

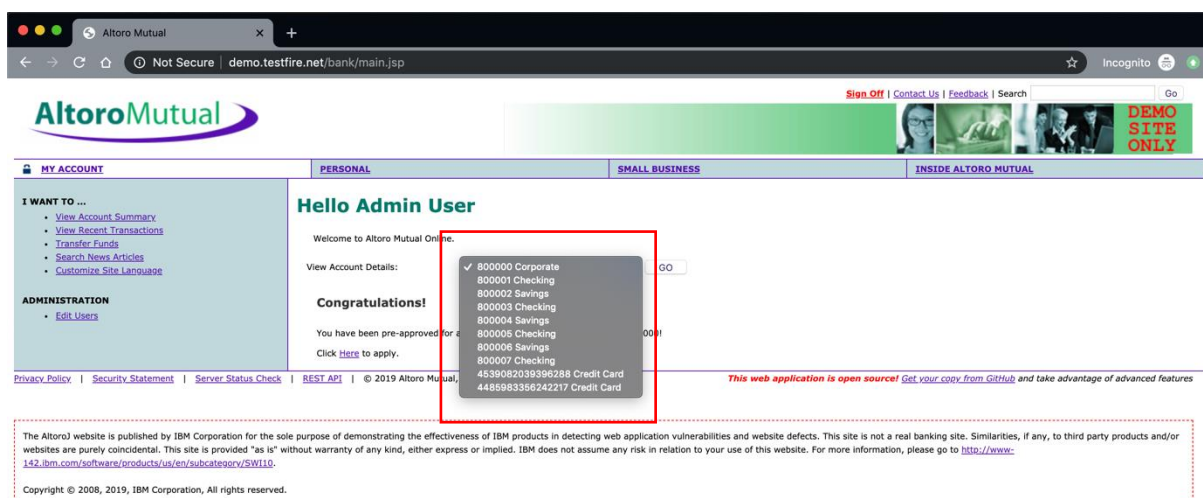
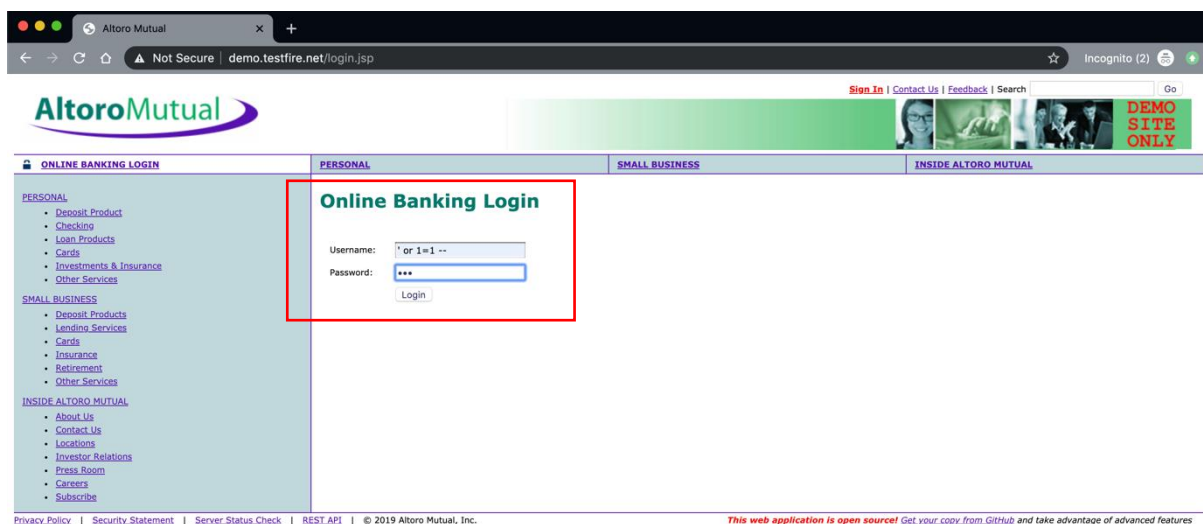
3. SQL Injection to show all recent transactions of all users:

Instead of username as **admin**, if we pass ' OR 1=1 -- it was observed that the system successfully signs in the user admin, but also fetches accounts of all user. To make sense let's look at the query we assumed in the first step.

```
query = "SELECT * FROM users  
WHERE username=' ' + username  
+ " ` AND password=' ' + password + " `";
```

If username is " OR 1=1 the query will return all users in the system.

The logic to fetch accounts is related to the result of the above query, therefore if the above query returns all users in the system, the query to fetch account numbers also fetches accounts belonging to every account in the system. With this, we can find out the recent transactions for all accounts of all users.



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/SWT10>.

Copyright © 2008, 2019, IBM Corporation, All rights reserved.