一、IDOR漏洞概述

1.1 水平越权简介

1.1.1 漏洞场景

一种同角色用户互相访问和操作私有数据的缺陷问题。常见的场景是系统应该只验证了访问和操作数据的角色，而未对数据做细分和校验，导致同角色的用户能够互相访问和操作各自的私有数据。

1.1.2 检测方法

通过替换相同权限用户的认证信息并且重放请求，对比原始请求和重放请求的状态码、响应内容相似度和长度等是否保持一致，如果保持一致则可能存在水平越权，否则不存在。

1.2 垂直越权简介

1.2.1 漏洞场景

一种低权限用户使用高权限用户的功能产生的缺陷问题。常见的场景是系统应用仅仅在菜单、按钮上做了显示层面的权限控制，未在底层进行权限校验，导致恶意用户只要获取对应菜单或按钮的请求，就可以达到权限提升的目的。

1.2.2 检测方法

通过替换不用权限用户的认证信息并且重放请求，对比原始请求和重放请求的状态码、响应内容相似度和长度等是否保持一致，如果保持一致则可能存在垂直越权，否则不存在。

1.3 未授权访问简介

1.3.1 漏洞场景

通过删除请求中的认证信息后重放请求，对比原始请求和重放请求的状态码、响应内容相似度和长度等是否保持一致，如果保持一致则可能存在未授权访问，否则不存在。

1.3.2 检测方法

一种不需要认证即可访问和使用某些功能和数据的缺陷问题。常见的场景是系统后台某些独立的功能未跟系统权限进行整合，导致某些功能通过模拟请求即可使用未授权的功能。

二、IDOR漏洞修复

2.1 紧急修复方案

检查提交CRUD请求的操作者（session获取）与目标对象的权限所有者（查数据库）是否一致。

2.2 底层权限设计

在调用数据接口额外提供userid（session获取），在进行每个CRUD请求的SQL语句中添加ownerid字段，验证userid是否等于ownerid。