

Reporte de Ciberseguridad – *Altoro Mutual*
Consultora: Los Chilaquiles



Los
Chilaquiles

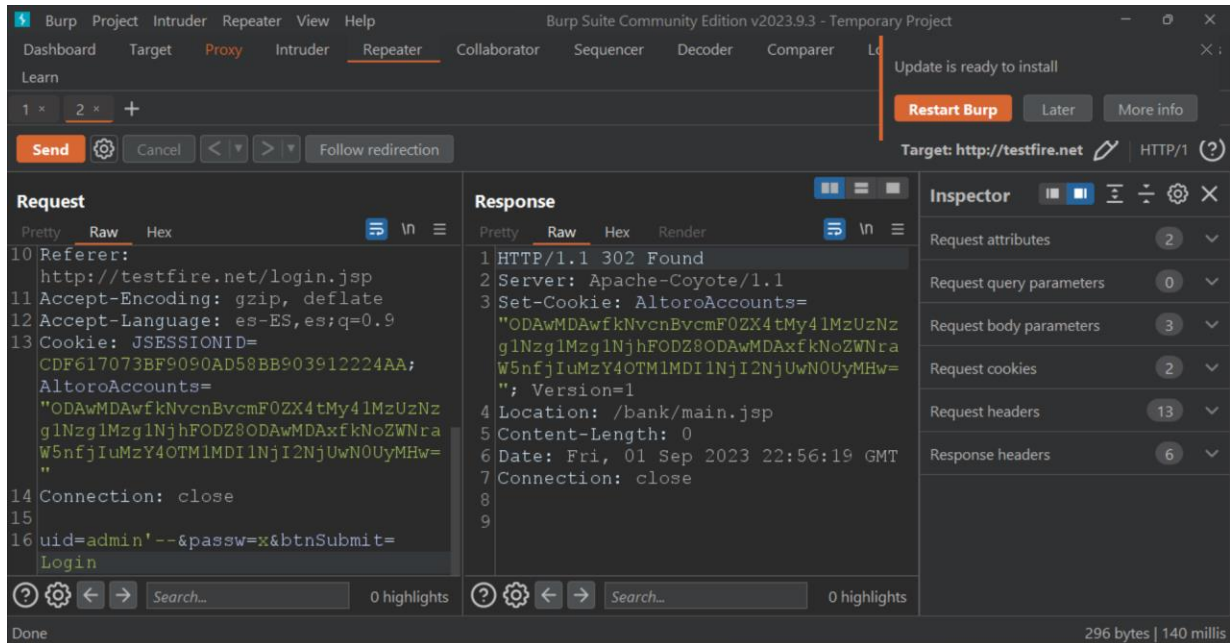
- Chávez Sánchez Juan Daniel
- Nabor Lira Iván Damián
- Piedras Cruz Felipe de Jesús
- Venegas Barrita Edgar

Ciudad de México, 1 de septiembre de 2023

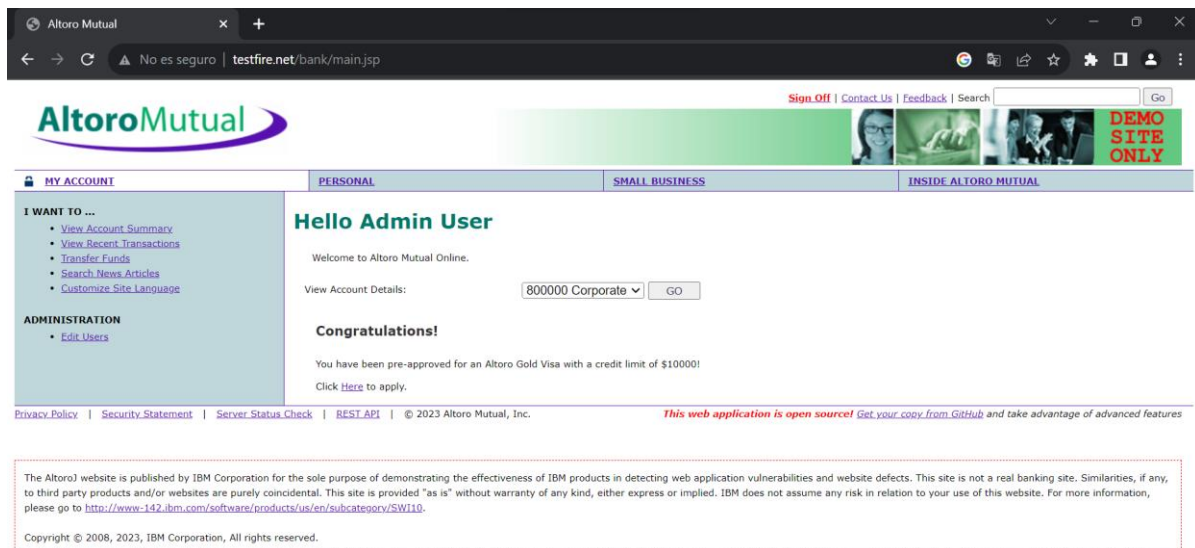
Vulnerabilidades:

SQL Injection

Se usó el payload **admin'--** para poder acceder como administrador a la página AltoroMutual.

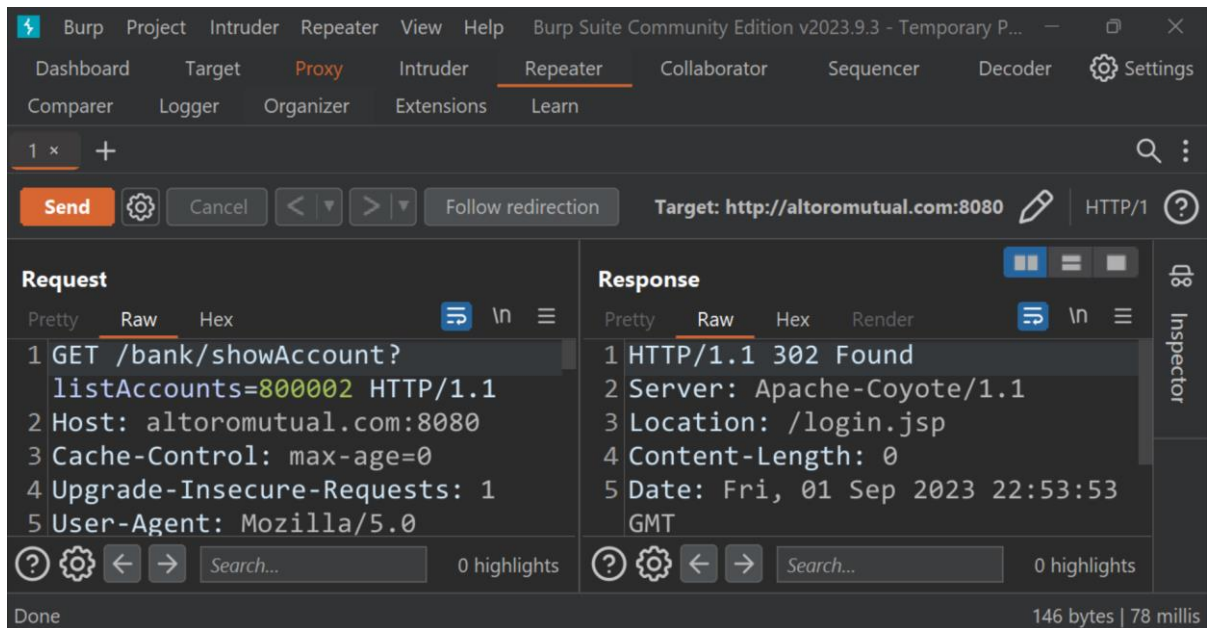


Obtenemos acceso como Admin y nos muestra que tenemos un crédito aprobado, lo cual es una vulnerabilidad preocupante.

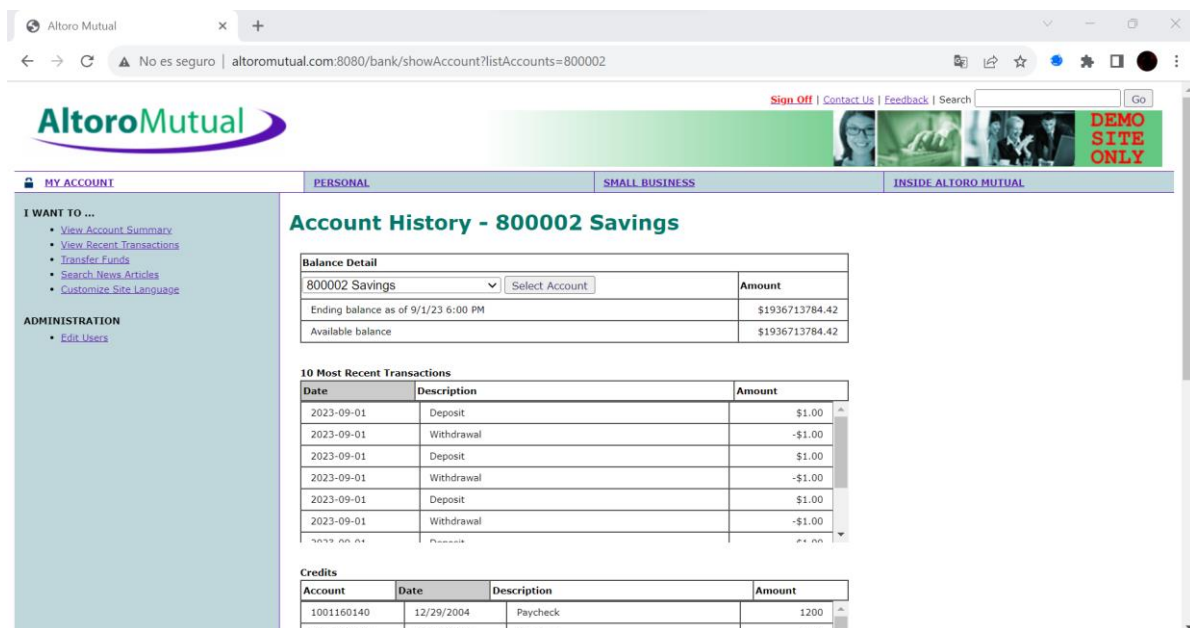


IDOR Insecure Direct Object Reference

Se modifico el parámetro listAccounts colocando un número diferente y permitió acceder a los datos de otro usuario



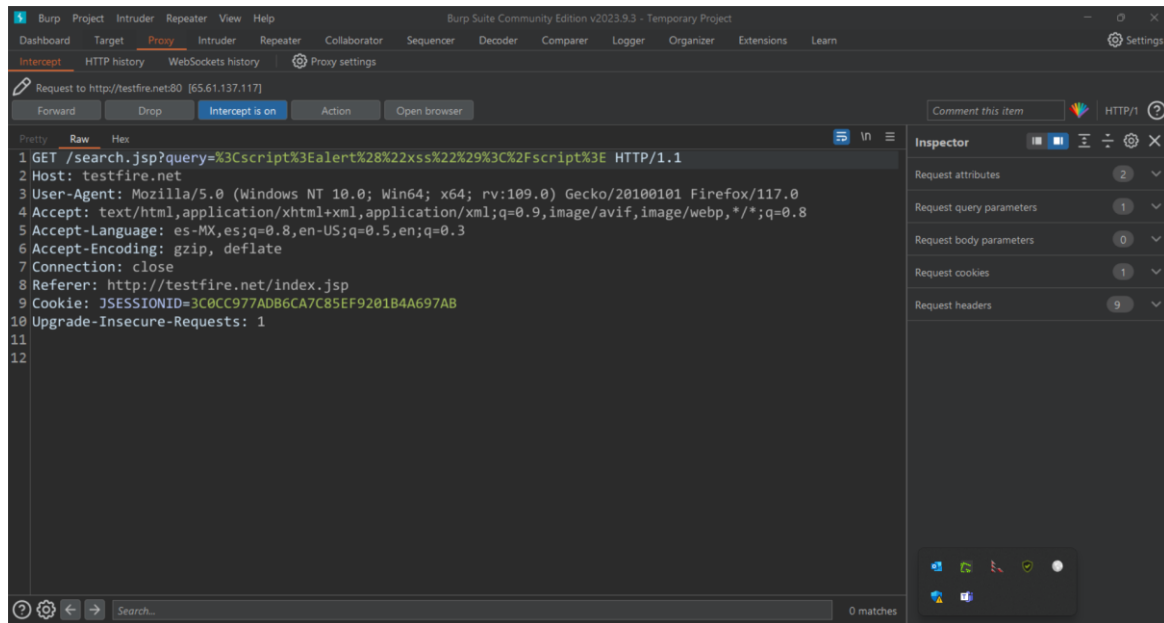
Aquí podemos observar cómo nos muestra información confidencial, en este caso el historial de cuenta del usuario.



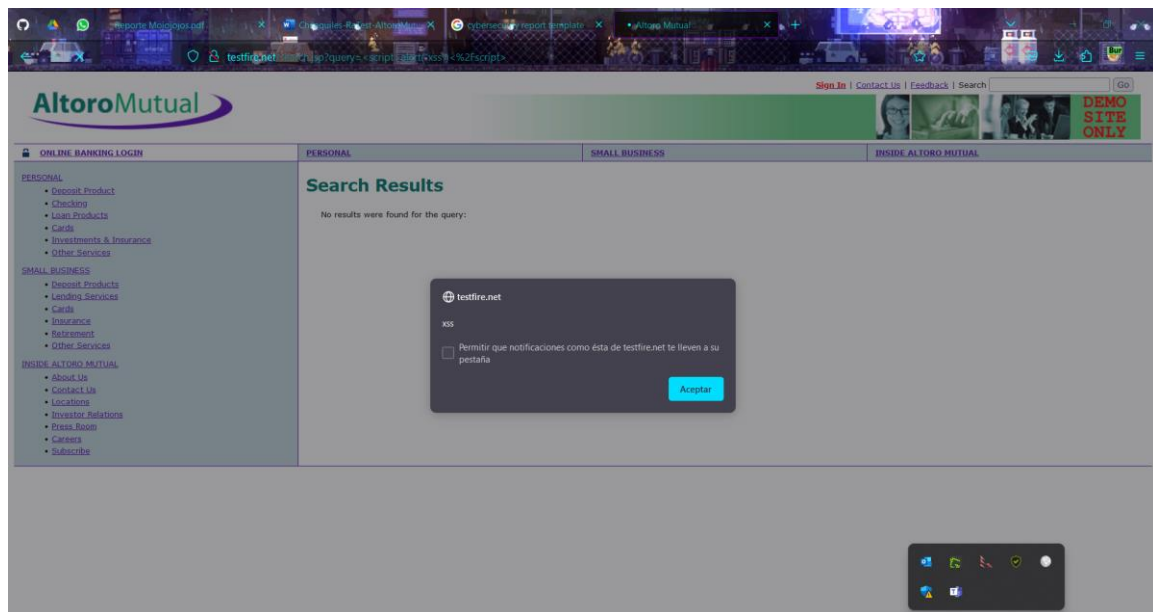
XSS:

El portal del banco Altoro Mutual tiene la capacidad de poder interpretar código Javascript dentro de su campo de búsqueda, para ejemplificar esto, se utilizó la sentencia ejecutada exitosamente:

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



La respuesta en el navegador se muestra en la siguiente captura de pantalla:



Misconfiguration (Insecure Error handling)

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

The screenshot shows the AltoroMutual website interface. The browser address bar displays "testfire.net/bank/transaction.jsp". The website has a navigation bar with links like "Sign Off", "Contact Us", "Feedback", and "Search". Below the navigation bar, there are tabs for "MY ACCOUNT", "PERSONAL", "SMALL BUSINESS", and "INSIDE ALTORO MUTUAL". The "MY ACCOUNT" tab is selected, and the "Recent Transactions" section is visible. The "Recent Transactions" table lists various transactions with columns for Transaction ID, Transaction Time, Account ID, Action, and Amount. The table shows a mix of deposits and withdrawals. The error message "No es seguro" is visible in the browser's address bar.

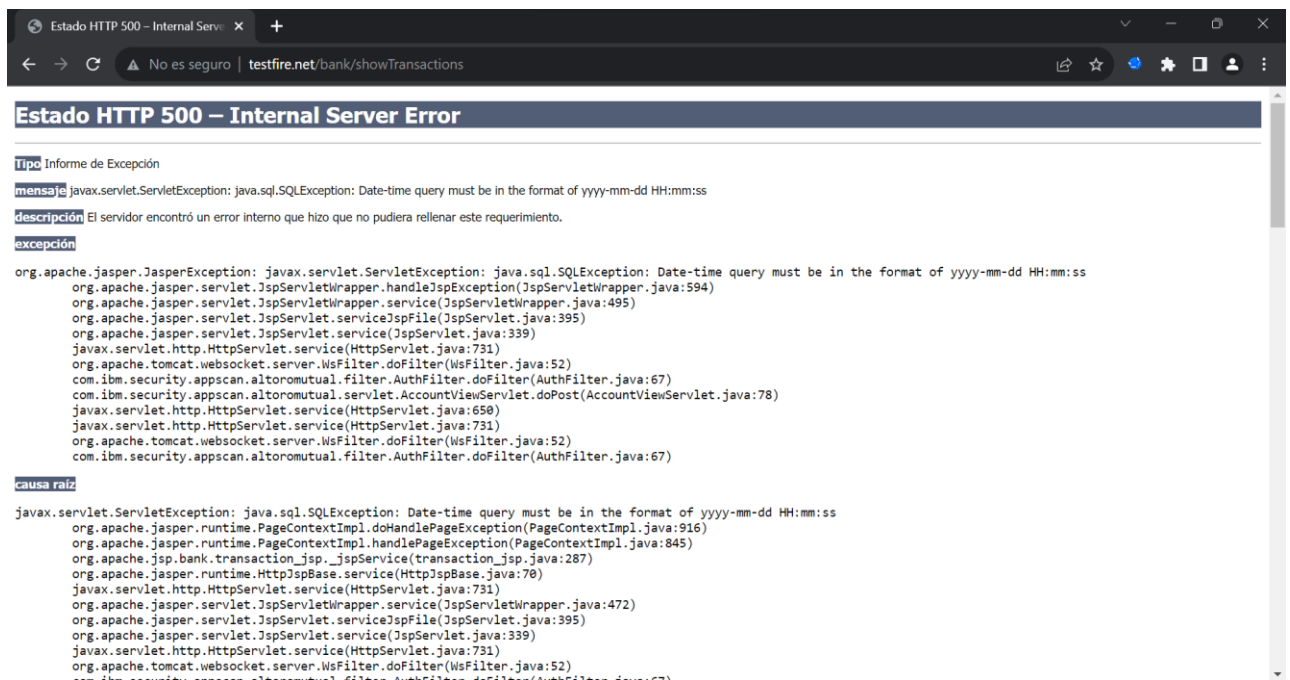
Transaction ID	Transaction Time	Account ID	Action	Amount
23162	2023-09-01 17:59	800001	Withdrawal	-\$1000000.00
22255	2023-09-01 16:30	800001	Deposit	\$999999999999.00
22254	2023-09-01 16:30	800000	Withdrawal	-\$999999999999.00
21707	2023-09-01 16:01	800000	Deposit	\$7.00
21706	2023-09-01 16:01	800001	Withdrawal	-\$7.00
21704	2023-09-01 16:01	800000	Withdrawal	-\$38388393.00
21595	2023-09-01 13:59	800001	Deposit	\$4444.00
21594	2023-09-01 13:59	800000	Withdrawal	-\$4444.00
21471	2023-09-01 13:45	800001	Deposit	\$10.00
21470	2023-09-01 13:45	800000	Withdrawal	-\$10.00
20649	2023-09-01 12:46	800001	Deposit	\$190.00
20648	2023-09-01 12:46	800000	Withdrawal	-\$190.00
20647	2023-09-01 12:45	800001	Deposit	\$150.00
20646	2023-09-01 12:45	800000	Withdrawal	-\$150.00
20645	2023-09-01 12:45	800001	Deposit	\$150.00

Al interceptar la petición con BurpSuite podemos ver como se manda la fecha.

The screenshot shows the Burp Suite interface with the "Intercept" tab selected. The "Request to http://testfire.net:80 [65.61.137.117]" is displayed. The "Intercept is on" button is highlighted. The "Raw" tab is selected, showing the raw HTTP request. The request is an "Accept:" request with various headers and a body. The body contains a date range: "startDate=2001-04-17a&endDate=2001-04-19a". The "Inspector" panel on the right shows the request details, including request attributes, query parameters, body parameters, cookies, and headers.

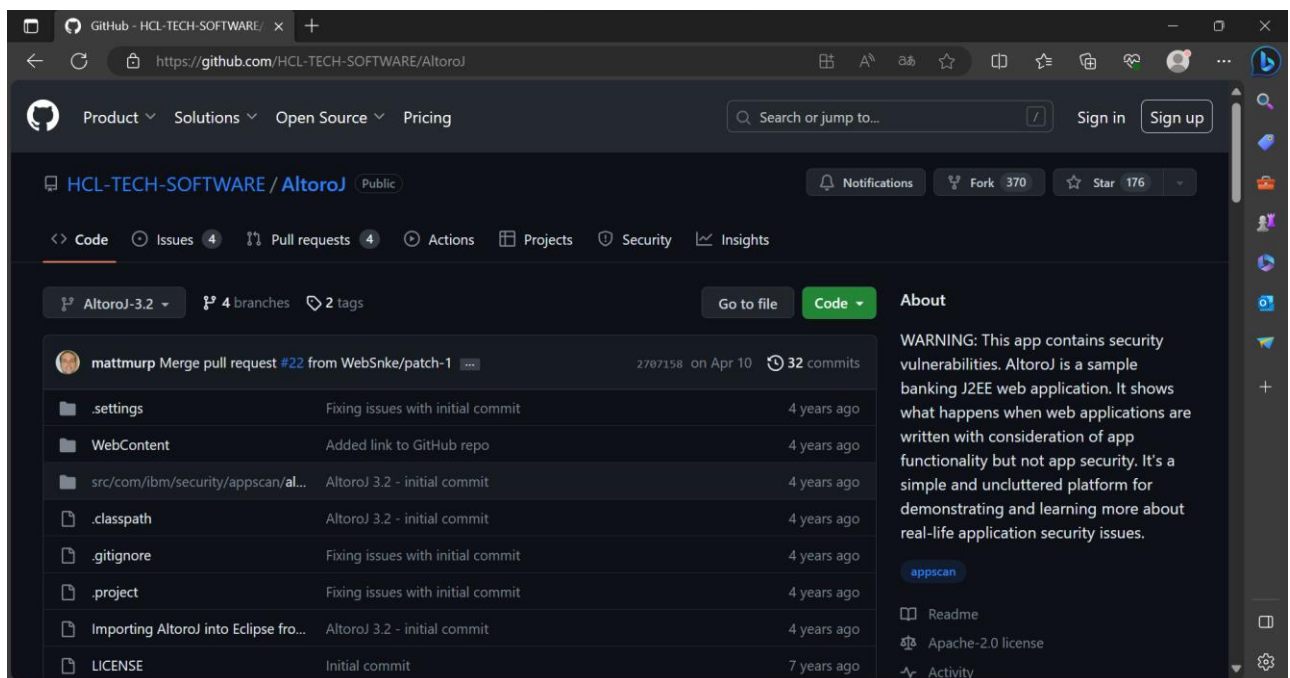
```
9 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,
image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;
q=0.7
10 Referer: http://testfire.net/bank/transaction.jsp
11 Accept-Encoding: gzip, deflate
12 Accept-Language: es-ES,es;q=0.9
13 Cookie: JSESSIONID=FEE7C6CF1F6BE478426383F161028042;
AltoroAccounts=
"ODAwMDAwfkNvcnBvcnF0ZX4tMy41MzUzNzg1Nzg1Mzg1NjhFODZ8ODAwMDAxfkNo
ZWwraW5nfjIuMzY4OTM1MDI1NjI2NjQwNUUyMHw="
14 Connection: close
15
16 startDate=2001-04-17a&endDate=2001-04-19a
```

Por último, en la página de Altoro Mutual nos manda un código de estado 500, haciendo referencia a una respuesta genérica que indica que el servidor encontró una condición inesperada que le impidió cumplir con la solicitud.



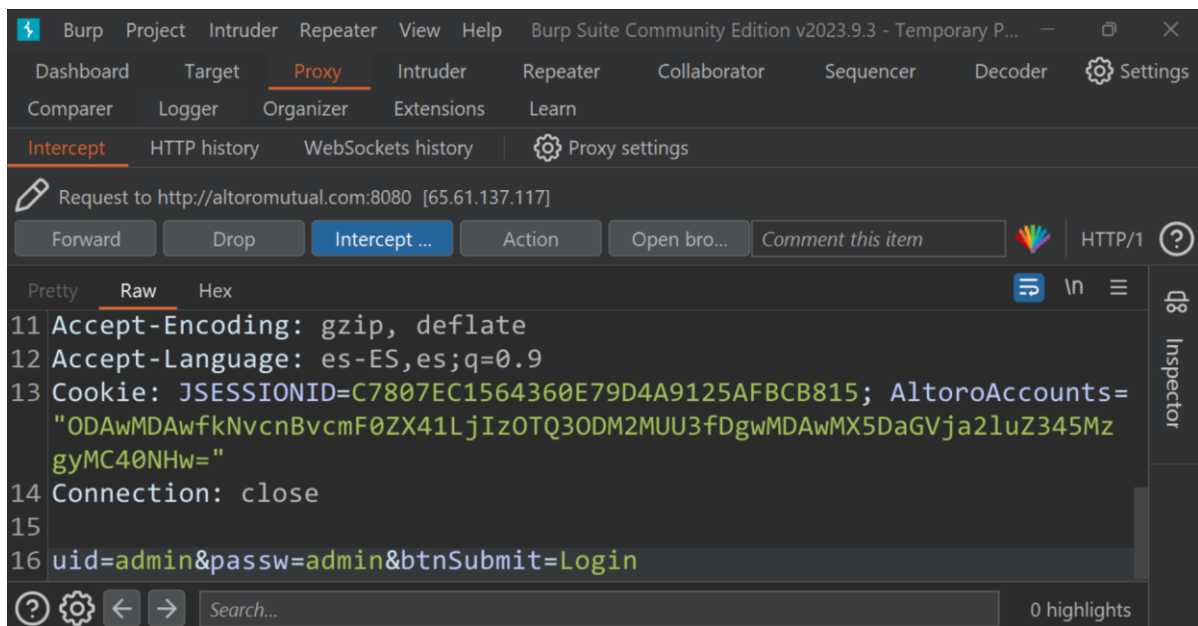
Data Exfiltration

De acuerdo al reporte se encontró la anotación de esta vulnerabilidad indicando que la página tiene un link de GitHub en la que se encontraron credenciales de acceso a la misma, pero esto fue hecho a propósito por los desarrolladores que advierten que ese repositorio es para una aplicación web vulnerable.

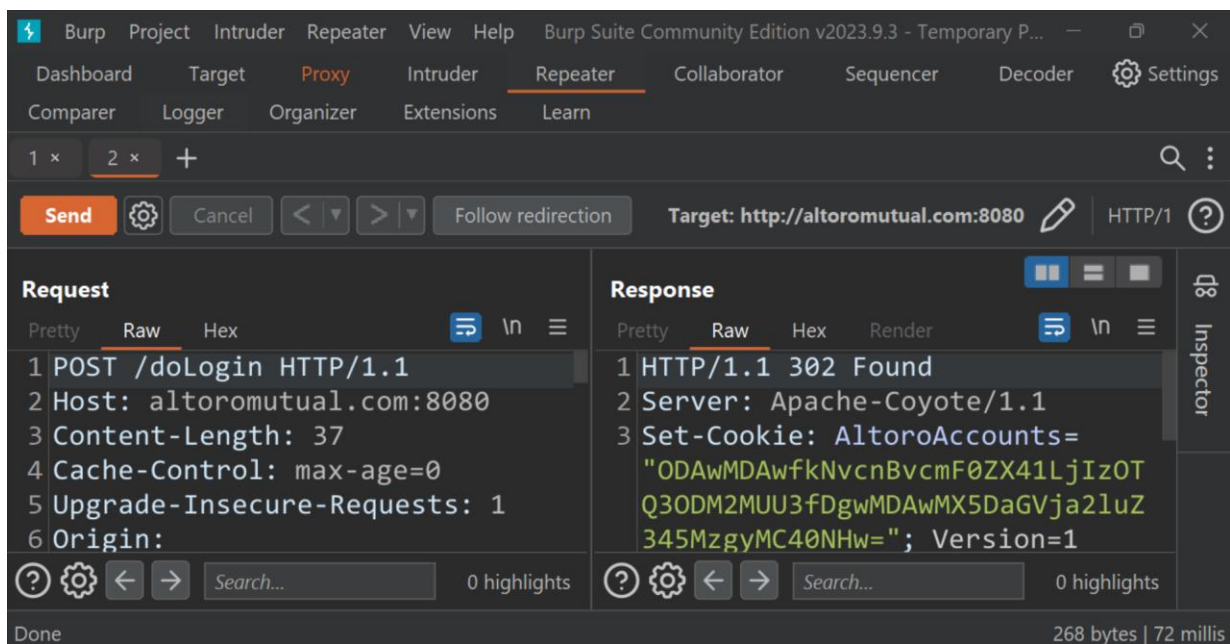


Default Credentials

La cuenta de administrador tiene admin como contraseña default



Enviamos la petición con el repeater para observar la respuesta




Así podemos acceder a la cuenta de administrador con las credenciales por default


Altoro Mutual

No es seguro | altoromutual.com:8080/bank/main.jsp

Sign Off | Contact Us | Feedback | Search

Go





MY ACCOUNT

I WANT TO ...

- [View Account Summary](#)
- [View Recent Transactions](#)
- [Transfer Funds](#)
- [Search News Articles](#)
- [Customize Site Language](#)

ADMINISTRATION

- [Edit Users](#)

PERSONAL

SMALL BUSINESS

INSIDE ALTORO MUTUAL

Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details:

800000 Corporate

GO

Congratulations!

You have been pre-approved for an Altoro Gold Visa with a credit limit of \$10000!

Click [Here](#) to apply.

[Privacy Policy](#) | [Security Statement](#) | [Server Status Check](#) | [REST API](#) | © 2023 Altoro Mutual, Inc.

This web application is open source! [Get your copy from Github](#) and take advantage of advanced features

The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to <http://www-142.ibm.com/software/products/us/en/subcategory/SW110>.

Copyright © 2008, 2023, IBM Corporation, All rights reserved.