IDORs

BY UNCLE RAT

Agenda

- What is it?
- Attack strategy
  - Methods and tools
  - Deep dive
- First vs second order IDOR

What is it?

What is it?

- IDOR= insecure direct object reference
- Broken access control + Direct object reference
- Made popular by the OWASP top 10
- In reality, another type of broken access control issue

What is it?

- Following must be true
  - Identifier exists in request (ex. UserID=64)
  - Broken access control issues exists
- Example
  - GET /invoice.php?id=12
  - POST /personalInfo.php {personId:23,name:"tester"}
  - GET /invoices/1234.txt

Attack strategy

Attack strategy – Methods and tools

- Automated testing
  - Burp match and replace
  - Auto repeater plugin
  - Authorize plugin
- Manual testing
  - Copy and paste URL
  - Execute JavaScript in the developer console
  - Replacing authentication headers in burp repeater

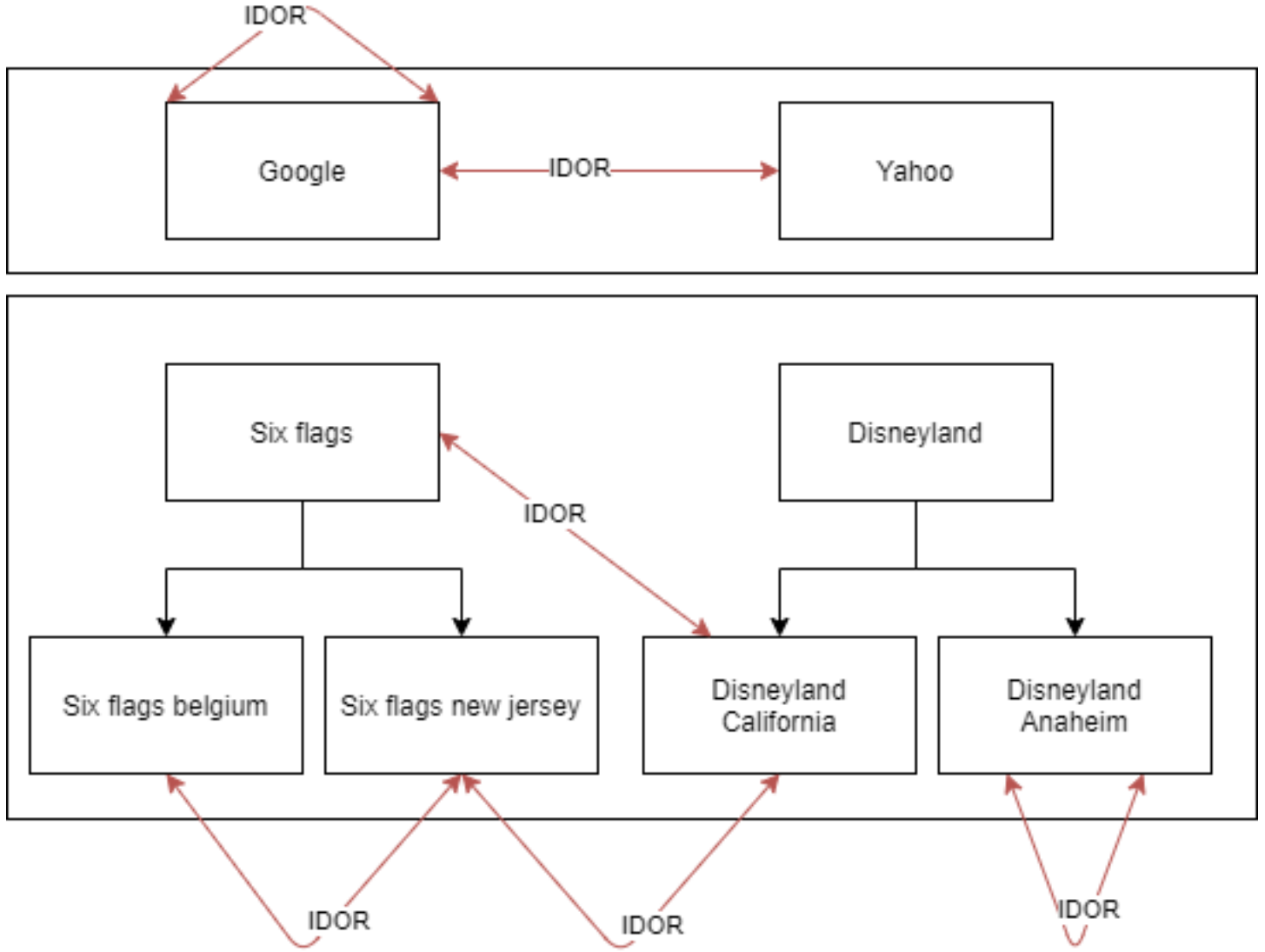
Attack strategy – deep dive

- Webshop
  - Test ALL the processes, including buying an item, returning an item, subscribing to a service,….
- Game
  - IDORs between users
- Newspaper
  - Subscription confirmations
- Bank
  - Test ALL the processes

Attack strategy

- B2B application with same tenant policy
  - If you can't create sub-accounts
    - IDORs between users of same tenant
    - IDORs between tenant
  - If you can create sub-accounts
    - Also test for IDORs between sub accounts
- B2B application with non-same tenant policy
  - If you can't create sub-accounts
    - IDORs between users of same tenant
  - If you can create sub-accounts
    - Also test for IDORs between sub accounts

Attack strategy



First vs second order IDOR

First vs second order IDOR

- Ex 1 GET to /receipt?id=4566 redirects to /succes if okay but to /error if unauthorised for call
  - Make call to /receipt?id=4566 while not authorized
  - Navigate to /succes instead of /error via burp intercept
  - Get shown receipt that is not yours
- Ex 2 Get /invoice?id=456 might not be possible
  - Make POST call to /print/invoices with the id of the invoice
  - Get shown the PDF you should not see
- Ex 3 The user is not able to edit products that are not theirs
  - Import product with the same name as the one you want to overwrite
  - Overwrite the product info