

IDOR



TABLE OF CONTENTS

01

What is IDOR

Basic overview

02

Intro. to Broken Access Control

Basic Definition

03

Exploitation

Exploiting our vulnerable WebApp

04

How to prevent this ?

Intro to MAC

05

Recap and Q/A

Fast Recap and Answering Questions

01

IDOR



What is IDOR?

- **IDOR** stands for **Insecure Direct Object Reference** and is a type of security vulnerability where an attacker can access unauthorized resources or perform actions on behalf of other users.
- **IDOR** is a type of **Broken Access Control** Vulnerability.



What is Access Control?

- **Access Control** is a fundamental security principle that ensures users are only able to access the resources and perform actions that they are authorized to do.
- So obviously **Broken Access Control** allows the users to access things that they are not allowed to.
- **Broken Access Control** always results due to logical flaws.



TABLE OF CONTENTS

01

What is IDOR

Basic overview

02

IDOR Example

Attack scenario example

03

Exploitation

Exploiting our vulnerable WebApp

04

How to prevent this ?

Intro to MAC

05

Recap and Q/A

Fast Recap and Answering Questions

02

IDOR Example



IDOR Example:


- Suppose that you have an account on some website and you can edit your profile information by visiting this url : https://website.com/profile?user_id=105,
Now what if you tried to change the **user_id** query parameter to be 106 instead of 105 ?!!
- If you could see the user's info as you are him, then you have discovered an IDOR .
- In **2019**, an IDOR was found in YouTube that was making an attacker to get any single frame of private videos. 



TABLE OF CONTENTS

01

What is IDOR

Basic overview

02

IDOR Example

Attack scenario example

03

Exploitation

Exploiting our vulnerable WebApp

04

How to prevent this ?

Intro to MAC

05

Recap and Q/A

Fast Recap and Answering Questions

03

Exploitation



TABLE OF CONTENTS

01

Attack overview

Basic overview

02

Intro. to Parameter Tampering

Basic Definition

03

Exploitation

Exploiting our vulnerable WebApp

04

Prevention

Intro to MAC

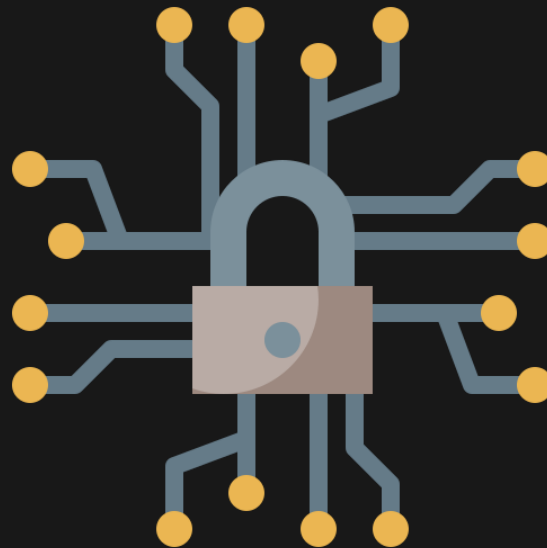
05

Recap and Q/A

Fast Recap and Answering Questions

04

Prevention



Message Authentication Code MAC

How to prevent this vulnerability?

- Input validation: validating user input on both client side and server side.
- Flowing the principle of least privilege.
- Avoiding to expose internal IDs or sensitive information.
- Use randomized and non-sequential identifiers.
- Secure session management: implementing strong session handling mechanisms.



Thank You

Presented by Saleh Adel

RESOURCES

<https://www.geeksforgeeks.org/insecure-direct-object-reference-idor-vulnerability/>
<https://bugs.xdavidhu.me/google/2021/01/11/stealing-your-private-videos-one-frame-at-a-time/>

