Insecure Direct Object Reference IDOR (Broken Access Control)
• **Eric Biako**
  
  Bsc. IT, CEH v9
  
  Information security officer @ E-connecta
  
  Moderator @ [https://legalhackmen.com](https://legalhackmen.com)

~# whoami
IDOR occurs when a user supplied input is unvalidated and direct access to the object requested is provided.
Get my document which number is “1000” please!

Get the document which number is “1002” please!

Hey! Don’t mention it!

Of course!
This dwells on session management where the user has to be authenticated and/or authorized.
IDOR (Broken Access Control)

http://mybank.com/balance?Id=7809
http://mybank.com/balance?Id=7811
http://mybank.com/balance?Id=7812
http://mybank.com/balance?Id=7813

Untrusted data
impact

- unauthorized information disclosure

- modification or destruction of data.

- performing a function outside of the limits of the user.
Enforce access control policies such that users cannot act outside of their intended permissions

Prevent it.....
Use hash function and use hashed values instead of normal numbers or strings.

Prevent it.....
Prevent it.....

www.example.com/user.php?id=12

www.example.com/user.php?id=ea3eda3d3w229

3
DEMO

BWAPP(www.itsecgames.com)
https://sourceforge.net/projects/bwapp/files/bWAPP/

OWASP WEBGOAT :
https://github.com/WebGoat/WebGoat
IDOR (Broken Access Control)