Insecure Direct Object Reference IDOR

(Broken Access Control)

OWASP

The Open Web Application Security Project

```
~# whoami
```

- Eric Biako

  Bsc. IT, CEH v9
  Information security officer @ E-connecta
  Moderator @ https://legalhackmen.com

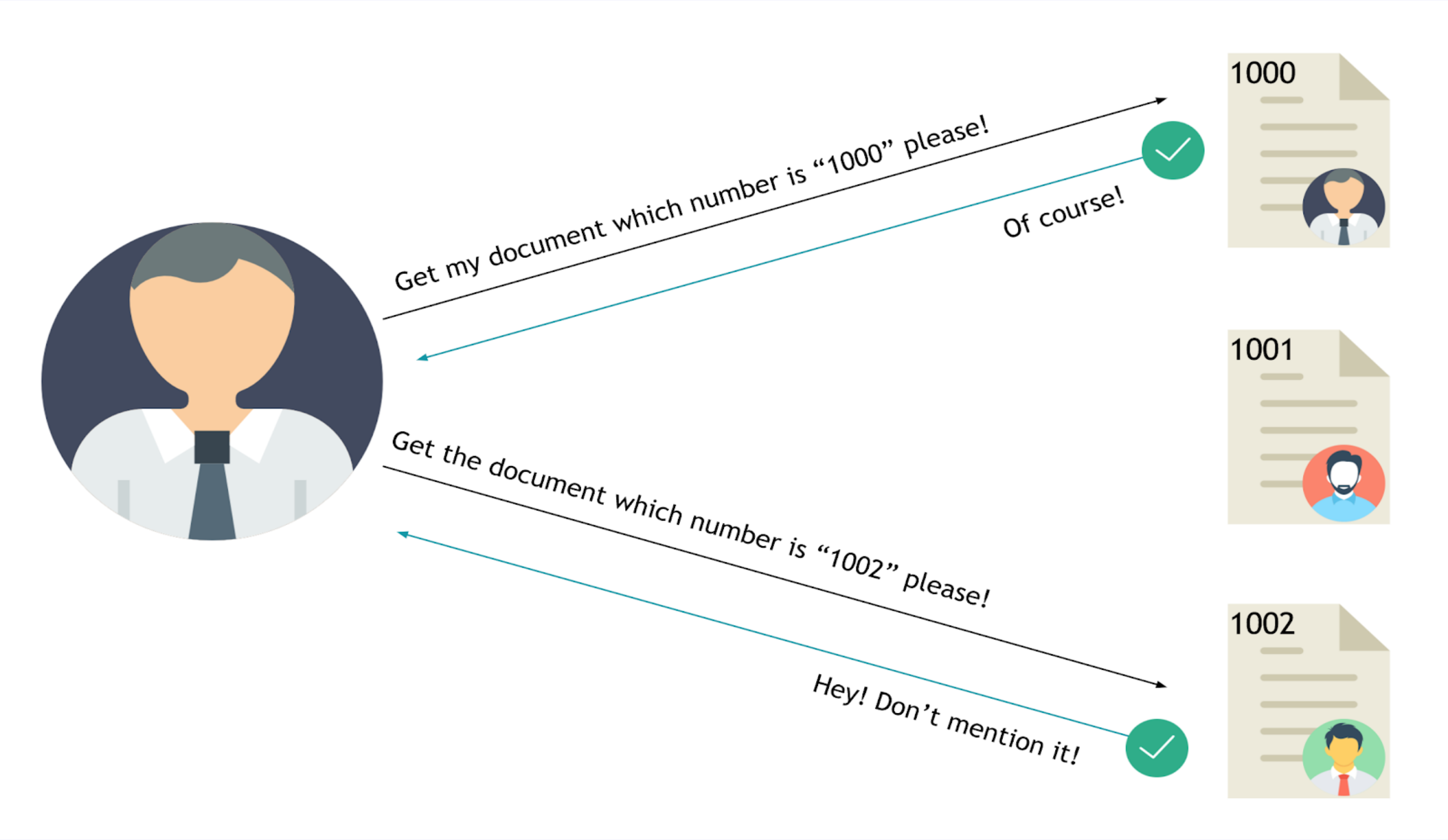
IDOR (Broken Access Control)

OWASP
The Open Web Application Security Project

IDOR occurs when a user supplied input is unvalidated and direct access to the object requested is provided.

IDOR (Broken Access Control)

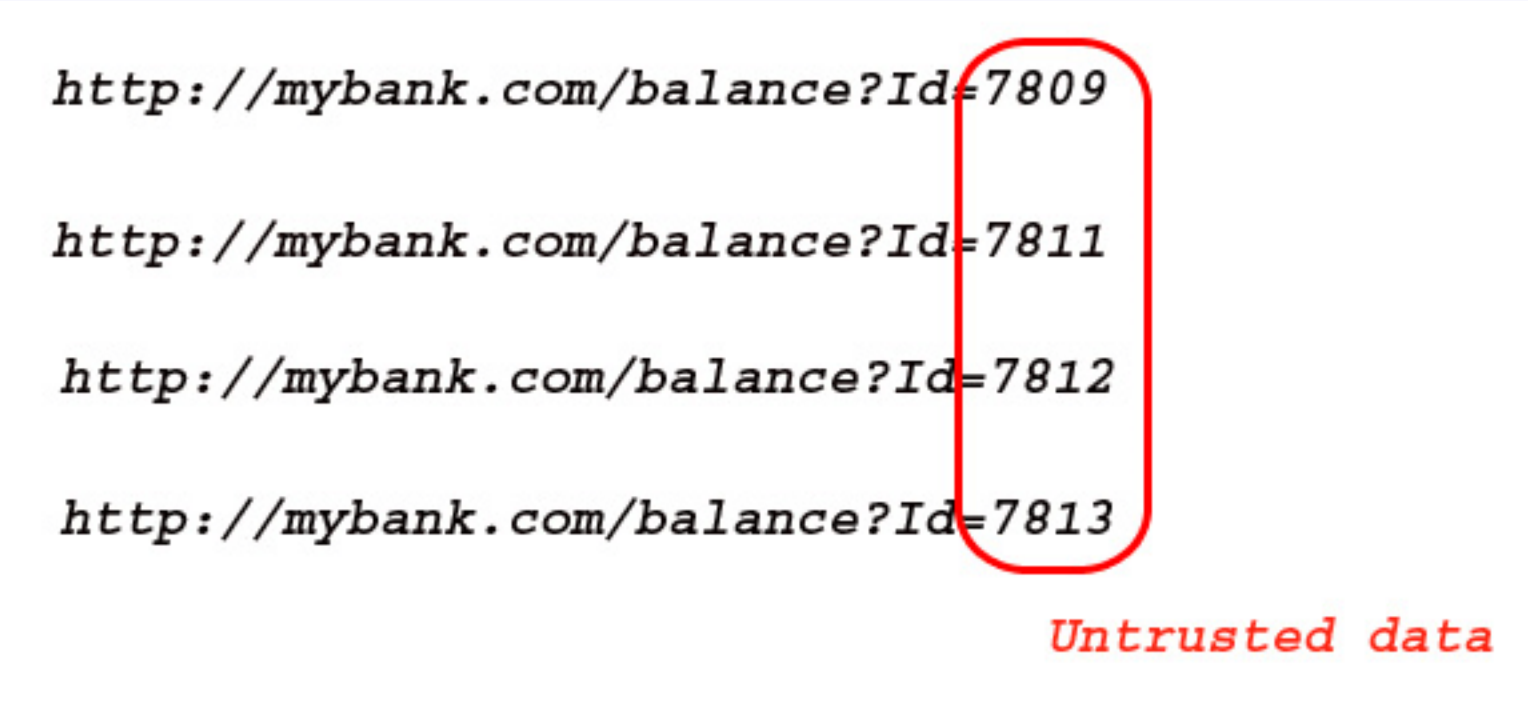
OWASP
The Open Web Application Security Project


1000
Get my document which number is “1000” please!
Of course!
1001
Get the document which number is “1002” please!
1002
Hey! Don’t mention it!

IDOR (Broken Access Control)

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.

IDOR (Broken Access Control)

Prevent it…..

Enforce access control policies such that users cannot act outside of their intended permissions

IDOR (Broken Access Control)

OWASP
The Open Web Application Security Project

Prevent it…..

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

IDOR (Broken Access Control)

OWASP
The Open Web Application Security Project

Prevent it.....

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

www.example.com/user.php?id=***ea3eda3d3w2293***

IDOR (Broken Access Control)

DEMO

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

OWASP WEBGOAT :
https://github.com/WebGoat/WebGoat

IDOR (Broken Access Control)

OWASP
The Open Web Application Security Project

- *https://www.bugcrowd.com/how-to-find-idor-insecure-direct-object-reference-vulnerabilities-for-large-bounty-rewards/*
- *https://www.gracefulsecurity.com/idor-insecure-direct-object-reference/*
- *https://codeburst.io/hunting-insecure-direct-object-reference-vulnerabilities-for-fun-and-profit-part-1-f338c6a52782*
- *https://medium.com/@woj_ciech/explaining-idor-in-almost-real-life-scenario-in-bug-bounty-program-c214008f8378*
- *https://blog.detectify.com/2016/05/25/owasp-top-10-insecure-direct-object-reference-4/*