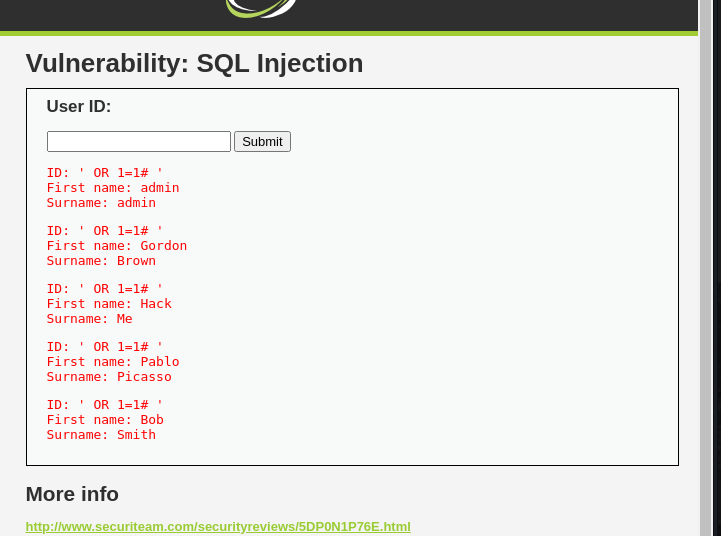
IP Metasploitable: 192.168.66.120/24

Bonus

-Replicare tutto a livello medium

-Verificare se è possibile inserire un utente tramite SQL injection

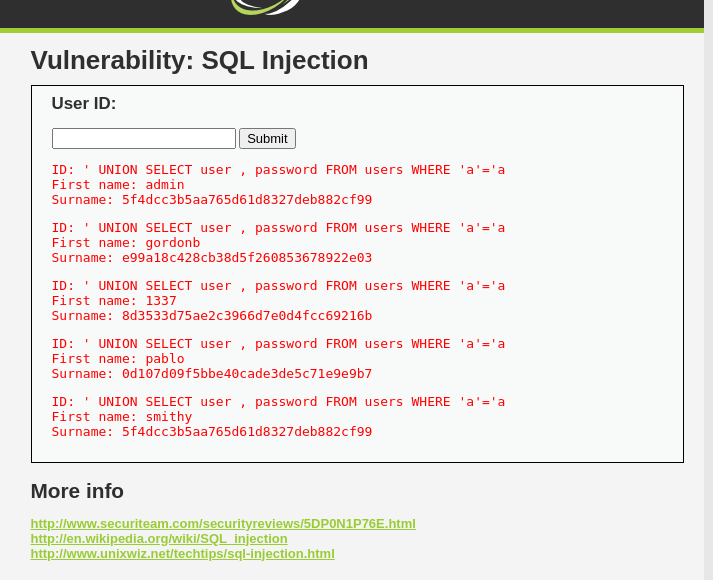
-Recuperare informazioni vitali da altri db collegati

-Creare una guida illustrata per spiegare ad un utente medio come replicare quest’attacco

Provo ad introdurre una stringa maliziosa come ‘ OR ‘1’=’1# come username, ci restituirà una lista di username e surname degli utenti presenti nel database.

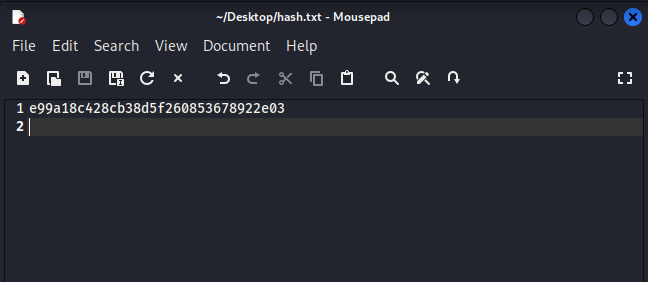
Essendo il nostro obbiettivo Gordon Brown, introduciamo un’altra stinga malevola del tipo:

‘UNION SELECT user, password FROM users WHERE ‘a’=’a

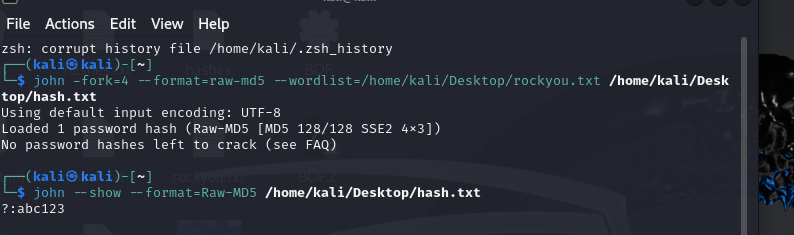


Ottenendo come risultato l’hash delle password di tutti gli utenti tra cui Gordon Brown.

Una volta copiato l’hash e incollato su un file di testo che prenderà il nome di hash.txt

Possiamo decodificarlo per ottenere la password in chiaro.

Per questo passaggio usiamo John the Ripper:



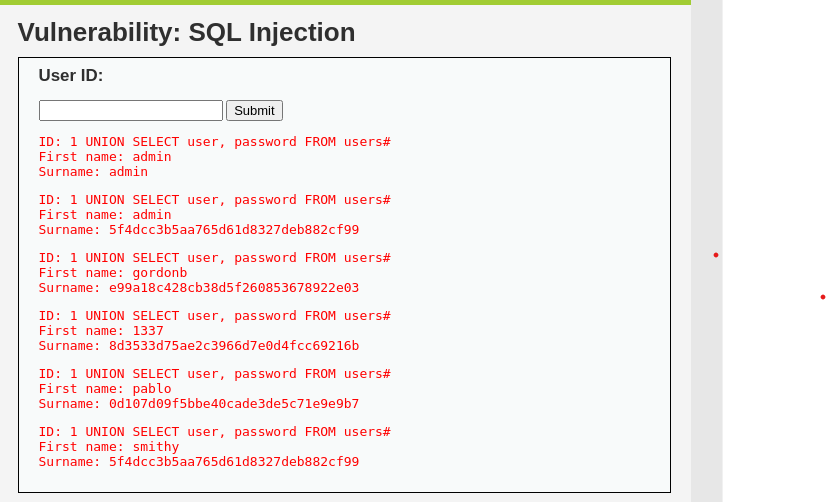
Specificando la libreria e il path che useremo, in questo caso rockyou.txt e specifichiamo il file .txt dove abbiamo salvato l’hash.

Come vediamo lo screenshot il tool ha trovato una password per Gordon Brown ovvero: abc123

BONUS:

Per il livello MEDIUM invece, cliccando su help in basso a destra, ci suggerisce che questo livello di sicurezza usa il: mysql\_real\_escape\_string() che possiamo semplicemente bypassare omettendo gli apici (‘)

Quindi : 1 UNION SELECT user, password FROM user#, come mostrato nello screenshot:



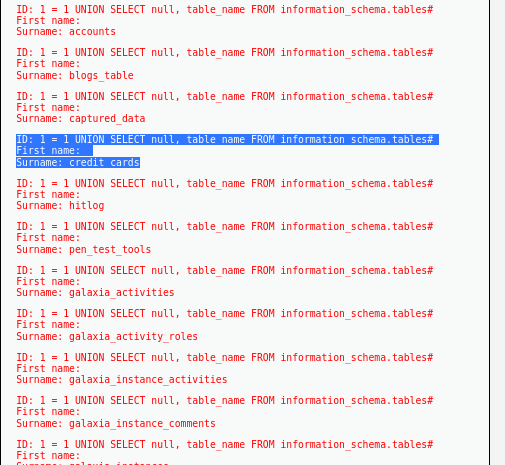
Come vediamo, ci restituisce gli hash delle password di tutti gli utenti ed il procedimento per decriptare l’hash e lo stesso che abbiamo usato prima con il livello di sicurezza LOW.

E ci ridarà come risultato la password: abc123.

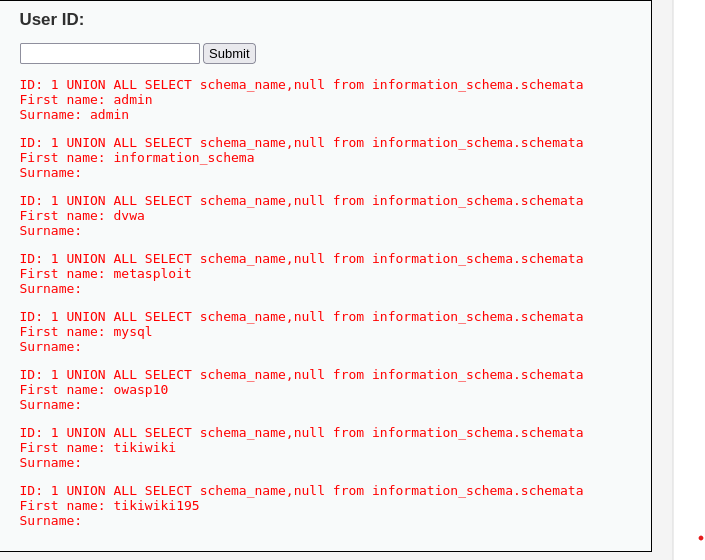
Per recuperare informazioni vitali all’interno del database utiliziamo la stringa:

1 = 1 UNION SELECT NULL, table\_name FROM information\_schema.tables

Che ci ridarà i nomi delle tabelle presente sul database, tra le quali possiamo osservare che sono presenti alcuni dati sensibili come, per esempio, i numeri di carte di credito.



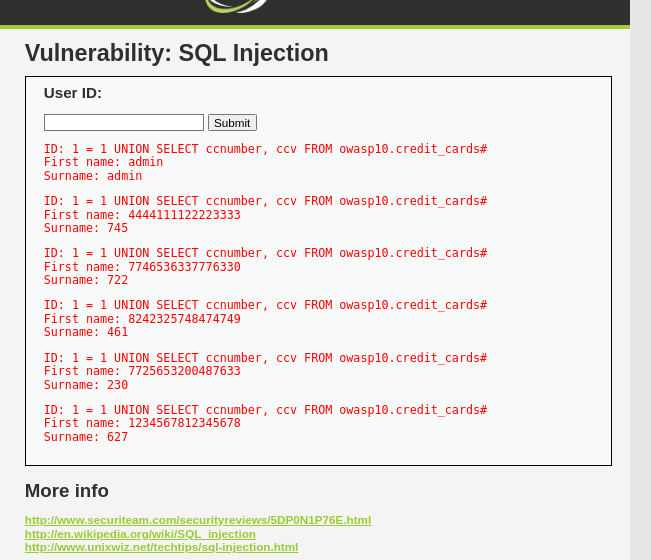
Vediamo tutti i database: 1 UNION ALL SELECT schema\_name,null FROM information\_schema.schemata

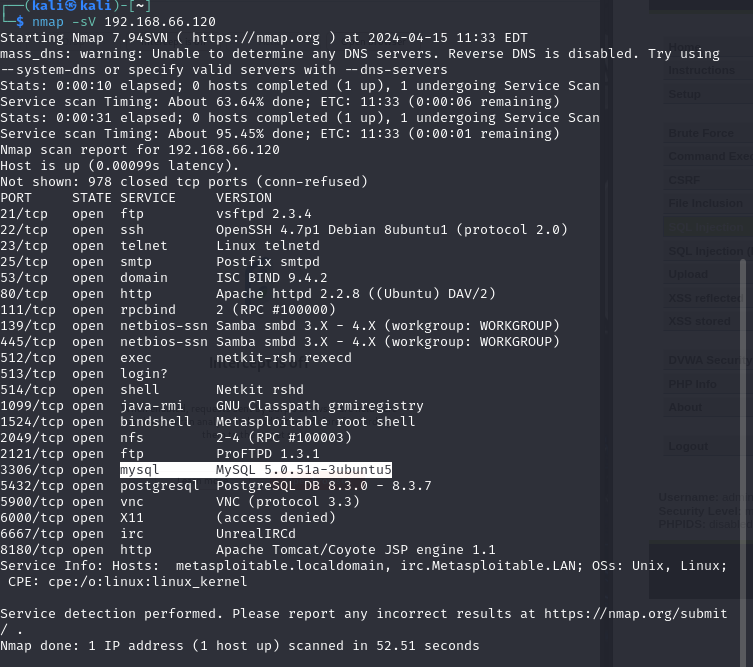


Per recuperare per esempio i numeri delle carte ho usato la stringa:

1 = 1 UNION SELECT ccnumber, ccv FROM owasp10.credit\_cards#

Seleziona i numeri delle carte di credito e i codici di verifica dalla tabella credit\_cards e dallo schema owasp10.credit\_cards#





Per quanto riguarda la creazione del nuovo utente vedendo la versione di MySQL 5.0.51a e osservando la documentazione non c’è la possibilità di creare un nuovo utente

(I punti deboli di questa categoria sono correlati alla gestione delle autorizzazioni, dei privilegi e di altre funzionalità di sicurezza utilizzate per eseguire il controllo degli accessi.)