Advent of Cyber 3 (2021)

[Day 1] **Web Exploitation** Save The Gifts :

-Insecure Direct Object References (IDOR) is a type of security vulnerability that occurs when an application allows an attacker to access a protected resource by modifying the value of a parameter that references the resource. For example, an IDOR vulnerability could allow an attacker to view the profile of another user by changing the parameter in a URL.user_id

-IDOR vulnerabilities can be exploited to gain unauthorized access to sensitive data, such as financial information, medical records, or intellectual property. They can also be used to launch denial-of-service attacks or to modify or delete data.

-There are a number of ways to exploit IDOR vulnerabilities. One common method is to use a tool like Burp Suite to fuzz the values of parameters that reference resources. This can be done by randomly changing the values of the parameters and observing the application's response. If the application returns different results for different values of the parameter, then it is likely that the parameter is vulnerable to IDOR.

-Another way to exploit IDOR vulnerabilities is to use a technique called path traversal. Path traversal is a method of accessing files or directories that are outside of the application's intended access control. This can be done by appending characters to the value of a parameter that references a file or directory. For example, an attacker could append the character to the parameter in a URL to access a file that is one level higher in the directory hierarchy...file_id

-IDOR vulnerabilities can be prevented by carefully designing and implementing applications. Developers should avoid using user-supplied input to directly reference resources. Instead, they should use a secure mechanism, such as a token, to represent resources. Developers should also carefully validate all user input to prevent attackers from injecting malicious code.

Here are some additional tips for preventing IDOR vulnerabilities:

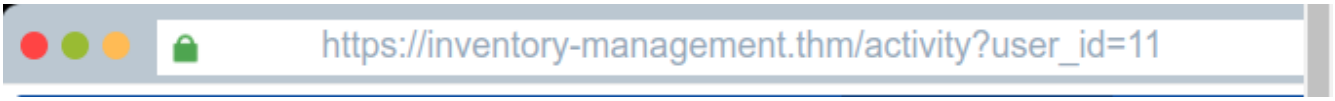
•Use parameterized queries instead of direct object references in database queries.

•Use input validation to prevent attackers from injecting malicious code into parameters.

•Use strong authentication and authorization mechanisms to protect resources.

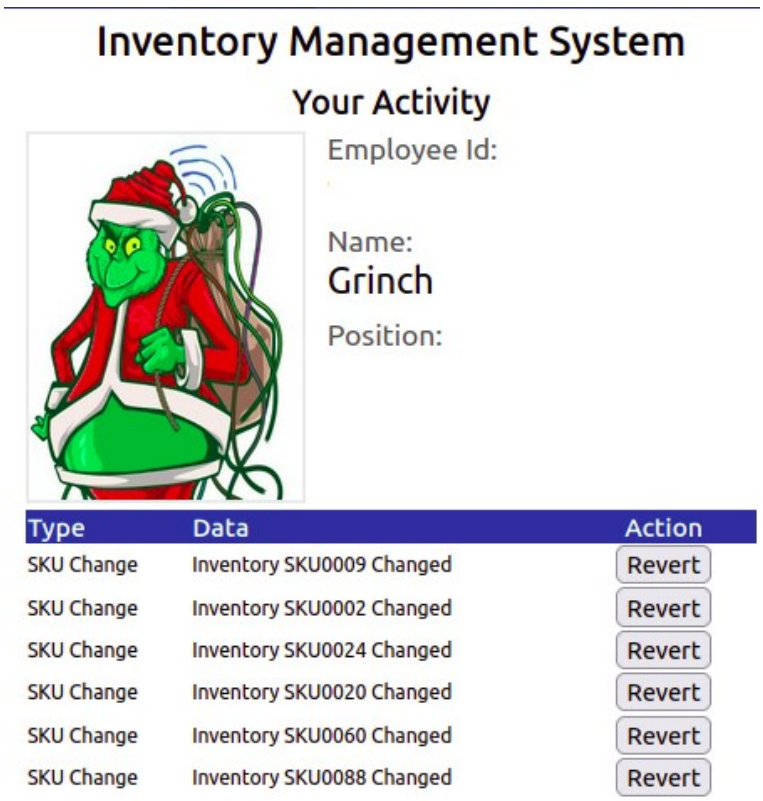
•Regularly scan your applications for IDOR vulnerabilities.

-The main purpose of this day was to learn about the IDOR vulnerability



-The main target is when a has changed user_id= ##
-The outcome will change, okay?

-Now we can change the id and answer the questions .



Answer the questions below :

-After finding Santa's account, what is their position in the company?

The answer : **The Boss!**

-After finding McStocker's account, what is their position in the company?
The answer : **Build Manager**

-After finding the account responsible for tampering, what is their position in the company?
The answer : **Mischief Manager**

-What is the received flag when McSkidy fixes the Inventory Management System?
The answer : **THM{AOC_IDOR_2B34BHI3}**

BY: Abdelwahab_Ahmed_Shandy