ASSIGNMENT – 1

CHECKING THE TOP 5 CWE VULNERABILITIES 2021

BY MOHIT YADAV

1. BROKEN ACCESS CONTROL:

Description:

The product does not restrict or incorrectly restrict access to a resource from an unauthorized actor.

BUSINESS IMPACT:

This weakness can have significant business impacts, like the effects of broken access control. Here's how it can affect a business:

Resource Allocation: Responding to a security incident consumes valuable resources. The IT team must investigate the vulnerability, implement fixes, communicate with stakeholders, and enhance security controls. This diverts resources from other critical projects.

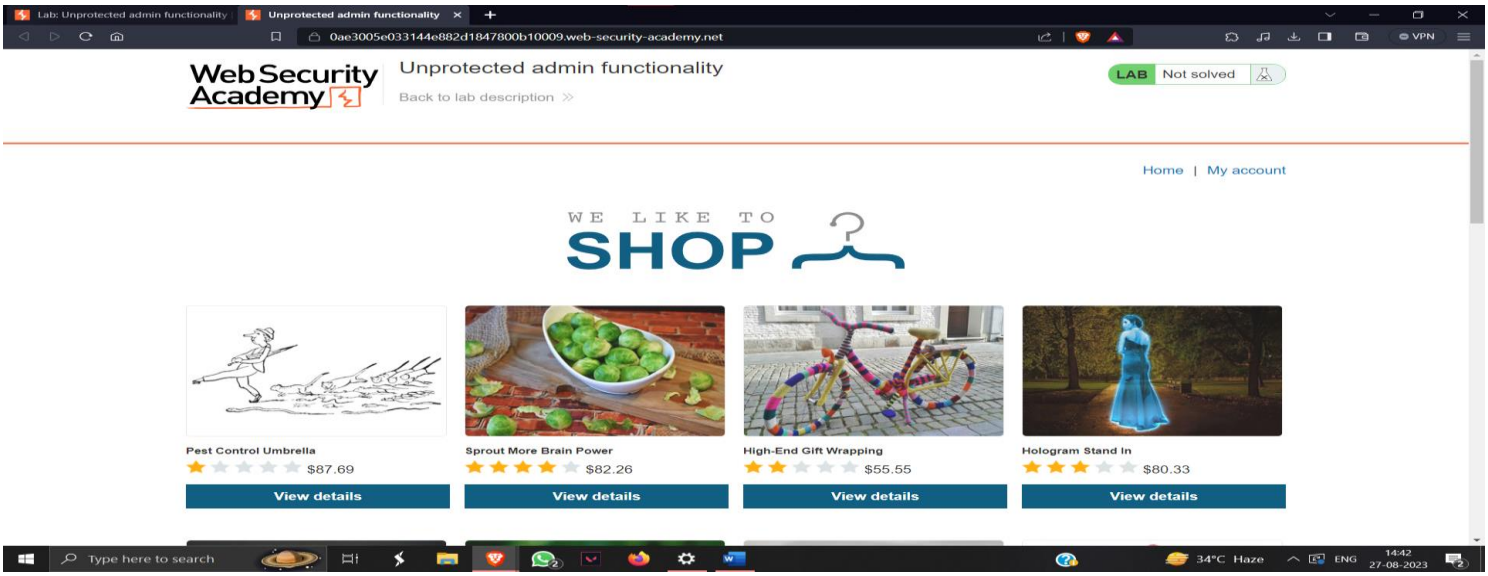
Business Continuity: If a security breach occurs due to improper access control, the application might need to be taken offline temporarily to address the issue. This downtime can disrupt business operations and lead to revenue loss.

Long-Term Impact: Even after addressing the immediate consequences of a vulnerability, companies might need to implement more stringent security measures. This can lead to delays in software development, increased costs, and decreased agility.

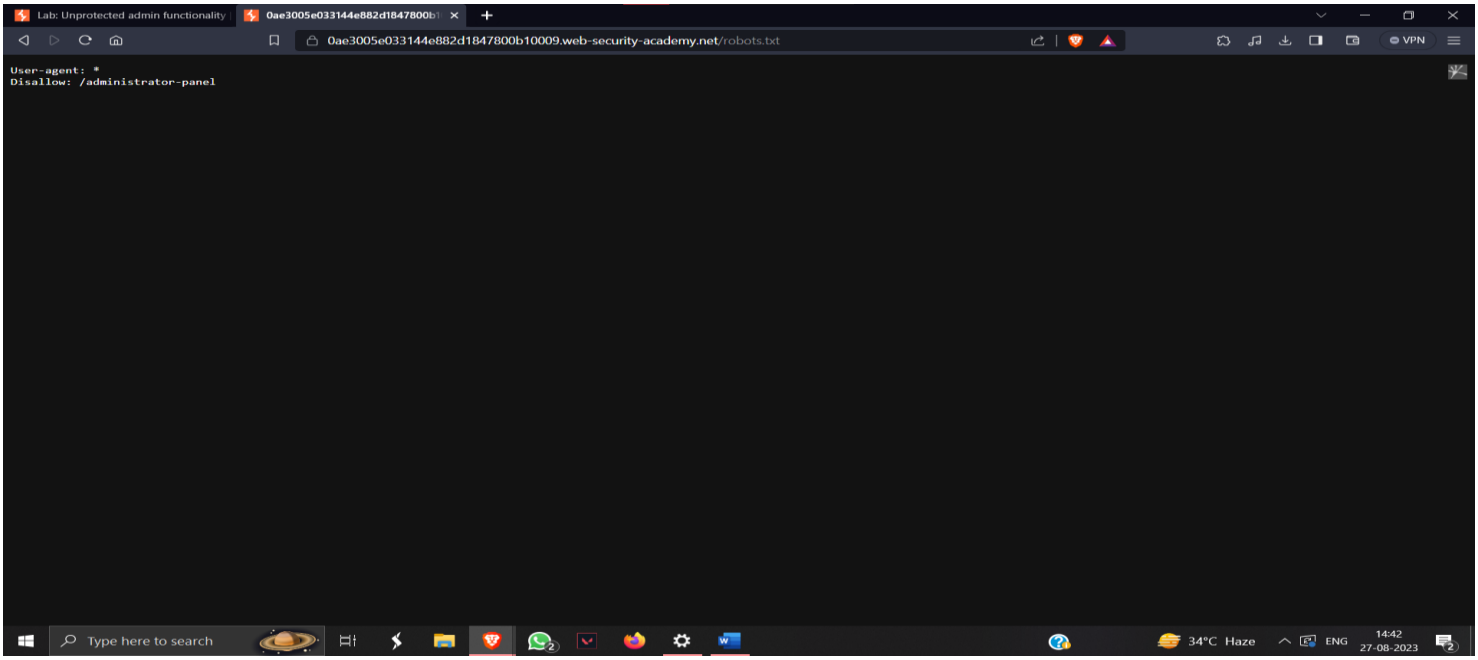
Loss of Customer Confidence: Customers may lose trust in the company's ability to protect their data and privacy, leading to decreased engagement and loyalty.

Now to implement this vulnerability,

We go to a shopping website:

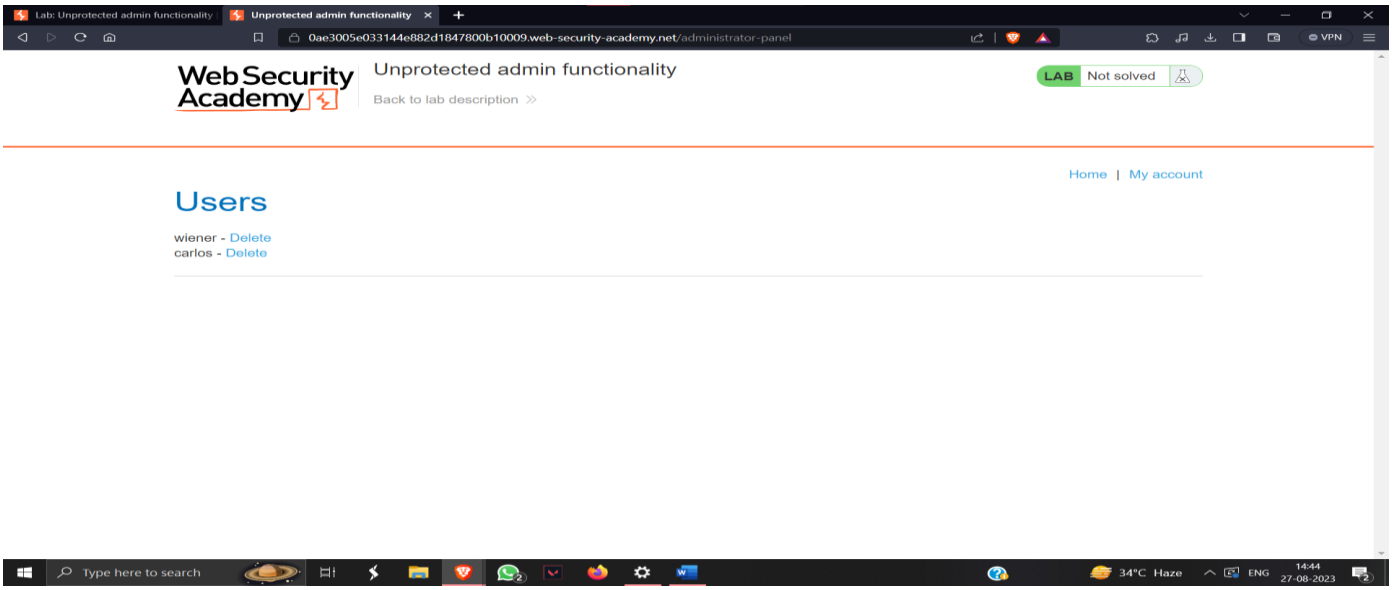


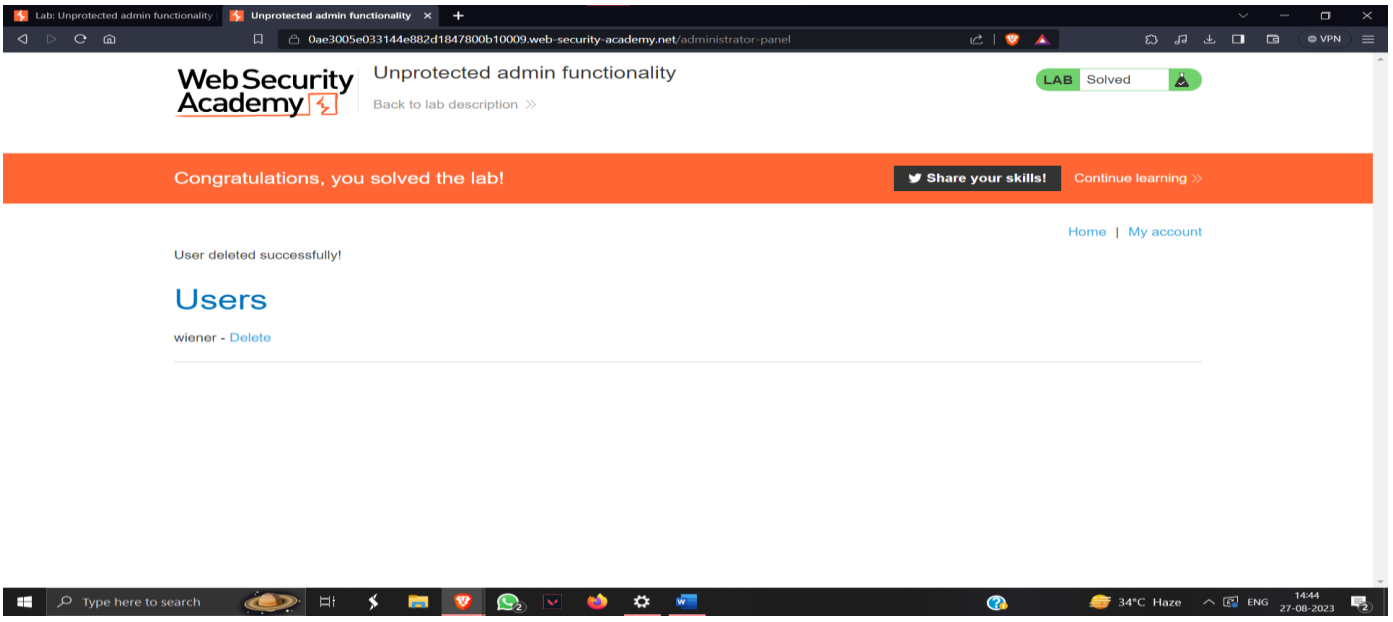
Now, we check if sensitive data is given in /robots.txt of the website.
We Get,



i.e., the site has a vulnerability of broken access control. Because we can use the Admin panel URL is given in the .txt URL

Therefore, we can access the admin panel of the website and delete or alter any account we want although we should not be able to access that.





Therefore, this website has a broken access control vulnerability.

2. CRYPTOGRAPHIC FAILURES:

Description:

The product stores or transmits sensitive data using an encryption scheme that is theoretically sound but is not strong enough for the level of protection required.

BUSINESS IMPACT:

This weakness can have serious business implications, as outlined below:

Data Exposure: Inadequate encryption strength can lead to unauthorized access to sensitive data. Attackers who exploit this weakness can decrypt encrypted data, potentially exposing sensitive information such as customer data, proprietary business information, and financial records.

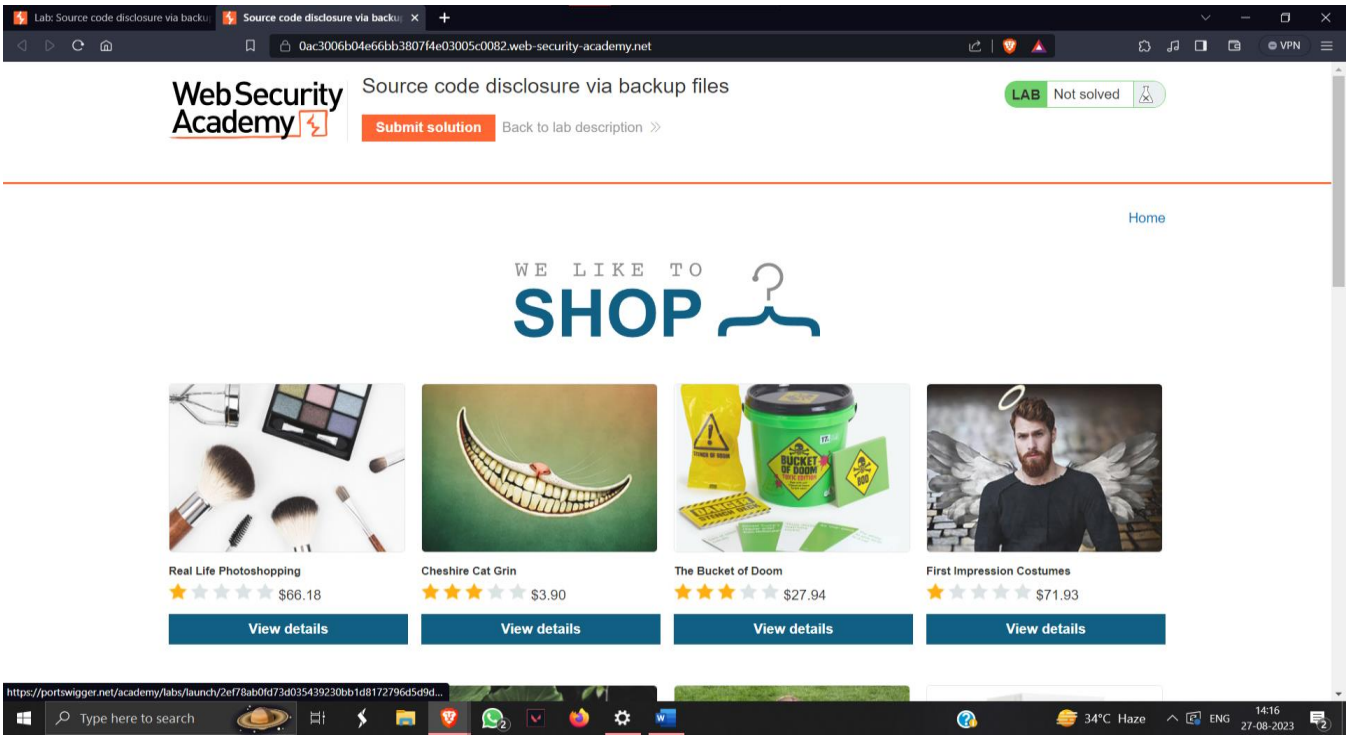
Data Breach: If attackers successfully decrypt sensitive data, it can lead to a data breach. This can result in legal and regulatory consequences, as well as damage to the organization's reputation.

Regulatory Non-Compliance: Many industries have regulations and standards that require certain levels of encryption to protect sensitive data. Inadequate encryption strength can lead to non-compliance with these regulations, resulting in fines, legal actions, and reputational damage.

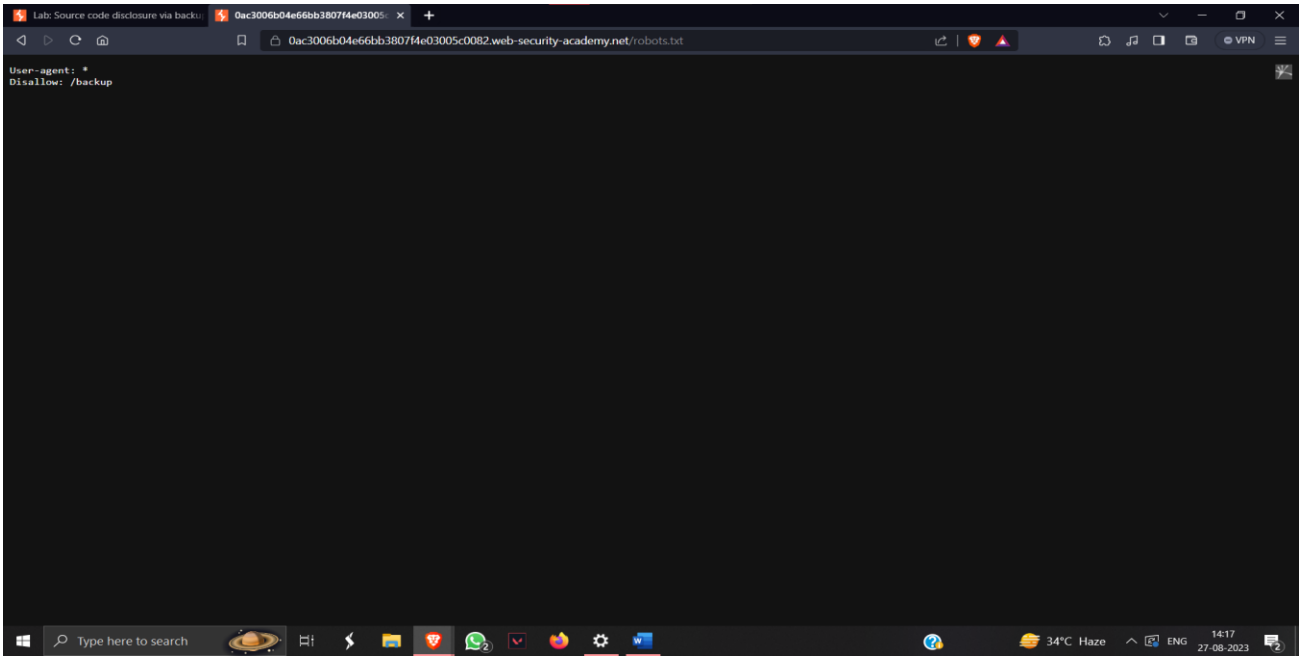
Legal Consequences: Organizations can face legal action from affected parties, such as customers or partners, if their data is compromised due to weak encryption. Legal battles can be expensive and harm the company's brand image.

Now to check this vulnerability,

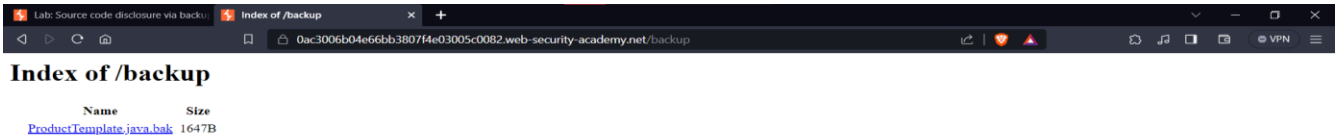
We go to a shopping website:



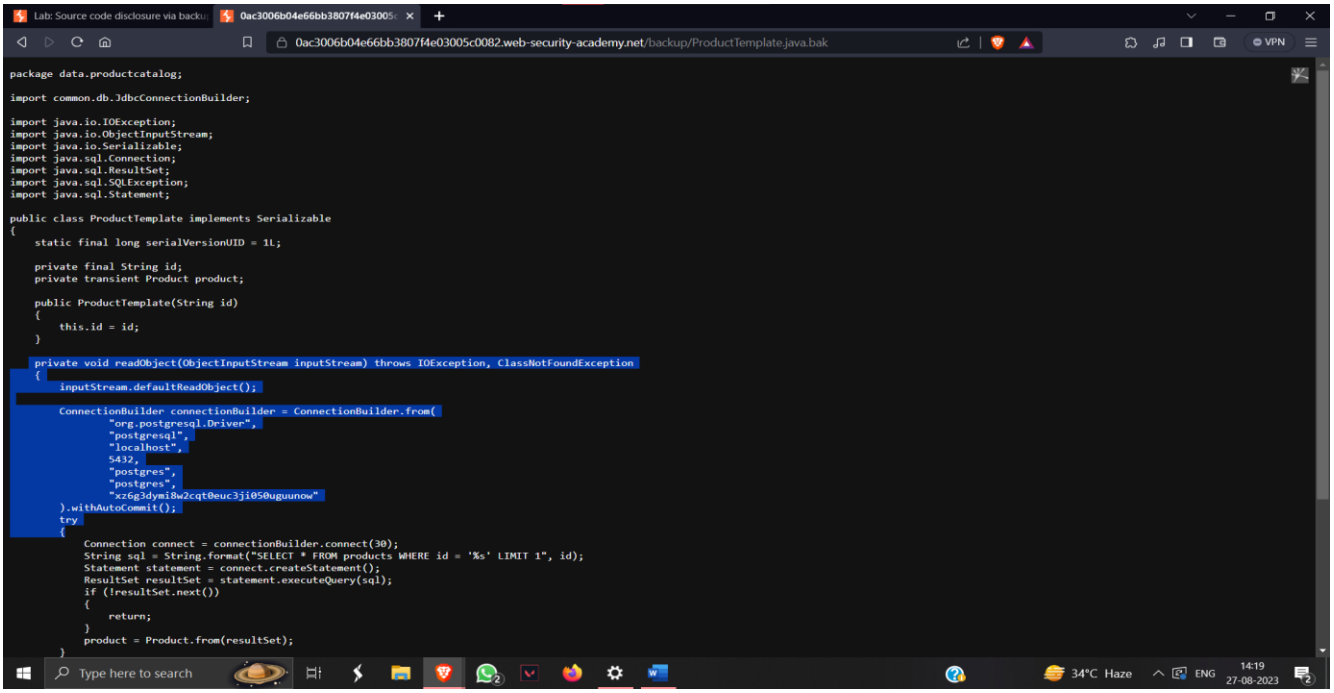
Change the URL of the website and add /robots.txt to find if there is some description.



We get a disallowed URL containing a link of backup file.



We use the URL in the SITE and get the decrypted password for the back up storage of website.



Therefore, we can say that the website has vulnerability in cryptographic failures as the password was not stored in encrypted manner.

3. INJECTION:

Description:

The product receives input from an upstream component, but it does not restrict or incorrectly restricts the input before it is used as an identifier for a resource that may be outside the intended sphere of control.

BUSINESS IMPACT:

This weakness can have significant business impacts, as outlined below:

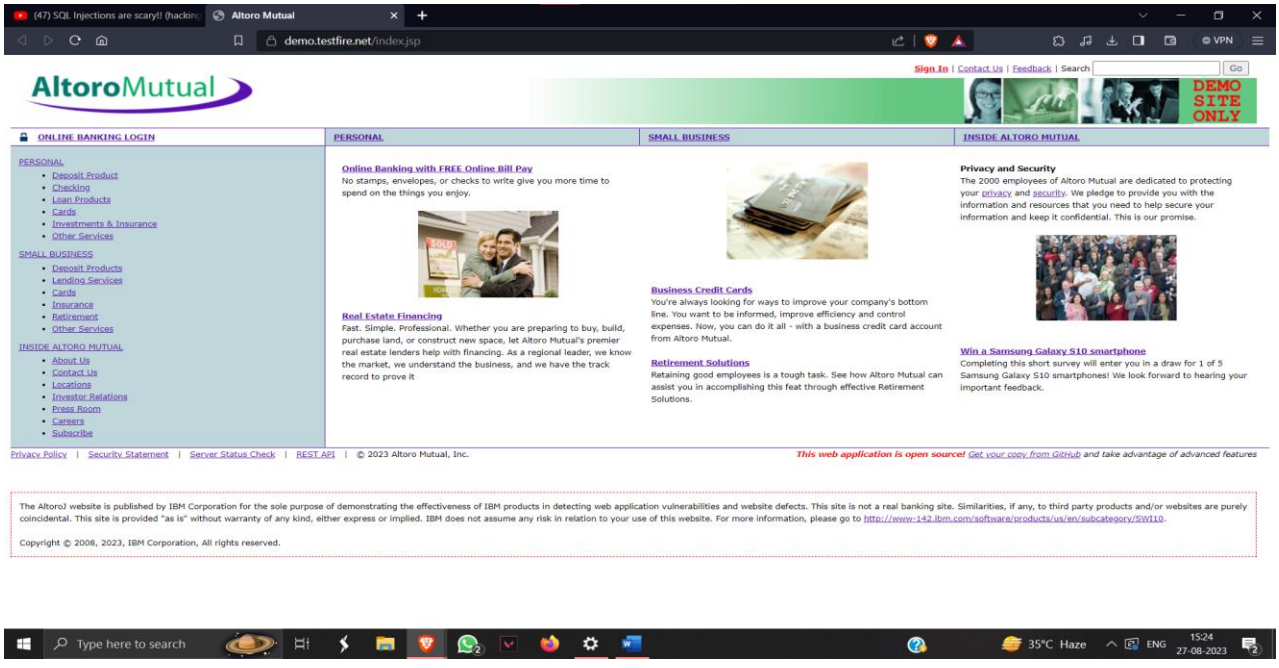
Unauthorized Access: Exploiting CWE-99 can allow attackers to access resources or functionalities they shouldn't be able to. This could include accessing sensitive data, privileged operations, or administrative functions, potentially leading to data breaches or unauthorized actions.

Data Leakage: Attackers could leverage resource injection to gain access to data they are not authorized to view. This data leakage can result in the exposure of confidential information, trade secrets, customer data, and intellectual property.

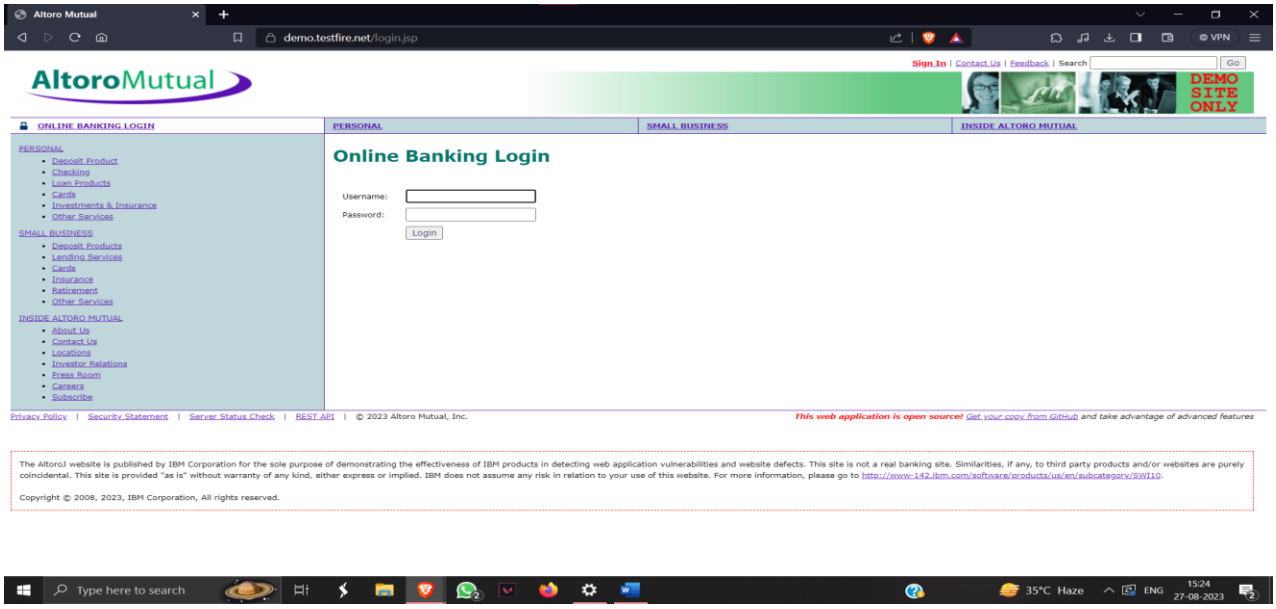
Unauthorized Actions: By manipulating resource identifiers, attackers might perform actions that they shouldn't be able to, such as modifying orders, altering account settings, or executing administrative tasks. These actions can disrupt business operations and damage data integrity.

To check this vulnerability, We:

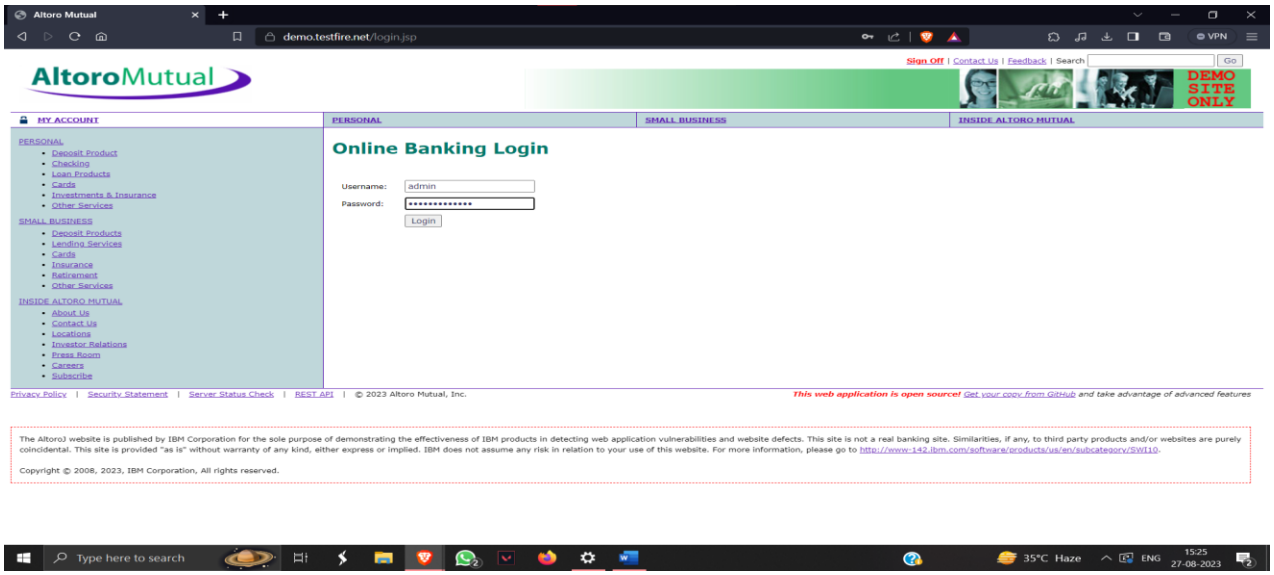
Visit a website. E.g., AltotoMutual



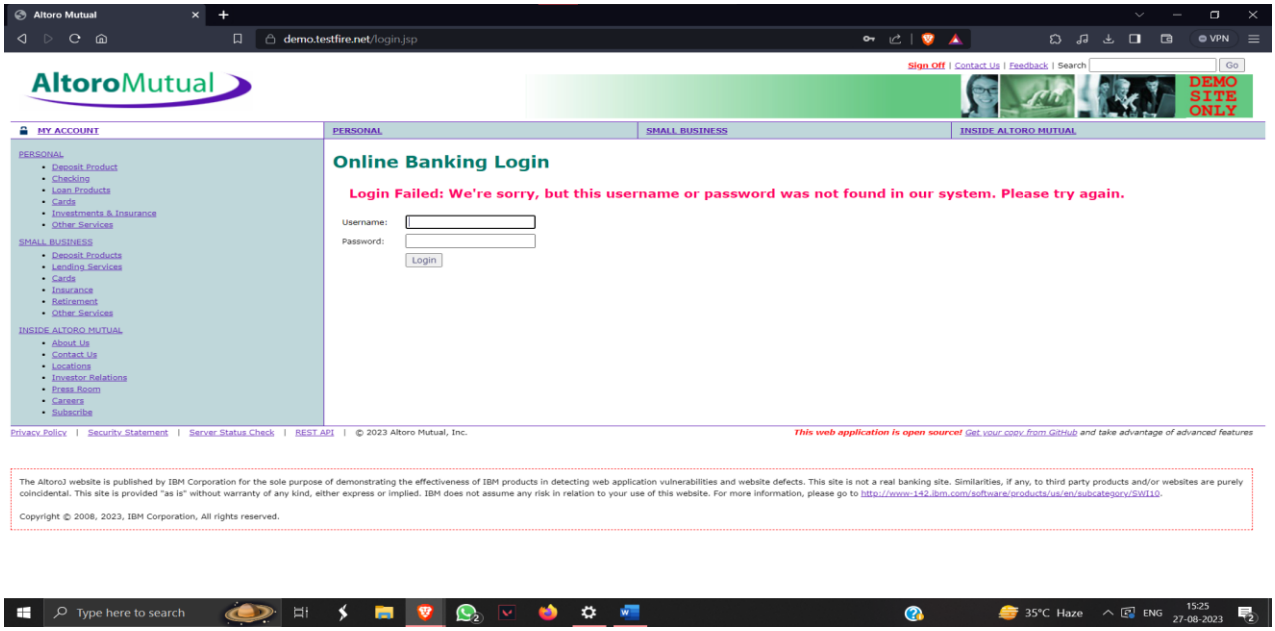
Go to the log in page:



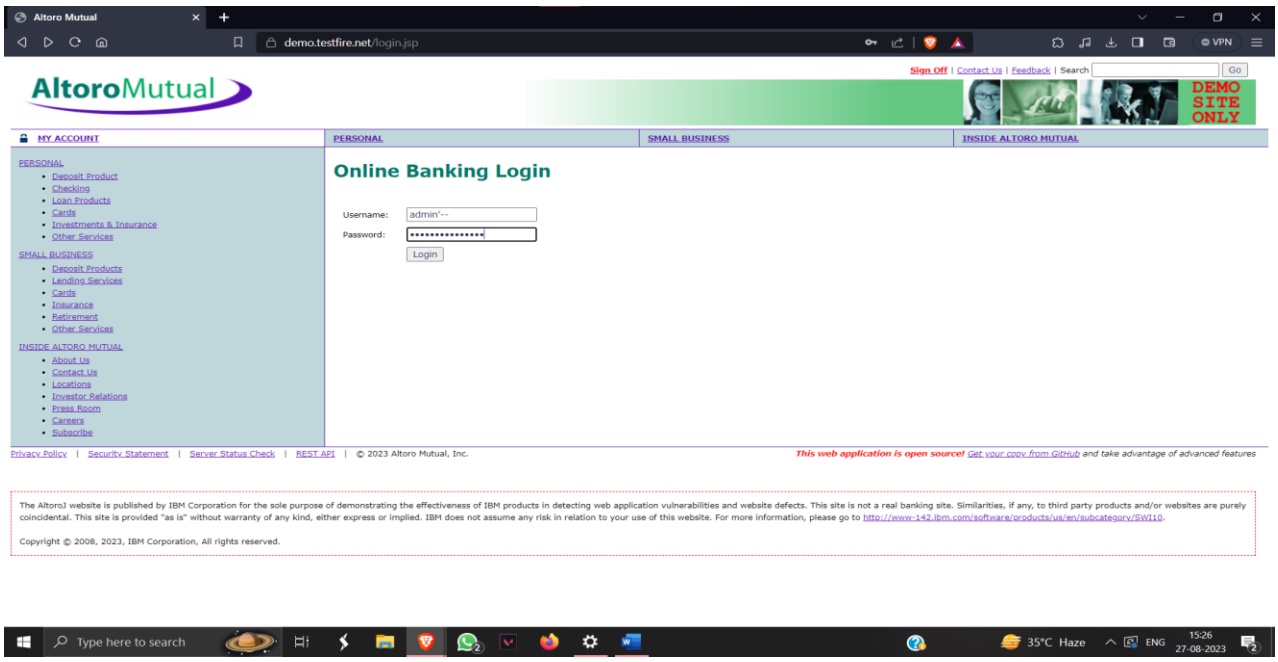
Try a random username and password:



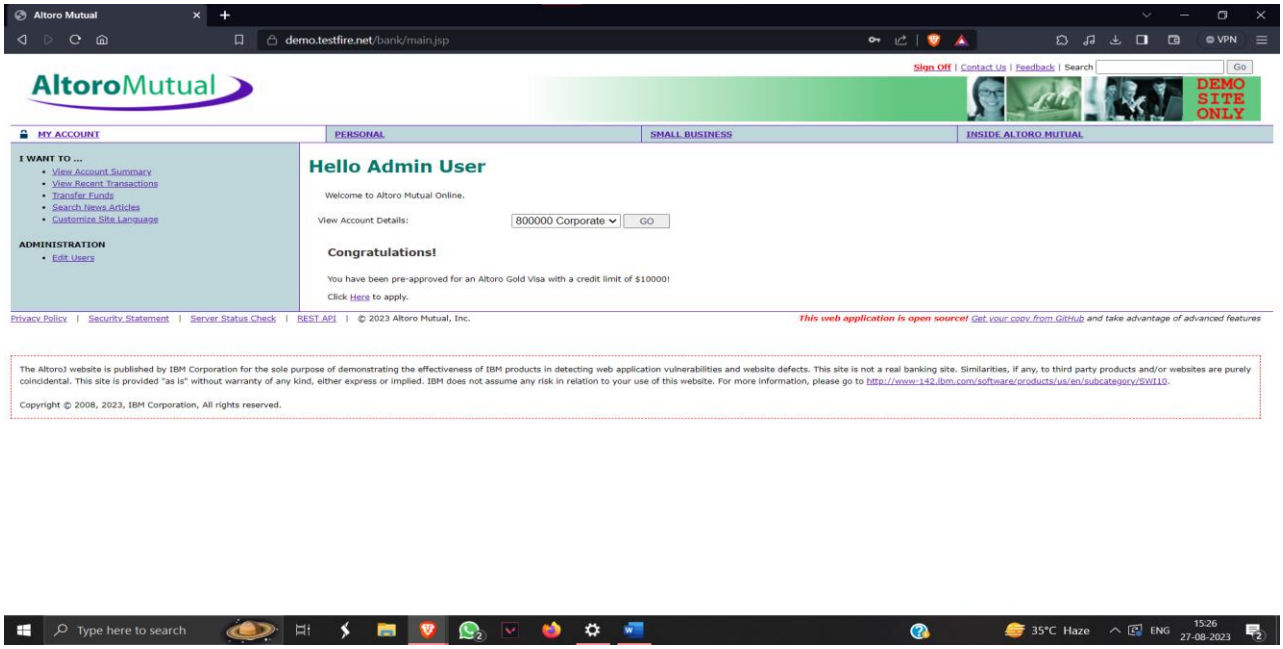
We get error saying wrong username and password.



Now we enter the username ending with "'--", what this does is check the SQL code and see if there is some vulnerability in it. If there is vulnerability, it's going to make the rest of the SQL statement as a comment and we will not require a password.



We successfully log in!!



Therefore, this website has SQL injection vulnerabilities.

4. INSECURE DESIGN:

Description:

The product violates well-established principles for secure design. This can introduce resultant weaknesses or make it easier for developers to introduce related weaknesses during implementation. Because code is centered around design, it can be resource-intensive to fix design problems.

BUSINESS IMPACT:

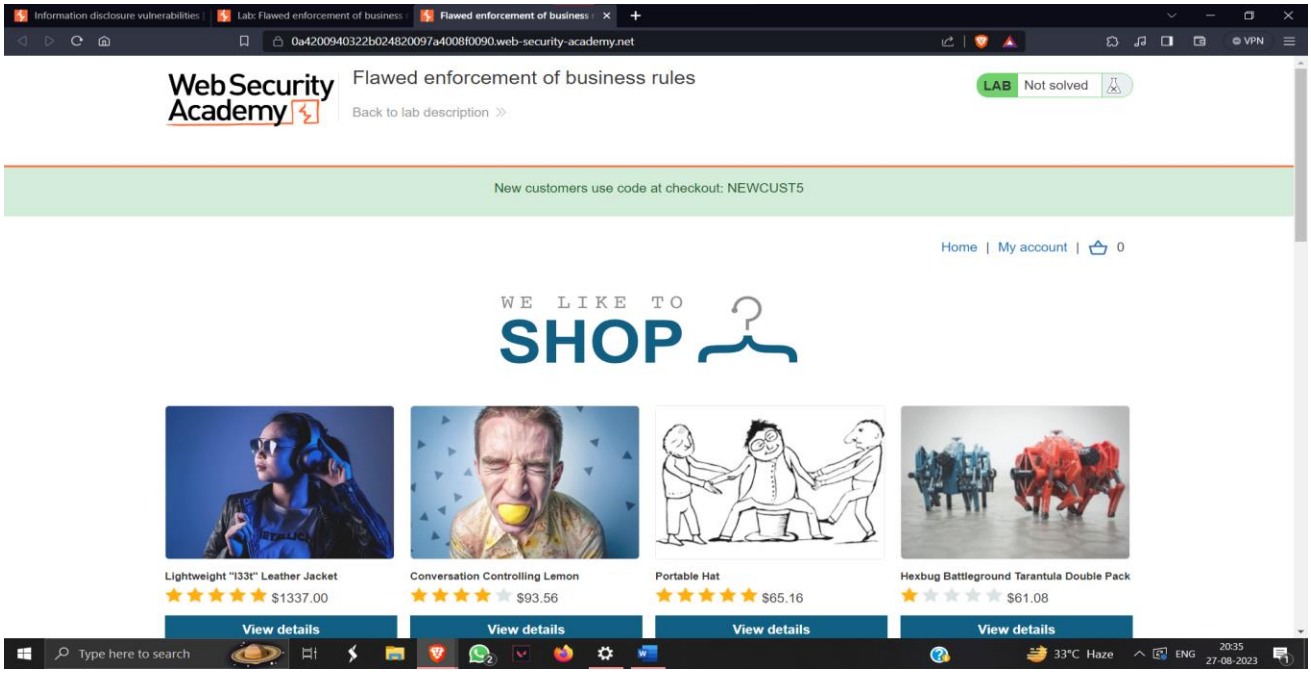
Security Vulnerabilities: Violating secure design principles can introduce vulnerabilities such as improper authentication, data leakage, privilege escalation, and more. These vulnerabilities can be exploited by attackers to compromise the application's security and gain unauthorized access to sensitive data or functionalities.

Reputation Damage: News of data breaches or security vulnerabilities can harm the organization's reputation. Customers and partners may lose trust in the organization's ability to protect their data, leading to reduced business and customer churn.

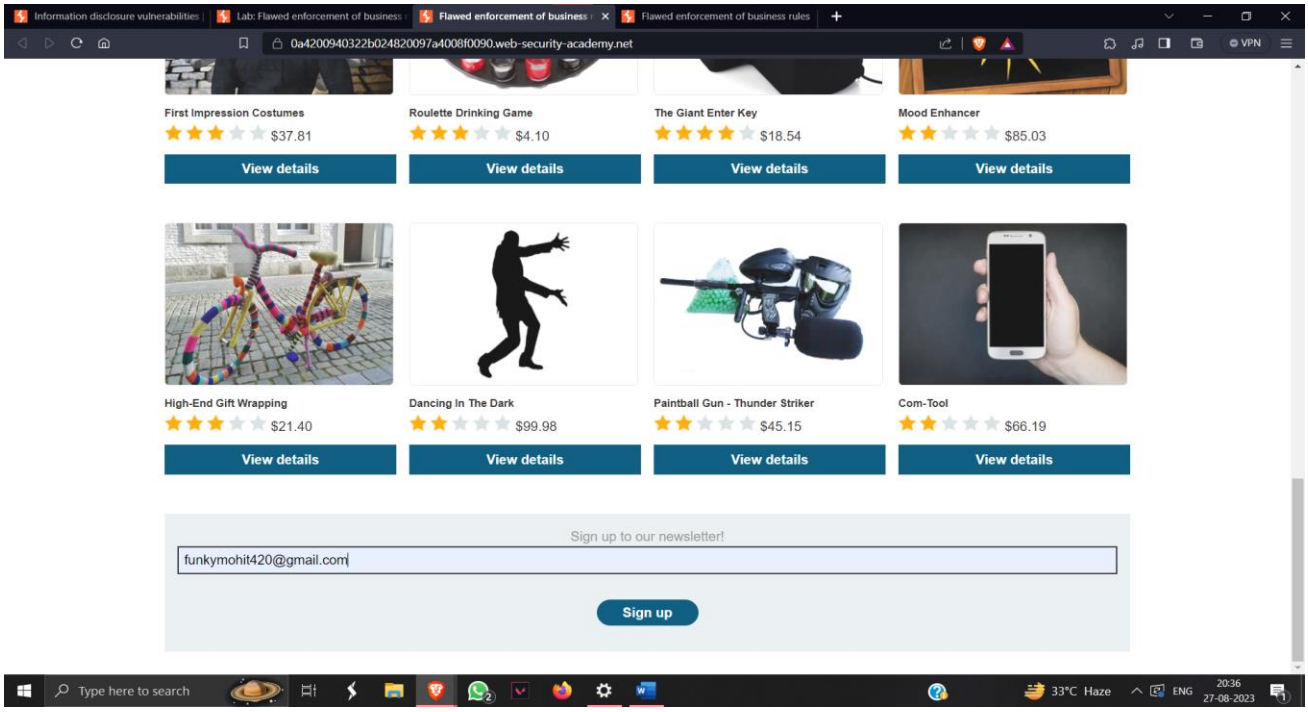
Legal and Regulatory Consequences: Depending on the type of data involved and industry regulations (e.g., GDPR, HIPAA), violations of secure design principles can lead to non-compliance, legal actions, fines, and reputational damage.

Now to implement or check this vulnerability.

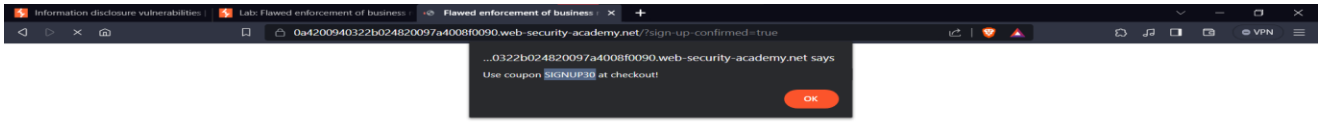
We visit a shopping website:

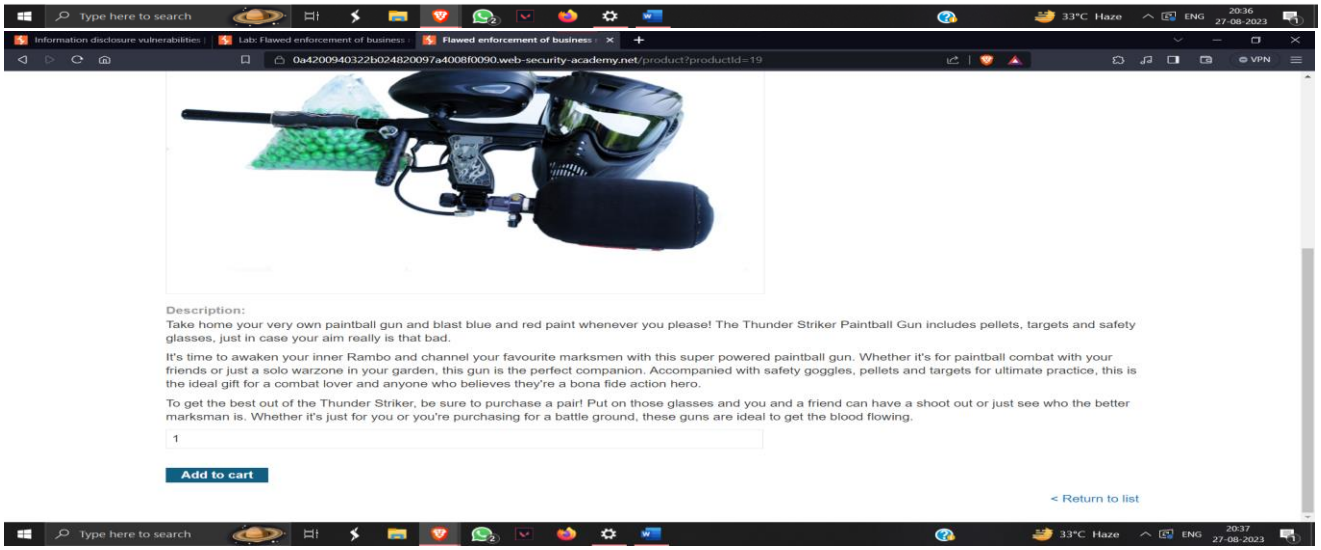


We can sign up without a password!!:

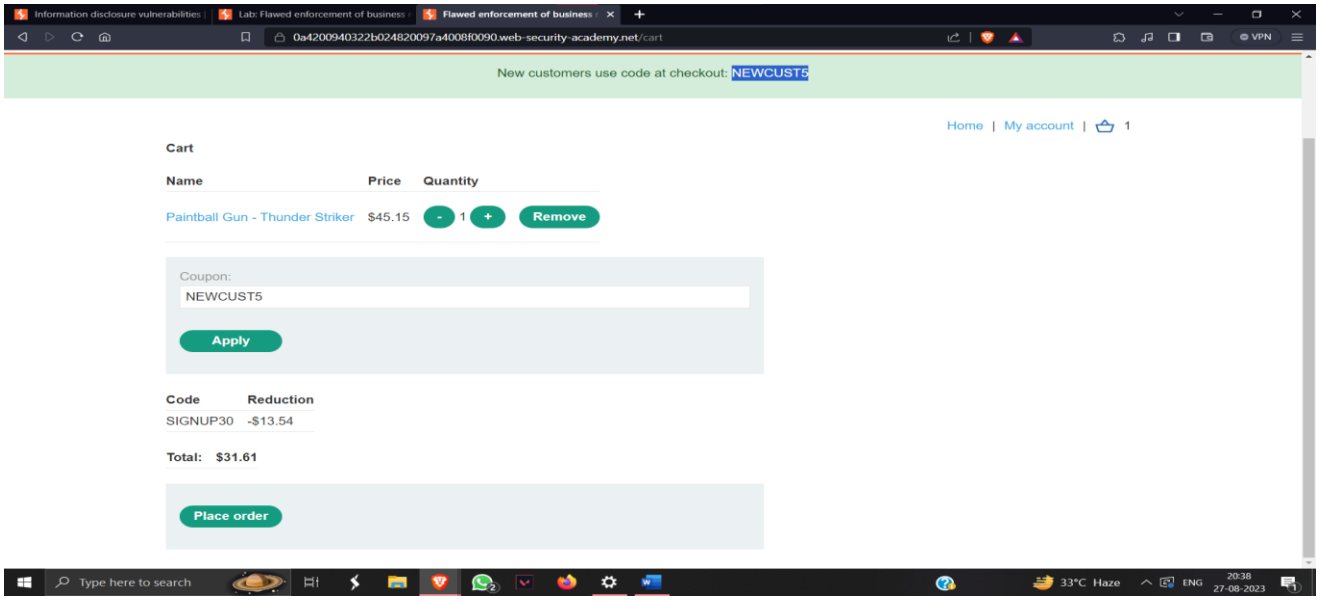


We get a COUPON code!!

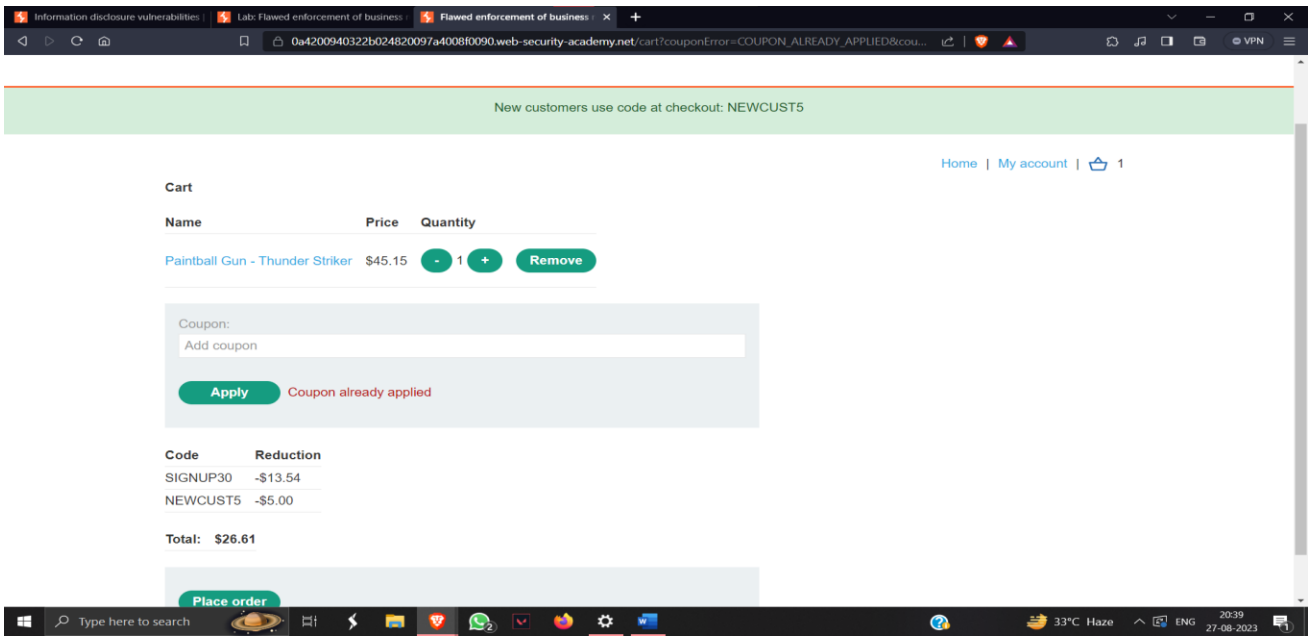




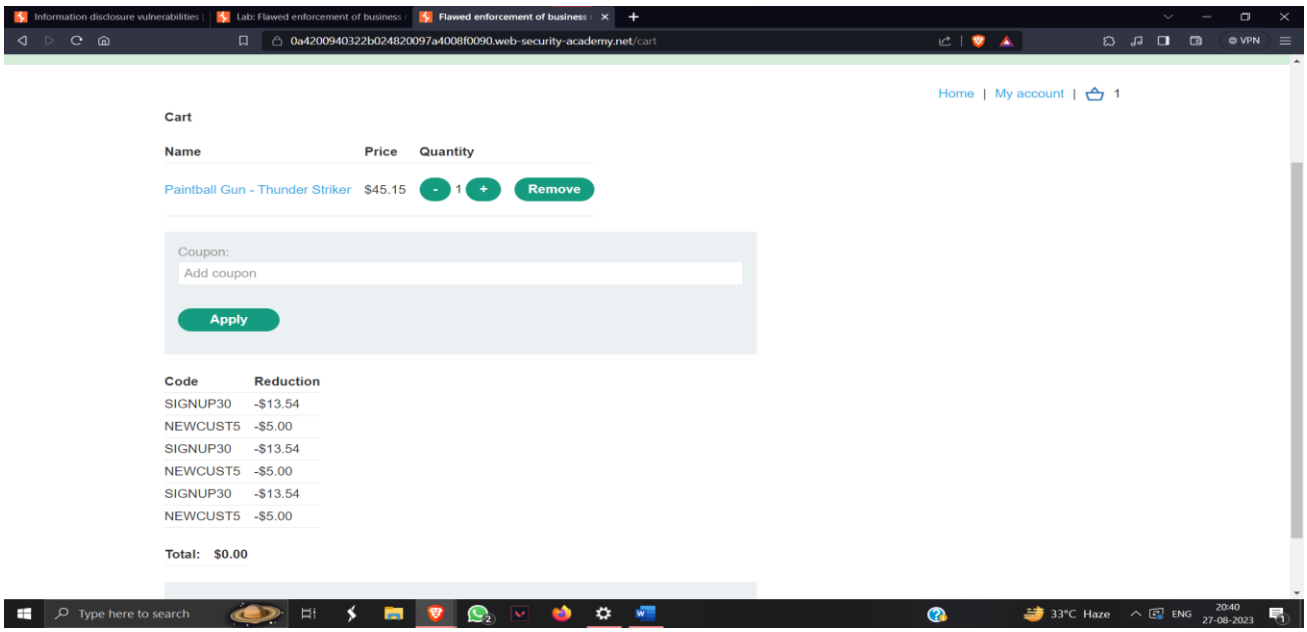
We proceed to check out and apply both our given COUPONS.



But we can’t apply for the same coupon again.



But if we enter both the coupons alternatively, then we can use both the coupons as many times.



We check out with Total 0$

Therefore, this website has an insecure build as many attackers can take advantage of this and can even guess the SQL code which may be more dangerous.

5. SECURITY MISCONFIGURATION:

Description:

Weaknesses in this category are typically introduced during the configuration of the software.

BUSINESS IMPACT:

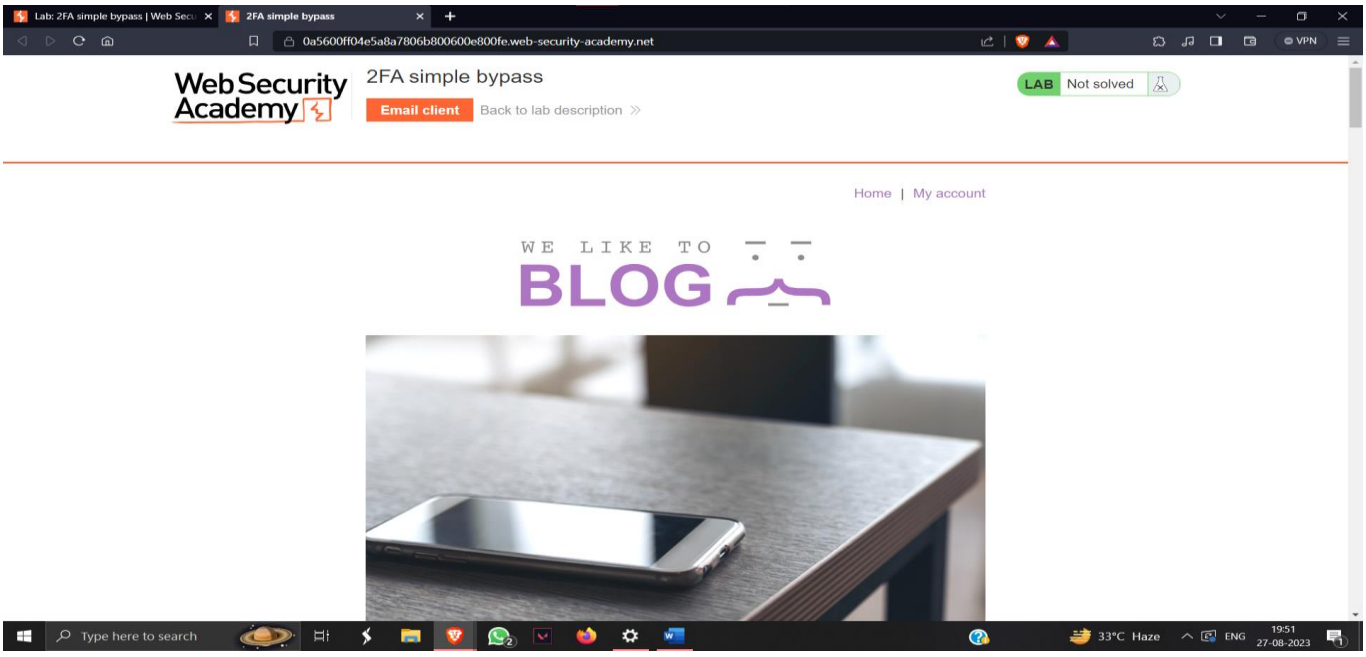
Operational Disruption: Misconfigurations can lead to technical glitches, outages, and reduced system performance, affecting business operations and customer experiences.

Long-Term Impact: Addressing misconfigurations might require ongoing monitoring and improvements to prevent recurrence. This can lead to increased maintenance costs and decreased agility in development.

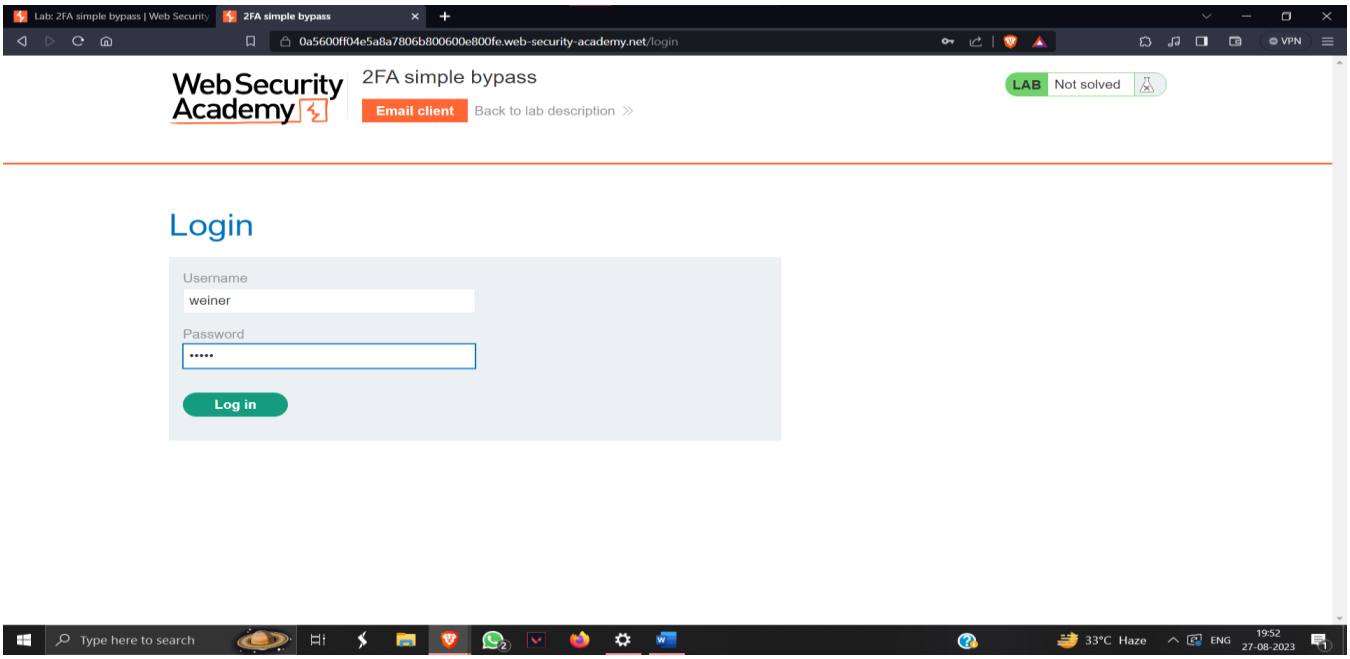
Regulatory Non-Compliance: Misconfigured settings can lead to non-compliance with industry regulations and standards, such as GDPR or HIPAA. This can result in legal actions, fines, and reputational harm.

Now to implement or to check the vulnerability;

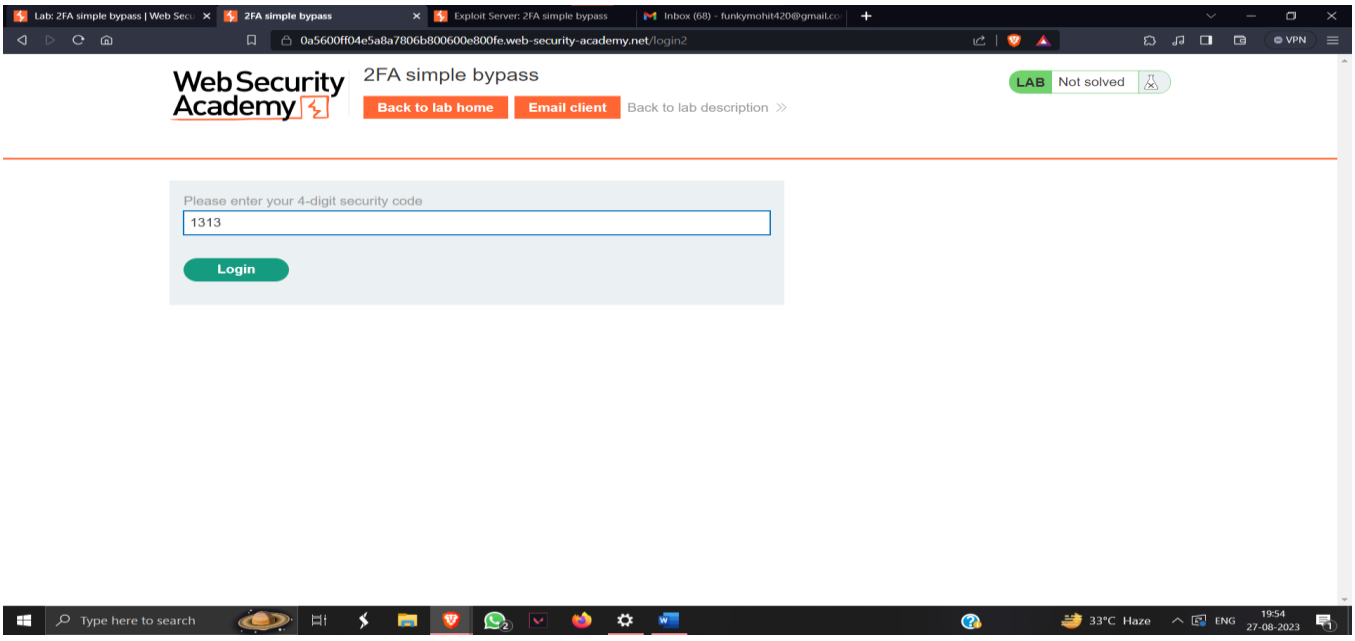
We got to a Blog wesbiste:



LOG IN USING THE GIVEN CREDENTIALS:

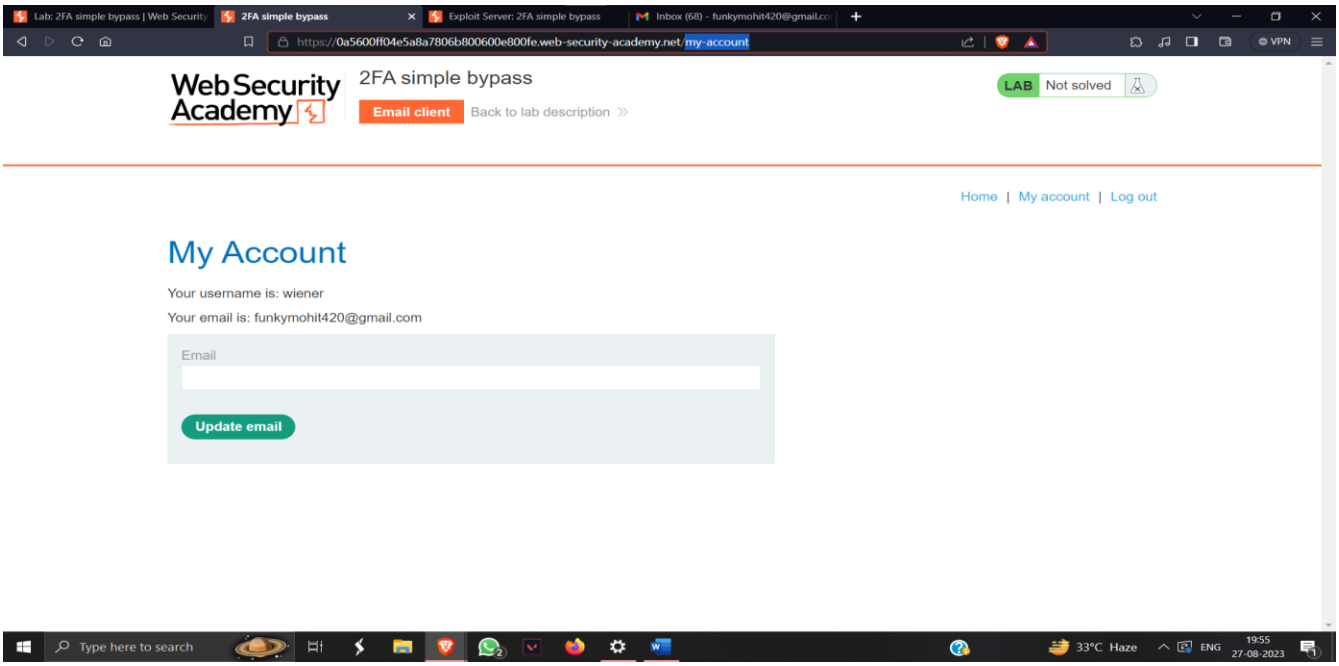


Enter the OTP given in the email:

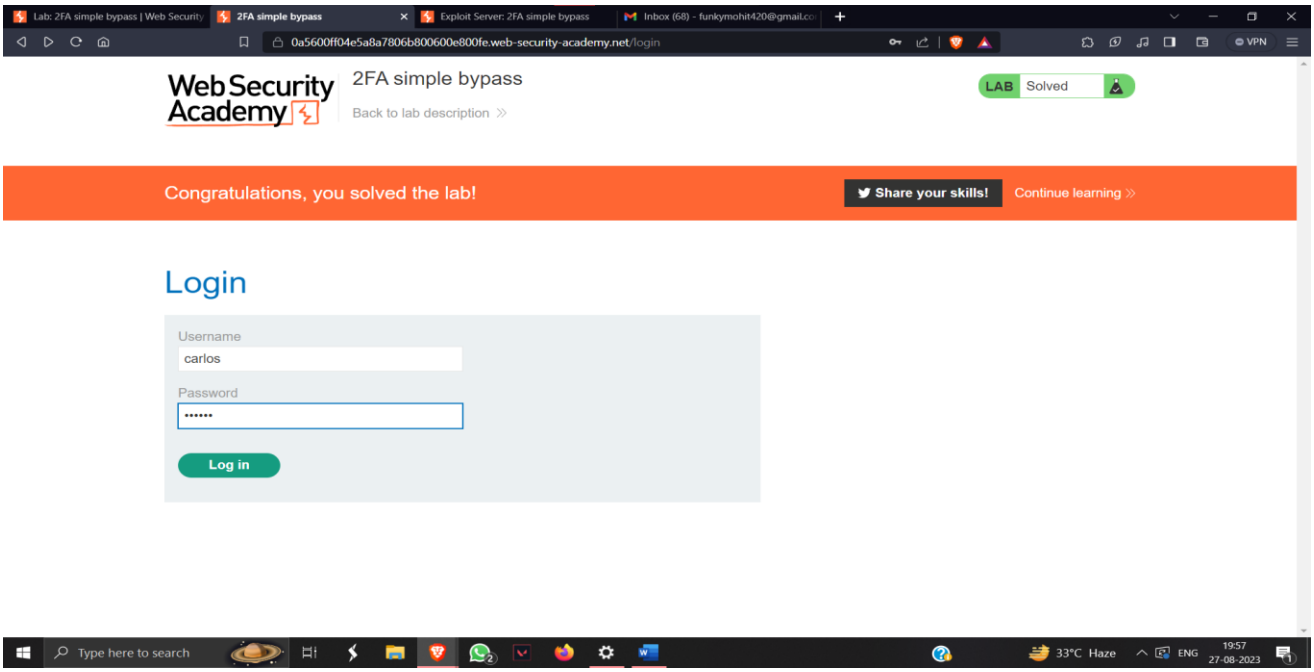


We logged in successfully.

Now we notice the URL of the logged in account.

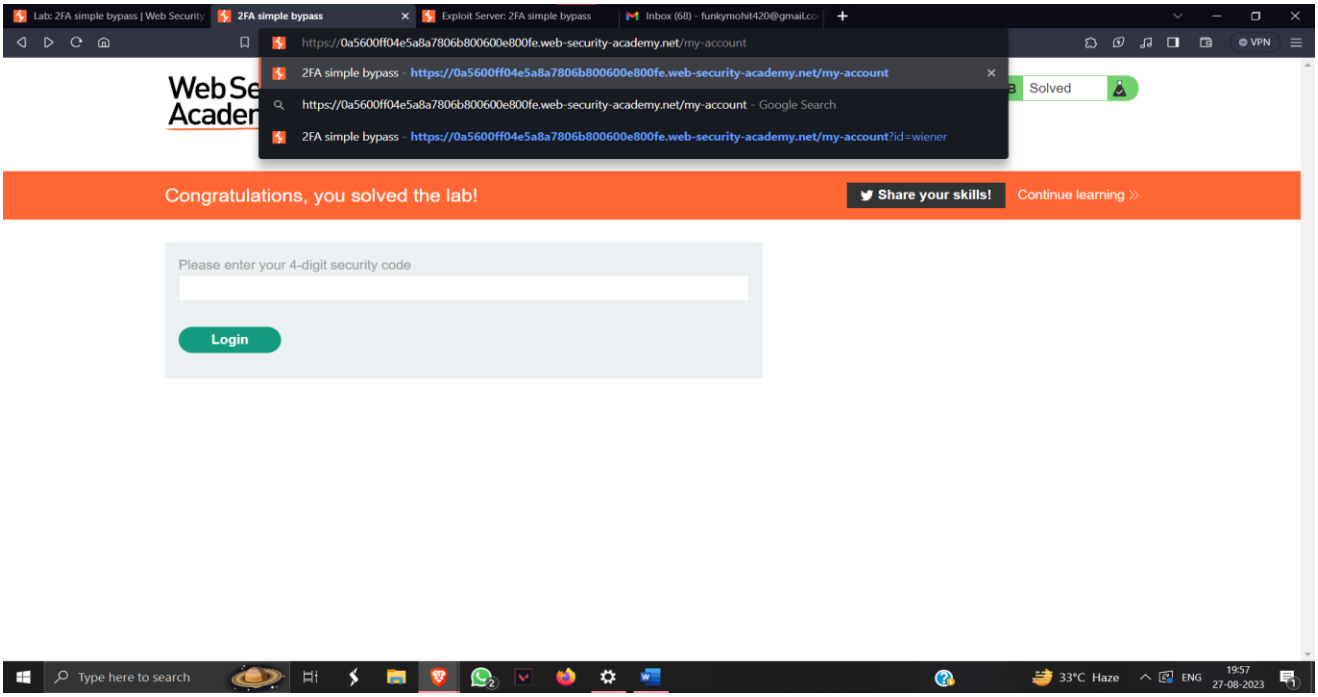


Now we log in with victim's credentials,

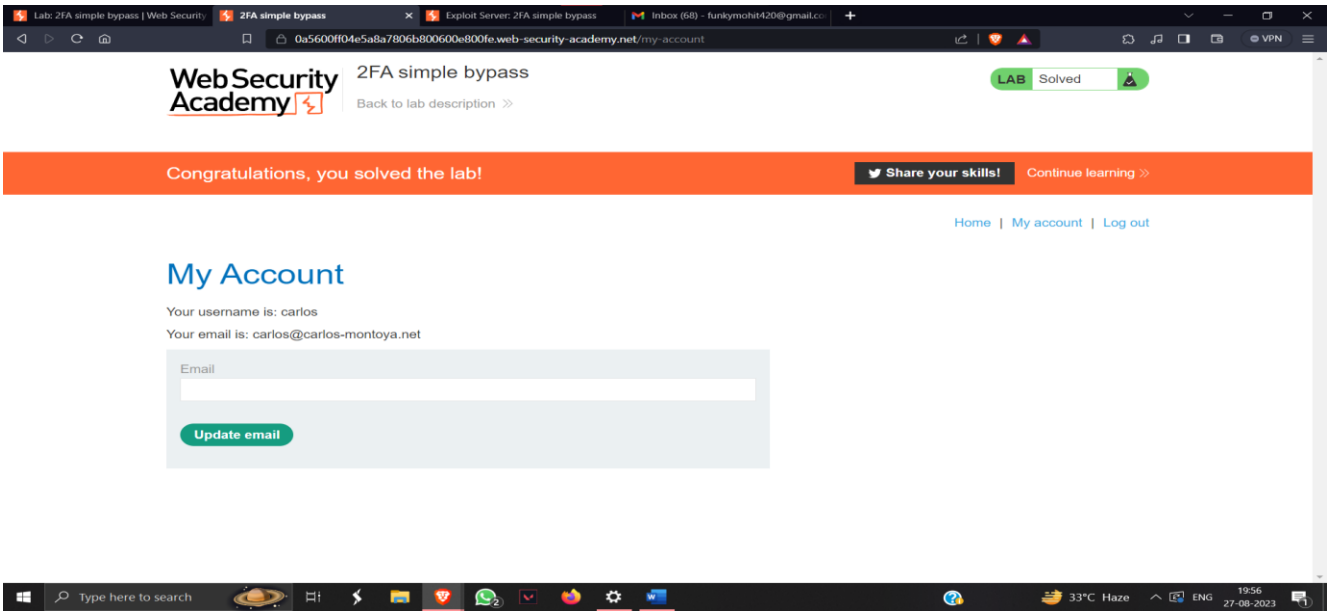


We don't have his email ID so we can't tell the OTP.

So, we changed the URL to the same URL of that of the logged in account.



WE LOG IN SUCCESSFULLY !!!



Therefore, this website has Security misconfiguration vulnerability.