## 数据安全实验

sql注入是通过用户输入内容来构造动态sql语句，进而获取后台数据库数据的网络攻击方式。

第一步是要找到注入点。通过手动注入，比如在链接上加上特定的字符或语句如’/?Id=1’,通过页面返回的信息判断是否存在注入点，即可以动态构造sql语句的输入空间。

找到注入点后，可以通过各种sql语句获得数据库信息，判断数据库中是否存在什么表，后台的登陆信息等。

在实际操作中，sql注入一般依赖于各种注入工具，实现快速的漏洞扫描，比如sqlmap。此外还有盲注,通过上传图片注入木马等方式出现，需要通过各种方法对是否存在注入漏洞进行进一步的渗透测试。

要解决sql注入问题，最重要的一点是，千万不能相信用户的输入；可以通过各种办法对用户的输入进行改造，如添加‘\_’字符；使之不能构造成sql语句；主要是要通过将用户的输入数据进行处理后，再与数据库进行交互，避免直接接触。

进行实验时，靶机出现错误，在网页中输入flag并提交时，mysql报错，无法跳转到下一环节。

解决办法：通过Xftp与靶机建立新的连接，更改靶机的web文件夹，并重新配置mysql，启动sql服务。

解决该问题后，重新进行sql注入。