

Perform Bypass Authentication

The screenshot shows a web browser window with multiple tabs open. The active tab is 'demo.testfire.net/login.jsp'. The page displays the AltoroMutual logo and navigation links. The 'PERSONAL' tab is selected, showing the 'Online Banking Login' form. The 'Username' field contains the payload 'admin' or '1'=1', and the 'Password' field is masked with asterisks. The 'Login' button is visible. A red dashed box highlights the footer text, which states that the website is published by IBM Corporation for the purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. It also includes a copyright notice for 2008, 2022, IBM Corporation.

AltoroMutual

[Sign In](#) | [Contact Us](#) | [Feedback](#) | Search [Go](#)

ONLINE BANKING LOGIN

PERSONAL | **SMALL BUSINESS** | **INSIDE ALTORO MUTUAL**

Online Banking Login

Username:

Password: [Show/Hide](#)

[Privacy Policy](#) | [Security Statement](#) | [Server Status Check](#) | [REST API](#) | © 2022 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/SWT10>.

Copyright © 2008, 2022, IBM Corporation, All rights reserved.

Payload used

These are the payload which I have used to bypass the authentication

- Username :admin'or'1'='1
- Password: admin'or'1'='1
- Username :admin' or '1'='1'--
- Password: admin' or '1'='1'--

What are the measures should be taken to prevent bypass authentication?

- 1 Mistakes from the web developer are
- Alpha numeric character are allowed only in user name
- 2: Database Admin is not properly encrypted in database