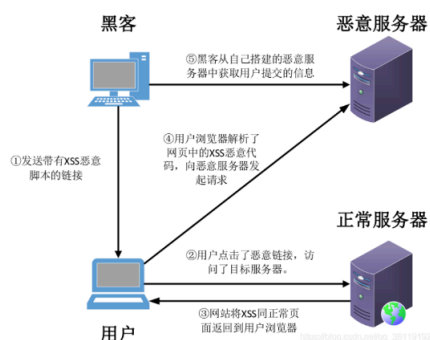


# 实验四 XSS 攻击

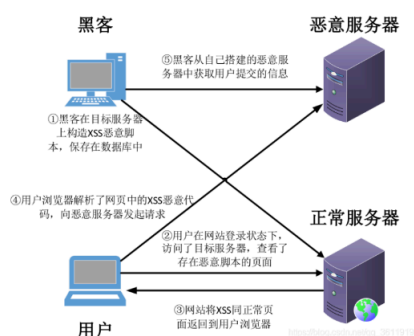
## 实验目的

- 理解跨站脚本攻击 (XSS, Cross Site Scripting) 的原理及分类。
- 掌握 XSS 攻击的常见方式及其实现手段。
- 利用 XSS Labs 靶场, 实践常见 XSS 攻击场景 (反射型、存储型、DOM 型)。
- 提高Web安全意识, 学习常见防护措施。

反射型XSS攻击流程



存储型XSS攻击流程



- 模拟执行不同类型的 XSS 攻击, 包括但不限于:
  - 反射型 (Reflected XSS)
  - 存储型 (Stored XSS)
  - DOM 型 (DOM-based XSS)
- 对攻击过程进行详细记录, 包括:
  - 攻击入口 (如 URL 参数、输入表单)
  - 注入的脚本代码
  - 攻击效果 (如弹窗、窃取 Cookie、页面篡改等)
- 学习并实现防御措施, 如输入验证、输出编码等。
- 撰写实验报告, 详细记录实验步骤, 总结实验过程、结果与心得。

# 实验内容

## 1. 实验环境说明

- 靶场平台：XSS Labs（远程环境地址：[靶场地址](#)）

欢迎来到XSS挑战



点击图片开始你的XSS之旅吧！

- 浏览器：建议使用 Chrome 或 Firefox
- 实验工具：Burp Suite、开发者工具（F12）、网络抓包工具等

## 2. XSS 攻击实践

### (1) 反射型 XSS

- 任务地址：

- [level 1](#)

欢迎来到level1

欢迎用户test



payload的长度:4

- [level 2](#)

欢迎来到level2

没有找到和test相关的结果。



payload的长度:4

- [level 3](#)



- **攻击方式:** URL 中注入脚本代码, 如: `<script>alert('反射型XSS')</script>`
- **触发机制:** 脚本代码被立即返回给用户并执行
- **截图:** 弹窗通关提示的截图
- **分析:**
  - 漏洞成因
  - 反射型 XSS 风险

## (2) 存储型 XSS

- **任务编号:**
  - [level 8](#)



- [level 9](#)



- **攻击方式:** 提交表单 (评论/留言) 中插入脚本, 如: `<script>alert('存储型XSS')</script>`
- **触发机制:** 其他用户访问该页面时脚本被加载并执行
- **截图:** 弹窗通关提示的截图
- **分析:**
  - 漏洞成因

- 存储型 XSS 风险

### (3) 选做

- 简要分析课前演示的 WannaCry 勒索病毒
  - 包括基本信息、传播方式、影响范围以及防护应对措施等。



## 参考资料

- XSS Labs 靶场项目
- OWASP XSS 攻击指南
- PortSwigger XSS Learning Lab
- [MDN Web Docs - XSS 简介](#)
- [CVE-2017-0144 EternalBlue \(永恒之蓝\)](#)
- [四川大学关于新型勒索病毒“永恒之蓝”的紧急应对措施](#)