## **RETO PROPUESTO**

Cada miembro del grupo resuelva un laboratorio diferente de Portswigger ya sea de SQL Injection y/o XSS (Cross-site scripting), adjuntar capturas de pantalla como evidencia de la resolución en el repositorio del coordinador en un directorio llamado RETO con subcarpetas nombradas con su NombreEstudiante\_ApellidoEstudiante.

#### **RETO #1 NIVEL APRENDIZ**

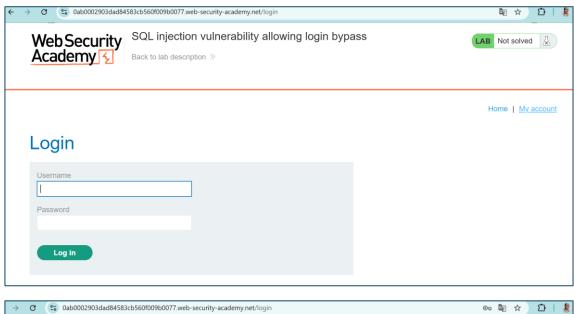
### Lab: SQL injection vulnerability allowing login bypass

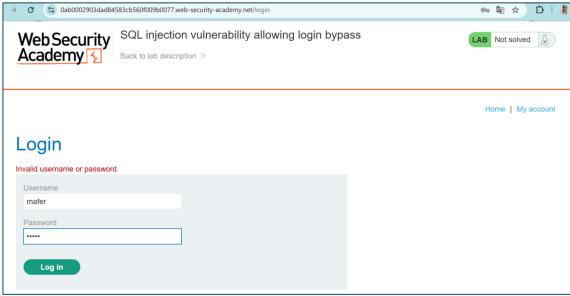
El objetivo de este laboratorio es encontrar la manera de autenticarse (iniciar sesión) usando el nombre de usuario "administrator", aprovechándose de una vulnerabilidad de inyección SQL existente en la función de inicio de sesión.

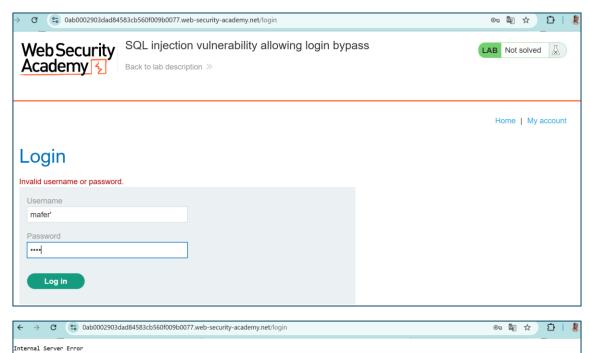


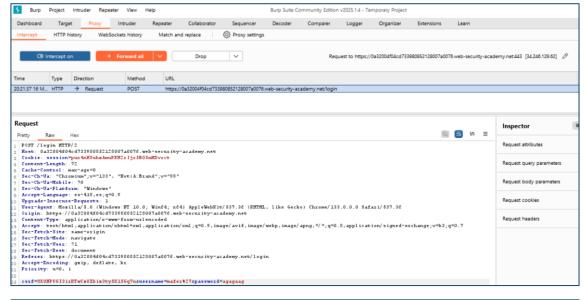


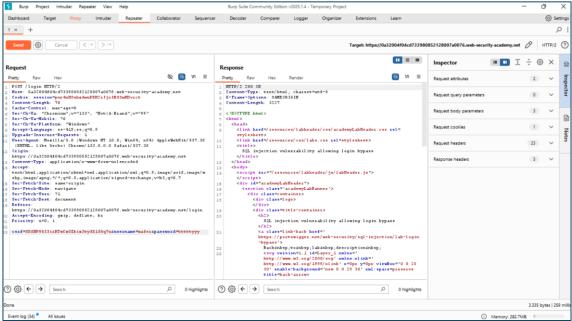
Nombre: María Fernanda Pacheco Grupo: 9

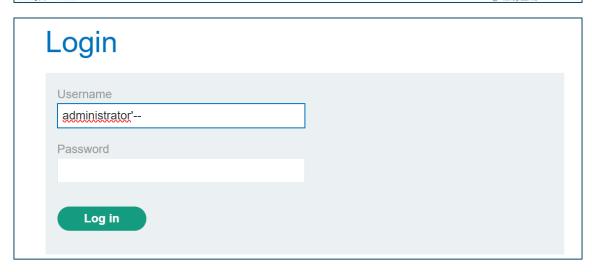


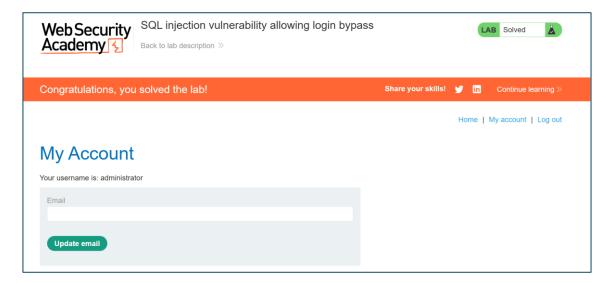




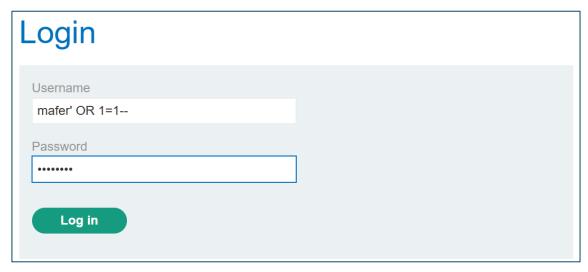


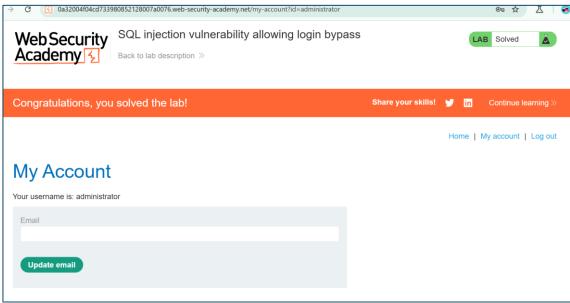






#### Otro método para bypassear el login:





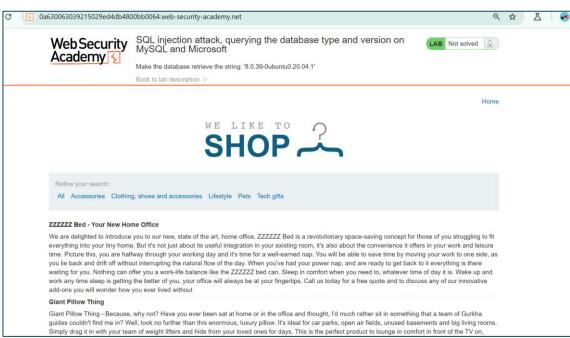
Nombre: María Fernanda Pacheco

#### **RETO #2 NIVEL FACULTATIVO**

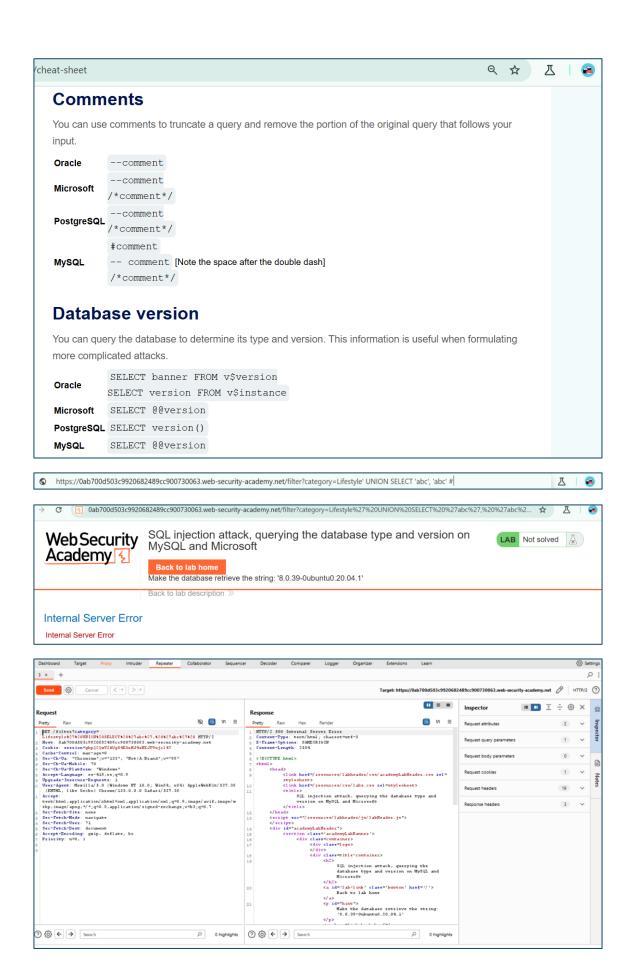
# Lab: SQL injection attack, querying the database type and version on MySQL and Microsoft

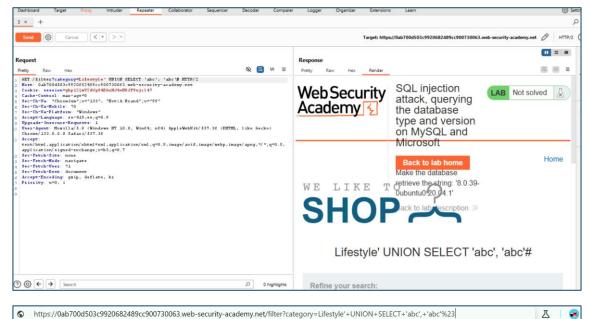
El objetivo de este laboratorio es usar un ataque UNION para recuperar todos los resultados de una consulta inyectada, ya que en este caso existe una vulnerabilidad de inyección SQL en el filtro de categoría de productos. Se debe averiguar el tipo y la versión de la base de datos en MySQL y Microsoft.

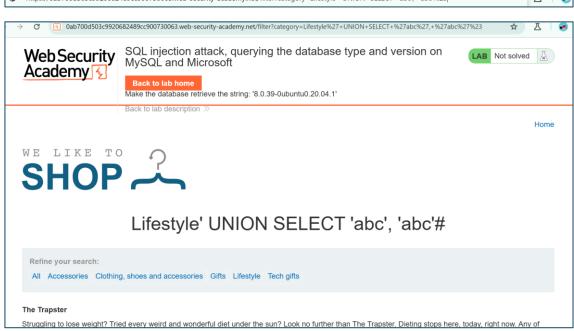


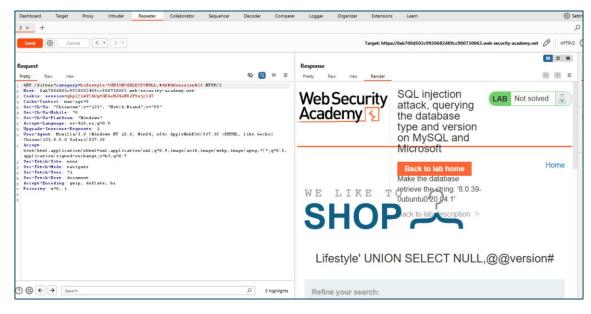


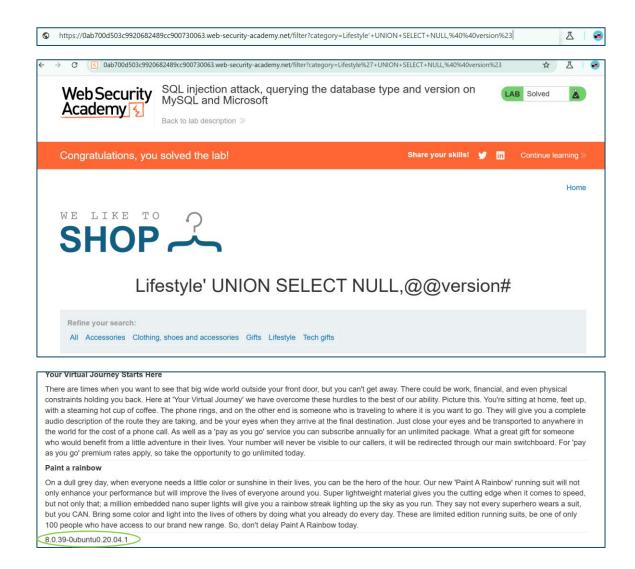
Nombre: María Fernanda Pacheco Grupo: 9











En ambos retos realizados se ha utilizado Burp Suite como herramienta esencial para interceptar el tráfico de las consultas y analizar las peticiones web. En la sección Repeater, se pueden realizar pruebas sobre los resultados de ejecutar diversas sentencias. Esta sección consta de dos áreas clave: Request y Response. En Request, podemos modificar el código de la consulta que estamos probando, mientras que en Response se mostrará el resultado de la ejecución de la misma.

Además, en la sección Response, existe una opción llamada Render, que permite ver una representación gráfica del resultado en la página web del laboratorio que estamos resolviendo, facilitando así la interpretación visual de la respuesta.