Gobustme

ctflearn.com

Jakub Kazimierski February 2023

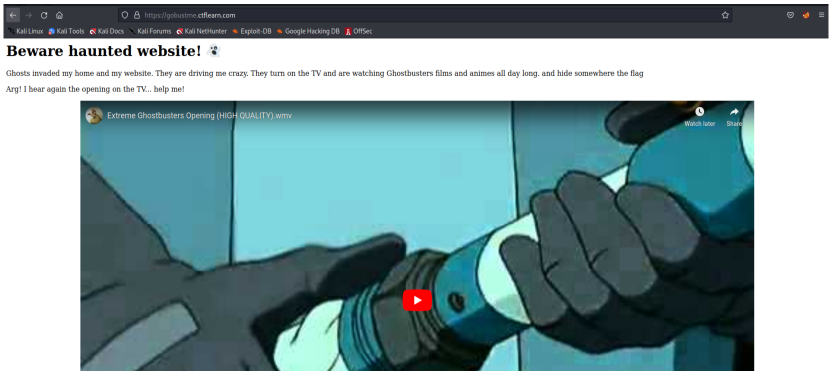
1 Introduction

This sheet meant to be a walkthrough of CTF challenge from ctf [4]. Here I try to explain step by step what metodology for solving this problem was taken along with actions which were needed. Some of steps will be showed on screenshots and some just explained along with commands used.

OS which was used for this presentation is Kali Linux in version 2022.4

2 Problem overview

Description of this task is short, we should exploit site: [5]. When we open link we get home page:

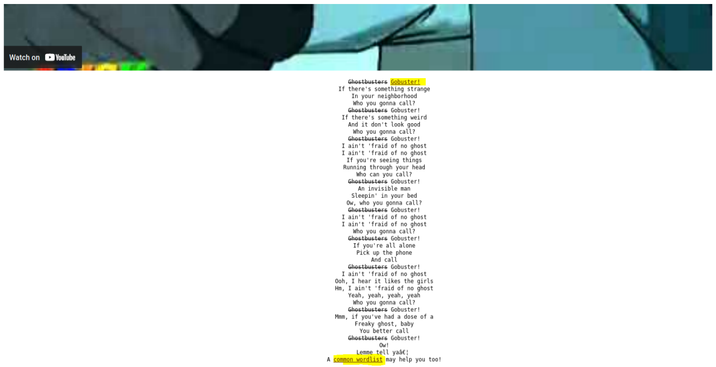


Beware haunted website!

Ghosts invaded my home and my website. They are driving me crazy. They turn on the TV and are watching Ghostbusters films and animes all day long. and hide somewhere the flag

Arg! I hear again the opening on the TV... help me!

Figure 1: Site home page part 1



~~Ghostbusters~~ Gobuster!
If there's something strange
In your neighborhood
Who you gonna call?
~~Ghostbusters~~ Gobuster!
If there's something weird
And it don't look good
Who you gonna call?
~~Ghostbusters~~ Gobuster!
I ain't 'fraid of no ghost
I ain't 'fraid of no ghost
If you're seeing things
Running through your head
Who can you call?
~~Ghostbusters~~ Gobuster!
An invisible man
Sleepin' in your bed
Ow, who you gonna call?
~~Ghostbusters~~ Gobuster!
I ain't 'fraid of no ghost
I ain't 'fraid of no ghost
Who you gonna call?
~~Ghostbusters~~ Gobuster!
If you're all alone
Pick up the phone
And call
~~Ghostbusters~~ Gobuster!
I ain't 'fraid of no ghost
Ooh, I hear it likes the girls
Hm, I ain't 'fraid of no ghost
Yeah, yeah, yeah, yeah
Who you gonna call?
~~Ghostbusters~~ Gobuster!
Mmm, if you've had a dose of a
Freaky ghost, baby
You better call
~~Ghostbusters~~ Gobuster!
Ow!
Lemme tell yaâ€¦
A common wordlist may help you too!

Figure 2: Site home page part 2

This site seems to have flag hidden somwhere, and to find it, we are suggested to use directory scanning tool Gobuster [1]. We are given some hints, highlited words are links to Gobuster instructions of usage [2] and wordlist [3] which gobuster can use for this challenge.

So let's start searching directories, below is command used:

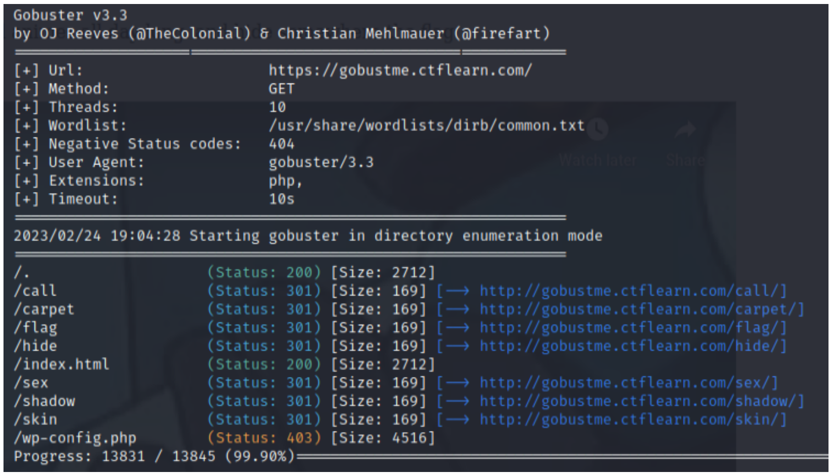
```
(Linux@terminal)—$ gobuster dir —u https://web.ctflearn.
    com/audioedit/ —w /usr/share/wordlists/dirb/common.txt
     —x php, jpg, txt
```

Listing 1: Used gobuster syntax

Flag used are for:

- dir - attack mode, to search directories,
- -u - defines url which will be attacked,
- -w - defines wordlist used for dictionary attack,
- -x - check if in searched direcotry contains files with those extensions, and names as in attached wordlist.

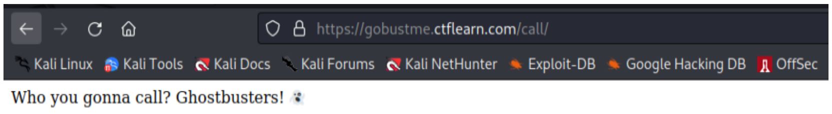
After command was run we get output:



```
Gobuster v3.3
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://gobustme.ctflearn.com/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.3
[+] Extensions:              php,
[+] Timeout:                 10s
===============================================================
2023/02/24 19:04:28 Starting gobuster in directory enumeration mode
===============================================================
/.                    (Status: 200) [Size: 2712]
/call                 (Status: 301) [Size: 169] [--> http://gobustme.ctflearn.com/call/]
/carpet               (Status: 301) [Size: 169] [--> http://gobustme.ctflearn.com/carpet/]
/flag                 (Status: 301) [Size: 169] [--> http://gobustme.ctflearn.com/flag/]
/hide                 (Status: 301) [Size: 169] [--> http://gobustme.ctflearn.com/hide/]
/index.html           (Status: 200) [Size: 2712]
/sex                  (Status: 301) [Size: 169] [--> http://gobustme.ctflearn.com/sex/]
/shadow               (Status: 301) [Size: 169] [--> http://gobustme.ctflearn.com/shadow/]
/skin                 (Status: 301) [Size: 169] [--> http://gobustme.ctflearn.com/skin/]
/wp-config.php        (Status: 403) [Size: 4516]
Progress: 13831 / 13845 (99.90%)===============================================================
```

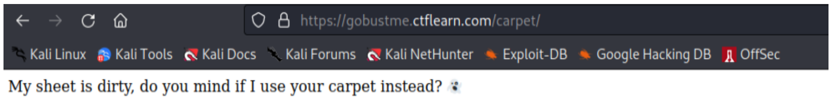
Figure 3: Returned directories

So now we should check them, maybe we will find something interesting:



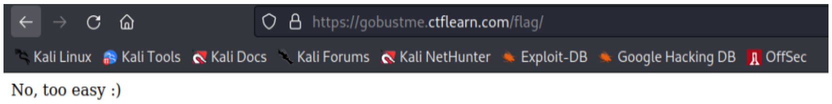
Who you gonna call? Ghostbusters! 👻

Figure 4: https://gobustme.ctflearn.com/call/



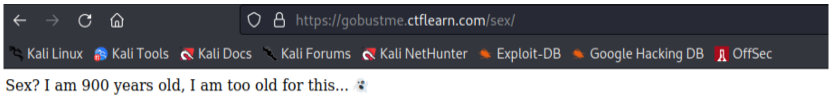
My sheet is dirty, do you mind if I use your carpet instead? 👻

Figure 5: https://gobustme.ctflearn.com/carpet/



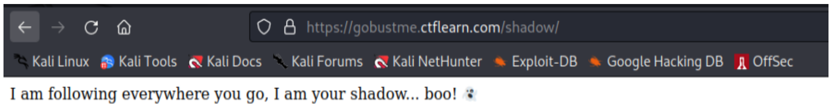
No, too easy :)

Figure 6: https://gobustme.ctflearn.com/flag/



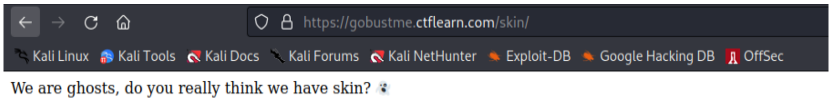
Sex? I am 900 years old, I am too old for this... 👻

Figure 7: https://gobustme.ctflearn.com/sex/



I am following everywhere you go, I am your shadow... boo! 👻

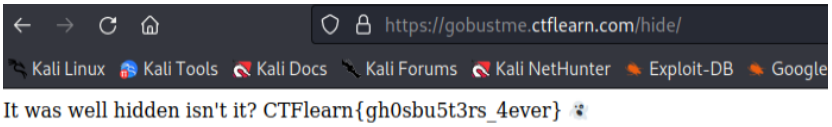
Figure 8: https://gobustme.ctflearn.com/shadow/



We are ghosts, do you really think we have skin? 👻

Figure 9: https://gobustme.ctflearn.com/skin/

It looks like mostly ghost are fooling around with us, but finally when we get to **/hide** directory:



It was well hidden isn't it? CTFlearn{gh0sbu5t3rs_4ever} 👻

Figure 10: https://gobustme.ctflearn.com/hide/

We get the flag: **CTFlearn{gh0sbu5t3rs_4ever}**

References

[1] Gobuster. https://www.kali.org/tools/gobuster/.

[2] Gobuster handbook. https://www.securitynewspaper.com/2019/11/04/bruteforce-any-website-with-gobuster-step-by-step-guide/.

[3] Gobuster handbook. https://raw.githubusercontent.com/v0re/dirb/master/wordlists/common.txt.

[4] Reference to site with this challenge. https://ctflearn.com/.

[5] Site to exploit. https://gobustme.ctflearn.com/.