CÁTEDRA DE CIBERSEGURIDAD CIBERUGR, INCIBE-UGR

Nombre	Juglar
Categoría	Web
Dificultad	Difícil
Puntos	500

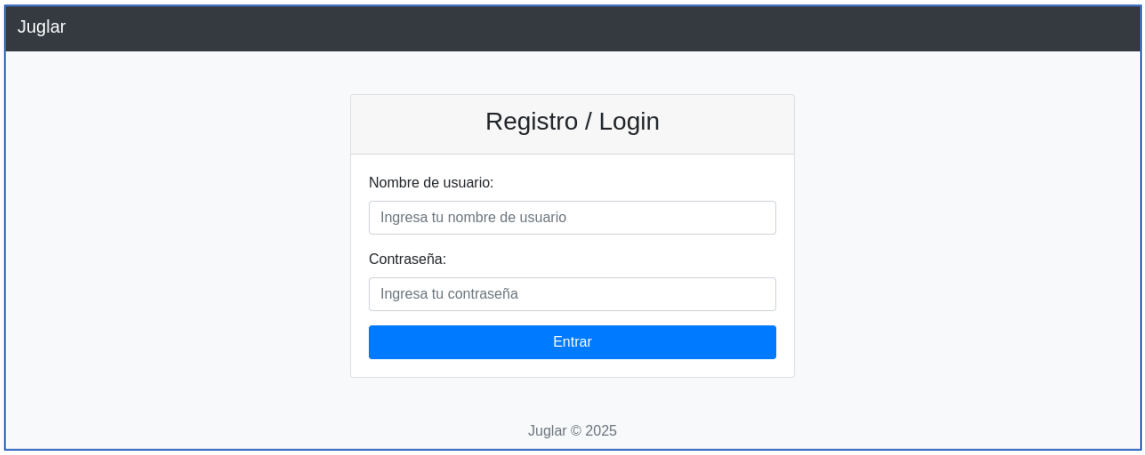
DESCRIPCIÓN DEL RETO

Los juglares tuvieron la audacia de ocultar sus secretos en versos y notas, dejando tras de sí un rastro críptico inofensivo a simple vista. Entre leyendas y relatos, se esconde la llave para descubrir un pasado lleno de enigmas. Atrévete a desvelar el legado oculto de los juglares y a romper el velo de un pasado en el que la pericia y el simbolismo se funden en el misterio.

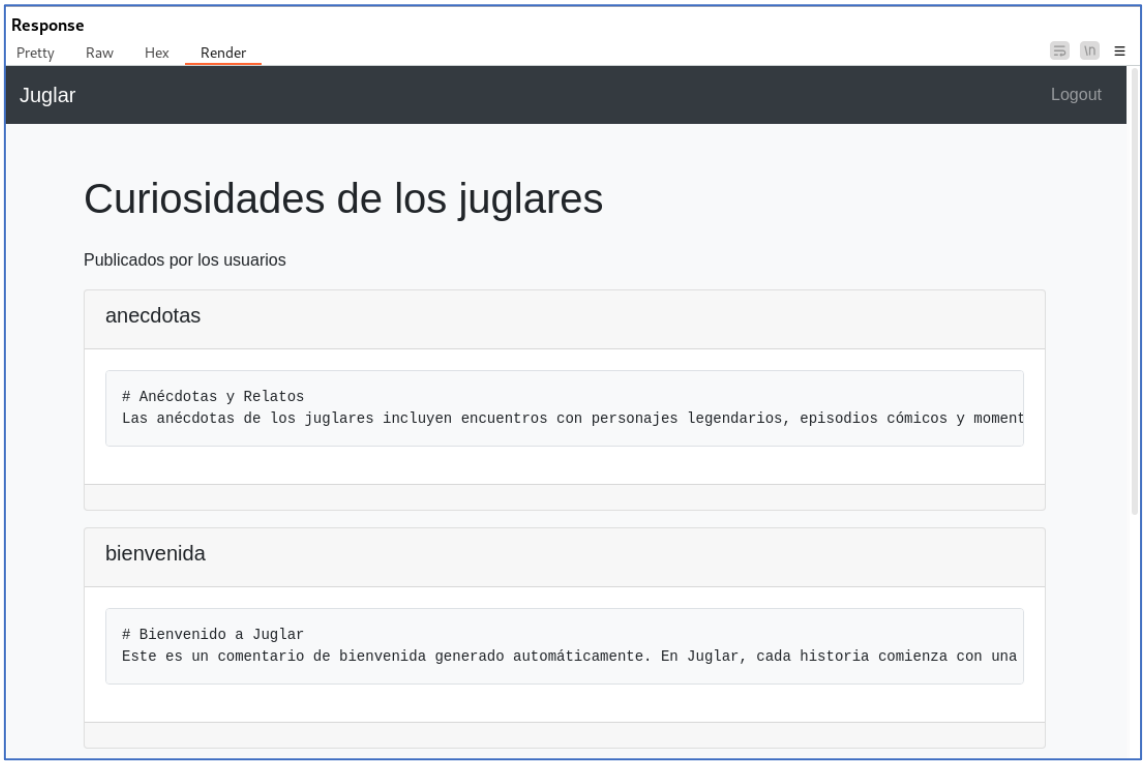
NOTA: La flag es un jpg: flag.jpg

WRITEUP

1. Accede a la web del enlace y encontraras una pestaña de registro / inicio de sesión. Al no tener un usuario creado, deberás de crear uno nuevo.

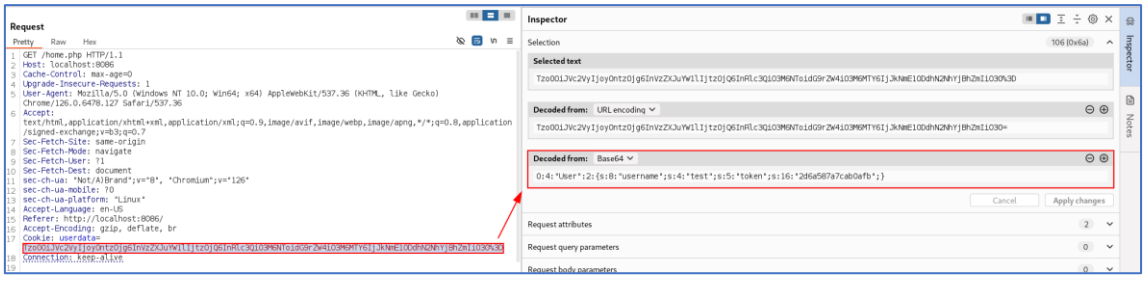


2. Abre Burp Suite e intercepta la petición al endpoint de /home.php y enviarla al Repeater.

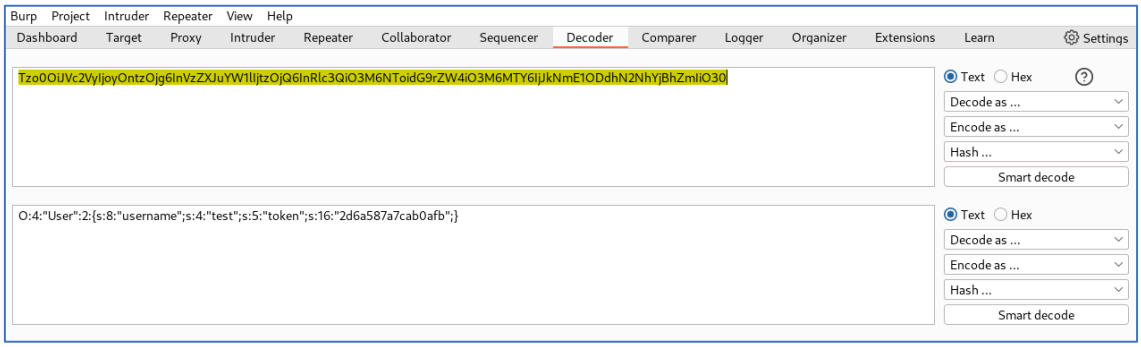


3. Analiza el formato de la cookie. Como se puede observar se trata de texto con formato de objeto PHP codificado en base64 que contiene el nombre del usuario autenticado junto con la longitud de la cadena y su tipo. En este caso:

```
0:4:"User":2:{s:8:"username";s:4:"test";s:5:"token";s:16:"2d6a587a7cab0afb"}
```



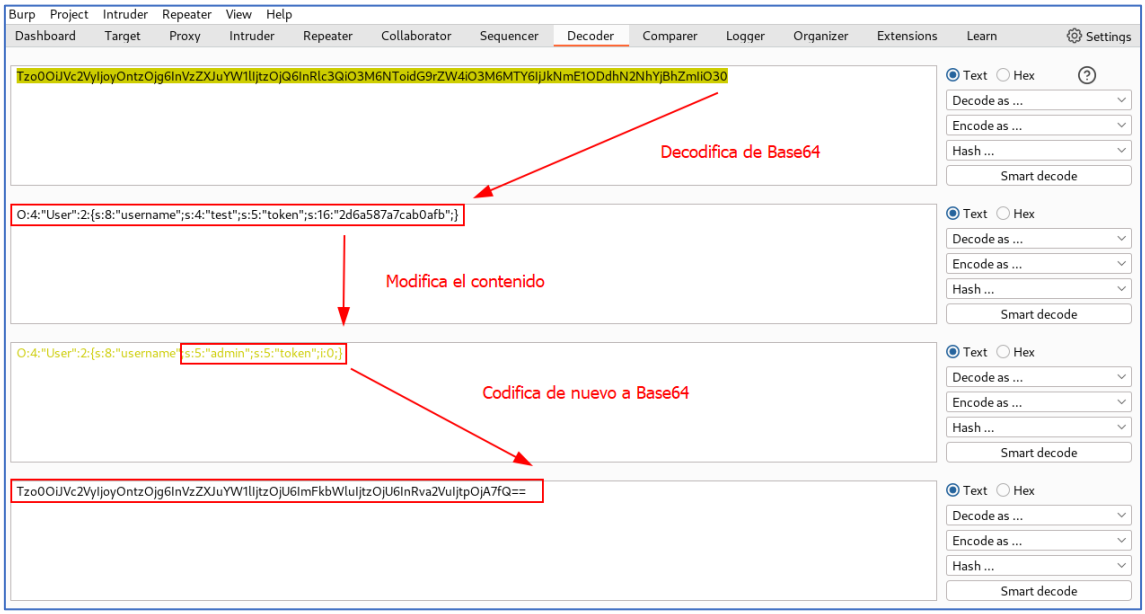
4. Envíala al Decoder.



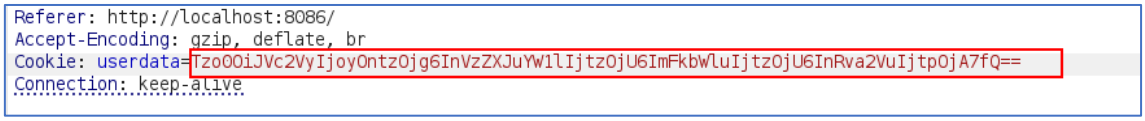
5. Modifícala por '5:admin' y aplica PHP Type Juggling al token poniéndolo como un entero (i:0). A continuación, vuelve a codificarla en formato Base64.

NOTA: PHP Type Juggling se basa en la conversión implícita de tipos en comparaciones laxas, lo que permite que un entero 0 se considere igual a una cadena no numérica, facilitando así la evasión de la validación.

```
O:4:"User":2:{s:8:"username";s:5:"admin";s:5:"token";i:0;}
```

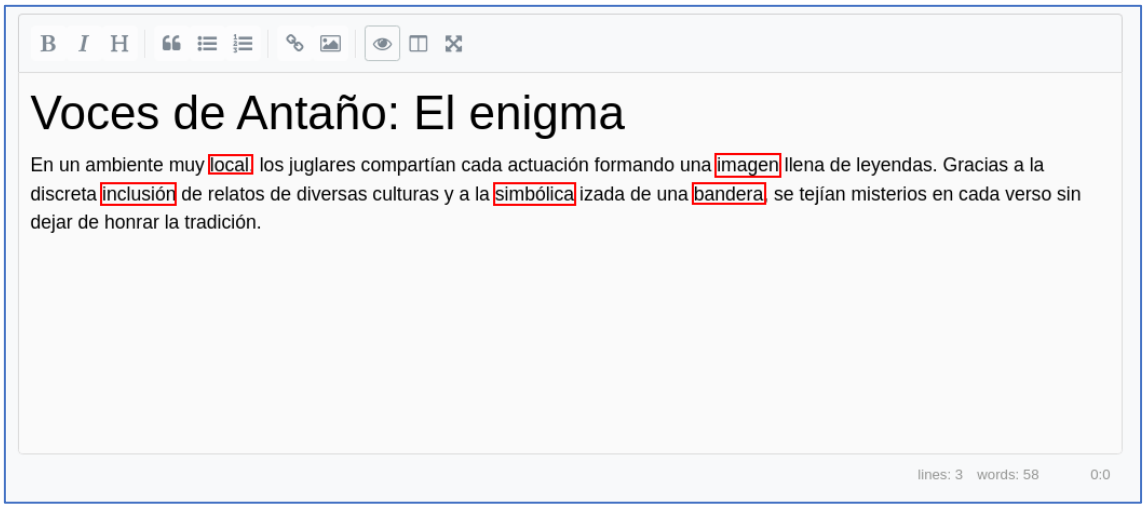


6. De vuelta en el Repeater, sustituye la cookie y vuelve a enviar la petición. Analiza la respuesta obtenida.

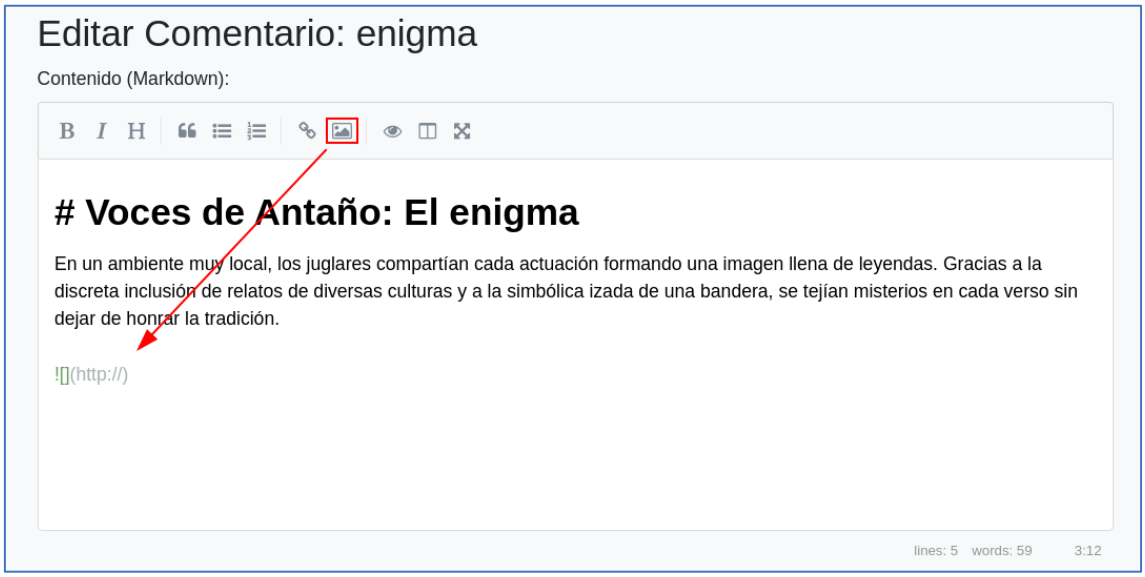


Como se puede observar, ahora aparecen las opciones de editar y borrar ficheros.

7. En el navegador, utiliza la cookie anterior y lee detenidamente todos los comentarios. Uno de estos contiene un enigma con palabras que pueden ayudar a deducir la segunda vulnerabilidad: Local File Inclusion.



8. Edita ese mismo comentario, pulsando el botón de añadir imagen.



9. A continuación, edita el enlace simbólico para que apunte a un fichero de imagen con el nombre de flag, probando distintos formatos. Luego pulsa el botón de vista dividida para previsualizar el contenido de Markdown.

```
![Flag](./flag.jpg)
```