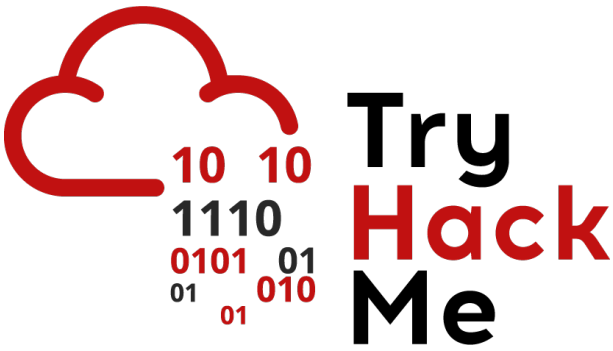
Writeup: Sala *Web Application Security*

Autor: Ismaeldevs

Plataforma: TryHackMe

4 de julio de 2025



Índice

1. Introducción **2**

2. Sala **2**

2.1. Tarea 1 – Introducción 2

2.2. Tarea 2 - Riesgos de seguridad de las aplicaciones web 2

2.3. Tarea 3 - Ejemplo práctico de seguridad de aplicaciones web 3

3. Conclusión sobre la Sala **6**

1. Introducción

En esta sala entenderemos los fundamentos de la seguridad en aplicaciones web, abordando los riesgos más comunes y cómo se manifiestan en entornos reales. También, aprenderemos conceptos clave como el modelo cliente-servidor, el OWASP Top 10 y vulnerabilidades como IDOR (Insecure Direct Object Reference), entre otras.

2. Sala

2.1. Tarea 1 – Introducción

En esta primera tarea nos adentramos en aprender qué es una aplicación web, la cual es un programa que se ejecuta en un servidor remoto y se puede usar simplemente mediante un navegador, sin instalar nada localmente. Además, nos introduce el concepto de bug bounty, donde empresas premian hallazgos de vulnerabilidades, lo que refuerza la relevancia de entender cómo funcionan estas aplicaciones y cómo pueden ser atacadas.

Una vez que entendemos qué es una aplicación web, procedemos a responder la siguiente pregunta.

Pregunta: What do you need to access a web application?
Respuesta: **Browser**

2.2. Tarea 2 - Riesgos de seguridad de las aplicaciones web

Ahora conoceremos un panorama de los principales riesgos en aplicaciones web, agrupados según el modelo **OWASP Top 10**.

- **Fallos en identificación y autenticación**
- **Control de acceso roto**
- **Inyección**
- **Fallos criptográficos**

Después de lograr comprender los diversos riesgos de seguridad de una aplicación web, pasamos a responder las siguientes preguntas.

Pregunta: 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?

Respuesta: **Identification and Authentication Failure**

Pregunta: You noticed that the username and password are sent in cleartext without encryption. What is the category of this security risk?

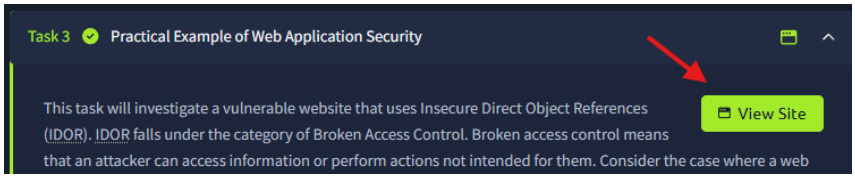
Respuesta: **Cryptographic Failures**

2.3. Tarea 3 - Ejemplo práctico de seguridad de aplicaciones web

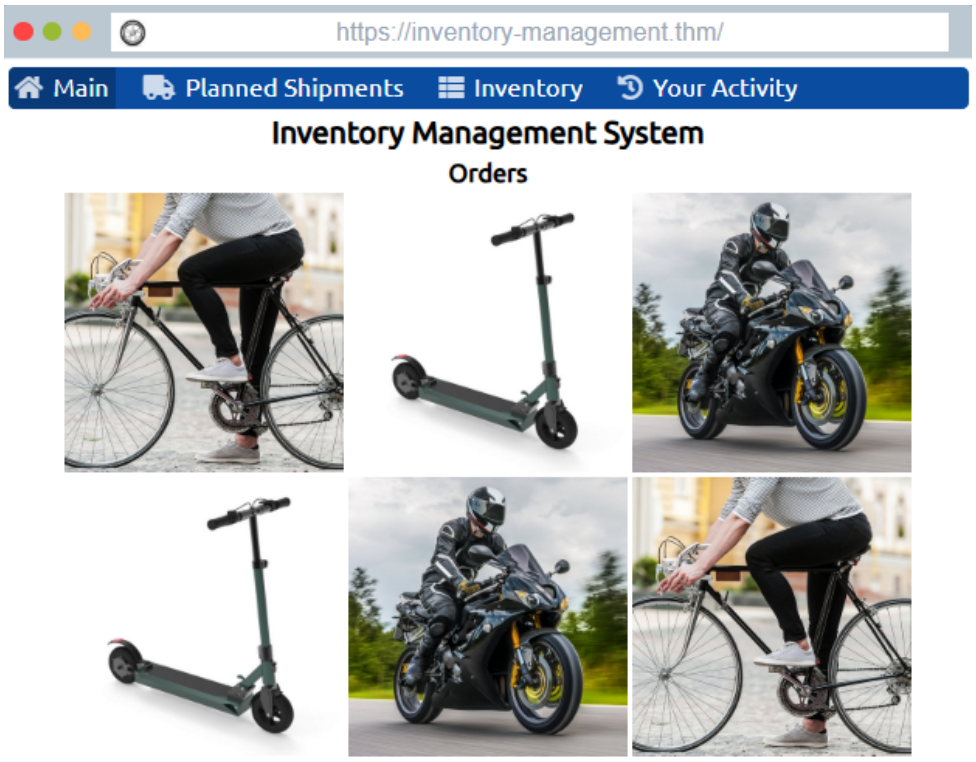
Realizaremos una práctica con un sitio web vulnerable que utiliza Referencias Directas a Objetos Inseguras (IDOR), que es un caso de control de acceso roto. La idea de esta tarea es que los objetos, como imágenes o cuentas de usuario, son accesibles mediante parámetros en la URL (id=16, id=17, etc.), y el sistema no verifica si el usuario está autorizado para ello.

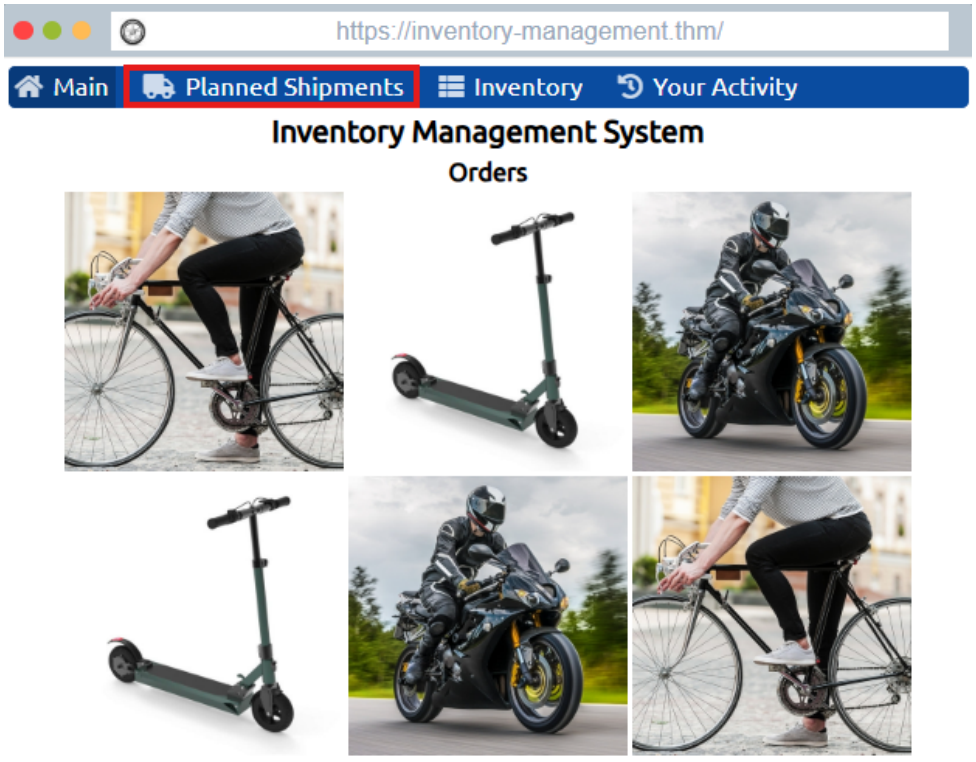
Pregunta: Check the other users to discover which user account was used to make the malicious changes and revert them. After reverting the changes, what is the flag that you have received?

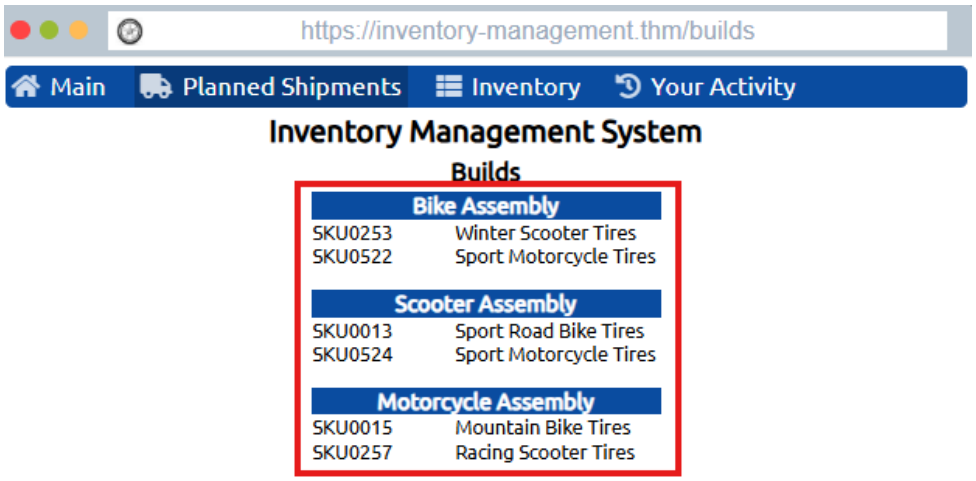
Después de entender como funciona la vulnerabilidad IDOR y la consigna de la tarea, hackearemos el sistema y desharemos los pasos del atacante. Para ello, desplegaremos el sitio haciendo clic en **View Site** en el lado superior de la tarea.



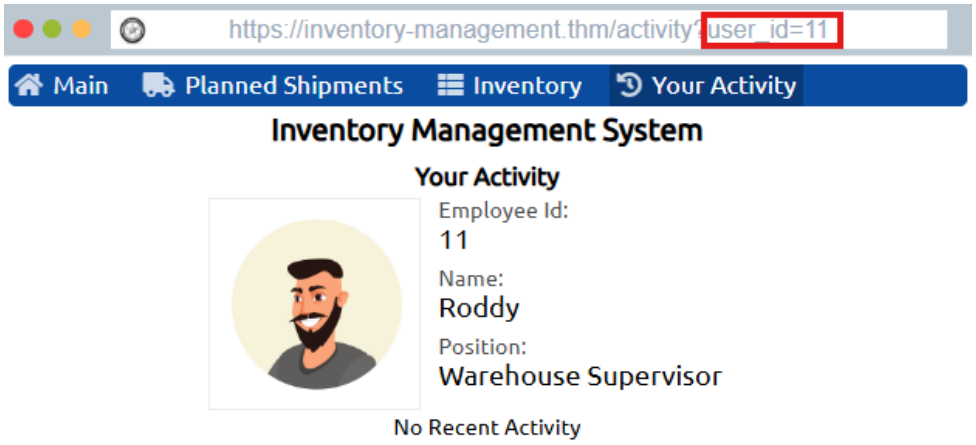
Una vez desplegado el sitio, podemos interactuar con él y notaremos que en la sección **Planned Shipments** un atacante ha manipulado las cosas como parte de sus planes de sabotaje.


https://inventory-management.thm/
Main
Planned Shipments
Inventory
Your Activity
Inventory Management System
Orders

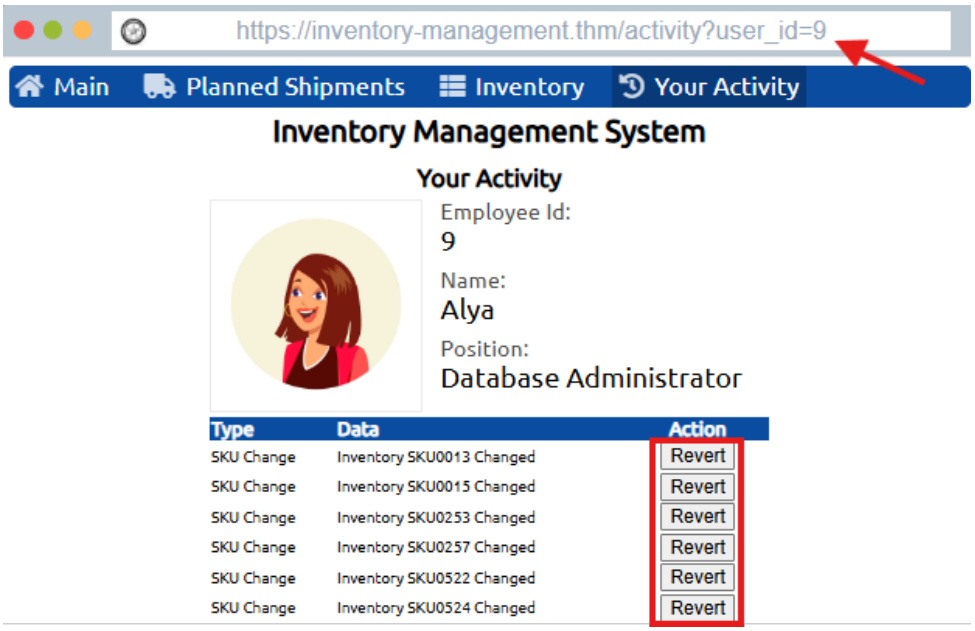

https://inventory-management.thm/
Main
Planned Shipments
Inventory
Your Activity
Inventory Management System
Orders



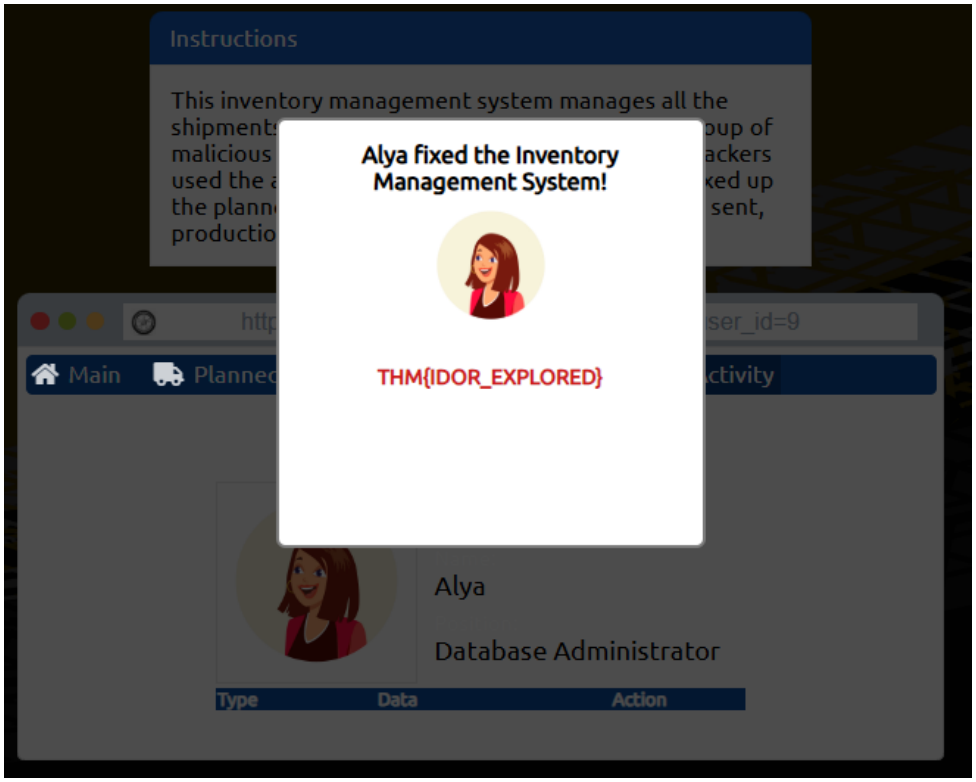
Debemos reparar esto, si no, todos los neumáticos irán al montaje equivocado. Aprovechando que la web es posiblemente vulnerable a IDOR, iremos a la sección **Your Activity** y manipularemos los paramentros de la URL para encontrar al usuario correspondiente para revertir la acción.



Desplazandonos entre los distintos ID por medio de la URL, encontramos que la cuenta se usó para realizar los cambios maliciosos fue el usuario con el ID 9. Procedemos revertir los envíos planificados.



Revertidos todos los envíos, procederá a saltar la alerta en pantalla.



Respuesta: **THM{IDOR_EXPLORED}**

3. Conclusión sobre la Sala

Al finalizar esta sala, entendemos cómo funcionan las aplicaciones web y los principales riesgos que enfrentan. Además, logramos aprender a identificar y analizar vulnerabilidades comunes como fallos de autenticación, control de acceso y exposición

de datos sensibles, sentando una base fundamental para continuar con estudios más avanzados en Web Pentesting o Bug Bounty.