|  |  |
| --- | --- |
| **Lab 6 – Access Control Vulnerabilities (IDOR)** | |
| **Name** | Tran Minh Triet |
| **Student ID** | SE172241 |

**Part 1: Answer the following questions**

1. What is an Insecure Direct Object Reference (IDOR), and how does it present a security risk in web applications?

An Insecure Direct Object Reference (IDOR) is a security vulnerability that occurs when a web application provides direct access to objects based on user-supplied input. In simpler terms, it occurs when an application exposes internal implementation objects to users without proper authorization checks. This can lead to unauthorized access to sensitive data or functionality.

Here's a breakdown of how IDOR works and the risks it poses:

1. Direct Object Reference

2. Insecure Handling of References

3. Security Risk

4. Examples

5. Prevention

In summary, IDOR is a security vulnerability where an attacker can manipulate references to gain unauthorized access to sensitive objects or functions within a web application. It underscores the importance of implementing robust authorization mechanisms to ensure that users can only access the data and functionality they are explicitly authorized to use.

1. How can attackers exploit IDOR vulnerabilities in a website, and what are some common techniques used in such attacks?

Attackers can exploit Insecure Direct Object Reference (IDOR) vulnerabilities in a website by manipulating object references to gain unauthorized access to sensitive data or functionality. Here are some common techniques used in IDOR attacks:

1. Changing Parameters in URLs or Forms

2. Sequential Object Reference (Predictable References)

3. Forced Browsing

4. Burp Suite and Proxy Tools

5. Browser Developer Tools

6. Cross-Site Request Forgery (CSRF)

7. Business Logic Abuse

To prevent these types of attacks, developers should implement strong access controls, validate user input, and ensure that proper authorization checks are in place. Regular security testing, including code reviews and penetration testing, can help identify and mitigate IDOR vulnerabilities before they can be exploited by attackers.

1. What types of functionality or data in a website can be affected as a result of an IDOR vulnerability being exploited?

Exploiting an Insecure Direct Object Reference (IDOR) vulnerability can have a wide range of impacts on the functionality and data of a website. The extent of the damage depends on the specific implementation of the vulnerable application. Here are some types of functionality or data that can be affected:

* Unauthorized Data Access
* Financial Data and Transactions
* Account Manipulation
* Confidential Information
* Administrative Functions

Challenge <[link](https://portswigger.net/web-security/access-control/lab-insecure-direct-object-references)>















