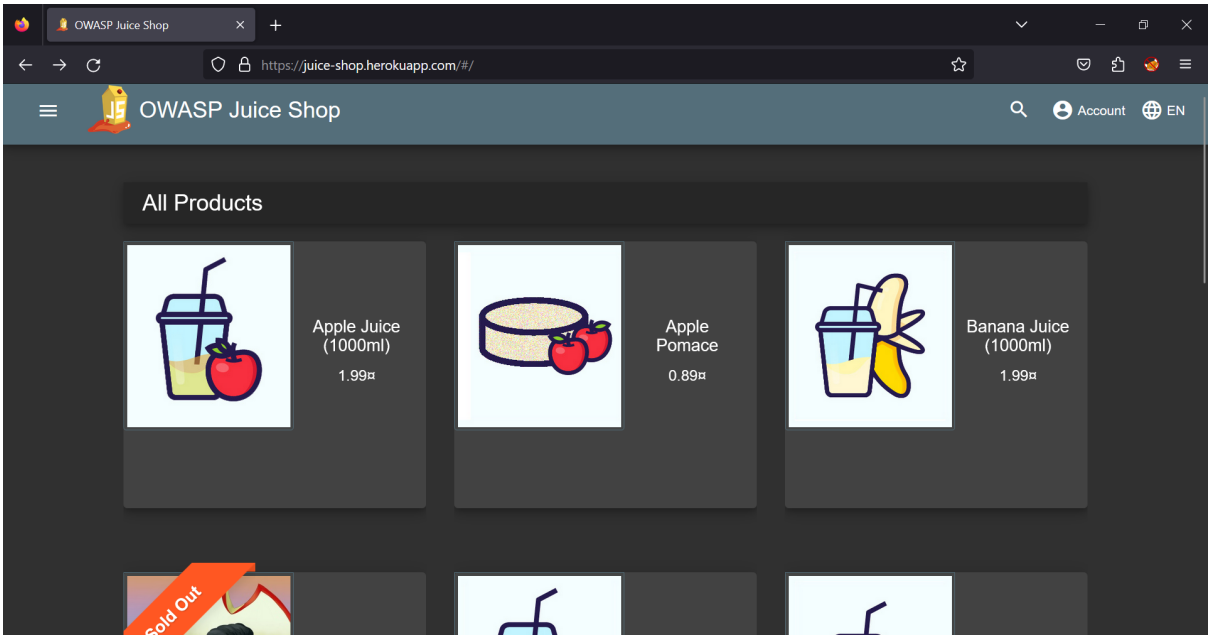
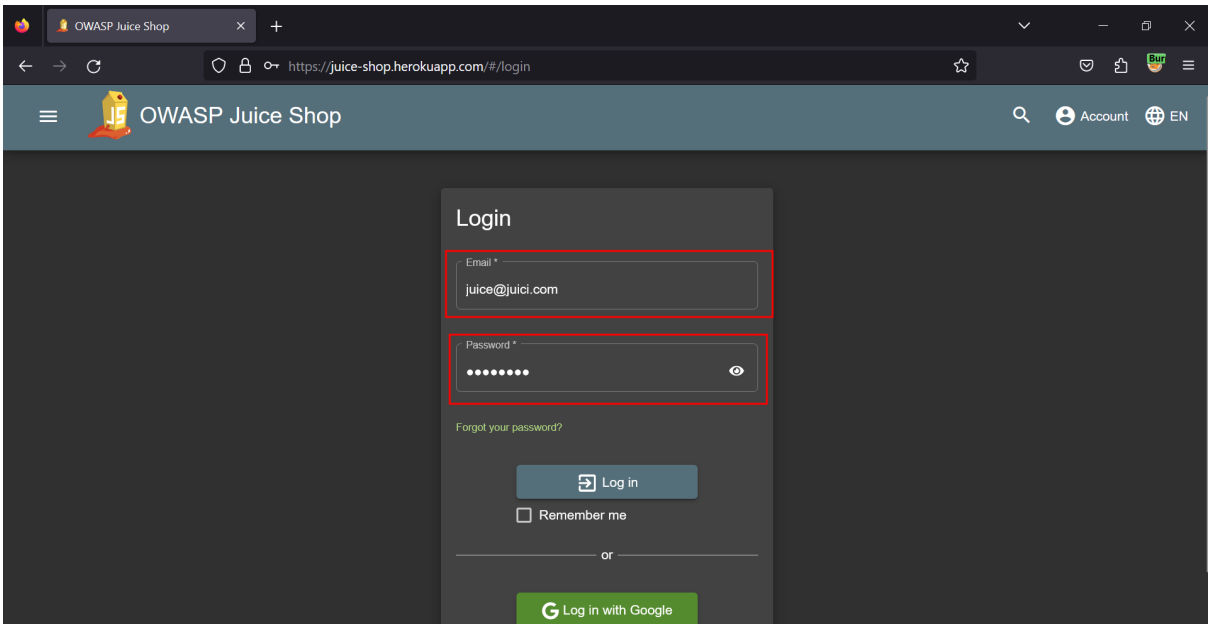
BlackDragons
Ejercicio de seguridad Aplicativa.

1.Inyección SQL:

Se ingresó a la sección de Account.

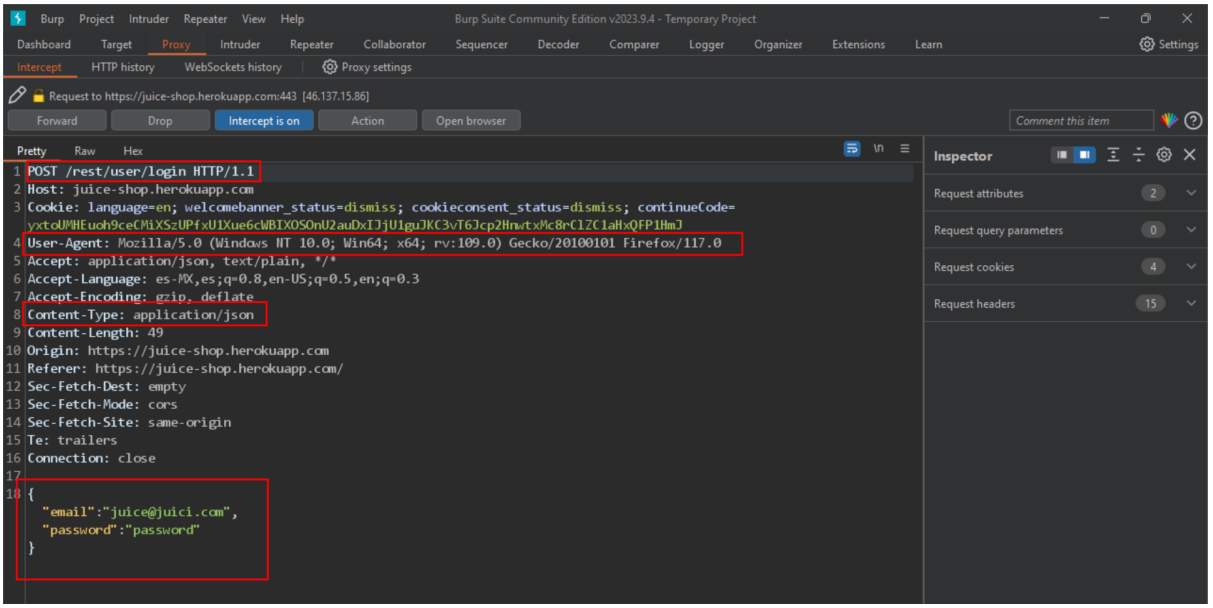


Se ingresaron credenciales x para poder ver la petición en BurpSuite.

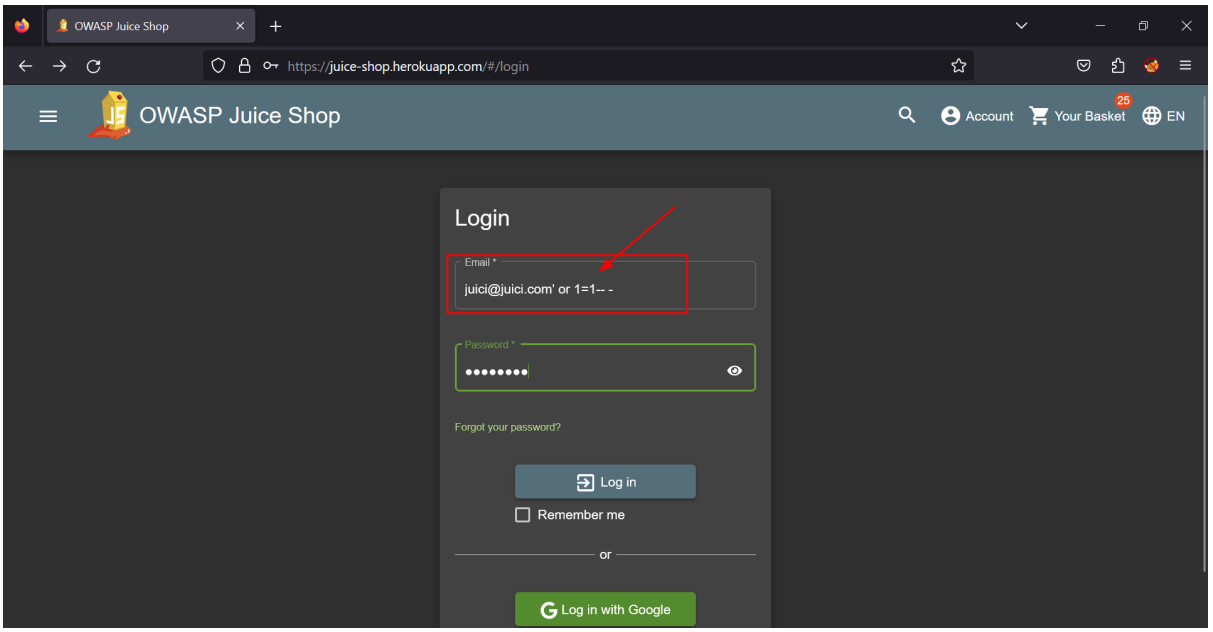


BlackDragons
Ejercicio de seguridad Aplicativa.

Observamos que las credenciales x aparecieron en el cuerpo y encontramos que acepta json y vemos que ocupa el método POST.

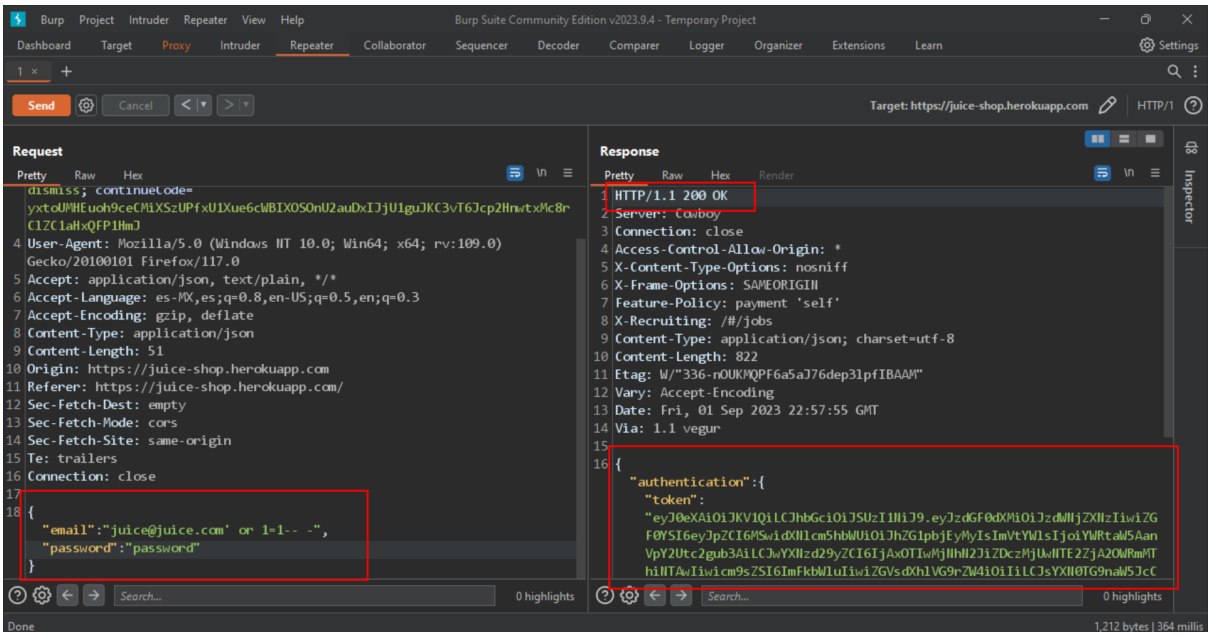


Encontramos que se puede acceder a su admin con las siguientes credenciales dirección de correo:' or 1=1-- -



BlackDragons
Ejercicio de seguridad Aplicativa.

En la pantalla de BurpSuite con repiter, se ve que regresa un código 200 ok y un token de autenticación.



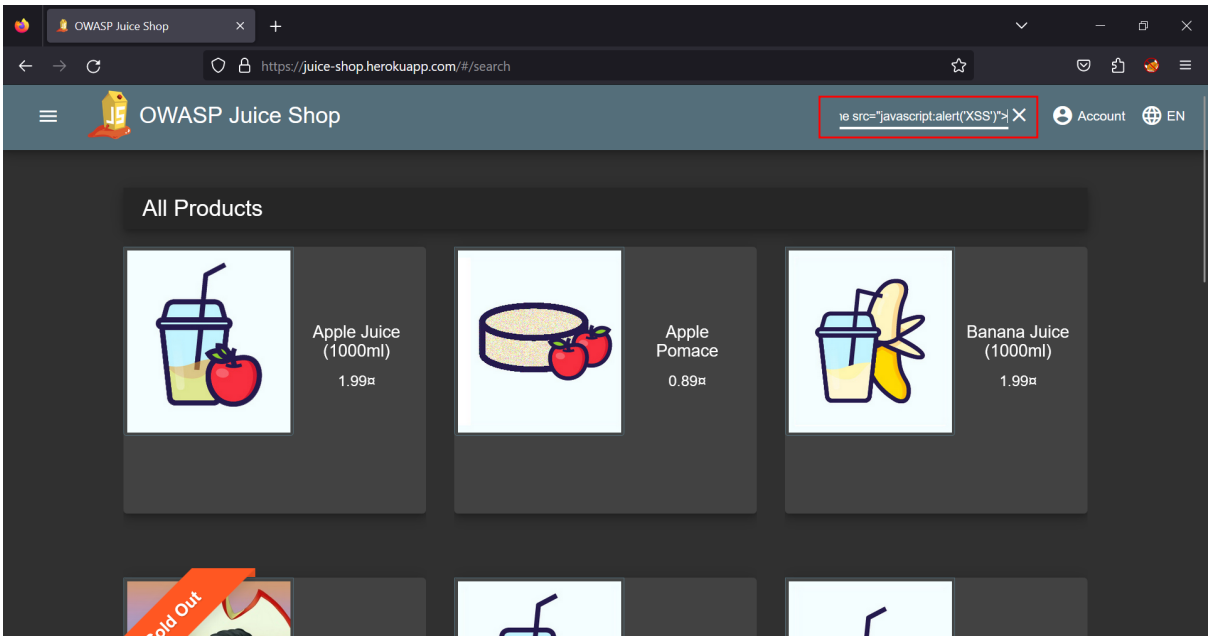
Mitigación:

Para mitigar una inyección SQL es importante sanitizar cualquier cadena de texto que sea ingresada en un campo de texto, es decir, cambiar a sus valores ASCII los caracteres especiales o directamente eliminarlos cuando sabemos de antemano que en un campo de correo electrónico no deberían existir ciertos caracteres.

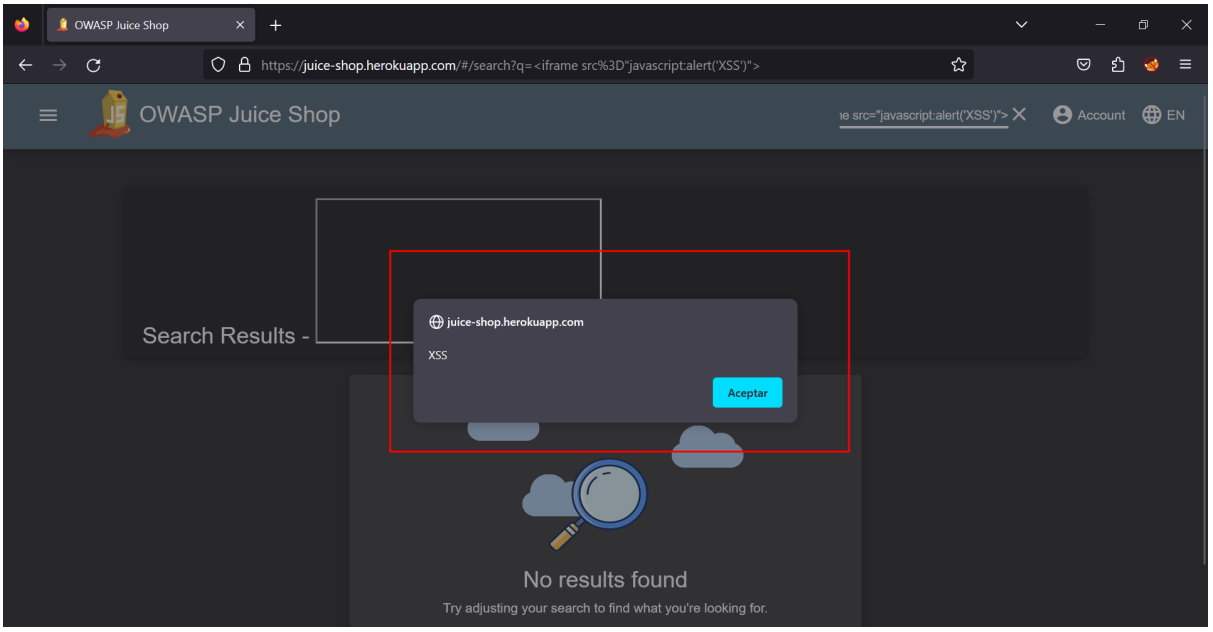
BlackDragons
Ejercicio de seguridad Aplicativa.

2. Cross-Site Scripting (XSS):

Si el script se ejecuta en la página, es posible que haya una vulnerabilidad XSS. encontramos que en el buscador se puede ingresar lo siguiente y ejecutar el código javaScript <iframe src="javascript:alert(`xss`)">



Al observar el mensaje de alerta confirmamos que la página es vulnerable a Cross-Site Scripting (XSS).



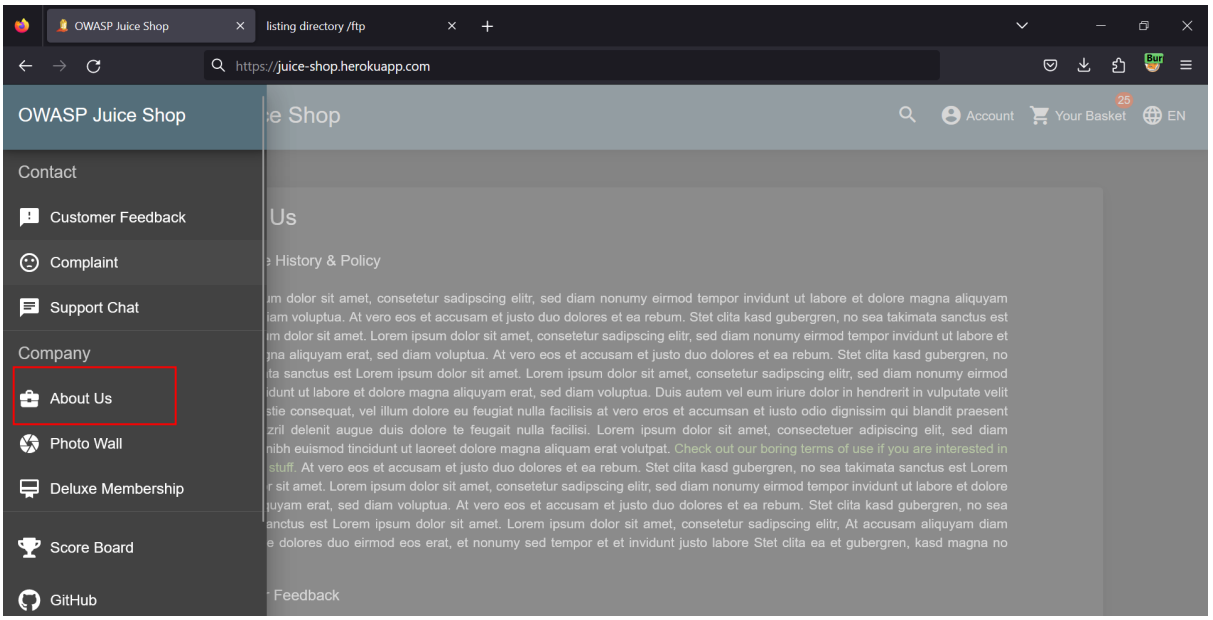
Mitigación:

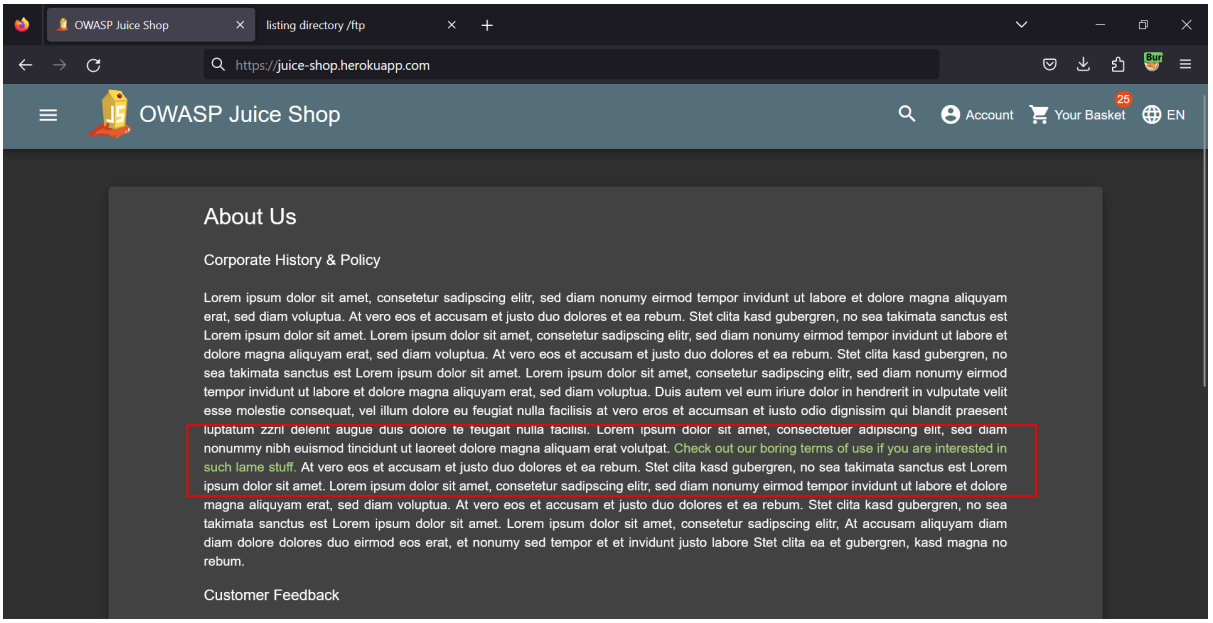
Es importante filtrar cualquier entrada que sea ingresada en campos de búsqueda, por lo cual se deberá sanitizar los caracteres especiales códificandolos para que no puedan ejecutarse scripts.

BlackDragons
Ejercicio de seguridad Aplicativa.

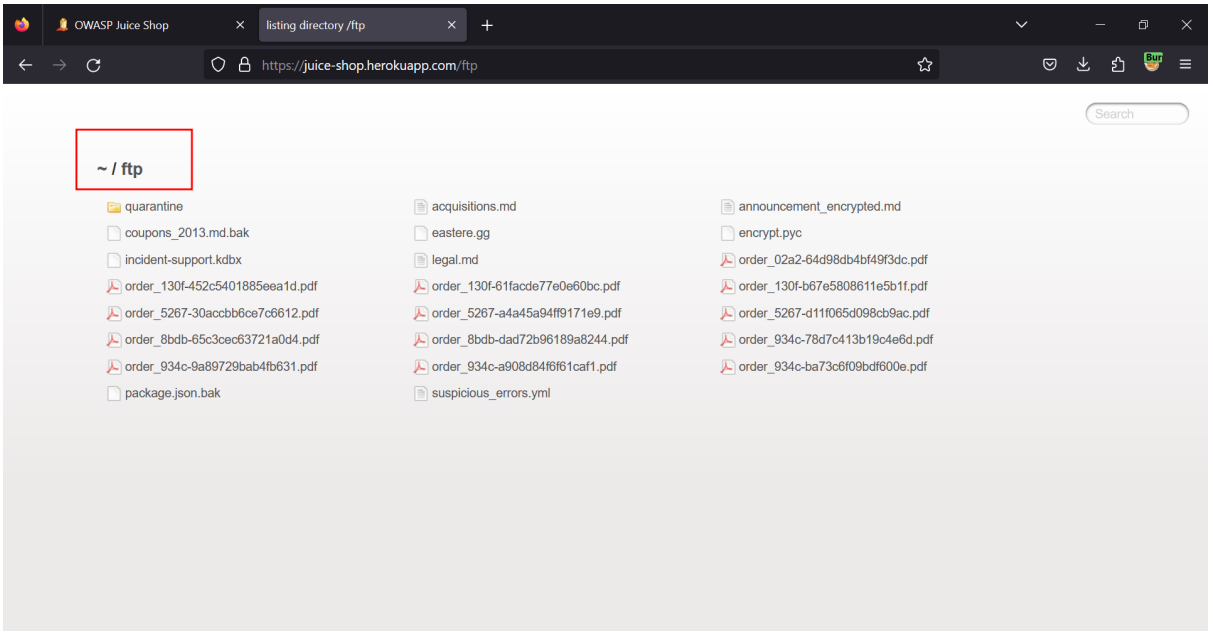
3. Vulnerabilidades de Acceso

Verifica que las áreas restringidas del sitio requieran autenticación adecuada y no permitan el acceso no autorizado.





BlackDragons
Ejercicio de seguridad Aplicativa.



directory listing tiene expuesta su carpeta ftp de transferencia de archivos en sus términos y condiciones de uso https://juice-shop.herokuapp.com/ftp/

Mitigación:

Para mitigar el acceso a recursos que deberían establecerse adecuadas políticas de y roles para acceder a los recursos y denegar el acceso a los recursos de manera predeterminada a menos que sean públicos.