HOR IGOR IDOR

Sessions

Two main points:

- Authentication «Who I am?»
- Authorization «Can I do that?»

Sessions

Often application uses different identification params such as:

- id
- pid
- uid
- etc.

in

- HTTP Headers
- Cookie
- Request params
- etc.

So...

If user can put another user's predictable or open identification parameter and get an access to/change confidential data, you meet:

DIOR
IGOR
IDOR - Insecure Direct Object
Reference

Logged in as user 27

GET /customer/27 HTTP/1.1 Host: mybank.com

...

HTTP/1.0 200 OK

<h1>1'm IGOR</h1>

GET /customer/28 HTTP/1.1 Host: mybank.com

...

HTTP/1.0 200 OK

<h1>1'm IDOR</h1>

Logged in as igor

GET /book?patient=igor HTTP/1.1
Host: med.com

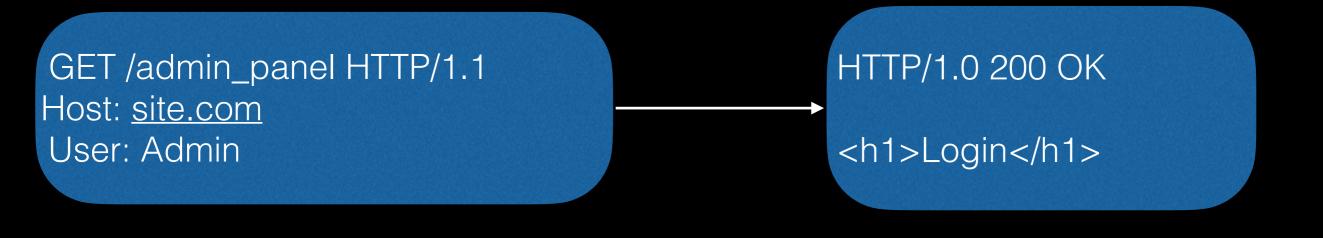
<h1>You got IGOR</h1>

GET /book?patient=idor HTTP/1.1 Host: med.com

. . .

HTTP/1.0 200 OK

<h1>You got IDOR</h1>

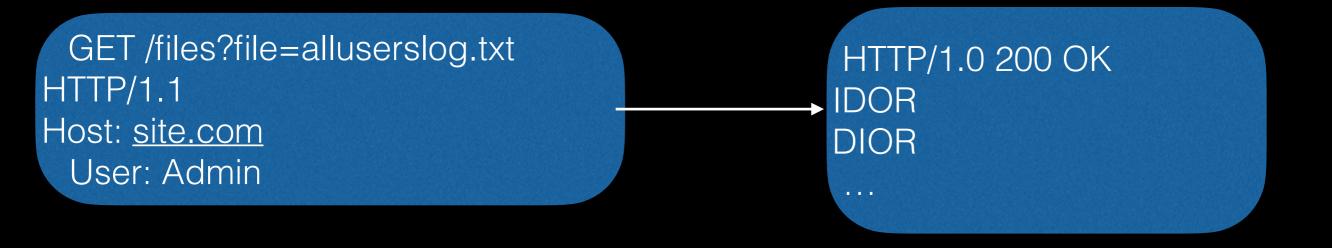


GET /admin_panel HTTP/1.1

Host: site.com

User: Common

yep, it's IDOR too, if admin_panel must be available only to admin



GET /files?file=alluserslog.txt

HTTP/1.1

Host: site.com

User: Common

HTTP/1.0 200 OK IDOR DIOR

yep, it's IDOR too, if alluserslog.txt must be available only for admin

Read only?

No, IDOR also could be found with data editing

Logged in as IGOR

GET /account?patient=idor&action=rename&new=newigor HTTP/1.1 Host: med.com

٠.,

HTTP/1.0 200 OK

<h1>IDOR is NEWIGOR now</h1>

Logged in as igor

GET /account?patient=igor&action=delete HTTP/1.1 Host: med.com

. . .

HTTP/1.0 200 OK

<h1>IGOR is dead</h1>

GET /account?patient=idor&action=delete HTTP/1.1 Host: med.com

HTTP/1.0 200 OK

<h1>IDOR is dead</h1>

