

2021-07-08 CTFer成长之路-SQL注入-总结

原创

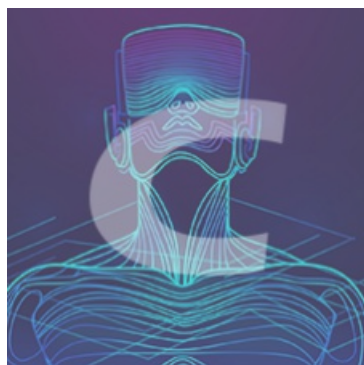
愚公搬代码 于 2021-07-08 14:49:15 发布 26729 收藏

分类专栏: [CTF成长之路](#)

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/aa2528877987/article/details/118573393>

版权



[CTF成长之路 专栏收录该内容](#)

32 篇文章 6 订阅

订阅专栏

注入的功效

前面讲述了SQL注入的基础和绕过的方法, 那么, 注入到底有什么用呢? 结合作者的实战经验, 总结如下。

- ❖ 在有写文件权限的情况下, 直接用INTO OUTFILE或者DUMPFILe向Web目录写文件, 或者写文件后结合文件包含漏洞达到代码执行的效果, 见图1-2-53。
- ❖ 在有读文件权限的情况下, 用load_file()函数读取网站源码和配置信息, 获取敏感数据。
- ❖ 提升权限, 获得更高的用户权限或者管理员权限, 绕过登录, 添加用户, 调整用户权限等, 从而拥有更多的网站功能。
- ❖ 通过注入控制数据库查询出来的数据, 控制如模板、缓存等文件的内容来获取权限, 或者删除、读取某些关键文件。
- ❖ 在可以执行多语句的情况下, 控制整个数据库, 包括控制任意数据、任意字段长度等。
- ❖ 在SQL Server这类数据库中可以直接执行系统命令。

```
-----+
| root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
```

SQL注入小结

本节仅选用了CTF中最简单的一些考点进行了简介，而实际比赛中会将很多的特性、函数进行结合。SQL注入类的MySQL题目中可以采用的过滤方法多种多样，同时由于SQL服务器在实现时的不同，即使是相同的功能，也会有多种多样的实现方式，而题目会将这种过滤时不容易考虑到的知识点或注入技巧作为考点。那么，为了做出题目或更深入了解SQL注入原理，最关键的是根据不同的SQL服务器类型，查找相关资料，通过fuzz得出被过滤掉的字符、函数、关键词等，在文档中查找功能相同但不包含过滤特征的替代品，最终完成对相关防御功能的绕过。

此外，平时多积累、多练习也会很有帮助，一些平台如sqli-labs (<https://github.com/Audi-1/sqli-labs>) 提供不同过滤等级下的注入题目，其中涵盖了大多数出题点。我们通过练习、总结，在比赛中总会能找到需要的组合方式，最终解决题目。