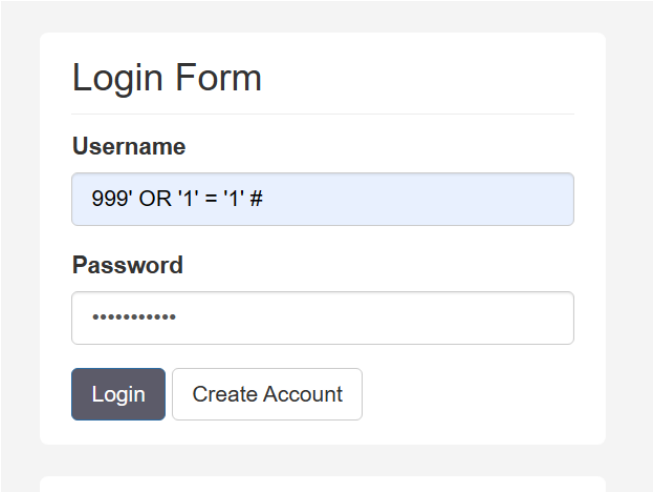
Puesta en producción segura

14 de noviembre de 2023

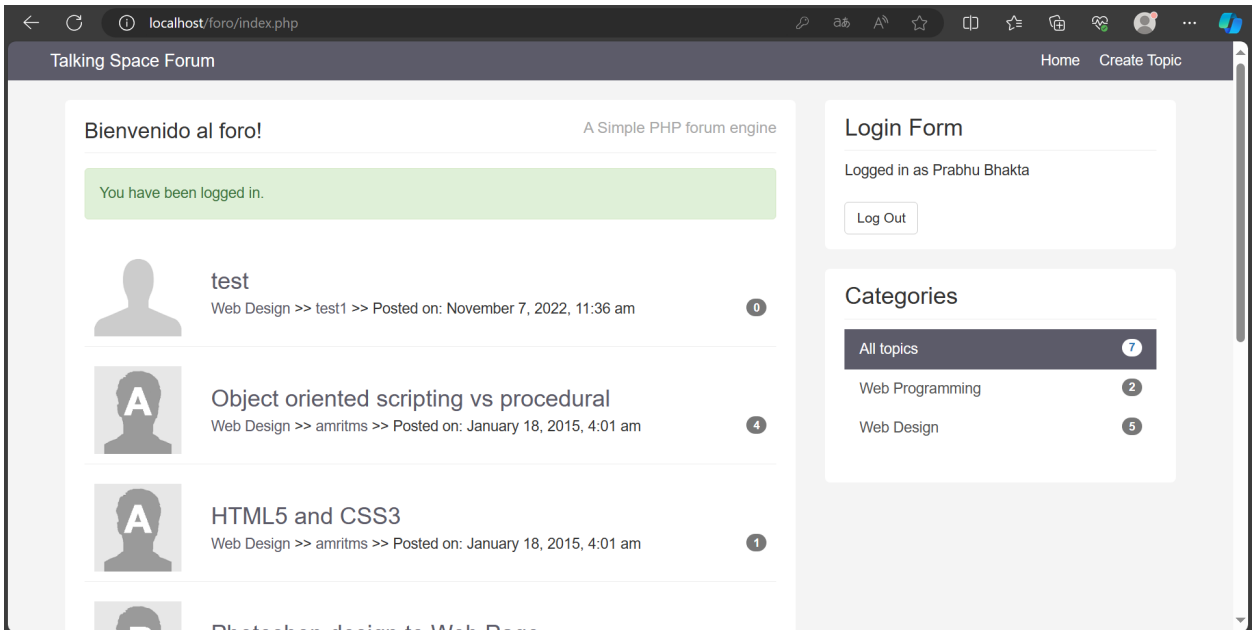
Práctica 2.2: Ataque en Login Foro

Jose Almirón Lopez

Comenzamos con un foro que presenta una vulnerabilidad en su sistema de inicio de sesión, permitiendo la ejecución de inyecciones SQL. Un ejemplo de esta amenaza es la consulta "**999' OR '1' = '1' #**", la cual ya examinamos en la práctica anterior.



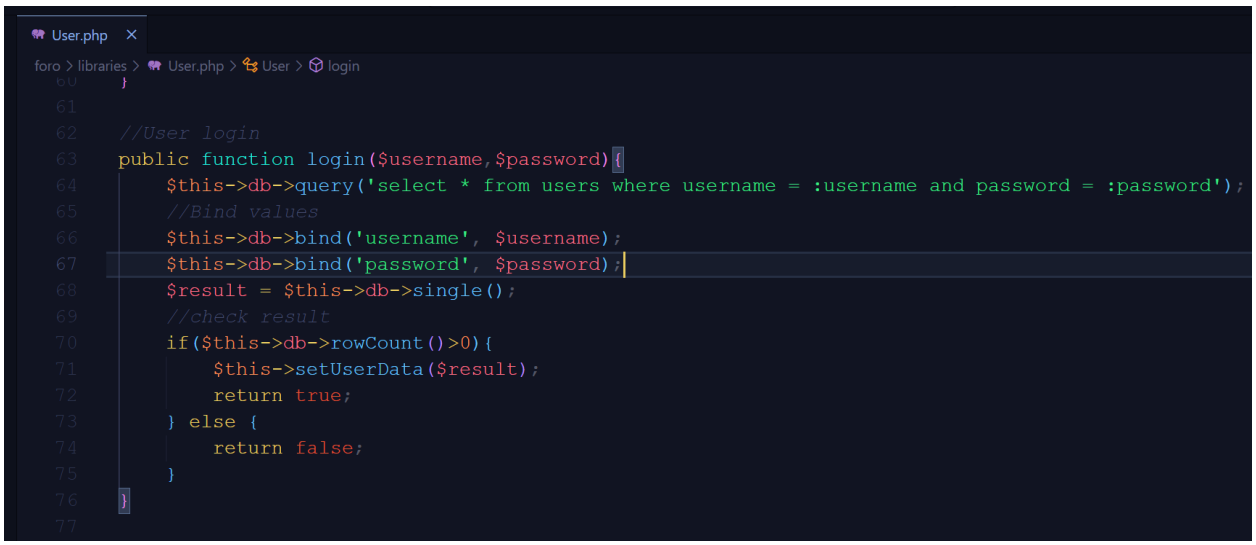
Con esta inyección SQL, podemos constatar que es posible acceder al foro al aprovechar la vulnerabilidad mencionada.



Al examinar el código proporcionado, podemos verificar que la vulnerabilidad está ubicada en la funcionalidad del inicio de sesión, específicamente en el archivo '**libraries/User.php**'. Al revisar la función de inicio de sesión, identificamos la consulta a la base de datos.

Con el fin de fortalecer la seguridad del código y prevenir inyecciones SQL, es esencial utilizar consultas preparadas en lugar de concatenar directamente los valores en la consulta SQL.

- He sustituido los valores directos en la consulta SQL mediante el uso de marcadores de posición (:username y :password).
- He empleado el método bind para vincular los valores reales a los marcadores de posición, asegurando así que los valores se escapen de manera adecuada y evitando la posibilidad de inyecciones SQL.



De esta manera, ya no es posible acceder al foro explotando la vulnerabilidad de inyecciones SQL.