


Demo Hacking page

[Altoro Mutual](#)

Try SQL injection:

Any password will do


PERSONAL	SMALL BUSINESS 
--------------------------	--

Online Banking Login

Syntax error: Encountered "test" at line 1, column 62.

Username:

Password:

PERSONAL	SMALL BUSINESS 
--------------------------	--

Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details:

Congratulations!

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

Click [Here](#) to apply.

Step 1: Begin by logging in with user privileges and navigate to the following URL: <https://altoromutual.com/bank/main.jsp> Once on the page, proceed to click on the Go button on “View Account Details” option.

PERSONAL SMALL BUSINESS

Hello John Smith

Welcome to Altoro Mutual Online.

View Account Details: 800002 Savings GO

Congratulations!

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

Click [Here](#) to apply.

Step 2: After accessing the “View Account Details” page, manipulate the URL parameter “id” to another user account id.

Altoro Mutual

MY ACCOUNT PERSONAL SMALL BUSINESS

Account History - 800002 Savings

Balance Detail

800002 Savings	Select Account	Amount
Ending balance as of 3/20/24 8:11 PM		\$73786976312025800000.00
Available balance		\$73786976312025800000.00

10 Most Recent Transactions

Date	Description	Amount
2024-03-20	Deposit	\$1000.00
2024-03-20	Withdrawal	-\$13000.00
2024-03-20	Withdrawal	-\$13000.00
2024-03-20	Withdrawal	-\$13000.00
2024-03-20	Withdrawal	-\$13000.00

By changing the URL you can view any account

The screenshot shows the AltoroMutual website's Online Banking Login page. The page is divided into two main sections: 'PERSONAL' and 'SMALL BUSINESS'. The 'PERSONAL' section is active, displaying the 'Online Banking Login' form. The form includes a 'Username' field with the text 'junit' and a 'Password' field with masked characters '*****'. A 'Login' button is positioned below the password field. To the left of the login form, there are two columns of navigation links. The first column, under the 'PERSONAL' heading, lists links for 'Personal Products', 'Investing', 'Loan Products', 'Auto', 'Investment & Insurance', and 'Other Services'. The second column, under the 'SMALL BUSINESS' heading, lists links for 'Deposit Products', 'Lending Services', 'Com', 'Insurance', 'Roth IRA', and 'Other Services'. Below these links, there is a section titled 'ABOUT US' with links for 'About Us', 'Contact Us', 'Locations', and 'Investor Relations'. At the bottom of the browser window, the Windows taskbar is visible, showing the 'Applications' window with a list of running processes. A red arrow points to the 'AltoroMutual.com' process in the taskbar.

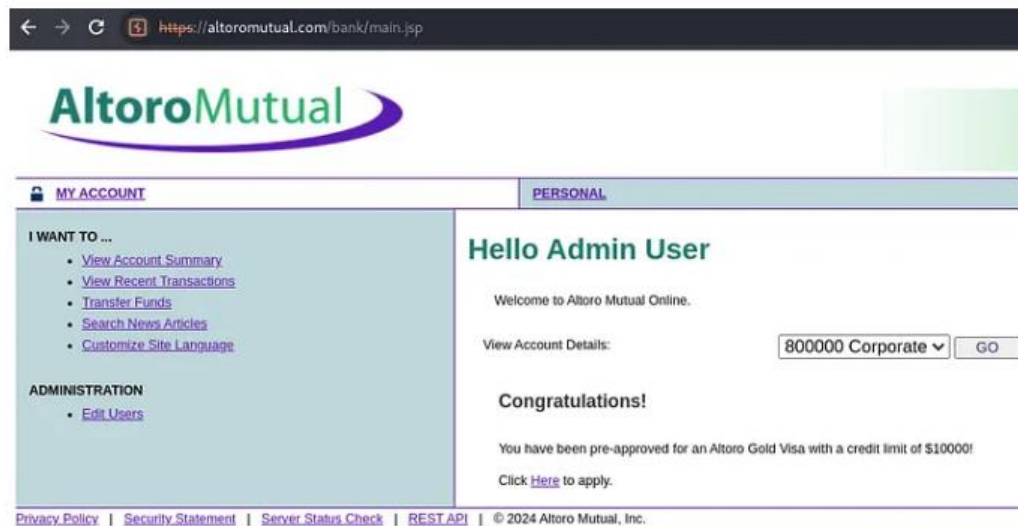
The screenshot shows a web browser displaying the Altoro website. The website has a navigation bar with links: [Sign Off](#), [Contact Us](#), and [Feedback](#). Below the navigation bar is a search bar and a "Go" button. The main content area features a large image with the text "DEMO SITE ONLY" and a button labeled "INSIDE ALTORO MUTUAL". An "Add Account" button is visible at the bottom of the page.

The Chrome DevTools Storage tab is open, showing the following data:

Name	Value	D	P	E	S	H	S	P	C	P
Altoro...	"ODAwMDAw...	d..	/	S..	1...					M.
JSESSI...	50564DD2F8...	d..	/	S..	4...	✓	✓			M.

Never leave default settings!

Step 1: Navigate to the sign-in page and log in as an administrator. Currently, the administrator password has not been changed, and you can use the default common username and password combination, such as username=admin and password=admin, to log in as an admin user in this application.



To prove it can be embedded in a hacked page

```
<html>

<head>

<title>Embed Website</title>

<body>

<h1>Hacked Website embedded here</h1>

<iframe src="https://demo.testfire.net/index.jsp" width="800" height="600"
frameborder="2"></iframe>

</body>

</html>
```

Make a basic webpage to test – save as hackPage.html