Equipo EABmodel

Miguel Salomón

Axel Aramis

Jesús Olmos

Actividad 2: Re-test Altoro

1- Vulnerabilidad XSS (Cross site scripting) en la barra de búsqueda, se logro explotar de la misma manera, colocando:

   <script>alert("hola")</script>

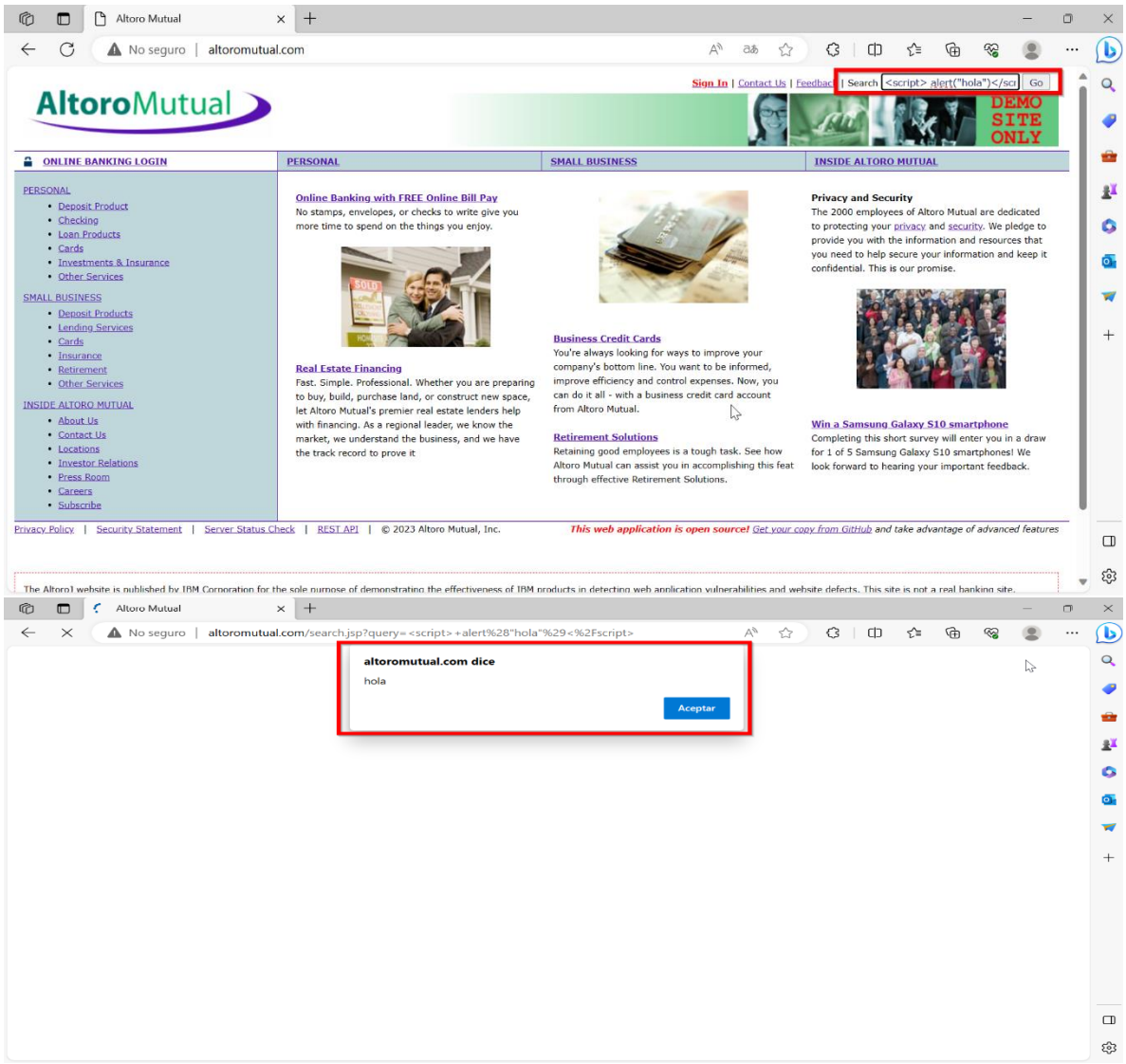
   XSS:

   Cross-Site Scripting (XSS) es una vulnerabilidad de seguridad en aplicaciones web que permite a un atacante inyectar scripts maliciosos en páginas web visitadas por otros usuarios. Estos scripts se ejecutan en el navegador de la víctima, lo que puede llevar a robo de datos, secuestro de sesiones o redirección a sitios web fraudulentos. Para prevenir XSS, las aplicaciones web deben validar y escapar adecuadamente todas las entradas del usuario y utilizar encabezados de seguridad HTTP como Content Security Policy (CSP).

   ¿Cómo mitigar XSS dentro de la URL?

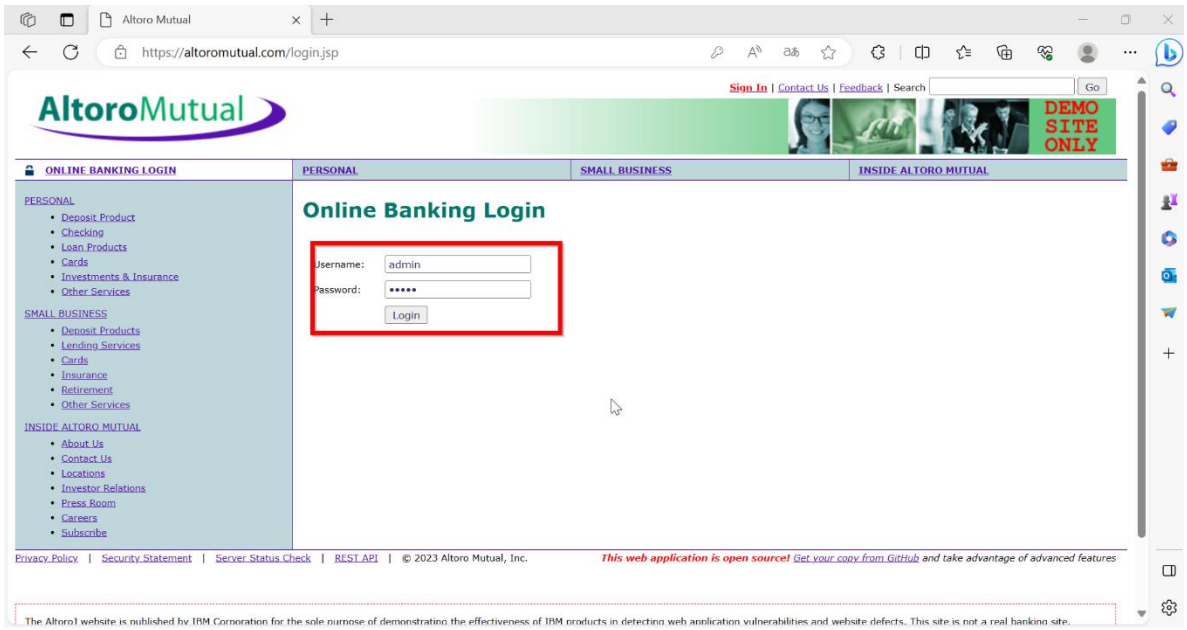
   Haciendo una comprobación de caracteres introducidos en la URL antes de ejecutar cualquier código.

   En este caso se espera un texto en la URL, por lo que no deberían permitirse caracteres tipo comillas dobles, comillas simples, símbolos de menor, mayor, más, menos, igual, punto y coma, paréntesis, corchetes, llaves, barras y contrabarras, no permitir palabras clave como: “script”, “php”, “javascript”, “css”, …, ni códigos escapados del tipo > (para símbolo >), < (para símbolo menor).



2- Tiene credenciales por defecto:
Las "credenciales por defecto" se refieren a las combinaciones de nombre de usuario y contraseña predeterminadas que se utilizan en dispositivos, sistemas o aplicaciones cuando se instalan por primera vez o se entregan al usuario. Estas credenciales están preconfiguradas por el fabricante o el proveedor de servicios para facilitar la configuración inicial del sistema

¿Cómo mitigar tener credenciales por defecto no configuradas?
Establezca y use un ciclo de desarrollo seguro apoyado en Profesionales en Seguridad de Aplicaciones para ayudarlo a evaluar y diseñar la seguridad y controles relacionados con la privacidad.
Integre el lenguaje y los controles de seguridad en las historias de usuario.
Integre verificaciones de viabilidad en cada capa de su aplicación (desde el frontend al backend).



3- Se sigue efectuando sql inyection en login:
SQL:

Una SQL Injection (Inyección SQL) es un tipo de ataque informático que se produce cuando un atacante manipula maliciosamente las entradas de un formulario o de una aplicación web para introducir código SQL no deseado en una consulta SQL. El objetivo de este ataque es comprometer la seguridad de la base de datos subyacente y acceder, modificar o eliminar datos de la misma, o incluso tomar el control del sistema.

¿Cómo mitigar ataques de inyección por SQL?

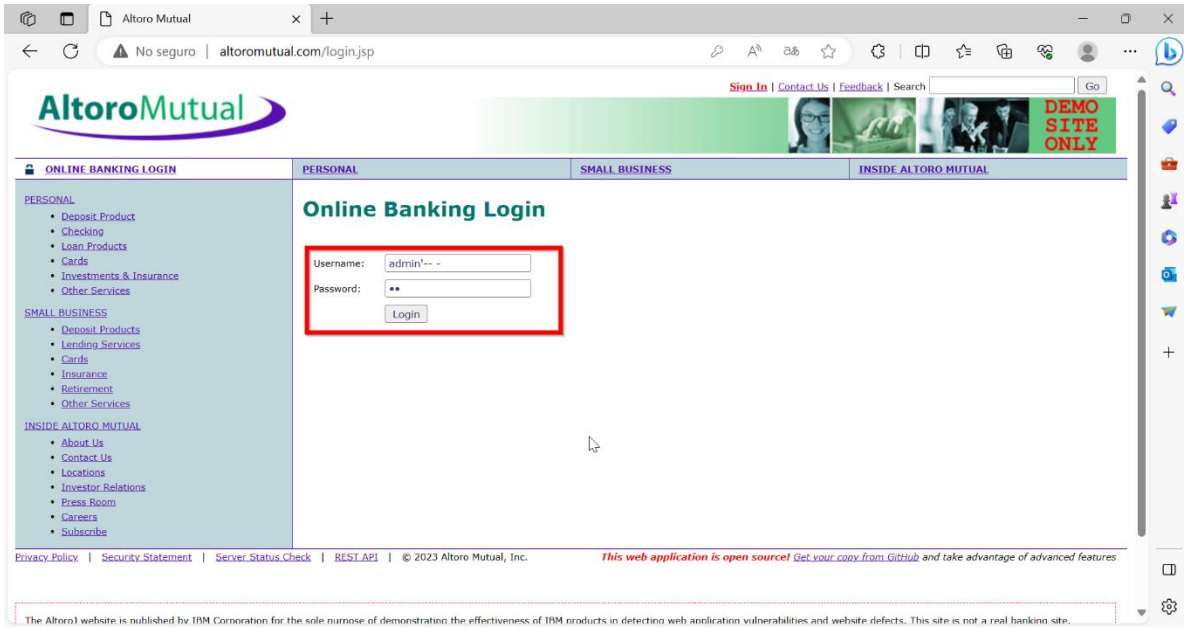
Enfoque de confianza 0

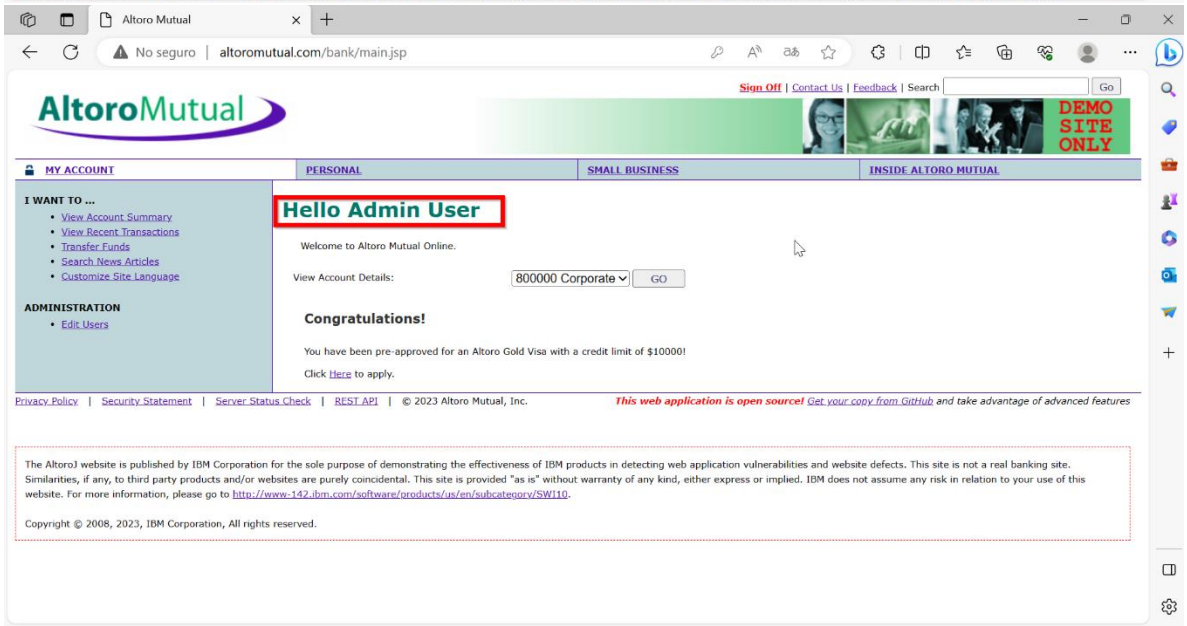
Limitar privilegios

Utilizar procedimientos almacenados

Utilizar consultas parametrizadas

Seguridad multicapa





4- El IDOR sigue presente el apartado bank account: Ya que podemos cambiar el valor del parámetro y ver la historial de otro usuario entonces se hace un Brocken Access control.

IDOR:

IDOR, o Insecure Direct Object Reference, es una vulnerabilidad de seguridad en aplicaciones web que permite a un atacante acceder a recursos o datos no autorizados al manipular las referencias a objetos directos, como archivos, bases de datos o registros, a través de la modificación de parámetros en una solicitud HTTP. En otras palabras, un atacante puede explotar una IDOR para obtener acceso a datos o funcionalidades que normalmente no debería tener permiso de acceder.

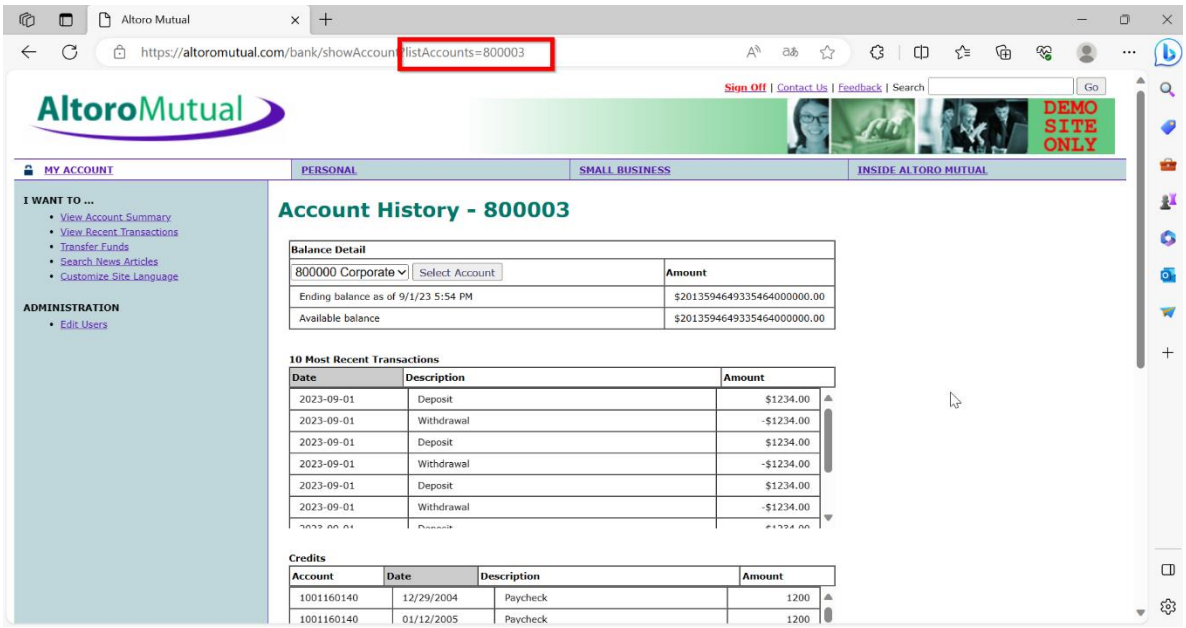
La vulnerabilidad IDOR suele ocurrir cuando una aplicación web no valida adecuadamente las solicitudes del usuario o no implementa una autenticación y autorización sólidas. Para prevenir esta vulnerabilidad, es esencial implementar un control de acceso adecuado y garantizar que los objetos a los que se hace referencia se autoricen correctamente antes de proporcionar acceso.

¿Cómo mitigar IDOR?

En el inicio de sesión debes implementar un sistema de cookies y crear las variables de la sesión.

Se debe cambiar el elemento afectado por la vulnerabilidad, cambiando el origen del parámetro para que no lo tome de una entrada proveniente del usuario, sino que recupere el valor del parámetro de la sesión actual.

Evitar mostrar referencias a objetos privados como claves o nombres de archivos.
Verificar que el acceso a los recursos mediante IDs, tenga un paso de verificación adicional para asegurar que el usuario tenga la autorización adecuada.
Asegúrate de que las consultas estén dirigidas al propietario del recurso, esto puede lograrse con la correcta implementación de mecanismos de control de acceso.
Analiza todos los objetos referenciados.

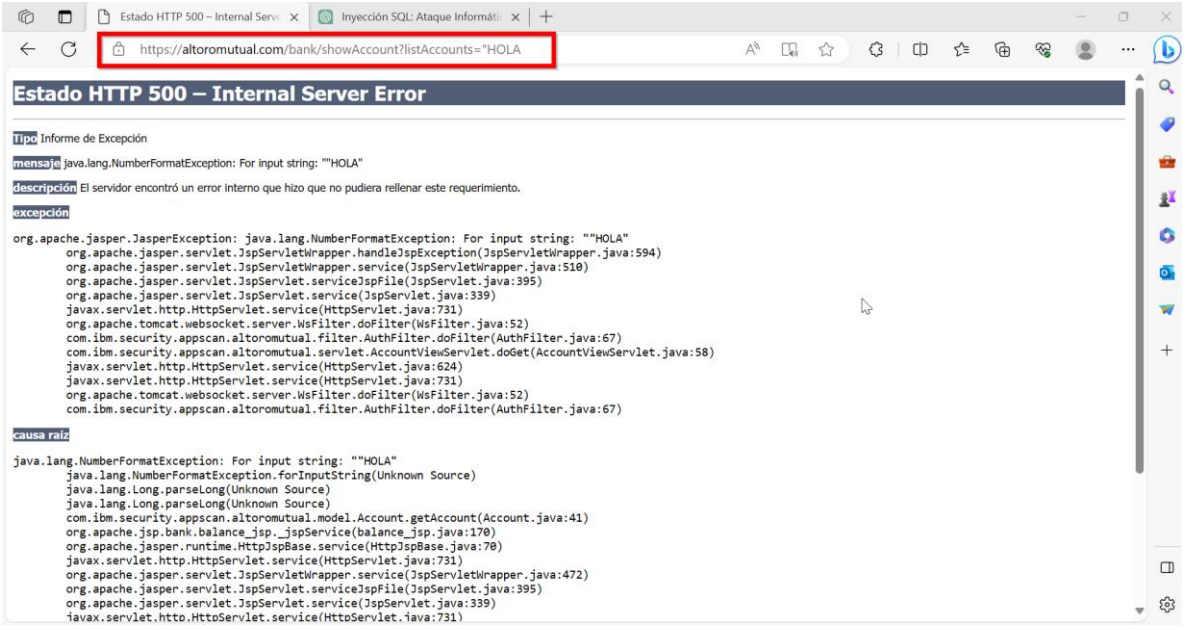


5- External Error 500: Se obtuvo al introducir la palabra hola en el url reemplazando el 8000, transformando un numero entero a string.
External Server Error" (Error de servidor externo) es un término que se utiliza para describir una situación en la que un servidor web o una aplicación web encuentra un problema al intentar comunicarse o interactuar con otro servidor o recurso externo en la red, como una base de datos remota, un servicio web de terceros o cualquier otro sistema alojado en otro lugar.

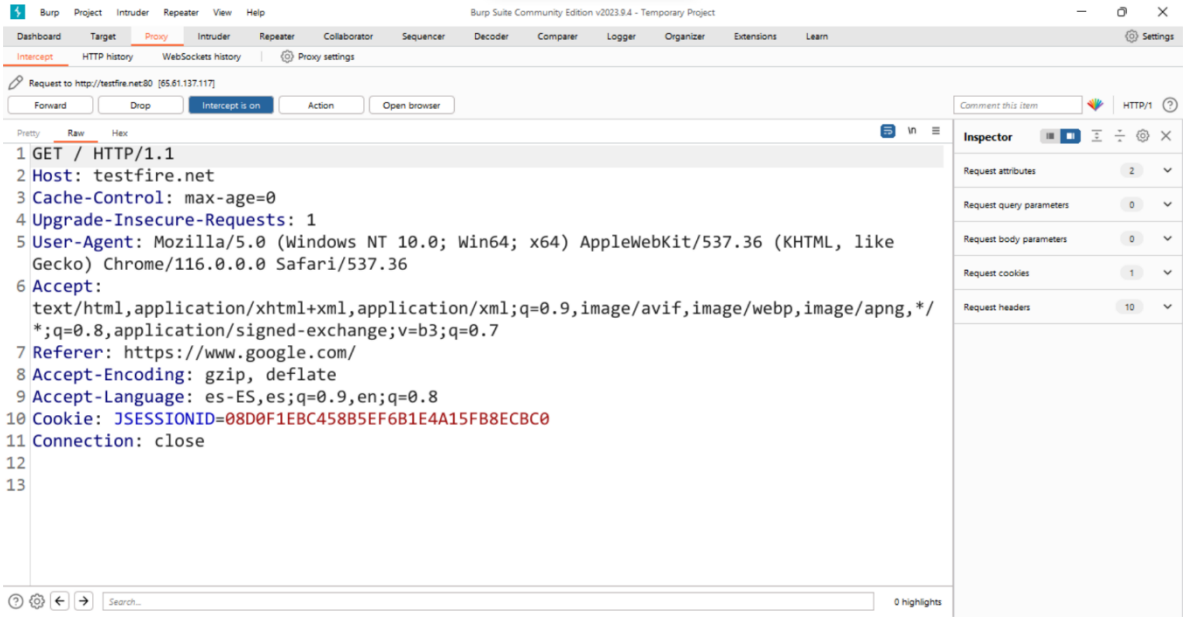
Estos errores pueden ocurrir por diversas razones, como problemas de conectividad, tiempo de espera agotado, falta de autenticación o autorización adecuada para acceder al servidor externo, o problemas en el propio servidor externo. Cuando un servidor web encuentra un "External Server Error", generalmente significa que no puede completar una solicitud o acción porque el recurso externo necesario no está respondiendo o funcionando correctamente.

¿Cómo mitigar errores de tipo External Server Error?

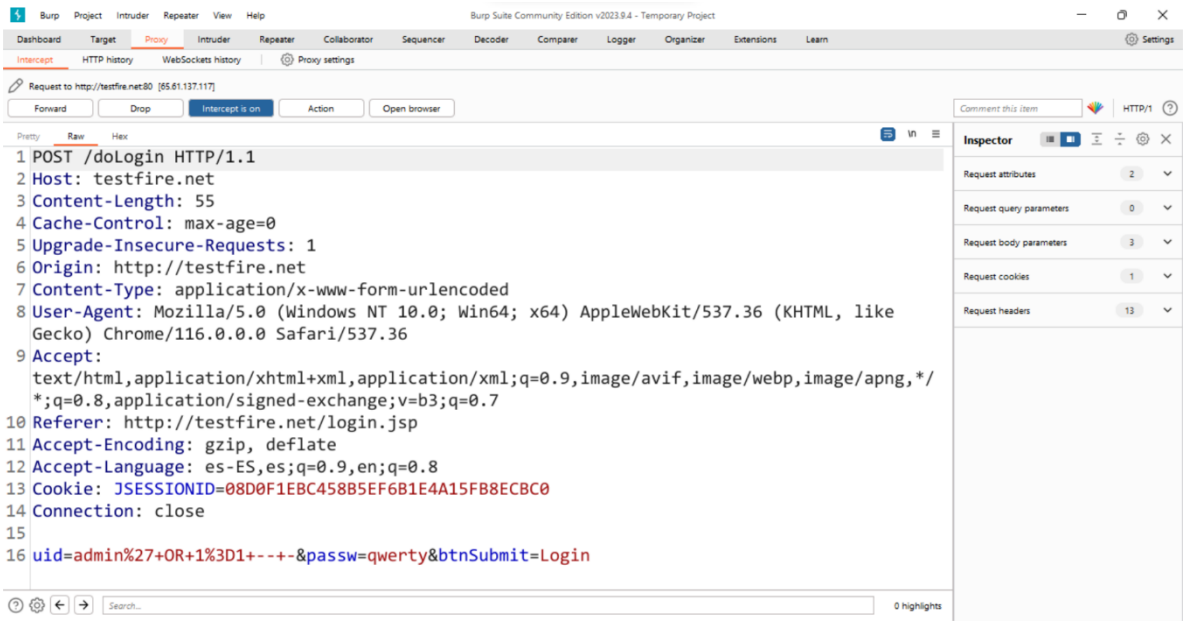
Si el error 500 está relacionado con un plugin o tema específico, puedes intentar desactivarlos para ver si eso resuelve el problema.
Si el problema es que el servidor no tiene suficientes recursos para manejar las solicitudes del sitio web, puedes intentar aumentar la cantidad de recursos disponibles para ver si eso lo soluciona.
Si se debe a un problema en el código de tu sitio web, puedes intentar corregir el código para solucionar el problema, o en último caso desactivarlo para ver si el sitio vuelve a funcionar y entonces eliminar o sustituir el código que lo provoca.
Intentar restaurar una copia de seguridad anterior de tu web para ver si tu sitio se recupera del error.



Burp: Por medio de Burp, pudimos capturar la petición que se le hace al sitio Altoro la cual se ve de la siguiente forma:



Por otra parte aquí se muestra el ataque de tipo inyección atravez de burp:



Así se ve durante el ingreso del payload y esta es la response de Altoro tras la ejecución del payload: