

Web Application Security

Learn about web applications and explore some of their common security issues.

Task 1 Introduction

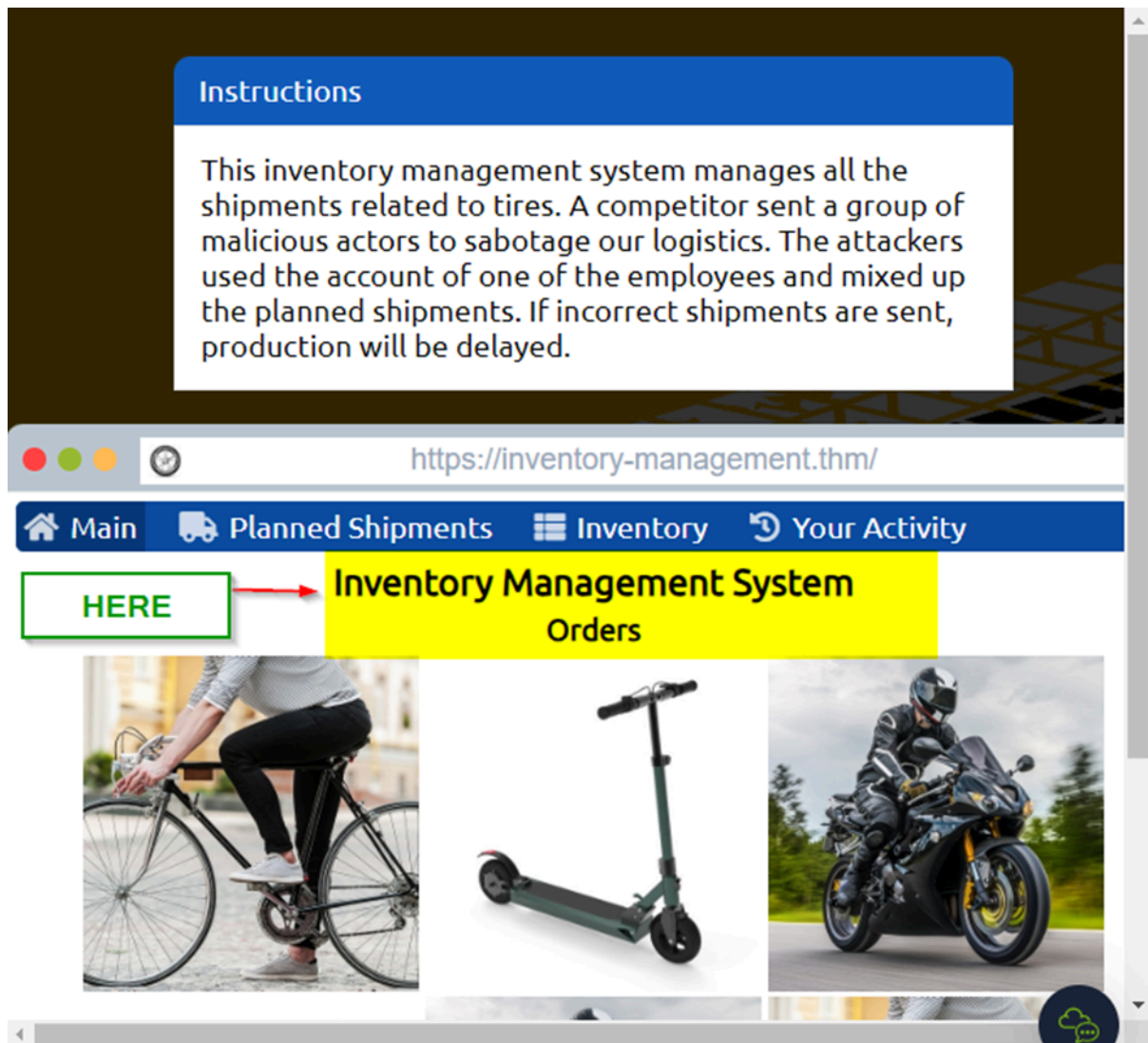
Question	Answer
What do you need to access a web application?	Browser

Task 2 Web Application Security Risks

Question	Answer
You discovered that the login page allows an unlimited number of login attempts without trying to slow down the user or lock the account. What is the category of this security risk?	Identification and Authentication Failure
You noticed that the username and password are sent in cleartext without encryption. What is the category of this security risk?	Cryptographic Failures

Task 3 Practical Example of Web Application Security

Upon clicking the "View Site" button, I was directed to a page displaying an Inventory Management System.



When I clicked on "Planned Shipments," I discovered evidence suggesting that an attacker has manipulated data as part of sabotage plans.

Where

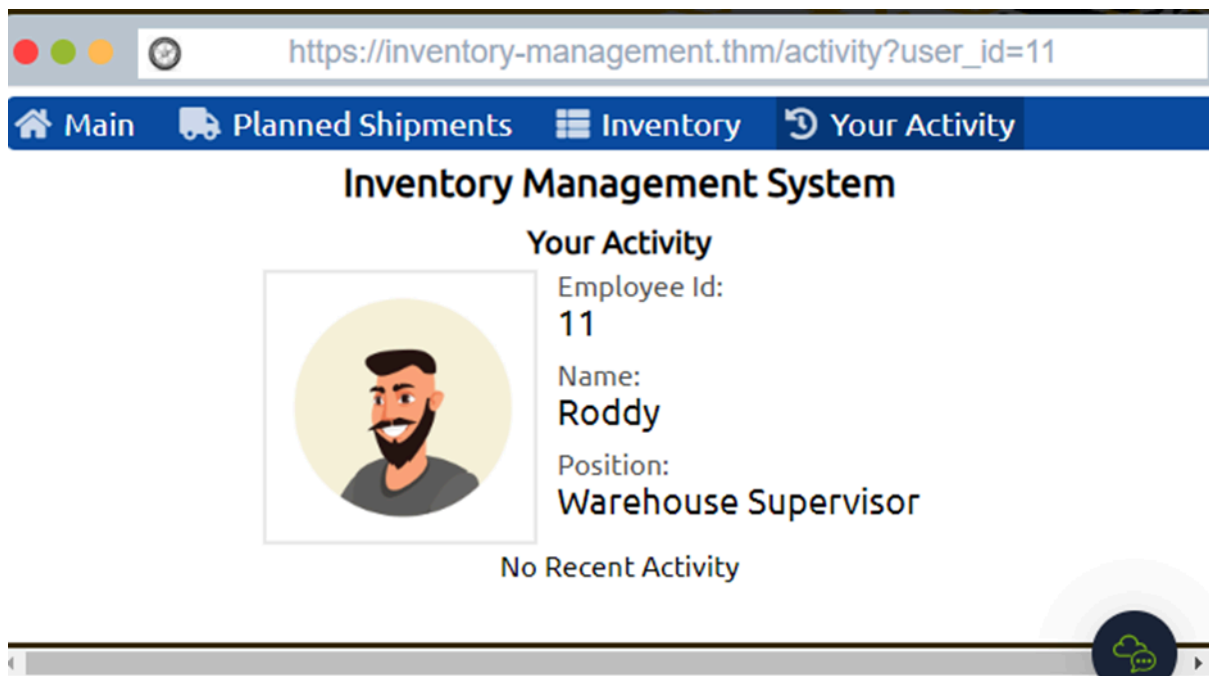
- SKU0253 and SKU0522 are listed under "Bike Assembly" (Winter Scooter Tires and Sport Motorcycle Tires).
- SKU0013 and SKU0524 are listed under "Scooter Assembly" (Sport Road Bike Tires and Sport Motorcycle Tires).
- SKU0015 and SKU0257 are listed under "Motorcycle Assembly" (Mountain Bike Tires and Racing Scooter Tires).

Correct listing should be

- SKU0013 and SKU0015 should be under "Bike Assembly" (Sport Road Bike Tires and Mountain Bike Tires).
- SKU0253 and SKU0257 should be under "Scooter Assembly" (Winter Scooter Tires and Racing Scooter Tires).
- SKU0522 and SKU0524 should be under "Motorcycle Assembly" (Sport Motorcycle Tires Sport Motorcycle Tires).

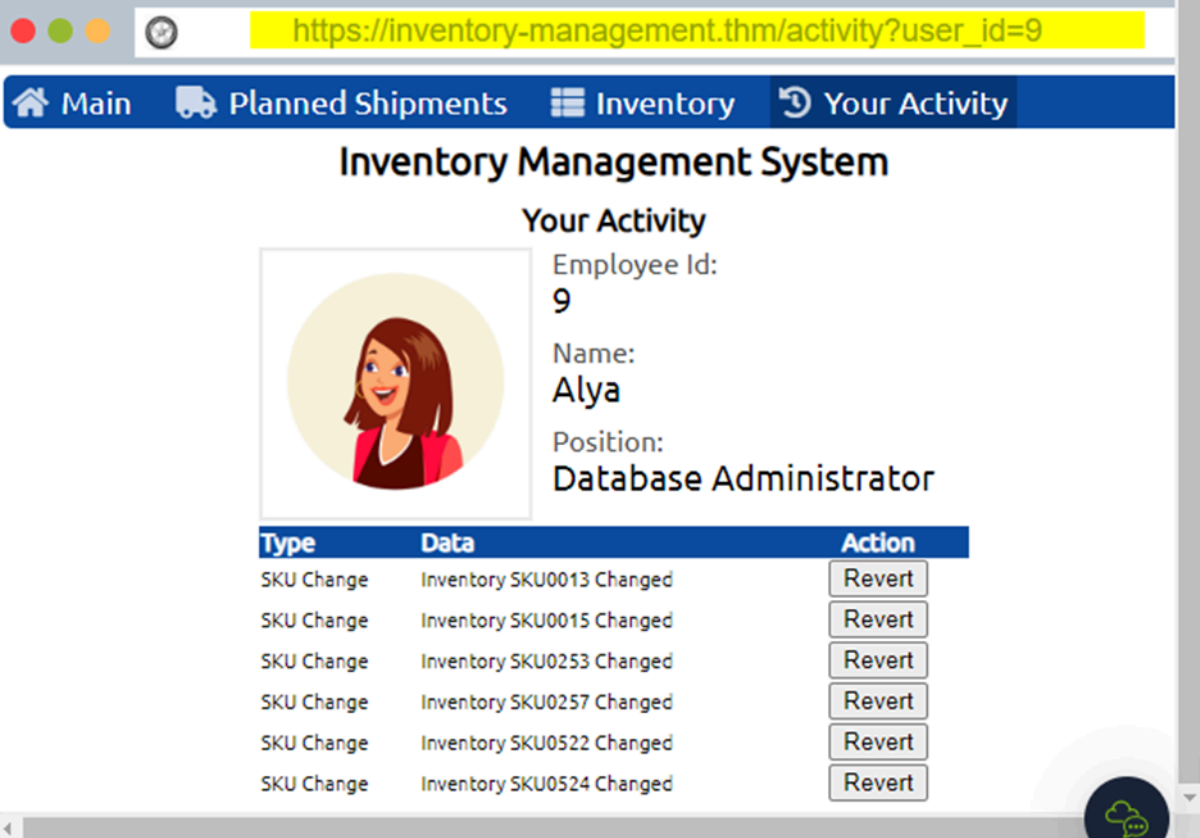
Exploitation

To counteract the attacker's actions and revert the system changes, I clicked on the "Your Activity" button, revealing the activity log of one of the users.



The website is vulnerable to Insecure Direct Object Reference (IDOR). This vulnerability allows attackers to access sensitive data belonging to other users by manipulating the ID parameter in the URL. For example, changing the ID parameter from 16 to 17 could expose sensitive data of another user. Similarly, an attacker could change the ID to 16 and access the sensitive data belonging to the original user.

After iterating through user IDs, I reached user 9 and discovered that the Alya account was responsible for the malicious alterations. I promptly reverted these changes.



The screenshot shows a web browser window with the URL `https://inventory-management.thm/activity?user_id=9`. The page title is "Inventory Management System" and the section is "Your Activity". It displays user information for Alya (Employee ID: 9, Position: Database Administrator). Below this is a table of activities:

Type	Data	Action
SKU Change	Inventory SKU0013 Changed	Revert
SKU Change	Inventory SKU0015 Changed	Revert
SKU Change	Inventory SKU0253 Changed	Revert
SKU Change	Inventory SKU0257 Changed	Revert
SKU Change	Inventory SKU0522 Changed	Revert
SKU Change	Inventory SKU0524 Changed	Revert

Getting the flag

I reverted the actions and got the flag: **THM{IDOR_EXPLORED}**

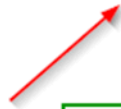
Instructions

This inventory management system manages all the shipments. A group of malicious hackers fixed up the plant and sent, the plant production.

Alya fixed the Inventory Management System!



THM{IDOR_EXPLORED}



Flag



Alya

Database Administrator

Type

Data

Action

