IDOR ATTACKS

COMPUTER NETWORKING

Time: 60 mins

Introduction

In this class, the student/s will learn how to perform IDOR attacks by modifying URLs and inspecting them. We will also prevent the IDOR attack using server information.

New Commands Introduced

selectedProduct['selling_price'] * data['quantity']	Calculates the product of selling price and quantity
'static/images/' + selectedProduct['image']	Defines the image path

Vocabulary

- IDOR vulnerability is caused by manipulating object identifiers used in a web application's URLs or parameters.
- Burp Suite is an integrated platform/graphical tool for performing security testing of web applications.

Learning Objectives

Student/s should be able to:

- ***Recall*** how web browsers can be enabled to view and edit a website's source code, including its HTML, CSS, JavaScript, and media files.
- ***Demonstrate*** the IDOR attack by altering the URL or inspecting the website.
- ***Explain*** how IDOR can be prevented.

Activities

Class Narrative: *(3 mins)*

- Brief the student/s that sometimes prices for products on websites may be overpriced and underpriced which can be a glitch or an attack on the website.

Concept Introduction Activity: *(4 mins)*

- Let the student/s observe that altering the website URL or modifying the properties or parameters can compromise the security and lead to IDOR attacks. Introduce different resources and disadvantages of direct access to the website.
- Explain how IDOR vulnerability can be misused and websites can be affected.
- Using the slides, explain that the student/s will learn:
    - to perform IDOR attack on URL
    - to perform IDOR attack using parameters
    - to prevent IDOR attacks

Activity 1: Perform IDOR Attack on URL *(16 mins)*

Teacher Activity: *(8 mins)*

- Display an example of URL changing with minute changes leading to new web pages and experiment the same with the toy website.
- Introduce and explain changing URL leading to change in web pages for different toys on sale.
- Demonstrate how to redirect to the "Home" page if the product is "Not for Sale".

Student Activity: *(8 mins)*

- Guide the student/s to try modifying the URL to view different products and then redirect the user to the home page.

Activity 2: Perform IDOR Attack using Parameters *(10 mins)*

- Recall that we viewed the parameters, properties and code for a website using the Inspect option.
- Explain how we will perform an IDOR attack by modifying the parameters, properties and code for the toy website using the Inspect option.
- Explain how we will alter the user API requests data like product price and quantity using the Inspect option to perform the IDOR attacks.
- Explain how we will perform the IDOR attack using Proxy and intercept on Burp Suite.

Student Activity: *(10 mins)*

- Guide the student/s to perform an IDOR attack by altering the price and quantity of a product on the front end using Inspect.
- Guide the student/s to perform an IDOR attack using Burp suite as a cybersecurity testing platform.

Activity 3: Prevent IDOR Attacks *(12 mins)*

- Explain how the IDOR attack can be prevented by calculating the bill using the server data instead of the front end.
- Demonstrate how we can secure the website by fetching the data from the server to calculate the bill of the products in the cart.

  Student Activity: *(6 mins)*

- Guide the students to calculate the bill using the server data instead of the website.

Introduce the Post class project: *(2 min)*

- Find the vulnerability in a small API in a company's website that can be used to fetch their user's data without access or authorization.

Test and Summarize the class learnings: *(5 mins)*

- Check for understanding through quizzes and summarize learning after respective activities.
- Summarize the overall class learning towards the end of the class.

Additional activities:

- Encourage the student/s to perform an IDOR attack by modifying the request parameters, properties and code for the toy website using Burp Suite.
- Encourage the student/s to modify the Toy Store website to accept important information from the server side and not rely on clients input for sensitive data.

State the Next Class Objective: *(1 min)*

- In the next class, student/s will learn to deploy viruses in a computer or a website.

U.S. Standards:

CSTA: 2-AP-11, 2-AP-12, 2-AP-13, 2-AP-14, 2-AP-19

Links Table		
Activity	Activity Name	Link
Class Presentation	IDOR ATTACKS	https://s3-whjr-curriculum-uploads.whjr.online/8d1076b0-d6a5-4782-815c-58672e6ff372.html
Explore Activity	IDOR ATTACKS	https://github.com/Tynker-Comput

		er-Networks/TNK-M16-C126-SAS-BP
Teacher Activity 1	Perform IDOR Attack on URL	https://github.com/Tynker-Computer-Networks/TNK-M16-C126-TAS-BP
Teacher Reference: Teacher Activity 1 Solution	Perform IDOR Attack on URL	https://github.com/Tynker-Computer-Networks/TNK-M16-C126-TAS
Student Activity 1	Perform IDOR Attack on URL	https://github.com/Tynker-Computer-Networks/TNK-M16-C126-SAS-BP
Teacher Reference: Student Activity 1 Solution	Perform IDOR Attack on URL	https://github.com/Tynker-Computer-Networks/TNK-M16-C126-SAS
Teacher Activity 2	Perform IDOR Attack using Parameters	https://github.com/Tynker-Computer-Networks/TNK-M16-C126-TAS-BP
Teacher Reference: Teacher Activity 2 Solution	Perform IDOR Attack using Parameters	https://github.com/Tynker-Computer-Networks/TNK-M16-C126-TAS
Student Activity 2	Perform IDOR Attack using Parameters	https://github.com/Tynker-Computer-Networks/TNK-M16-C126-SAS-BP
Teacher Reference: Student Activity 2 Solution	Perform IDOR Attack using Parameters	https://github.com/Tynker-Computer-Networks/TNK-M16-C126-SAS
Student Activity 3	Prevent IDOR Attacks	https://github.com/Tynker-Computer-Networks/TNK-M16-C126-SAS-BP
Teacher Reference: Student Activity 3 Solution	Prevent IDOR Attacks	https://github.com/Tynker-Computer-Networks/TNK-M16-C126-SAS
Student's Additional Activity 1	Perform IDOR using Parameters	https://github.com/Tynker-Computer-Networks/TNK-M16-C126-SAS-BP
Teacher Reference: Student's Additional Activity 1 Solution	Perform IDOR using Parameters	https://github.com/Tynker-Computer-Networks/TNK-M16-C126-SAS
Student's Additional Activity 2	Prevent the IDOR	https://github.com/Tynker-Computer-Networks/TNK-M16-C126-SAS-BP
Teacher Reference: Student's Additional Activity 2 Solution	Prevent the IDOR	https://github.com/Tynker-Computer-Networks/TNK-M16-C126-SAS
Post Class Project	Ethical IDOR Testing	https://github.com/Tynker-Computer

		-Networks/TNK-M16-C126-PCP-BP
Teacher Reference: Post Class Project Solution	Ethical IDOR Testing	https://github.com/Tynker-Computer-Networks/TNK-M16-C126-PCP