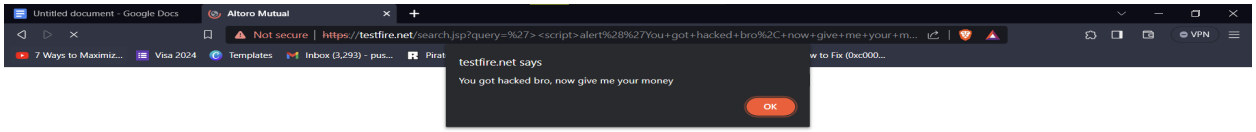
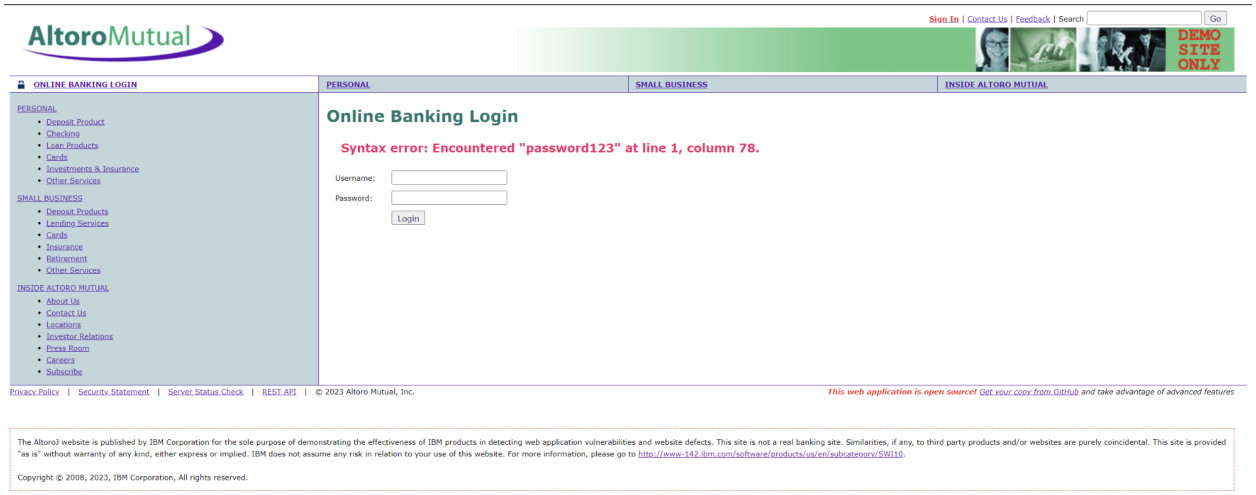
AI for Cybersec
Assignment 1

1) **Injection**

Injection attacks happen when untrusted data is sent to a code interpreter through a form input or some other data submission to a web application. For example, an attacker could enter SQL database code into a form that expects a plaintext username. If that form input is not properly secured, this would result in that SQL code being executed. This is known as an SQL injection attack.



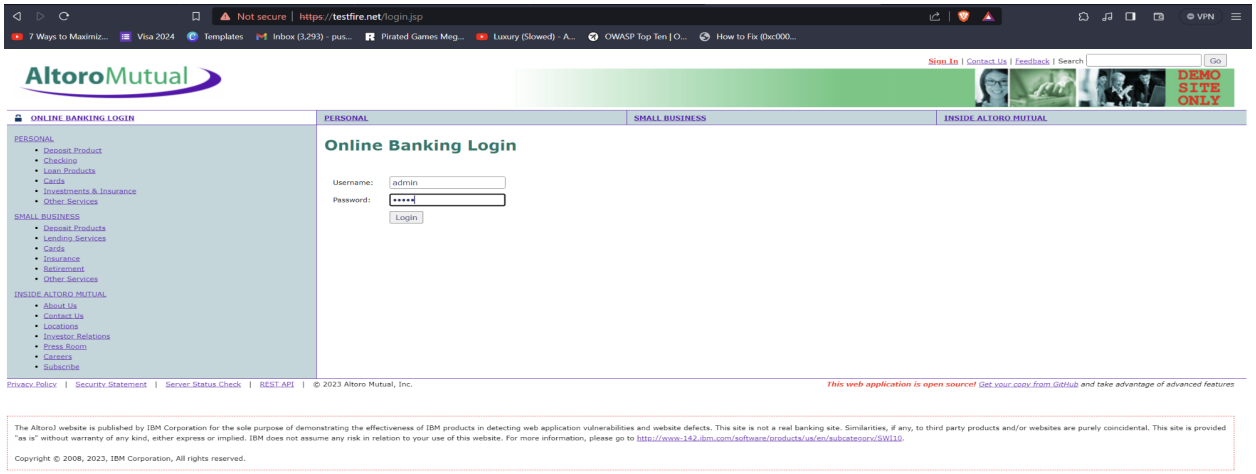

As we can see, This website is vulnerable to HTML Injections
This error shows that the website is vulnerable to SQL injections.

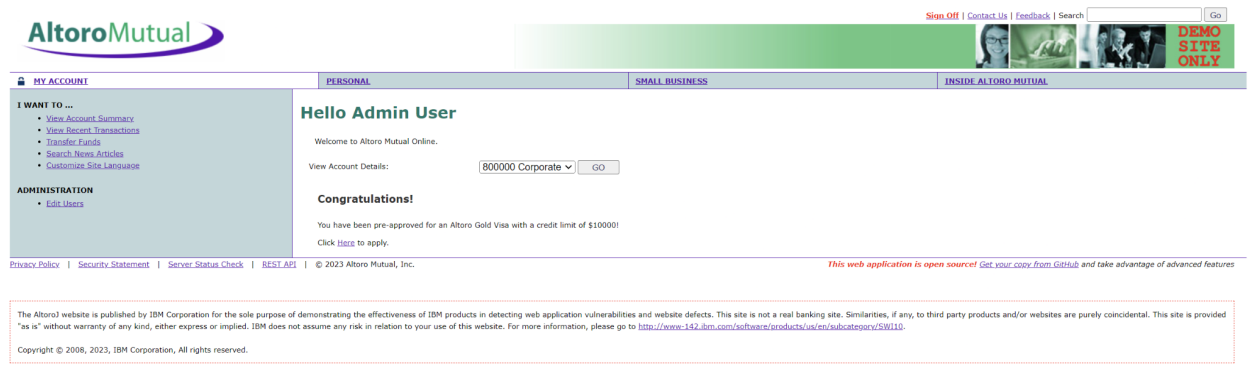



Basically if the query returns true, we can log in, but since this db is vulnerable to sql injection, we can write a basic statement that is true, inorder to get a true response and trick system into authenticating us.
– is comment.

2. **Broken Authentication**

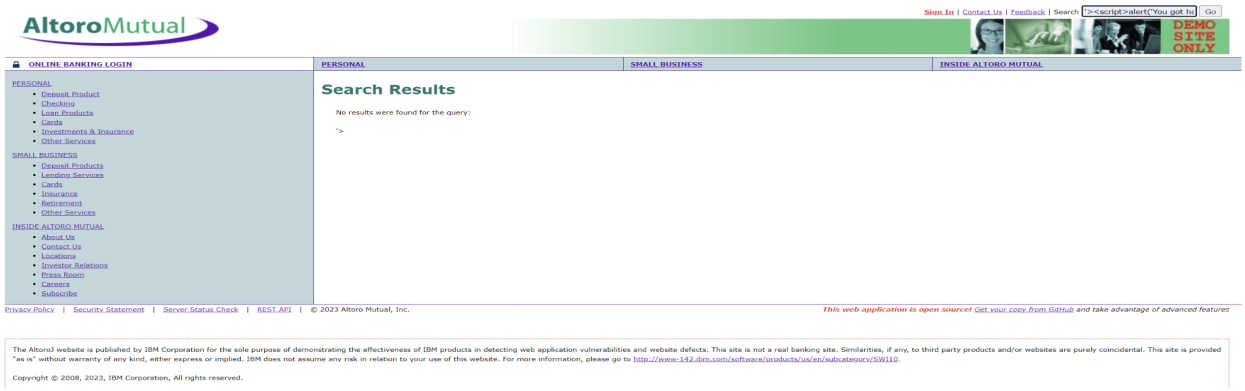
If the users identity is able to be spoofed or jeopardized.
Permitting wellknown passwords..
Permitting Automated Attacks like credential stuffing.
Permitting bruteforce attacks.
Wellknown common passwords are used here.

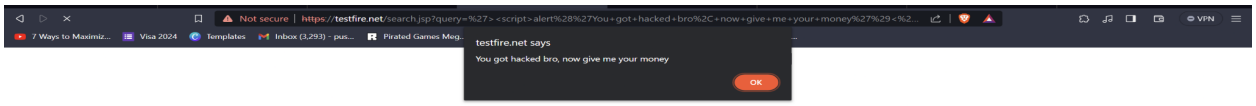



Using wellknown password as Admin/Admin we logged in easily.

**3) Cross Site Scripting (XSS)**
By using HTML we can see that this website is vulnerable to XSS attacks.
Ex: **'><script>alert('You got hacked bro, now give me your money')</script>**




4) **Broken Access Control**

If user is able to go outside of their intended permissions we have a case of Broken Access Control.

Ex is modifying the URL of page to get there.

https://testfire.net/bank/showAccount?listAccounts=4539082039396288 OR

https://testfire.net/bank/showAccount?listAccounts=4485983356242217

Even though i am not logged into this different users account. I can still access by just pasting the URL alone.