

Aguilar Navarrete Erick David
Monjaraz Galicia Ricardo Adrian
Pineda Pineda Yaotzin

Se encontro una vulnerabilidad XSS en la barra de busqueda



si ingresamos

`<script>alert("hola")</script>`

Tiene credenciales por defecto

Tiene una vulnerabilidad de SQLi ya que comentamos en la consulta la parte del password

[PERSONAL](#)[SMALL BUSINESS](#)

Online Banking Login

Username:

Password:

Se encontro un IDOR

← ↻ ⚠ No seguro | altoromutual.com:8080/bank/showAccount?listAccounts=800000

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

Account History - 800000 Corporate

Balance Detail	
800000 Corporate	Amount
Ending balance as of 8/28/23 6:59 PM	\$52394783.61
Available balance	\$52394783.61

10 Most Recent Transactions

Date	Description	Amount
------	-------------	--------

Ya que podemos cambiar el valor del parametro y ver la historia de otro usuario entonces se hace un Broken Access control

No seguro | altoromutual.com:8080/bank/showAccount?listAccounts=800001

AltoroMutual

Sign Off | Contact Us | Feedback | S

MY ACCOUNT

PERSONAL

SMALL BUSINESS

INSIDE

I WANT TO ...

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

ADMINISTRATION

- Edit Users

Account History - 800001 Checking

Balance Detail	
800001 Checking <div>Select Account</div>	Amount
Ending balance as of 8/28/23 7:00 PM	\$93820.44
Available balance	\$93820.44

10 Most Recent Transactions

Secure Error

No seguro | altoromutual.com:8080/bank/showAccount?listAccounts=hola

Estado HTTP 500 – Internal Server Error

Tipo

Informe de Excepción

mensaje

java.lang.NumberFormatException: For input string: "hola"

descripción

El servidor encontró un error interno que hizo que no pudiera rellenar este requerimiento.

excepción

```
org.apache.jasper.JasperException: java.lang.NumberFormatException: For input string: "hola"
  org.apache.jasper.servlet.JspServletWrapper.handleJspException(JspServletWrapper.java:594)
  org.apache.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:510)
  org.apache.jasper.servlet.JspServlet.serviceJspFile(JspServlet.java:395)
  org.apache.jasper.servlet.JspServlet.service(JspServlet.java:339)
  javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
  org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
  com.ibm.security.appscan.altoromutual.filter.AuthFilter.doFilter(AuthFilter.java:67)
  com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet.doGet(AccountViewServlet.java:58)
  javax.servlet.http.HttpServlet.service(HttpServlet.java:624)
  javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
  org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
  com.ibm.security.appscan.altoromutual.filter.AuthFilter.doFilter(AuthFilter.java:67)
```

causa raíz

```
java.lang.NumberFormatException: For input string: "hola"
  java.lang.NumberFormatException.forInputString(Unknown Source)
  java.lang.Long.parseLong(Unknown Source)
  java.lang.Long.parseLong(Unknown Source)
  com.ibm.security.appscan.altoromutual.model.Account.getAccount(Account.java:41)
  org.apache.jsp.bank.balance_jsp._jspService(balance_jsp.java:170)
  org.apache.jasper.runtime.HttpJspBase.service(HttpJspBase.java:70)
  javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
  org.apache.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:472)
```