Week 1 - IDOR

What is IDOR?

IDOR - Insecure Direct Object Reference

allows attackers to manipulate references to gain access to unauthorized data.

For instance, a website that has your sensitive user sending the requests poorly can be intercepted by a hacker to find different data for potentially different users.

How is it done?

For this week, we will have challenges to solve on Security Shepard to manipulate requests and gain data.

Prerequisites

In order us to do an IDOR attack, we must know the basics of a request that is being sent back and forth between you, and the server.

There can be attributes in the requests such as headers, cookies, bodies and so forth. Just with the correct manipulation, if the website isn't secured properly, the hacker can infiltrate the website.

Ways to defend against it

Do not send requests that are not secured properly.

For instance, don't send a request that will fetch a user's data by their id without some sort of security mechanism and without their id being encrypted.