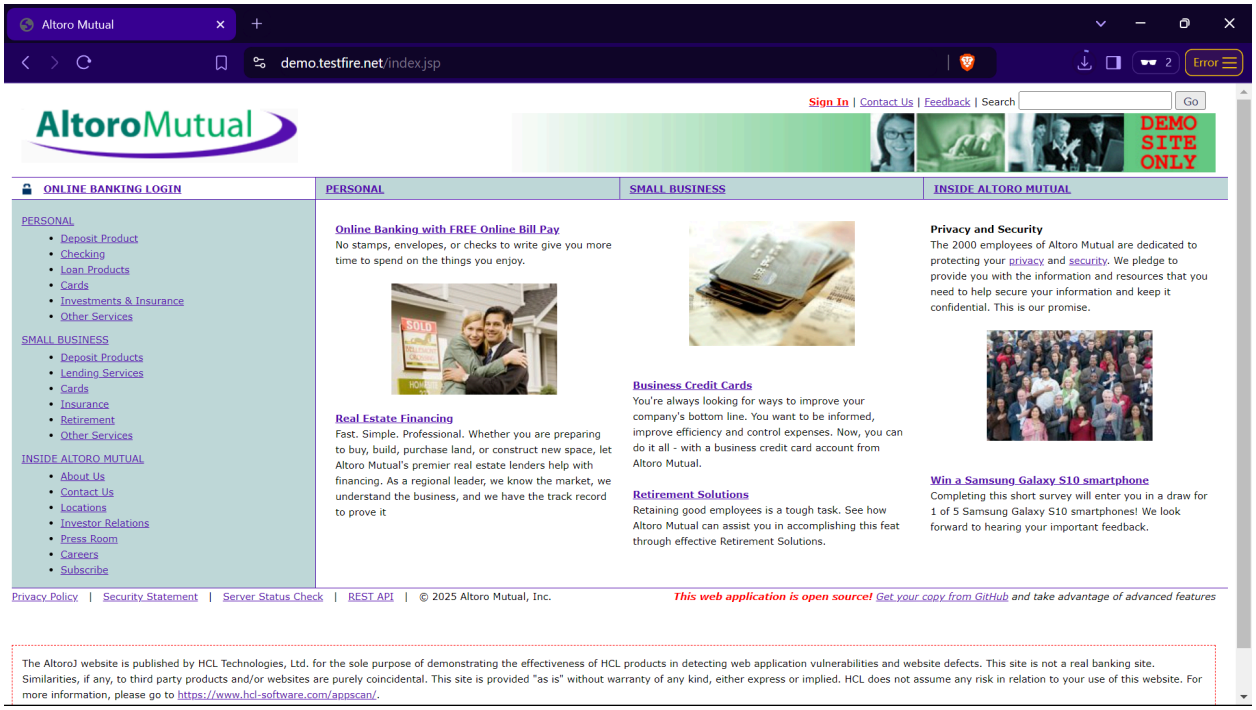
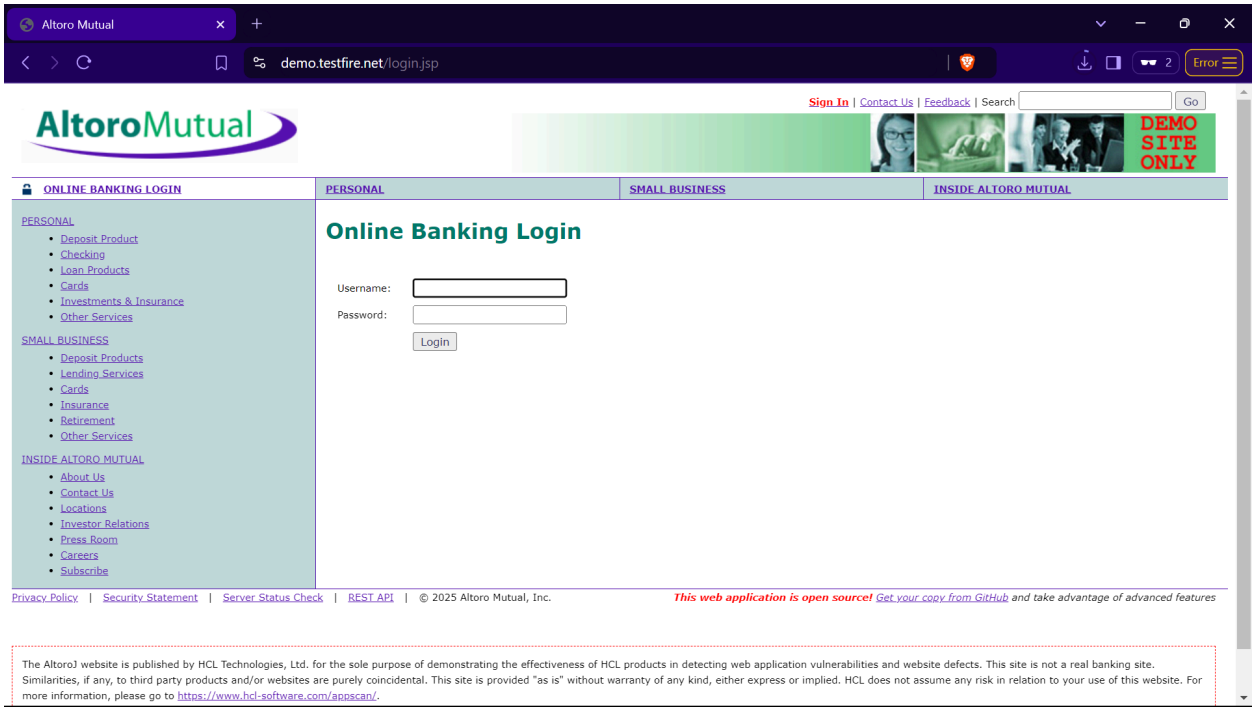
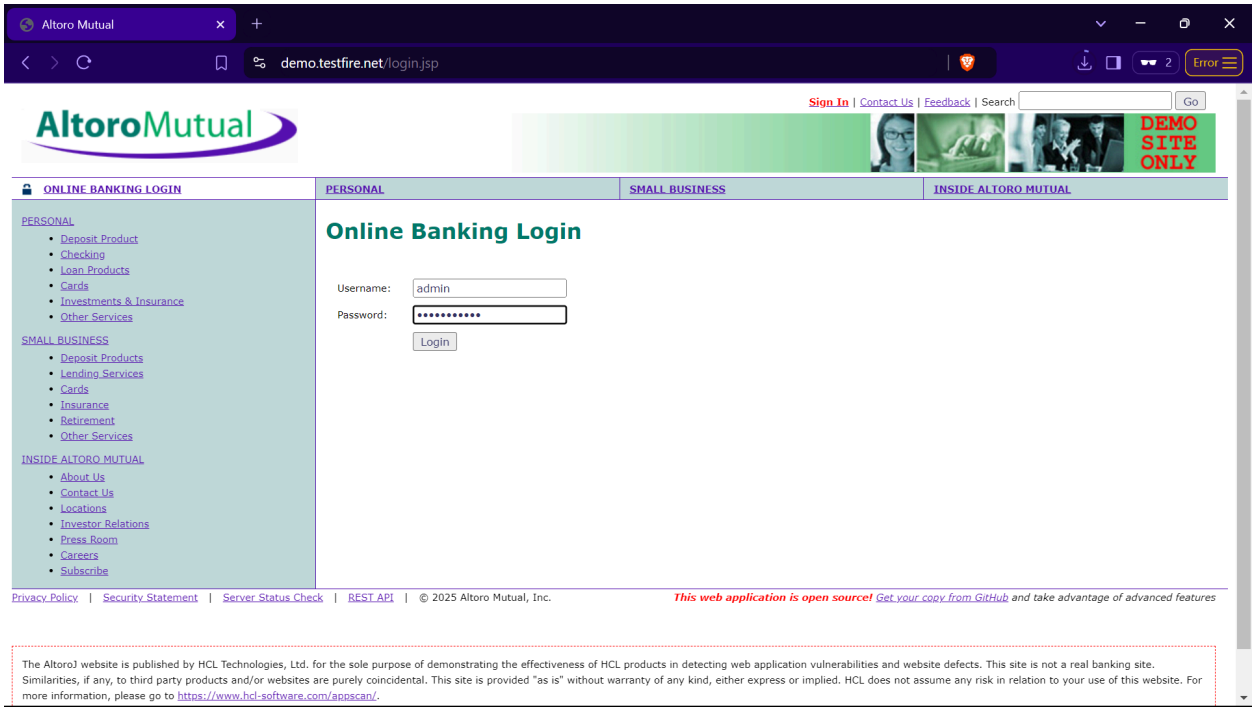


Navigate to the login page of the vulnerable website. And Click Sign in where we enter our malicious credentials



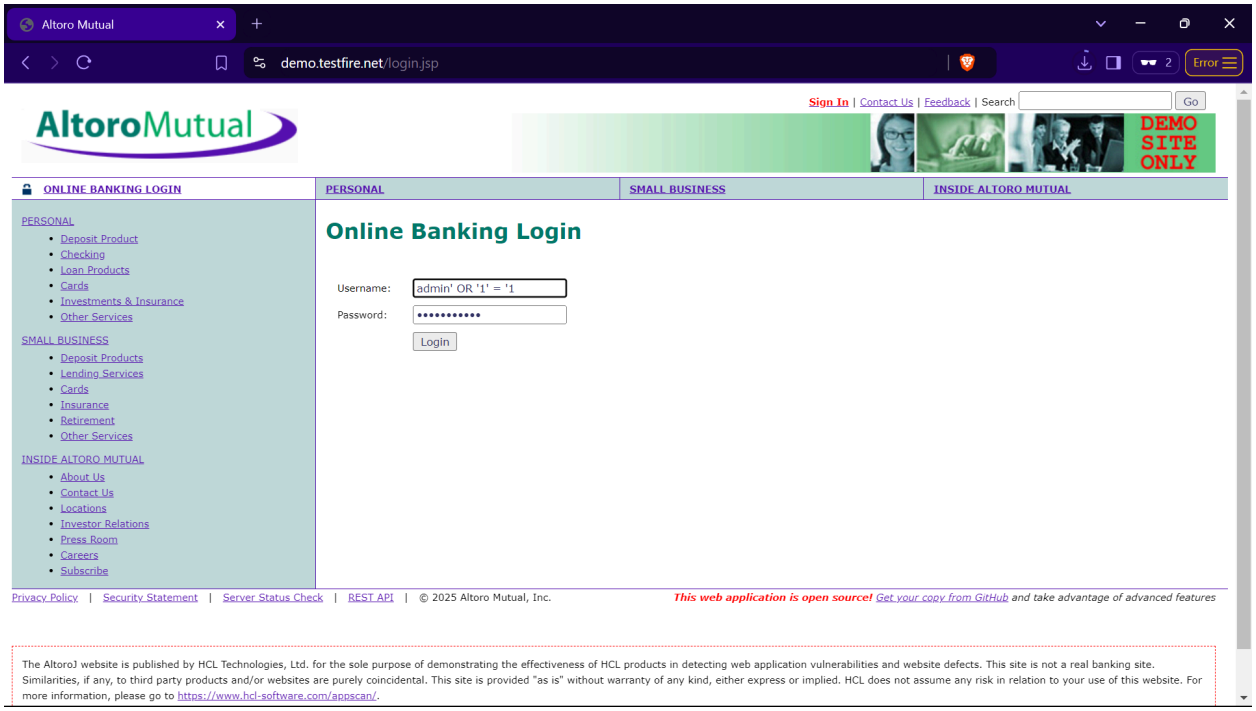
The above is the Login page of the Vulnerable Site where we perform our attack.

Suppose we want to get into the admin panel of the page, But we do not know the credentials,We just type in the User id and some random password as shown below.When we try we fail obviously.



In the frontend it looks like this for us. But in the back end it looks something like this to the server.

So now let us trick the server with our malicious code so it looks something like this.

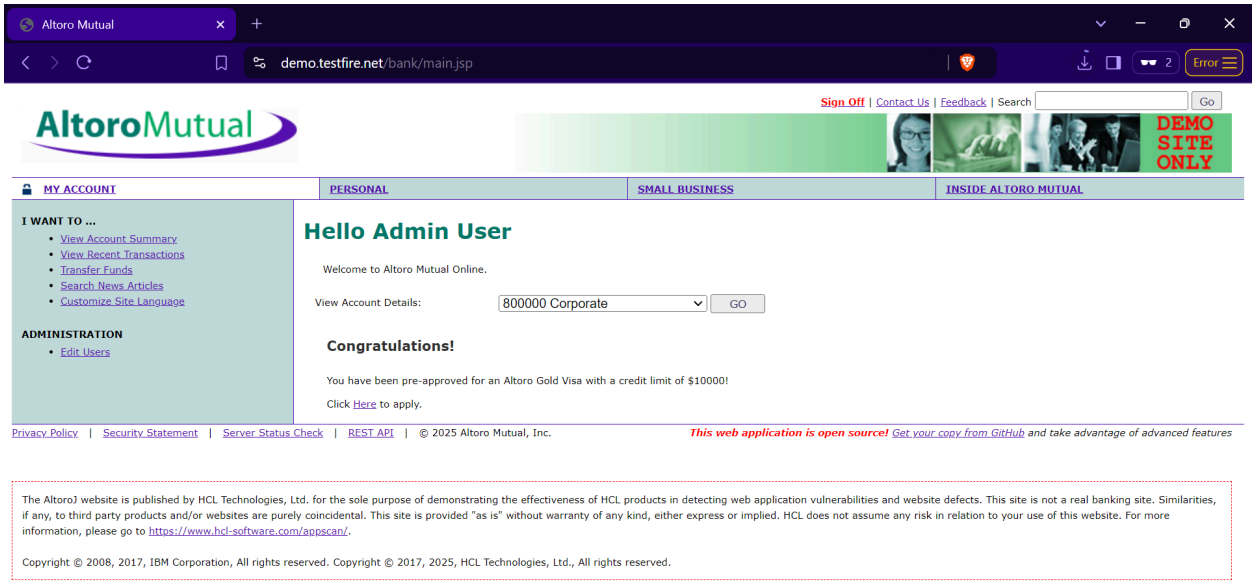


It may look weird in the front end, but in the back end it looks like this.

```
SELECT * FROM users WHERE username ='admin' OR '1'='1' AND password='password123'
```

It makes sense here,Doesnt it?
So what exactly is happening?
We have written an OR case which after failing the AND case automatically executes.And in the OR we have written a statement which is always true and hence the successful execution of the

SQL command takes place.



There is also an other way to do it. Using Comments in SQL. I recommend you to try it yourself.