逻辑漏洞概述

Web漏洞-逻辑漏洞 第1课

360
网络安全学院

教学目标

- 了解逻辑漏洞的定义
- 了解访问控制与访问控制模型

课程时长：50分钟

参考资料：《黑客攻防技术宝典 Web实战篇》

目录

逻辑漏洞概述

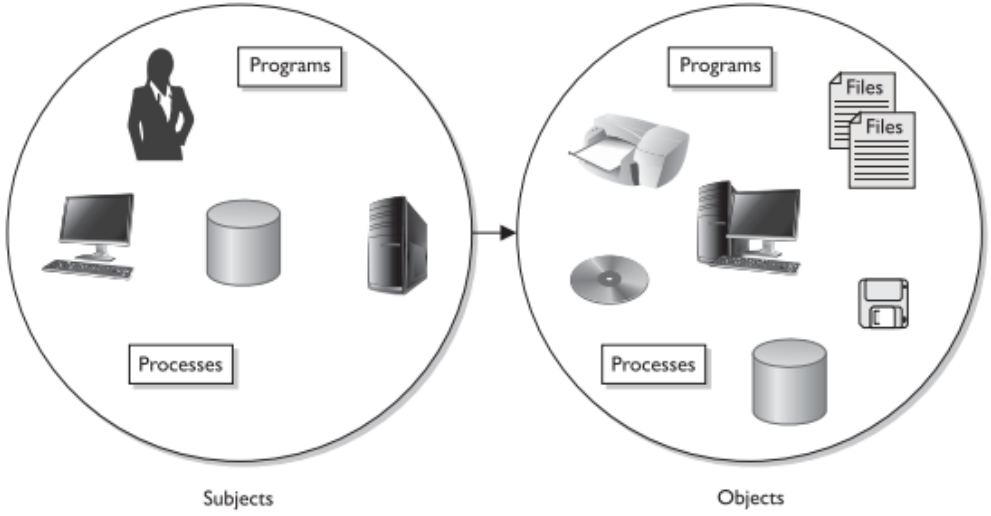
PART 01

访问控制概述

访问控制概述

访问

在某种程度上来说，信息安全就是通过控制如何访问信息资源来防范资源泄露或未经授权修改的工作。访问是主体（Subject）和客体（Object）之间的信息流动，主体是访问中主动的实体，可以是人、程序、进程等；客体是被动的实体，可以是文件、光盘、数据库等。

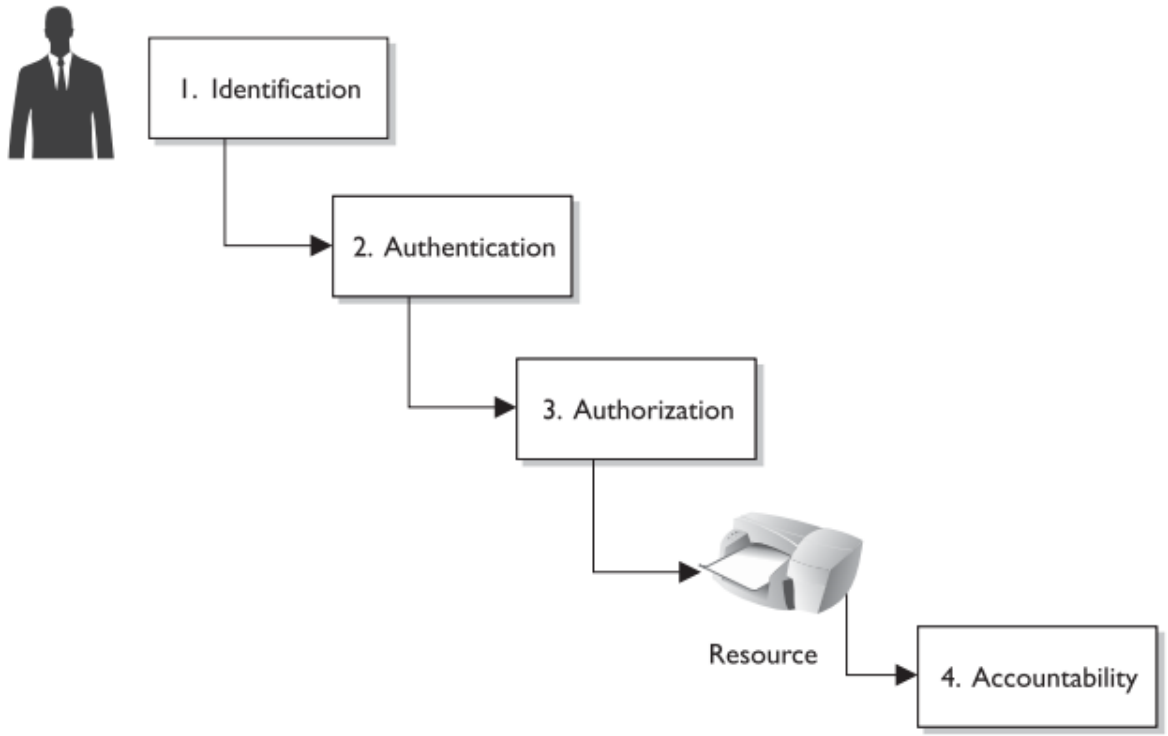


访问控制概述

访问控制

主体访问客体通常需要4个步骤：

- Identification --- 身份标识
- Authentication --- 身份验证
- Authorization --- 授权
- Accountability --- 审计



访问控制概述

访问控制模型

访问控制模型是规定主体如何访问客体的一种架构，目前主要分为三种：

- 自主访问控制（Discretionary Access Control，DAC）
  - 由客体的属主自主的对客体进行管理，自主的决定是否将访问权限授予其他主体。
- 强制访问控制（Mandatory Access Control，MAC）
  - 安全策略由管理员配置，访问控制由系统实施，安全策略是高于一切的存在。
- 角色型访问控制（Role-Based Access Control，RBAC）
  - 使用集中管理的控制方式来决定主体和客体如何交互，更多的用于企业中，根据不同的职位来分配不同的权限。

PART 02

逻辑漏洞概述

逻辑漏洞概述

什么是逻辑漏洞

随着网络安全法的实施、企业和用户安全意识的提高，Web安全已经成为了重点关注的方向。诸如使用安全开发框架、部署安全防护设备等防护手段的使用，使得网站的常规漏洞越来越少。以SQL注入为例，由于其危害巨大，常年稳居OWASP Top 10的第一位，目前很多Web开发框架在底层就直接杜绝的SQL注入问题。

但“逻辑漏洞”一词却更加热门，很可能成为Web漏洞的主战场。之所以称之为“逻辑漏洞”，是因为在代码之后是人的逻辑，人更容易犯错，所以逻辑漏洞一直都在。而且由于逻辑漏洞产生的流量多数为合法流量，一般的防护手段或设备无法阻止，也导致了逻辑漏洞成为了企业防护中的难题。

目前业务逻辑问题也成为了企业关心的问题之一。

逻辑漏洞概述

360 网络安全学院

- 逻辑漏洞的分类
  - 验证机制缺陷
  - 会话管理缺陷
  - 权限管理缺陷
  - 业务逻辑缺陷

PART 03

验证机制

验证机制

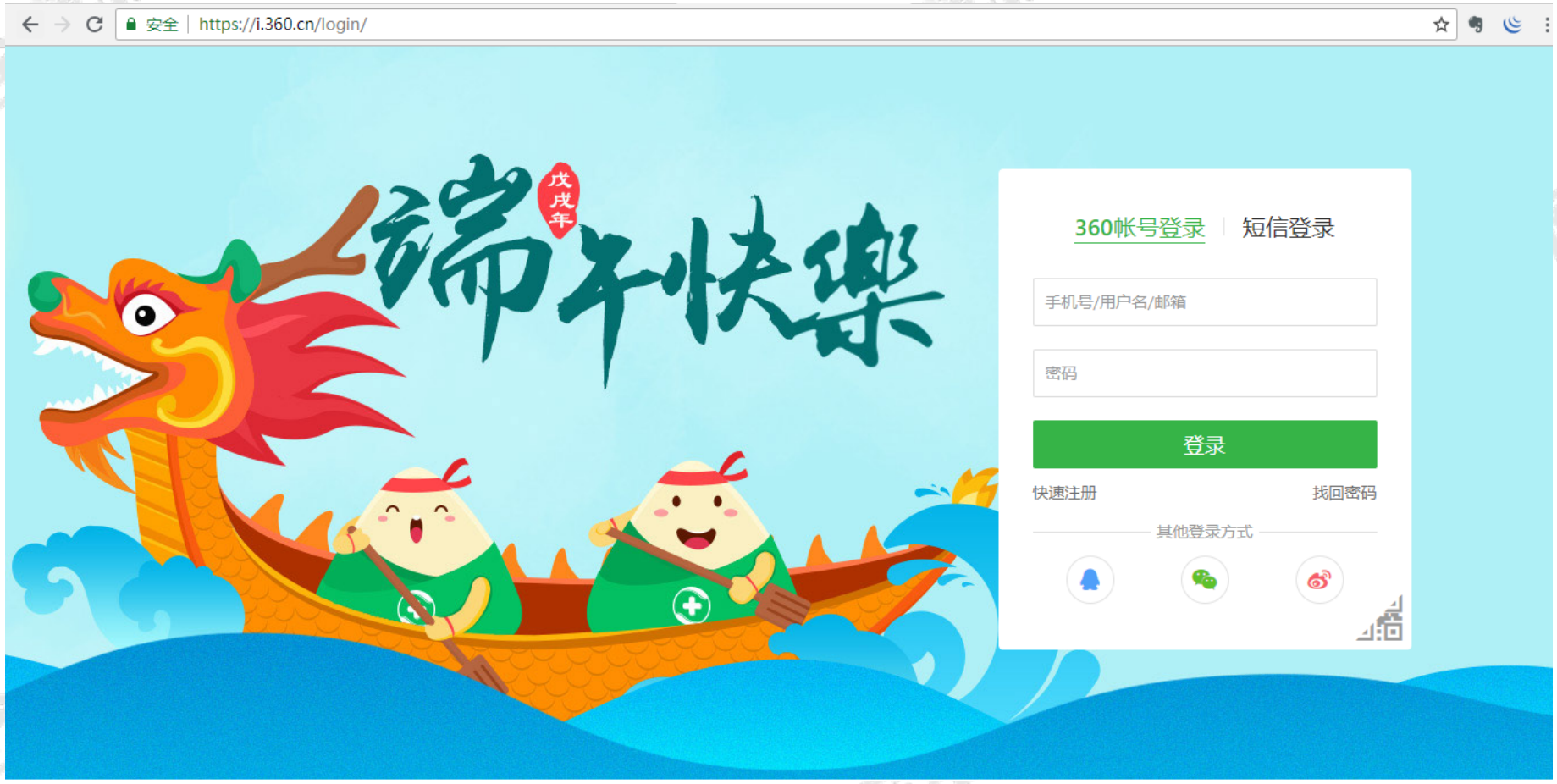
- 身份标识（Identification）：
  - Who knows：　某人所知道的内容
  - Who has：　某人所拥有的物品
  - Who is：　某人的身份

- 验证机制

验证机制是信息系统安全机制中最简单、最前沿的一种机制。最常见的方式是信息系统要求用户提交用户名与密码，正确则允许用户登录，错误即拒绝用户登录。

验证机制

- 讨论：如何攻击验证机制？



PART 04

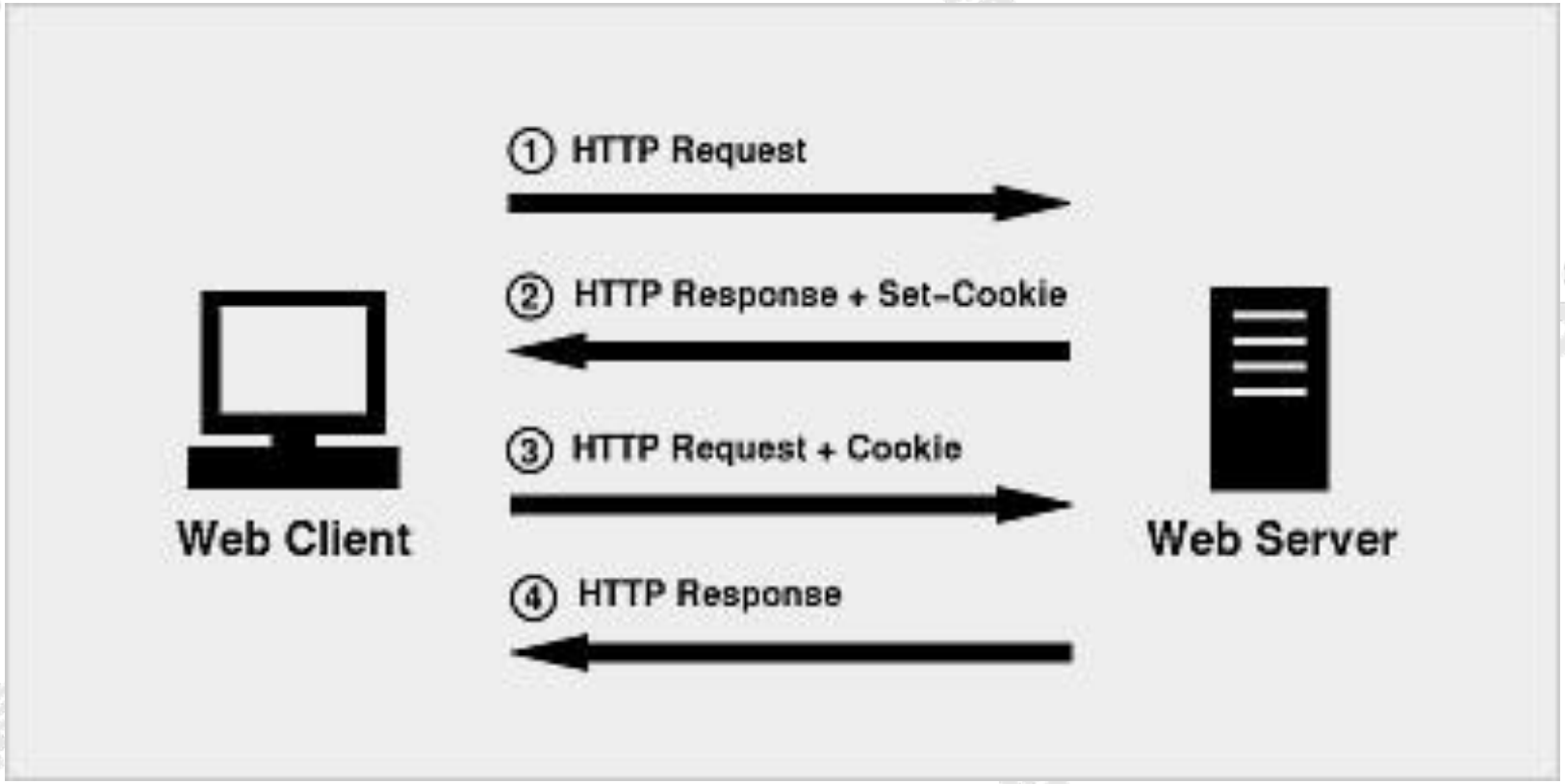
会话管理

会话管理

- HTTP协议
  - 无连接
    - 每次连接只处理一个请求。服务器处理完客户的请求，并收到客户的应答后，即断开连接，采用这种方式可以节省传输时间。
  - 无状态
    - 指协议对于事务处理没有记忆能力，服务器不知道客户端是什么状态。
    - 即我们给服务器发送 HTTP 请求之后，服务器根据请求，会给我们发送数据过来，但是发送完，不会记录任何信息。
  - 会话
    - 执行会话最简单、最常见的方式是向每名用户发布一个唯一的会话令牌或标识符，用户在每一个请求中提交这个令牌。

会话管理

- 讨论：如何攻击会话管理机制？



PART 05

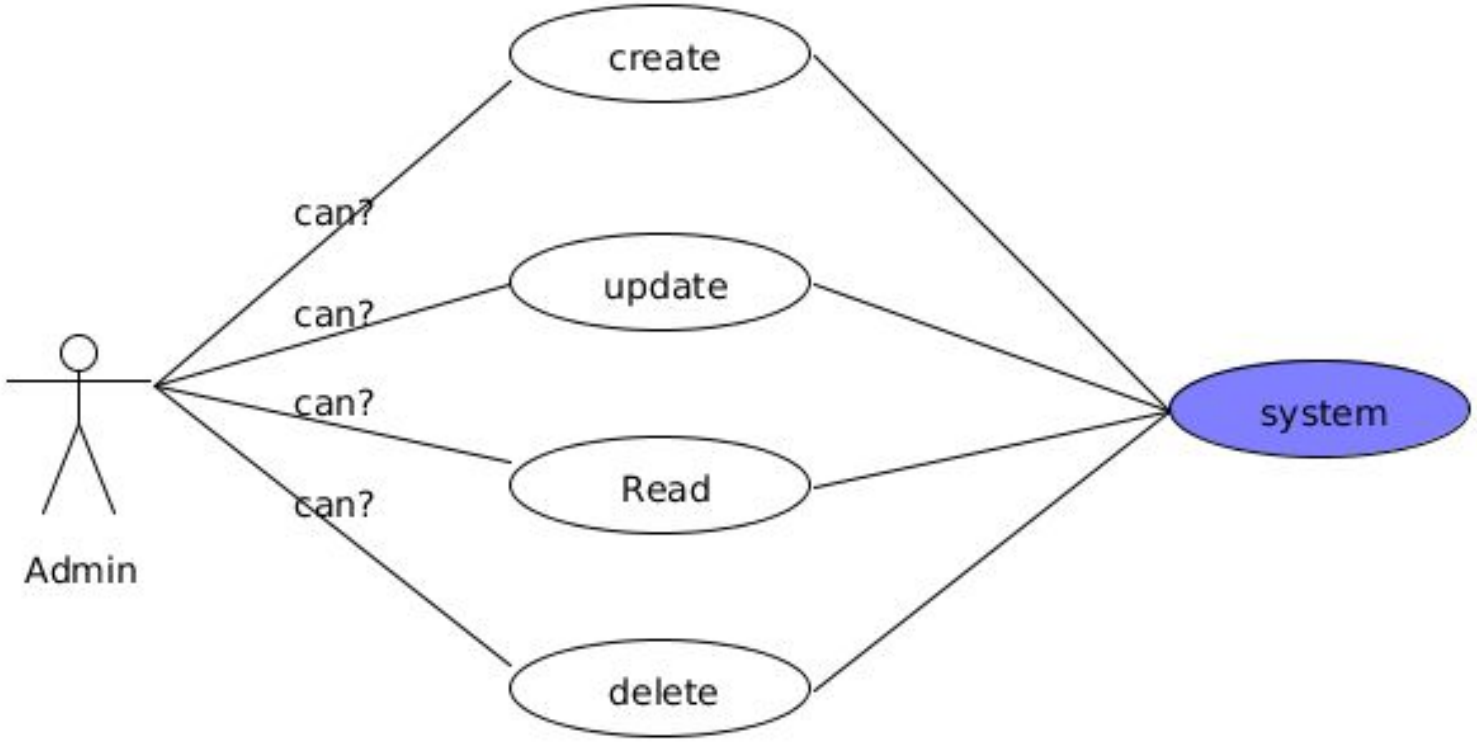
权限控制

权限控制

- 权限管理（Authorization）
  - 从控制力度来看，可以将权限管理分为两大类：
    - 1. 功能级权限管理
    - 2. 数据级权限管理
  - 从控制方向来看，也可以将权限管理分为两大类：
    - 1. 从系统获取数据，比如查询订单、查询客户资料
    - 2. 向系统提交数据，比如删除订单、修改客户资料

会话管理

- 讨论：如何攻击权限控制机制？



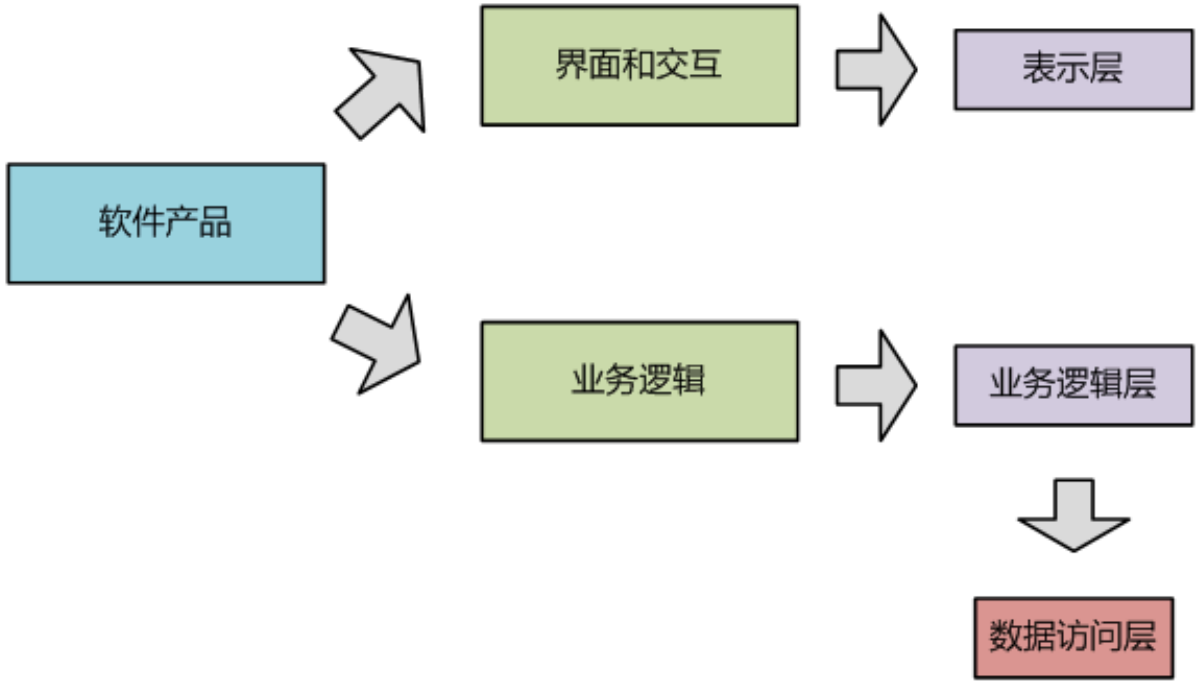
逻辑漏洞概述

PART 06

业务逻辑

业务逻辑

- 业务逻辑
  - 每个业务系统都具有不用的业务逻辑，而业务逻辑背后就是人的逻辑，充分了解业务逻辑有助于找出其中的问题所在。



谢谢

360
网络安全学院