实验吧-后台登陆（writeup系列）

原创

tnt阿信 于 2018-06-04 12:24:27 发布 2264 收藏

分类专栏： Web安全 文章标签： 实验吧 后台登陆

本文链接：https://blog.csdn.net/he_and/article/details/80565703

前言

> 本系列博文系实验吧的writeup，我希望通过此方式记录下自己的学习轨迹，也给大家一个参考，欢迎与我讨论交流

右键查看审查元素就可以看到源码中的逻辑判断。我们重点关注下这里的sql语句：

```
$sql = "SELECT * FROM admin WHERE username = 'admin' and password = '".md5($password,true)."'";```
看到密码被md5加密了，是不是感觉没戏了？
其实我们还是有办法的，MD5也是存在注入的，从sql语句中可以知道，只要我们的password经过MD5加密过后然后再转换成字符串是这样的：``
`' or '<trash>```
就可以完成注入，
>注:这里的转换成字符串是自动进行的

我们现在需要做的就是找到一个这样的字符串，顺手贴一个：ffifdyop
```