20200803信息安全实训

笔记本:	我的第一个笔记本		
创建时间:	2020/8/3 13:53	**更新时间:**	2020/8/3 19:30
作者:	820410740@qq.com		
URL:	https://www.cnblogs.com/lxfweb/p/12859591.html		

逻辑漏洞

了解什么是逻辑漏洞
定义特性是指应用程序执行的逻辑存在某种缺陷。

为什么会出现这种漏洞
大部分逻辑缺陷表现为开发者在思考过程中做出的特殊假设存在明显或隐含的错误，通俗点来说，有的开发者会这样认为，如果发生A，就会出现B，因此我执行C。没有考虑如果发生X会怎么样，这种错误的假设会造成许多安全漏洞。

容易出现的位置
有哪些是常见的逻辑漏洞
密码找回、交易支付、密码修改、账号注册、越权访问、突破限制等

https://www.cnblogs.com/lxfweb/p/12859591.html

1.首先尝试正确操作流程，记录数据包
2.分析数据包，找到有效数据部分
3.推测数据构造方法
4.构造数据包验证猜测

对验证码、密码进行爆破

pikachu 越权
DVWA 验证码绕过