

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.

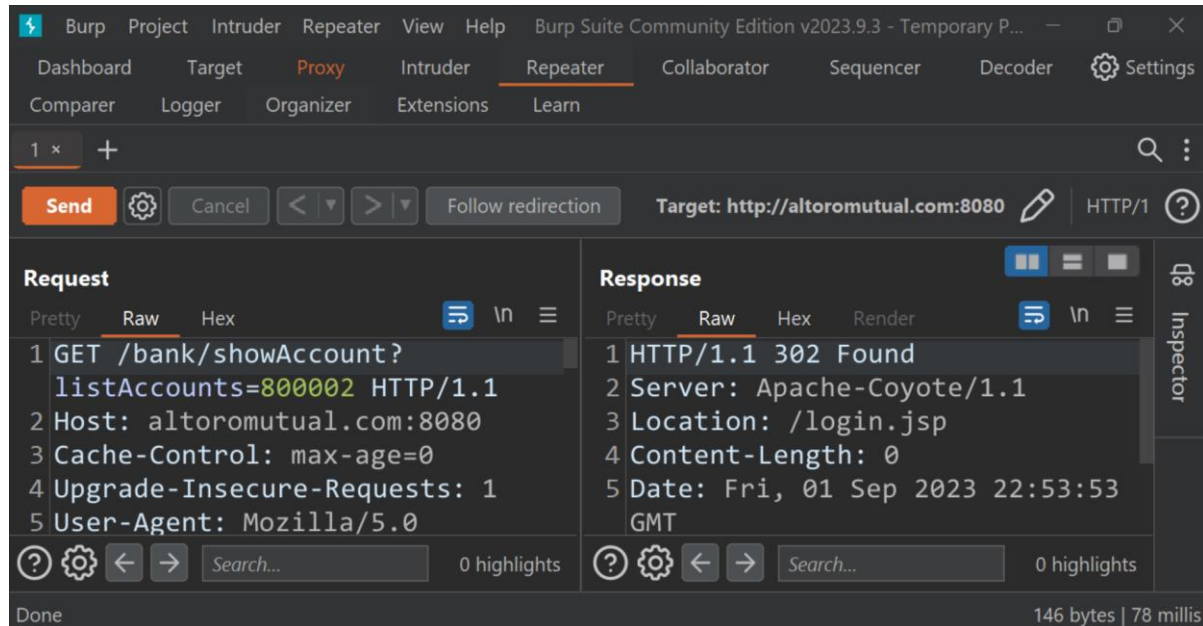
The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. A request is being sent to `http://testfire.net/login.jsp` with a payload of `uid=admin'--&passw=x&btnSubmit=Login`. The response shows a successful login as an administrator, with a 'Set-Cookie' header indicating the user is logged in. The 'Inspector' panel on the right shows the request and response details.

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

The screenshot shows the AltoroMutual website interface. The user is logged in as 'Admin User'. The 'MY ACCOUNT' section shows account details, including a credit limit of \$100,000. The 'ADMINISTRATION' section shows a link to 'Edit Users'. The footer contains a disclaimer about the website being a demonstration of IBM products.

IDOR Insecure Direct Object Reference

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



The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. The target is set to `http://altoromutual.com:8080`. The request is a GET to `/bank/showAccount?listAccounts=800002`. The response is a 302 Found status, indicating a redirect.

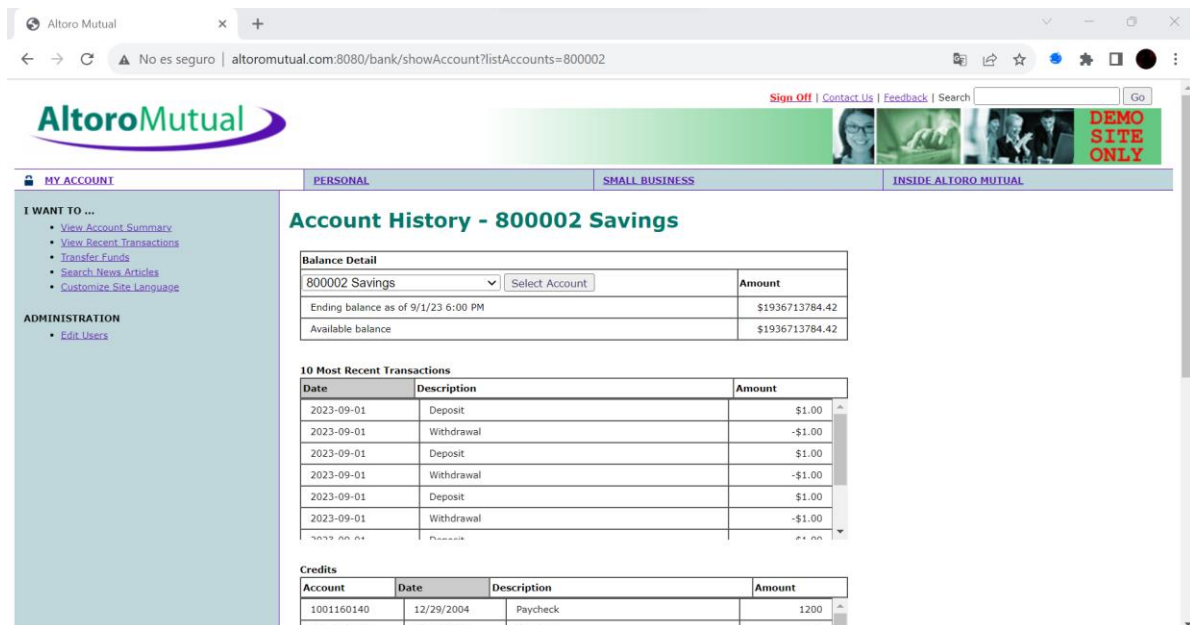
Request

```
1 GET /bank/showAccount?listAccounts=800002 HTTP/1.1
2 Host: altoromutual.com:8080
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0
```

Response

```
1 HTTP/1.1 302 Found
2 Server: Apache-Coyote/1.1
3 Location: /login.jsp
4 Content-Length: 0
5 Date: Fri, 01 Sep 2023 22:53:53 GMT
```

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



The screenshot shows the Altoro Mutual website. The user is logged in as '800002 Savings'. The page displays the account history, including a balance detail and a list of recent transactions.

Balance Detail

800002 Savings	Select Account	Amount
Ending balance as of 9/1/23 6:00 PM		\$1936713784.42
Available balance		\$1936713784.42

10 Most Recent Transactions

Date	Description	Amount
2023-09-01	Deposit	\$1.00
2023-09-01	Withdrawal	-\$1.00
2023-09-01	Deposit	\$1.00
2023-09-01	Withdrawal	-\$1.00
2023-09-01	Deposit	\$1.00
2023-09-01	Withdrawal	-\$1.00

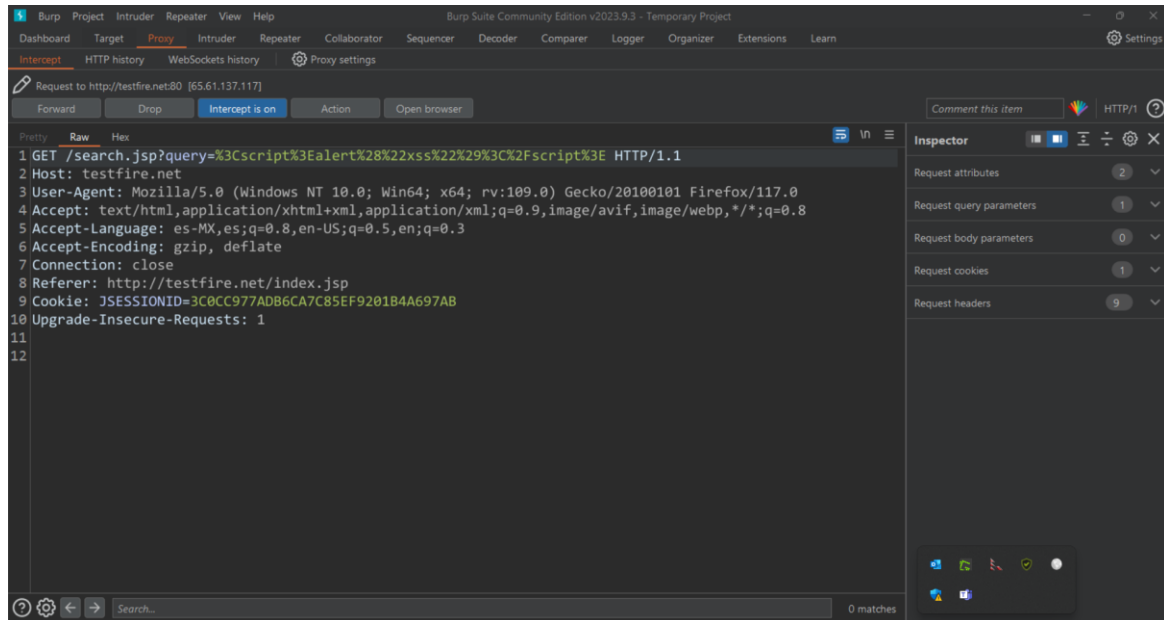
Credits

Account	Date	Description	Amount
1001160140	12/29/2004	Paycheck	1200

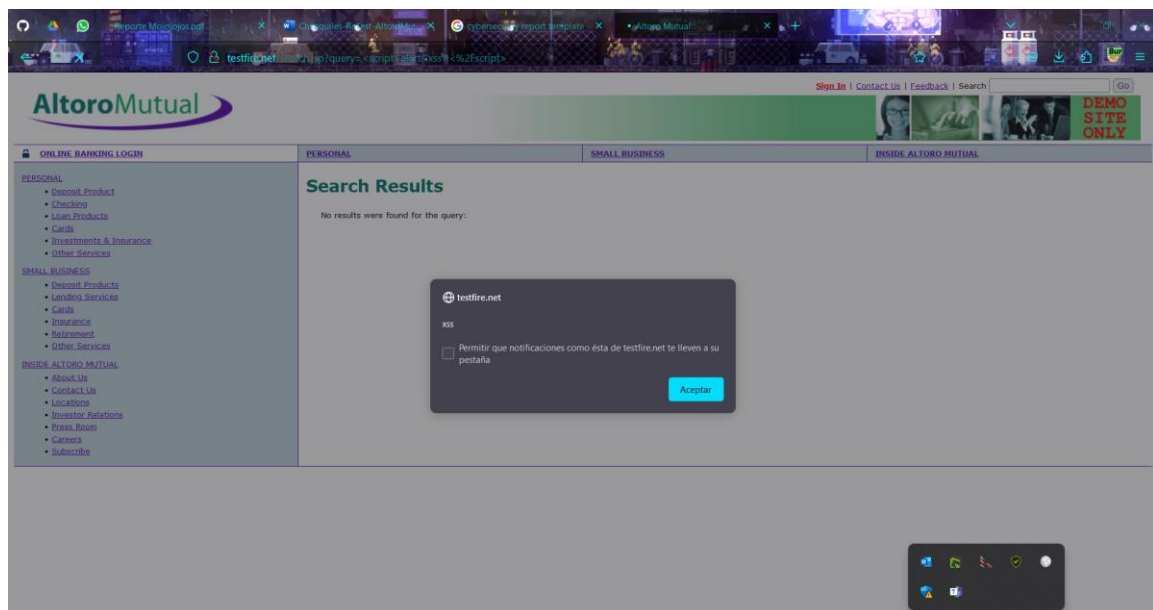
XSS:

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)

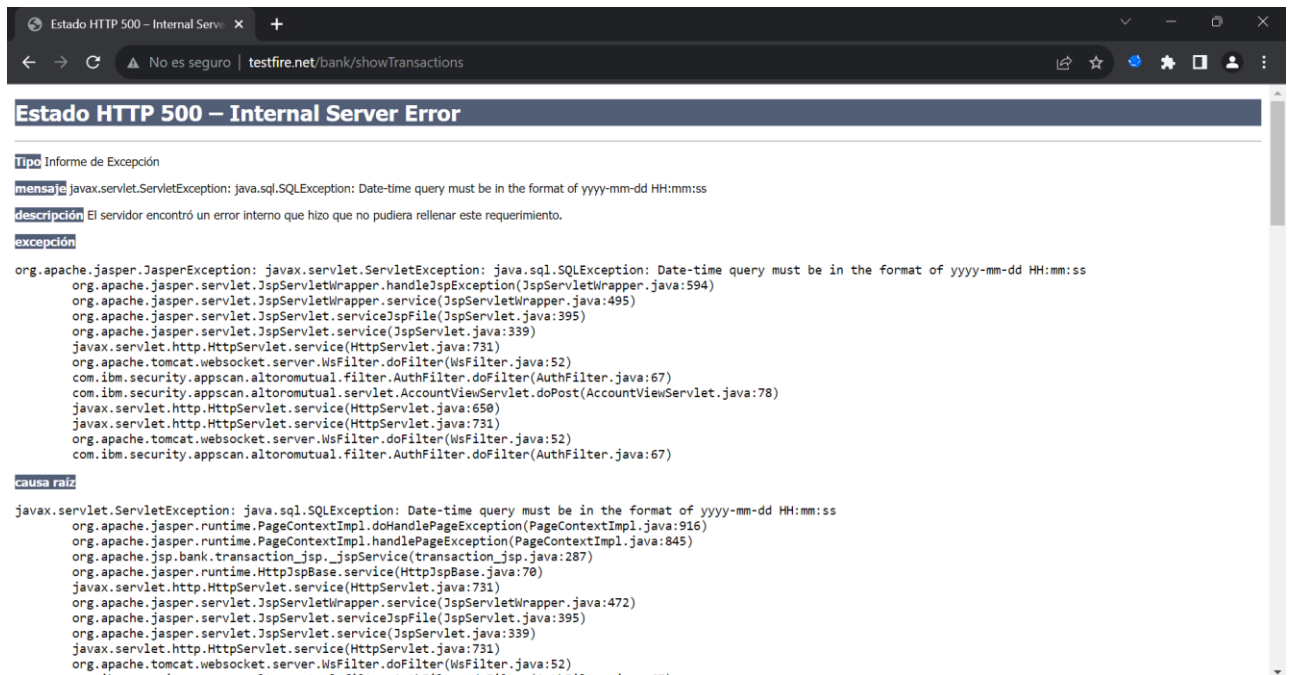
Al insertar una letra donde la página no lo esperaba, en este caso en la fecha, se logró un mensaje de error con información de SQL, mismo error que podría ser abusado para hacerle SQL injection.

Transaction ID	Transaction Time	Account ID	Action	Amount
23162	2023-09-01 17:59	800001	Withdrawal	-\$100000.00
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.

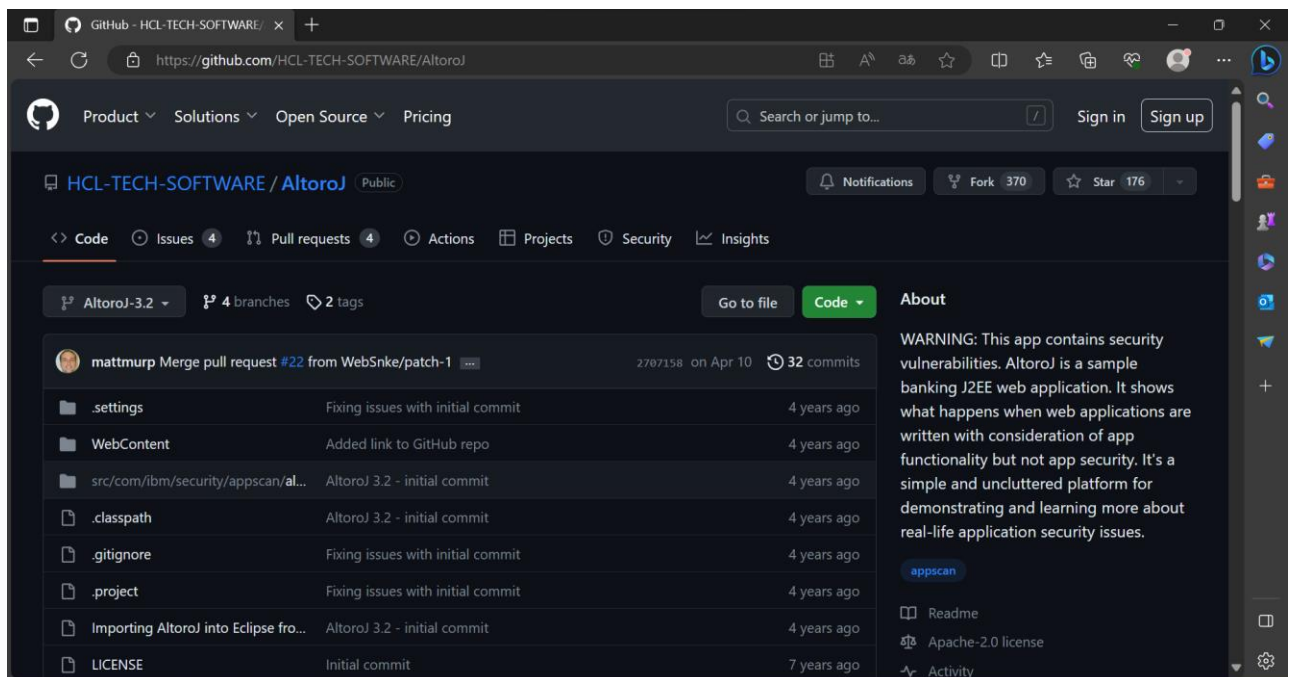
```
9 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,
image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;
q=0.7
10 Referer: http://testfire.net/bank/transaction.jsp
11 Accept-Encoding: gzip, deflate
12 Accept-Language: es-ES,es;q=0.9
13 Cookie: JSESSIONID=FEE7C6CF1F6BE478426383F161028042;
AltoroAccounts=
"ODAwMDAwfkNvcnBvcnM0ZDZ8ODAwMDAwfkNo
ZWNaW5nfjIuMzY4OTM1MDI1NjI2NjQwNUUyMHw="
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.



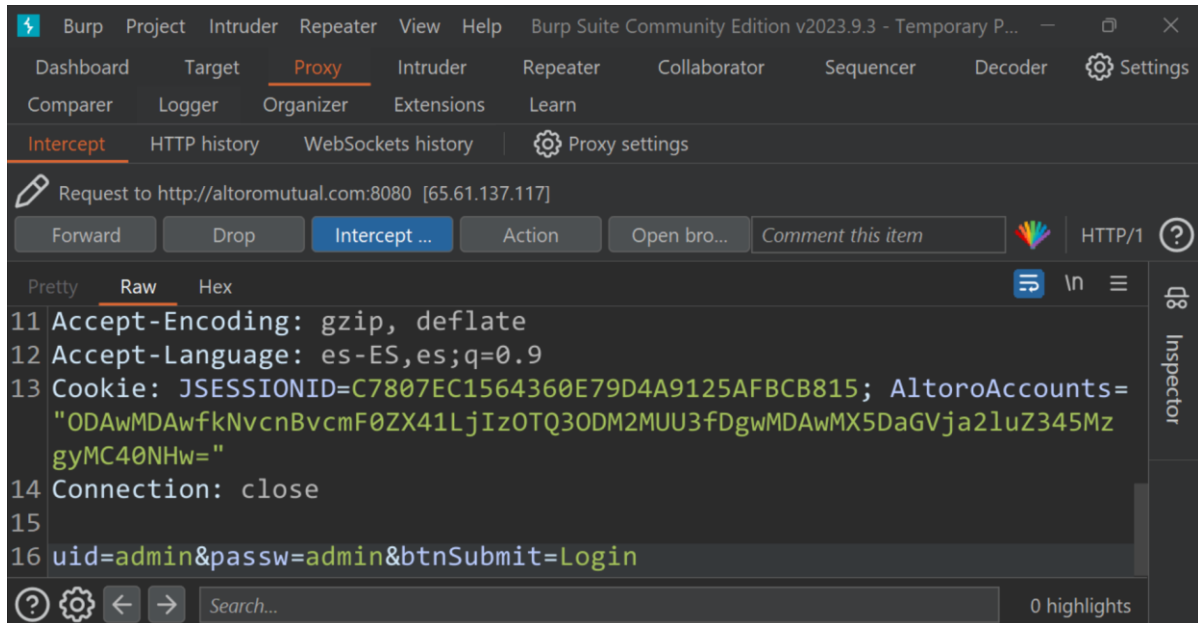
Data Exfiltration

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.

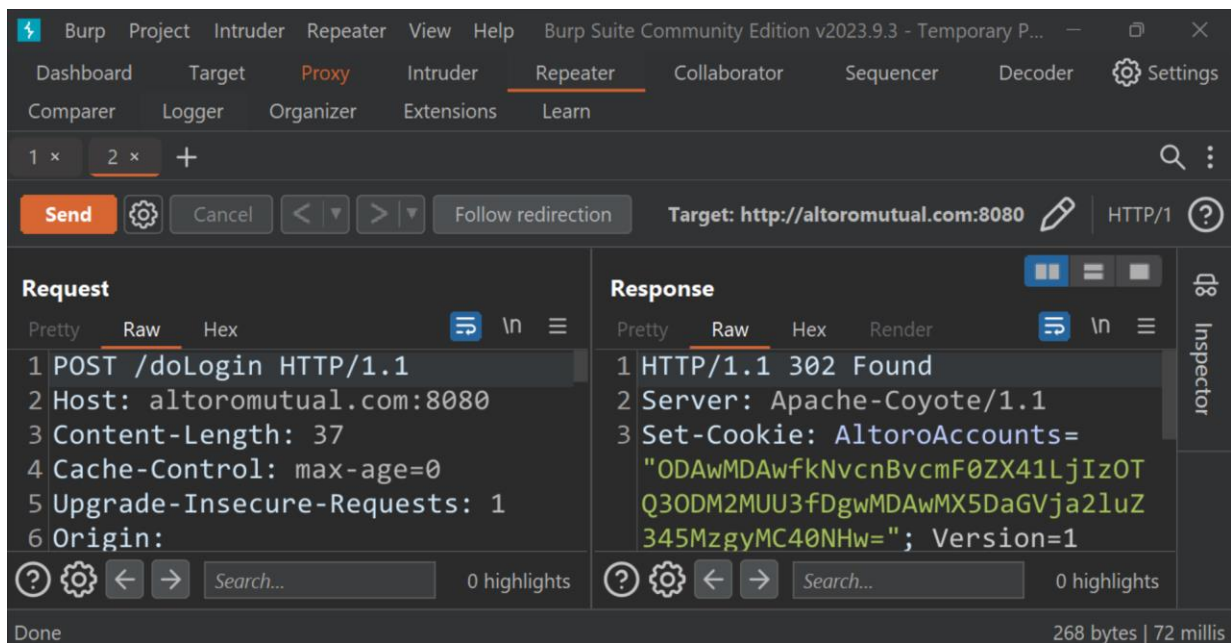


Default Credentials

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

The screenshot shows a web browser window with the URL `altoromutual.com:8080/bank/main.jsp`. The page features the Altoro Mutual logo and a navigation bar with links for [Sign Off](#), [Contact Us](#), and [Feedback](#). A search bar is also present. Below the navigation bar, there are four tabs: **MY ACCOUNT**, **PERSONAL**, **SMALL BUSINESS**, and **INSIDE ALTORO MUTUAL**. The **PERSONAL** tab is selected, displaying a "Hello Admin User" message. The user is welcomed to the Altoro Mutual Online platform. Below the greeting, there is a "View Account Details" section with a dropdown menu showing "800000 Corporate" and a "GO" button. A "Congratulations!" message follows, stating that the user has been pre-approved for an Altoro Gold Visa with a credit limit of \$100,000. A link to "Click Here to apply" is provided. The footer contains links for [Privacy Policy](#), [Security Statement](#), [Server Status Check](#), and [REST API](#), along with the copyright notice "© 2023 Altoro Mutual, Inc.". A red banner at the bottom states: "This web application is open source! Get your copy from [Github](#) and take advantage of advanced features". A disclaimer box at the bottom explains that the 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. It states that the site is not a real banking site and that similarities to third-party products are purely coincidental. The disclaimer also includes a link to <http://www-142.ibm.com/software/products/us/en/subcategory/SW10>.