Integrantes:

- Yutsent Rios Velazquez
- García Delgado Ian Ricardo
- Mario Eduardo Quiroga Bernal

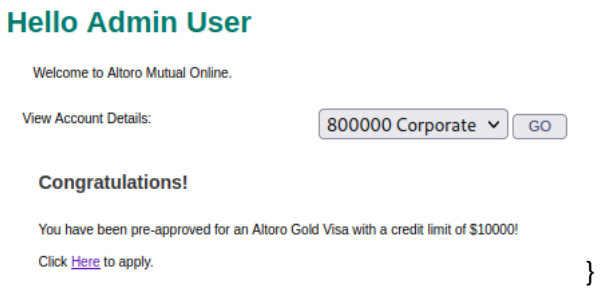
Default credentials

Se ingreso a la página http://testfire.net/, posteriormente accedimos al login (http://testfire.net/login.jsp), donde se introdujeron las credenciales por defecto:

Username: admin

Password: admin

Obteniendo así al dashboard de admin



}

Cross Site Scripting (XSS)

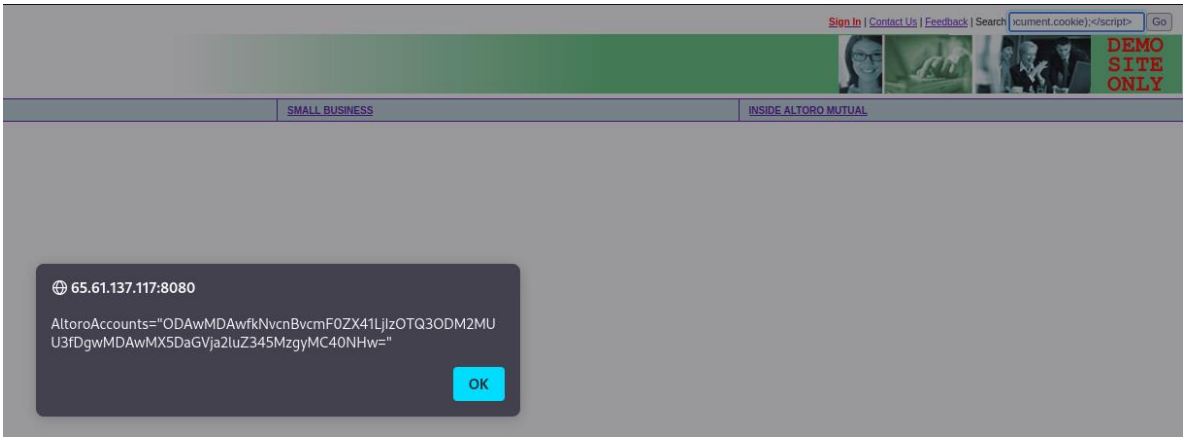
Se ingreso a la pagina principal y se ingresó en el buscador el script:

<script>alert ("Hola mundo");</script>

Esto muestra una alerta, lo que demuestra que se puede inyectar código en el lado del cliente.

De igual forma, se utilizó el script:

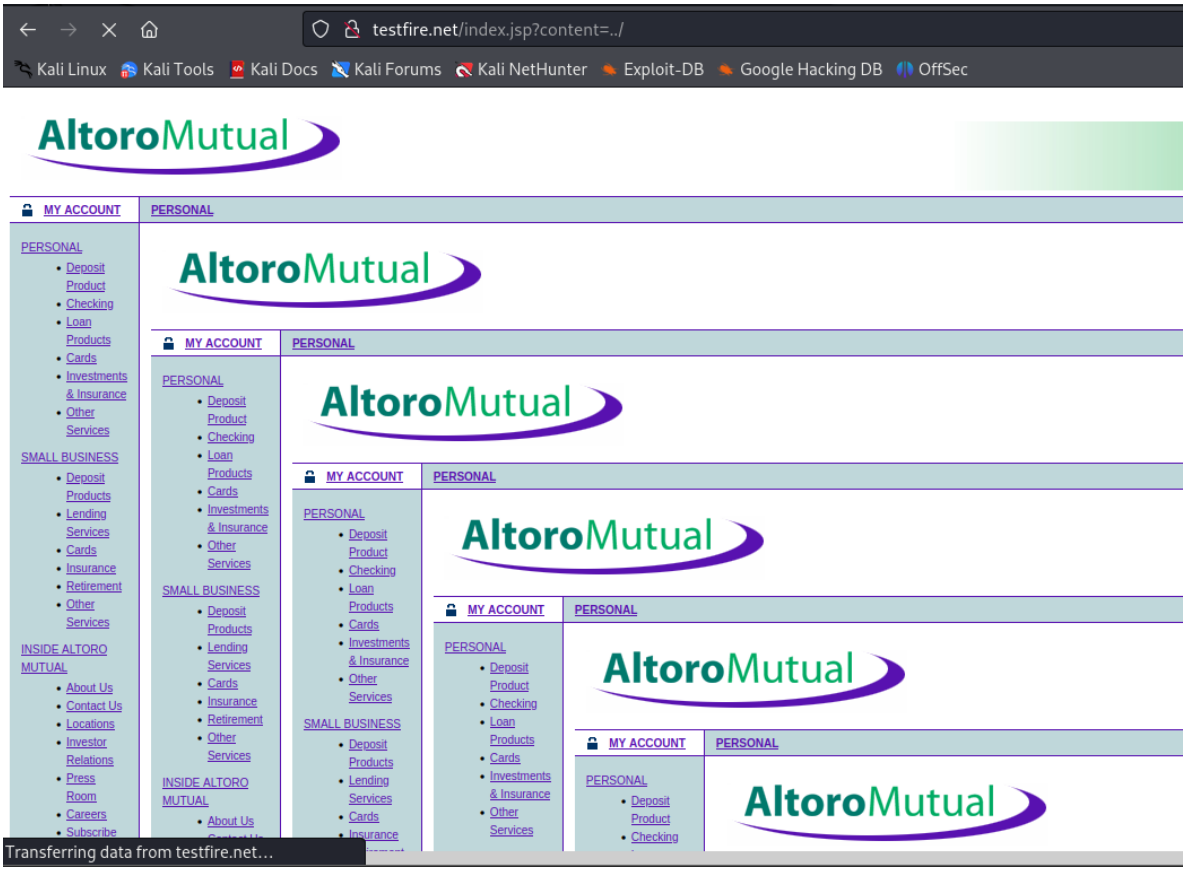
<script>alert (document.cookie);</script>



Esto nos permite ver las cookies del usuario activo en ese momento.

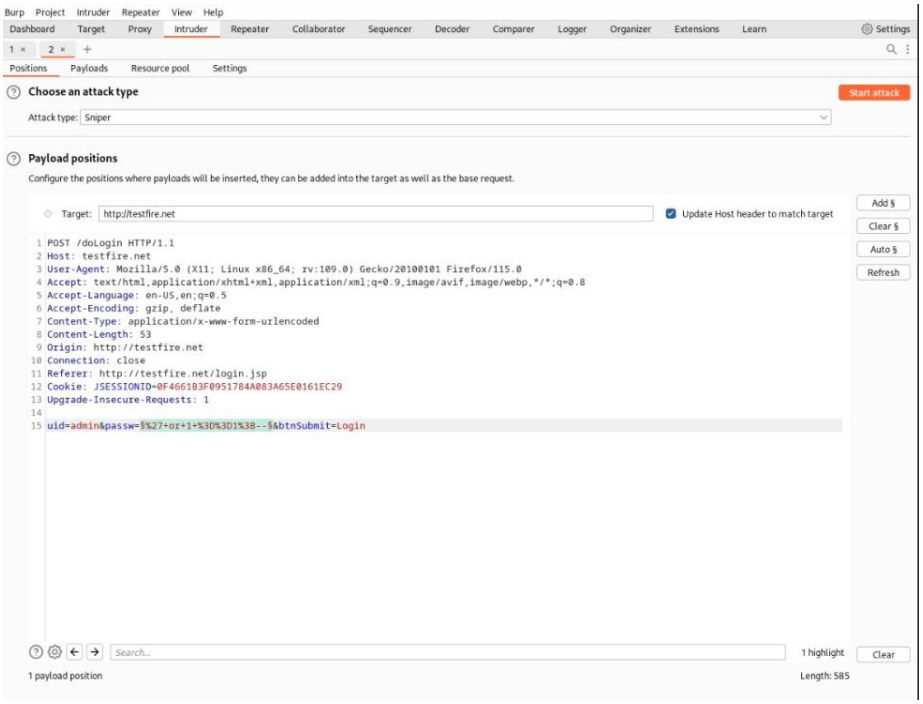
Local File Inclusion (LFI)

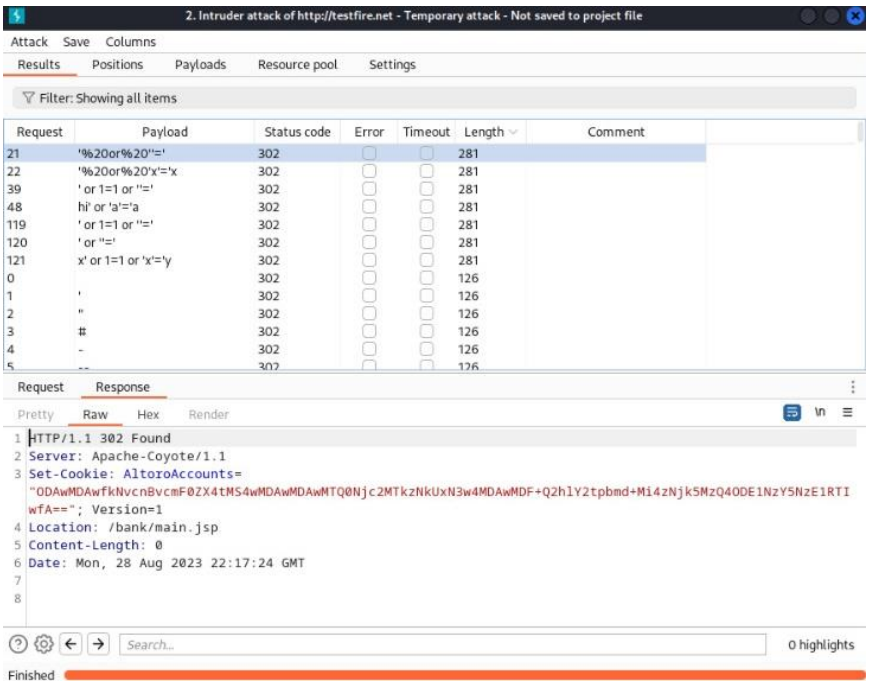
Se utiliza un directory path trasversal para acceder a directorios que se encuentren anteriores al directorio del servidor web, por lo que se acceden a archivos a los que no se debería poder.



SQL injection

Se utilizó el proxy Burp Suite para interceptar las peticiones que se realizan al servidor. Se intercepta la petición de la página login, en donde se especifica tanto el usuario como la contraseña que el usuario ingreso anteriormente. Posteriormente se utiliza el intruder con una lista de payloads comunes para SQLi y se determinan 7 inyecciones exitosas.





Insecure Direct Object Reference (IDOR)

Teniendo acceso al usuario administrador, se visitó el apartado transfer. Donde te daba la opción de hacer una transferencia entre dos cuentas. Si se hace el intento de ingresar la misma cuenta, la página muestra un error que comenta que la cuenta no puede ser la misma. Sin embargo, al interceptar la petición con Burp Suite, es posible transferir entre la misma cuenta.