|  |  |
| --- | --- |
| Class | IAW301 |
| Name | Trần Ngọc Anh |
| IC No. | HE151461 |
| Date & Time | 29/6/2022 |

**LAB 23**

**Insecure Direct Object Reference**

**1, IDOR là gì ?**

- IDOR là **Insecure Direct Object Reference.** Lỗ hổng này nằm trong TOP 10 lỗ hổng nguy hiểm mà OWASP đã đưa ra.

**2,Nguyên nhân.**

- Nguyên nhân sâu xa của lỗ hổng IDOR nằm ở cơ chế phân quyền và kiểm soát truy cập người dùng trên website.

- Việc website không phân quyền đúng cũng như kiểm soát chặt chẽ việc truy cập tài nguyên của user trên hệ thống dẫn đến việc truy cập trái phép từ kẻ tấn công.

- Việc sử dụng tham chiếu truy cập tới đối tượng là một cách làm tiện lợi nhưng nếu không phân quyền rõ ràng , cụ thể thì việc này lại tiềm ẩn nguy cơ lộ dữ liệu rất nguy hiểm.

**3, Lỗ hổng trên có thể khai thác được để làm việc gì.**

- Cho phép truy cập trái phép thông tin của người dùng khác.

- Nặng hơn nữa là thực hiện thay đổi hoặc xóa dữ liệu của người dùng khác

===> Vì vậy lỗ hổng này có mức độ nguy hiểm rất cao, gây hậu quả nghiêm trọng tới người dùng. Đặc biệt là các hệ thống có dữ liệu quan trọng của người dùng như: mạng xã hội, tài chính - ngân hàng, y tế,…  
**4, Cách khắc phục.**

- **Phân quyền chặt chẽ người dùng:**

+ Luôn kiểm tra quyền truy cập của mỗi người dùng ở tất cả các request. Việc kiểm tra phân quyền luôn luôn cần thực hiện trên phía server, không kiểm tra ở phía client.

- **Tránh tham chiếu trực tiếp tới đối tượng:**

**+ Thay vì tham chiếu trực tiếp tới đối tượng ví dụ như customers?customer\_id=123 thì chúng ta sẽ thực hiện hash giá trị id thành chuỗi ngẫu nhiên: customers?customer\_id=**F1244AD6A71A9C6C9E08BA6D819D119FBD7944D0

+ Tuy nhiên phương pháp này không giúp chống hoàn toàn được hacker nhưng sẽ làm khó tấn công IDOR hơn do chuỗi hash khá khó đoán.