

CÁTEDRA DE CIBERSEGURIDAD CIBERUGR, INCIBE-UGR

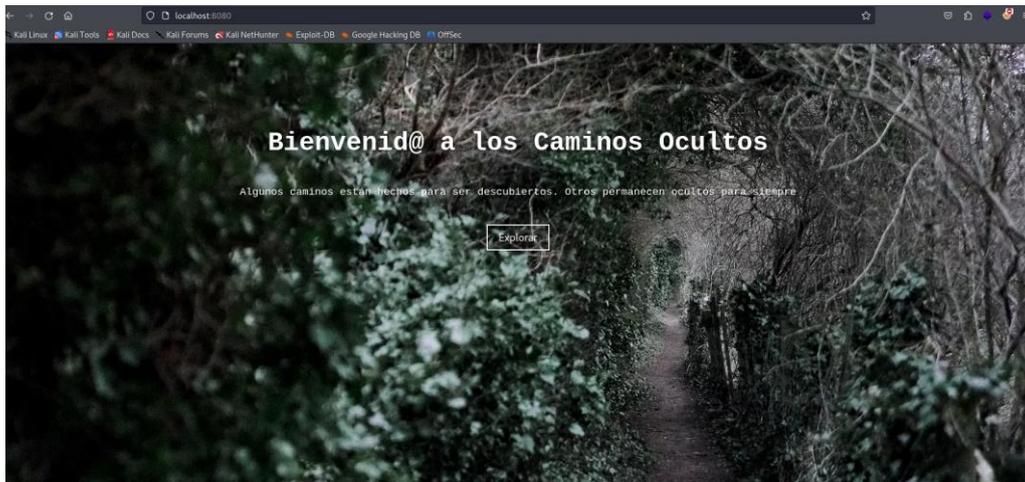
Nombre	Hidden Paths
Categoría	Web
Dificultad	Muy fácil
Puntos	100

DESCRIPCIÓN DEL RETO

Explora las profundidades de un sitio web en busca de información. No todo lo que existe está a la vista, y algunos caminos pueden revelar más de lo que parece. ¿Tienes lo necesario para descubrirlos?

WRITEUP

1. Accede a la página y verifica que no se puede interactuar con nada:



Nota: El botón de Explorar no hace nada, solo está como pequeña distracción.

2. Utiliza una herramienta para la enumeración de directorios/archivos. En este caso se ha utilizado gobuster con una wordlist de seclists, pero cualquier otra herramienta y wordlist es perfectamente válida:

```
gobuster      dir      -u      http://<ip>:7777      -w  
/usr/share/seclists/Discovery/Web-Content/common.txt
```

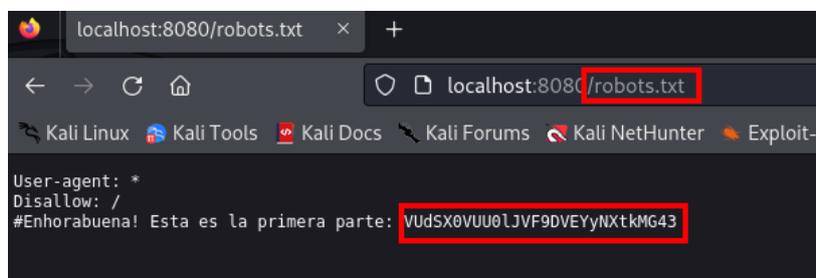
```

└─# gobuster dir -u http://localhost:7777 -w /usr/share/seclists/Discovery/Web-Content/common.txt
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:                http://localhost:7777
[+] Method:             GET
[+] Threads:           10
[+] Wordlist:           /usr/share/seclists/Discovery/Web-Content/common.txt
[+] Negative Status codes: 404
[+] User Agent:        gobuster/3.6
[+] Timeout:           10s
=====
Starting gobuster in directory enumeration mode
=====
/.hta                (Status: 403) [Size: 199]
/.htaccess           (Status: 403) [Size: 199]
/.htpasswd           (Status: 403) [Size: 199]
/index.html          (Status: 200) [Size: 1848]
/robots.txt          (Status: 200) [Size: 94]
/sitemap.xml         (Status: 200) [Size: 186]
Progress: 4734 / 4735 (99.98%)
=====
Finished

```

Nota: Si decides usar una wordlist diferente, asegúrate de que incluya las líneas “robots.txt” y “sitemap.xml”. Esto es importante porque Gobuster (y el resto de las herramientas de fuzzing) solo buscará los archivos o directorios que estén en la wordlist. Si estos nombres no están en la lista, la herramienta no podrá detectarlos ni mostrarlos en los resultados.

3. Ve a la ruta /robots.txt, donde se encuentra la primera parte de la flag codificada en base 64:

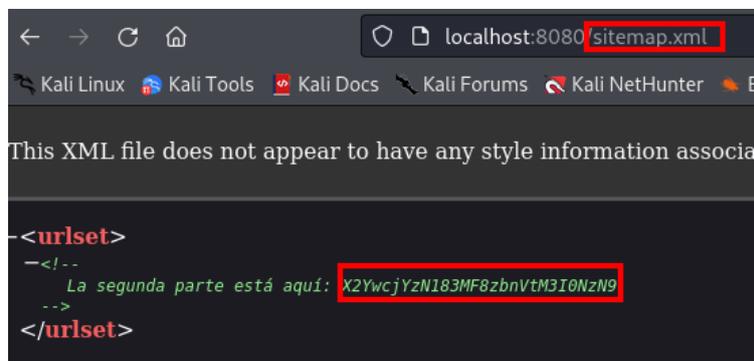


```

localhost:8080/robots.txt
-----
User-agent: *
Disallow: /
#Enhorabuena! Esta es la primera parte: VUdSX0VUU01JVF9DVEYyNXtkMG43

```

4. Ve a la ruta /sitemap.xml, donde se encuentra la segunda parte de la flag:



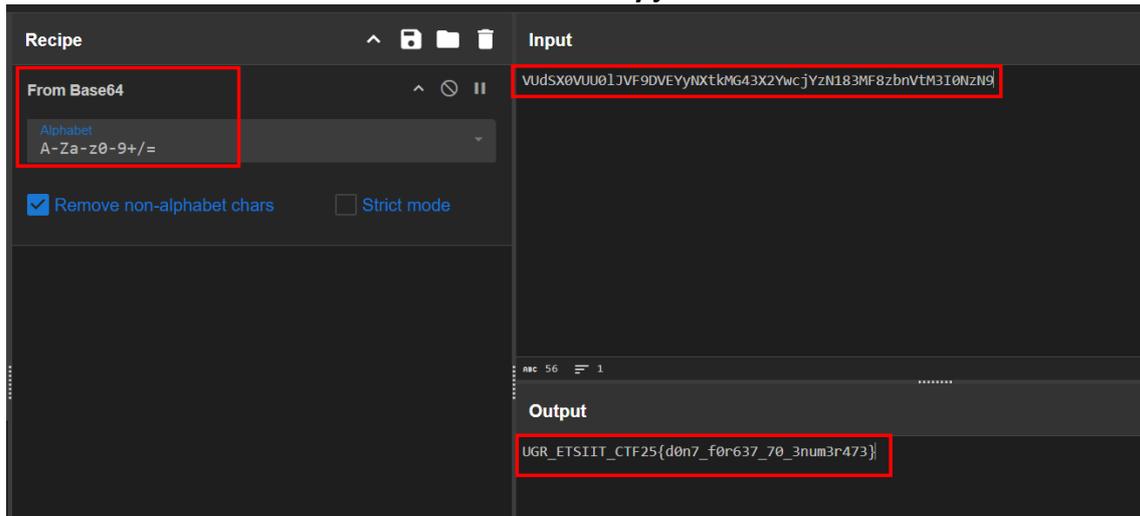
```

localhost:8080/sitemap.xml
-----
This XML file does not appear to have any style information associated with it.

<urlset>
  <!--
  La segunda parte está aquí: X2YwcjYzn183MF8zbnVtM3I0NzN9
  -->
</urlset>

```

5. En Cyberchef (<https://gchq.github.io/CyberChef/>), junta ambas partes y decodifica la flag:



The screenshot shows a CTF tool interface with a 'Recipe' panel on the left and an 'Input' and 'Output' panel on the right. The 'Recipe' panel is titled 'From Base64' and includes a dropdown menu set to 'Alphabet' with the character set 'A-Za-z0-9+/=' selected. Below the dropdown are two checkboxes: 'Remove non-alphabet chars' (checked) and 'Strict mode' (unchecked). The 'Input' panel contains a red-bordered text box with the Base64 string: 'VUdSx0VUU01JVF9DVEYyNXtkMG43X2YwcjYzN183MF8zbnVtM3I0NzN9'. The 'Output' panel contains a red-bordered text box with the decoded flag: 'UGR_ETSIIIT_CTF25{d0n7_f0r637_70_3num3r473}'.