**SSCBS**

**MAYANK CHOPRA**

**ROLLNO -23719**

**4) Insure Design**

**Description: -**

When designing applications developers are recommended to built secure design patterns because lack of security in the design phase can lead to various weakness, attacks know as insecure design vulnerability, it can also lead to unprotected storage of credentials, trust boundaries, generating error message, showing sensitive information.

**Impact-**

Major impact of this vulnerability is to destroy the sensitive information of any individual or organization.

References-

[Insecure Design OWASP Top 10 - Vulnerability Explained (crashtest-security.com)](https://crashtest-security.com/insecure-design-vulnerability/)

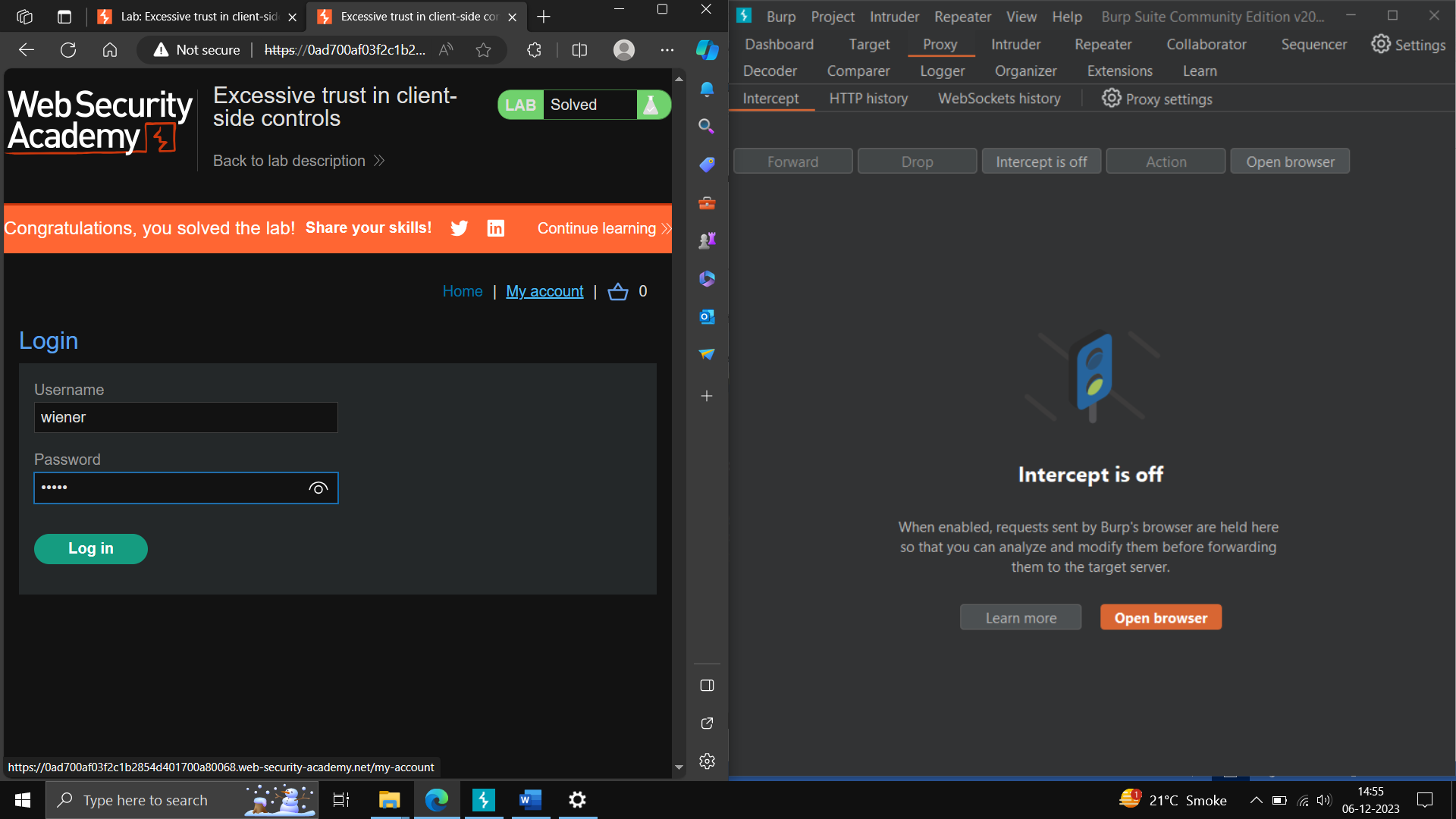
**Preventions-**

Develop a secure development lifecycle

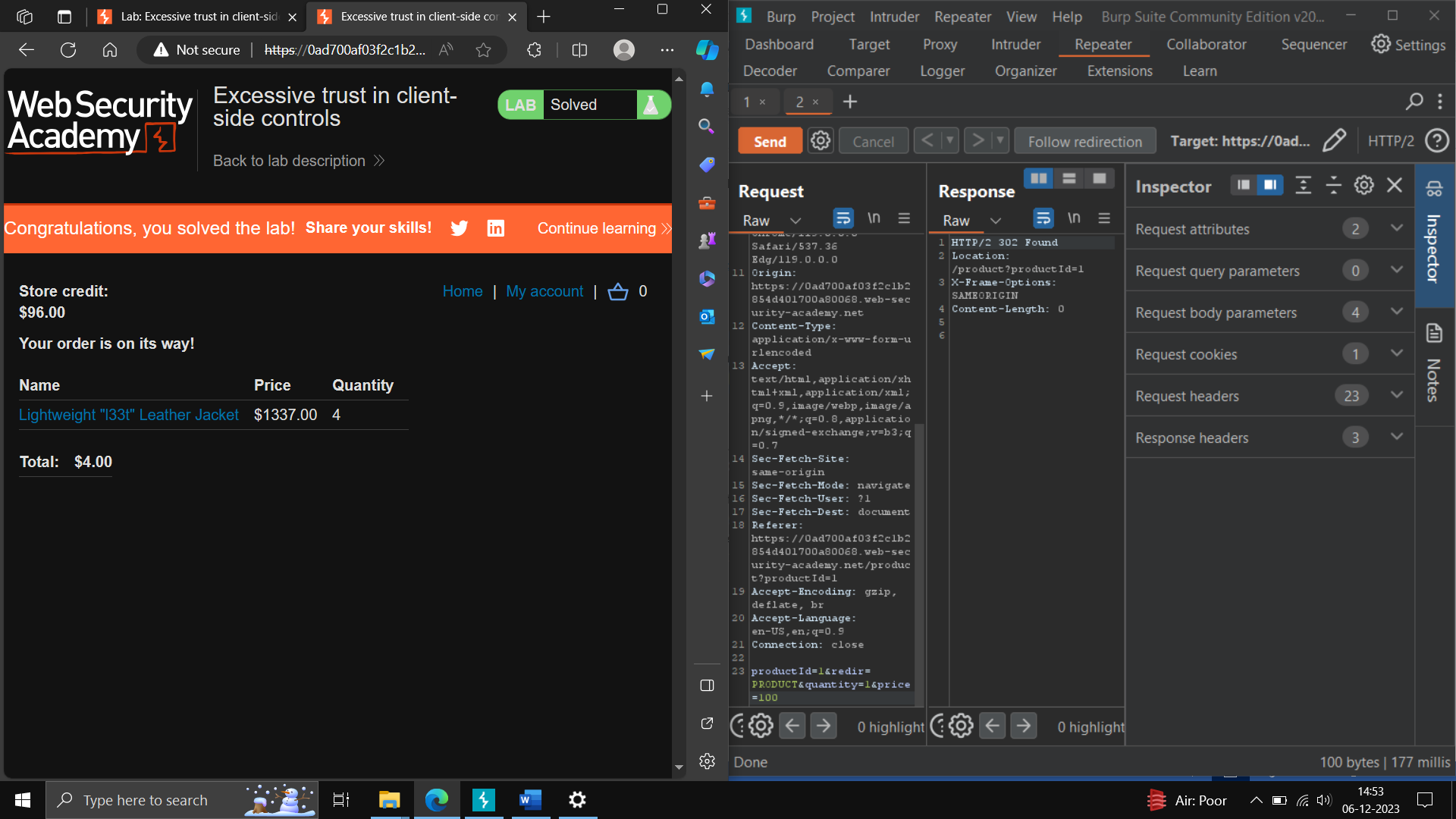
There must be a continuous testing, logic building.

POC –

Step1) open the website -> my account ->enter username and password, select any option from the website.



Step2) on the Intercept, click on add to cart in the website -> send the request to repeater-> off the intercept -> in the repeater change the cost according to your credit limit -> come to website, place the order -> reload the website



………………………………………………………………………………………………….

**5) Security Misconfiguration**

**Description:**

It arises in the website, server when configuration is not properly configured. It is important to ensure the application frameworks and servers and secure settings.

**Impact-**

By this vulnerability we can access someone account information, unsecure files, unencrypted files

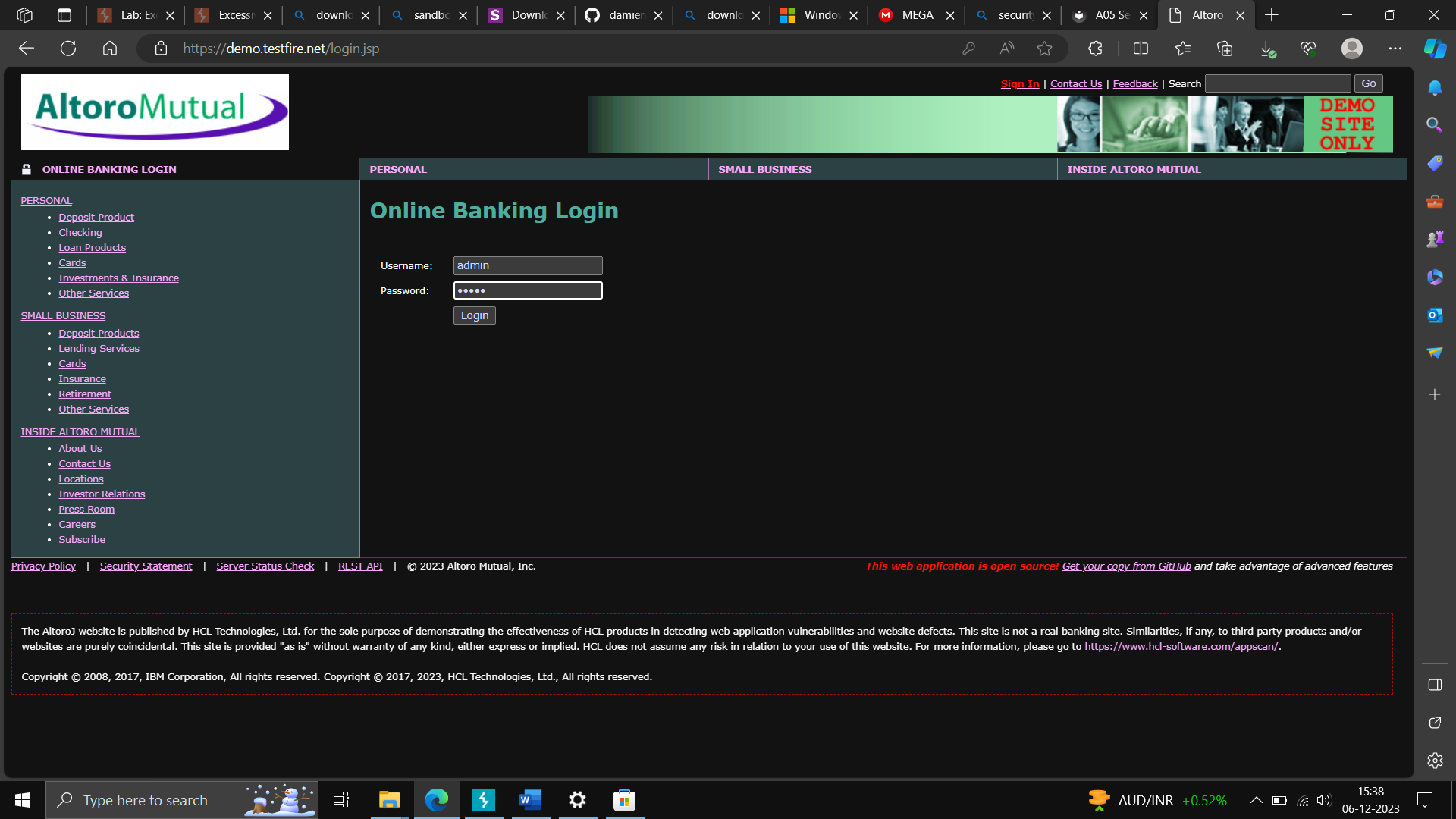
Preventions –

There should be regular test for the website security, there should regular audits, we should avoid unused features.

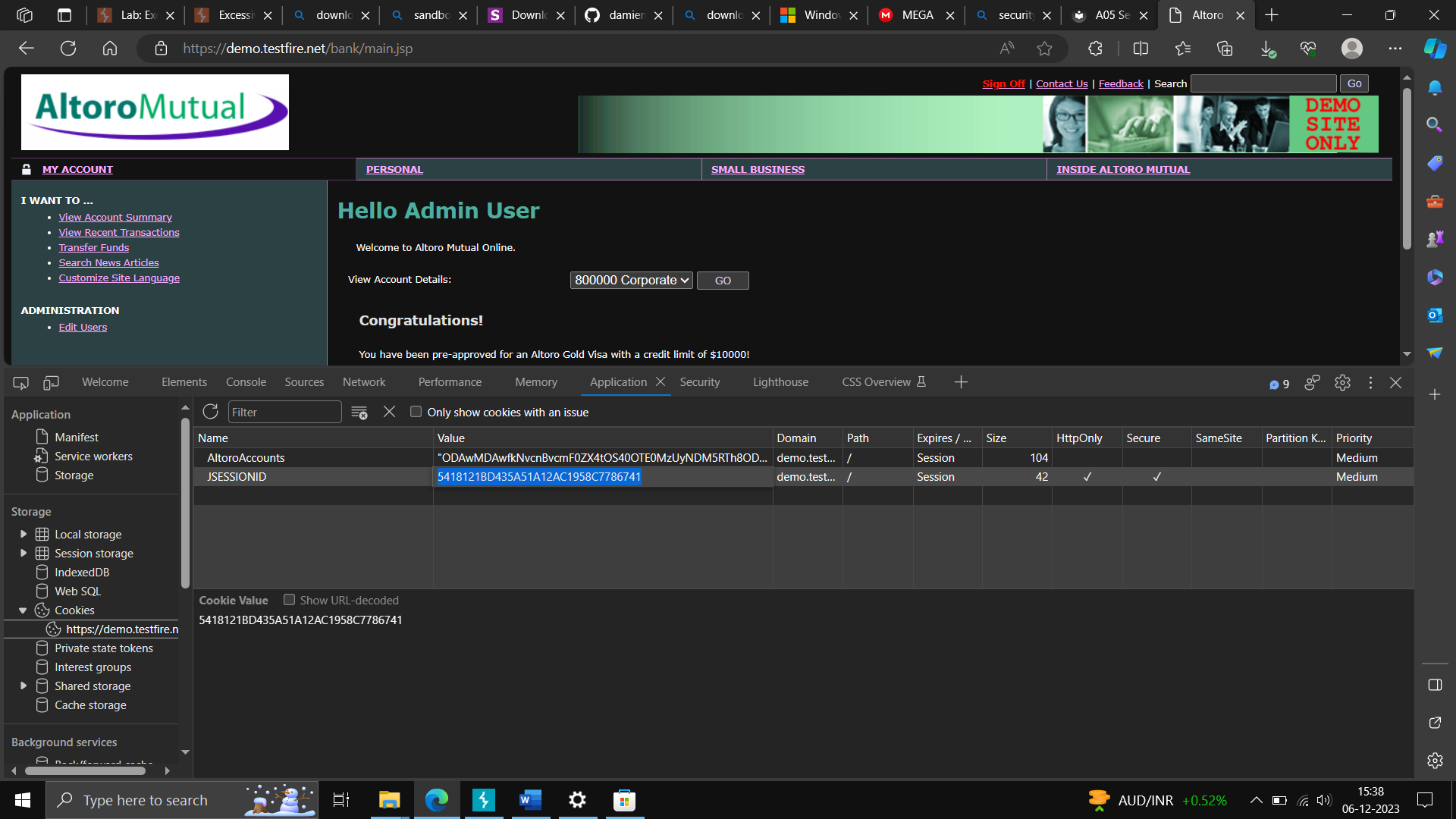
References- [A05 Security Misconfiguration - OWASP Top 10:2021](https://owasp.org/Top10/A05_2021-Security_Misconfiguration/)

POC

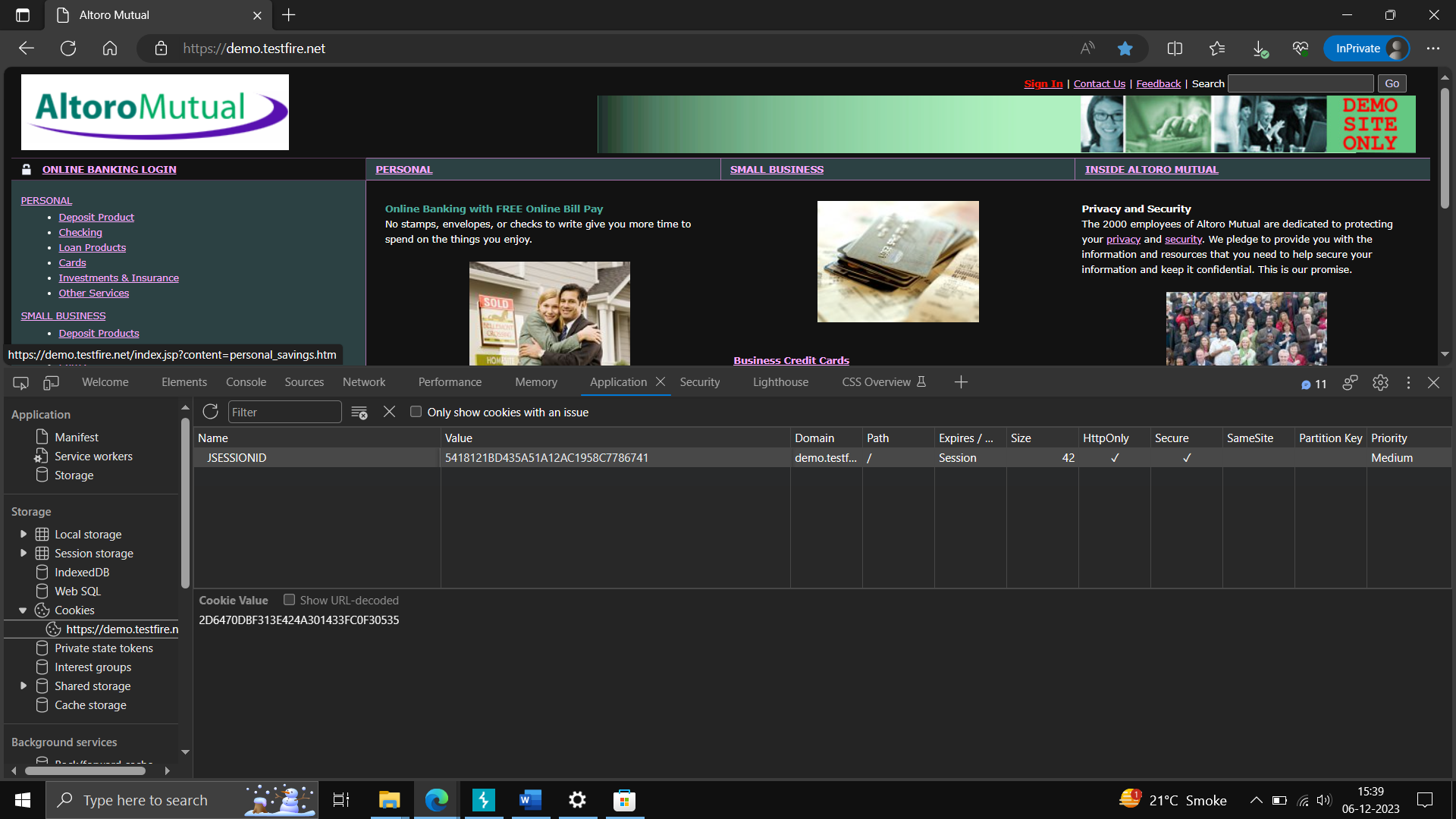
Step1-) open demo.testfire.net-> login as user name admin, password admin -> click on login ->



Step2) On the dashboard, right click inspect -> Storage/Application -> go on cookies -> view the site->copy the session -> paste in notepad ->



Step3)-go on any another browser like chrome, open the same website in browser-> right click on the screen, go on inspect element-> go on application->check the cookies and edit it with the cookies paste in notepad.



This attack is also called as Session Hijacking.