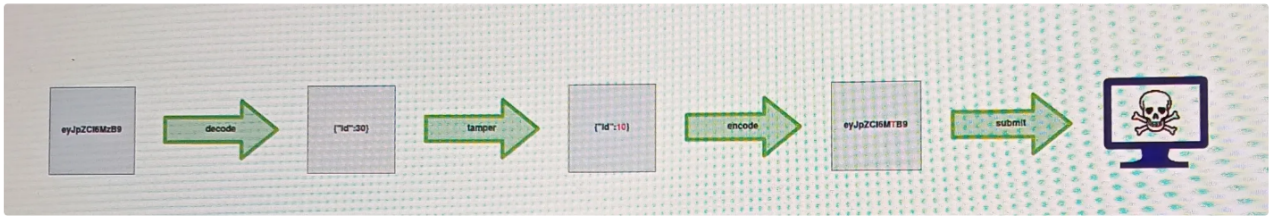
Stands for Insecure Direct Object Reference and is a type of access control vulnerability.

For example, link you click goes to http://online-service.thm/profile?user_id=1305, and you can see it. Curiosity gets the better of you, and you try changing the user_id value to 1000 instead , and to your surprise, you can see another user.

Encoded IDs

When passing Data, from page to page either by post data, query strings, or cookies, web developers will often first take the raw data and encode it. Encoding ensures that the receiving web server will be able to understand contents. Encoding changes binary data into an ASCII string commonly using the a-z, A-Z, 0-9 and = which is base64 most common that easy to spot.



Hashed IDs

Bit more complicated to deal with than encoded ones, but they may follow a predictable pattern, such as being the hashed version of the integer value. For example, the id number 123 would become 202cb962.....b70 if md5 hashing were in use.

It's worthwhile putting any discovered hashes through a web such as crackstation.net matches.

Unpredictable IDs

If the id cannot be detected using the above methods, an excellent method of IDOR detection is to create 2 accounts and swap the id numbers between them. If you can view the other user's Content using their id number while still being logged in with a different account, you've found a valid IDOR vulnerability.

Remember,developer Option practice....