Mission Name
The Erase

Historical Context
Ethan utilizes his level 5 datacard, known as Fence, to infiltrate the Skytech facility. His objective is to uncover specific details on his identification card, erase his personal information, and gain temporary access to the Lazarus Citizens database.

Technical Synopsis
Inside the Skytech premises, Ethan will engage with the Lazarus Citizens system. This task is facilitated through a webpage simulation, which harbors a common web vulnerability related to file inclusion. Ethan is tasked with exploiting this vulnerability to seize control of the system.

Mission Outline
Ethan, leverage your Fence datacard to navigate the citizen search function and secure control of the Skytech system. Your mission requires you to return with evidence of your successful system compromise. Best of luck!

Detailed Assignment
Ethan, with the assistance of the level 5 datacard (Fence), ventures into the Skytech facility. His mission revolves around identifying crucial information on his identification card, purging his personal data, and obtaining temporary entry into the Lazarus Citizens records.

Operational Venue
ASUNCION | PARAGUAY

Tools

- User: fen
- Password: f3nc3_p4ssw0rd

Questions

What is the parameter vulnerable?

- page

What is the name of the vulnerability?

- LFI

Full path of flag

- /var/www/deploys/skytech/src/Security/Core/User/flag.txt

Items

1. Check out parameter page.
2. Try to call a local file in parameter page.
3. Brute force paths to find the flag, use knowledge from easy challenges or other skytech web challenge.

Categories

- Web
- Local file inclusion

Write Up

Upon accessing the Lazarus Skytech system with the provided credentials, you'll discover that the user search form includes a "page" parameter in the URL, indicative of a Local File Inclusion (LFI) vulnerability.

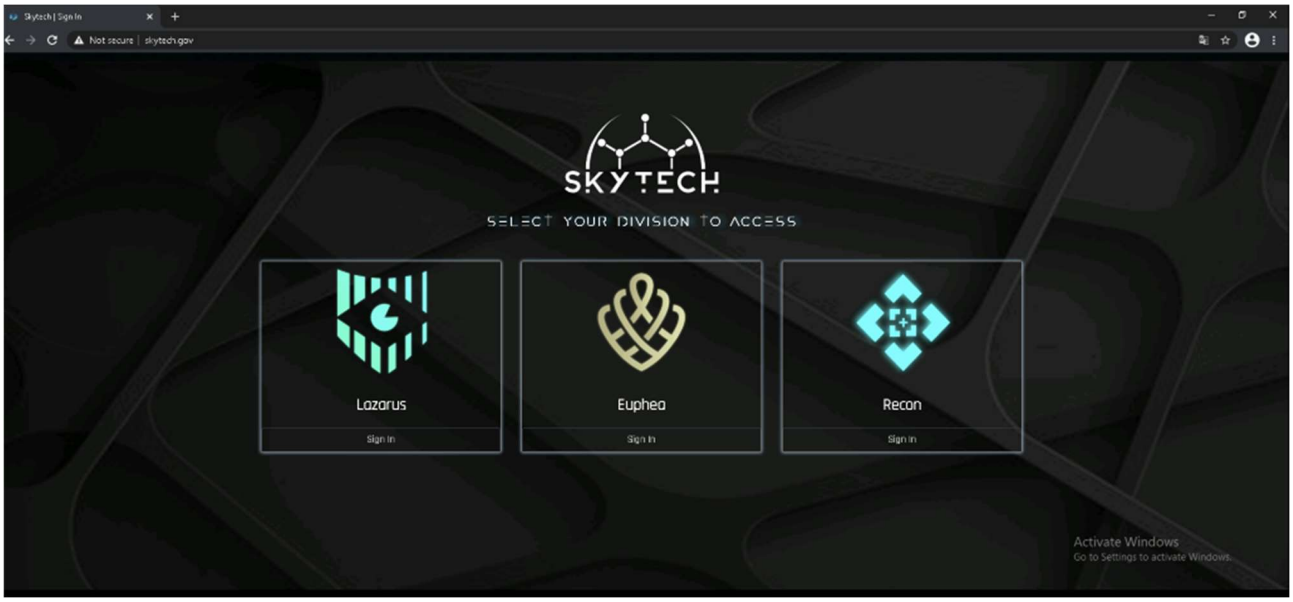

Figure 1

The vulnerability can be confirmed by accessing system files, such as:

- URL?page=/etc/passwd

To exploit this vulnerability for flag retrieval, a brute force approach can be employed to read files across the system. This involves systematically attempting various paths based on common or known directory structures, including those suggested by previous Skytech challenges, typical Symfony framework hierarchies, or other logical guesses.
Given the hint towards Symfony's directory structure, the flag can be located at:

- URL?page=/var/www/deploys/skytech/src/Security/Core/User/flag.txt

When conducting the brute force search, you may encounter several decoy messages indicating "Not Here" at paths like:

- /home/flag.txt
- /var/www/deploys/skytech/public/flag.txt

These messages serve as indicators that the explored paths are incorrect but also confirm the presence of the LFI vulnerability, guiding the search towards the correct file location. To automate the brute force process, one could use a script to iterate through a dictionary of potential file paths.

This script would attempt to load each path via the LFI vulnerability and check the response for the flag content or indicative error messages, efficiently narrowing down the search to the correct file path where the flag is stored.

Flag Information

flag{LFI_blind_search_is_c0rr3ct}