

20200707信息安全实训

笔记本： 我的第一个笔记本

创建时间： 2020/7/7 8:06

更新时间： 2020/7/7 17:24

作者： 820410740@qq.com

xss攻击：

用户输入的恶意的js语句，拼接到页面HTML代码中去执行。

xss(js)标识：

1.<script>alert(1)</script>

2.伪协议：

123

3.事件型触发方法：

逻辑漏洞：是利用开发者在开发程序时的逻辑思维的错误

什么是逻辑漏洞

- 网站开发人员再建设网站的时候，由于验证不严格，造成的bug
- 能干什么
 - 任意用户重置密码
 - 提权/越权
 - 任意金额购买
 - 验证码绕过
 -

- 手机号

- 抓包，尝试修改手机号，将验证码发送到自己的手机

- 邮件

- 先自己注册一个用户，点击重置，
- 分析邮件中的连接
- 不加密，加密策略太弱

支付漏洞

xss:存储型xss、反射型xss

文件上传 iis nginx

wapplayzer

蚁剑

sql注入 xss 文件上传 支付漏洞 弱口令 webshell + 黑客 白帽 授权

渗透测试报告：危害 过程 如何防御

intruder(bp)

海德拉 (kali)

app渗透

钓鱼网站 钓鱼邮箱

钓鱼获取他人定位 2-5公里

爆破密码

字典爆破

sniper狙击手)

battering ram (攻城锤)

pitch fork (草叉模式)

cluster bomb (集束炸弹)

作业 第一章 sql注入 (判断)

第二章 cookie注入 (判断)

第三章 任意金额支付 后台爆破 (第二章的后台尝试)

截图 分析 格式整齐