安全小课堂第八十六期【web漏洞挖掘之SQL注入】

原创：京东安全 京东安全应急响应中心 3月5日

随着网络时代的飞速发展,网络安全问题越来越受大家的关注，而SQL注入攻击是最流行的攻击手段之一，SQL注入导致的安全问题数不胜数。那么它的攻击是如何展开的,我们又将如何防御它呢？

JSRC **安全小课堂第八十六期**，邀请到**莫须有**作为讲师就**web漏洞挖掘之SQL注入**为大家进行分享。也感谢白帽子盆友的精彩提问与互动~

参数预编译方式防止sql注入的技术原理是什么？

京安小妹

莫须有：

在使用参数化查询的情况下，数据库系统不会将参数的内容视为SQL指令的一部分来处理，而是在数据库完成SQL指令的编译后，才套用参数运行，因此就算参数中含有破坏性的指令，也不会被数据库所运行。因为对于参数化查询来说，查询SQL语句的格式是已经规定好了的，需要查的数据也设置好了，缺的只是具体的那几个数据而已。所以用户能提供的只是数据，而且只能按照需求提供，无法更进一步做出影响数据库的其他举动来。

讲师

mybatis框架环境下最容易出现sql注入的场景有哪些？

京安小妹

莫须有：

第一种是模糊查询

这种场景可以通过采用预编译机制，避免SQL语句拼接的问题，从根源上防止SQL注入漏洞的产生；

第二种是in之后的参数

这种场景可以使用康将自带循环指令解决SQL语句动态拼接的问题；

第三种是order by之后的参数

这种场景可以在java层面做映射来解决

讲师

如何在研发阶段通过技术手段避免sql注入？

京安小妹

莫须有：

这里推荐三种方式：参数预编译、正则表达式过滤传入参数、字符串过滤

横向渗透。

如何感知到sql注入漏洞正在被利用？

京安小妹

莫须有：

对数据库进行监测，党对数据库进行操作时，自动对执行的SQL语句进行语义分析，并划分威胁等级，根据划分的威胁等级进行不同的处理；

创建蜜罐数据库，当对蜜罐数据库进行操作时，直接触发警报并阻断该IP的访问

讲师

如何高效扫描sql注入漏洞？

京安小妹

莫须有：

高效扫描SQL注入需要从两个角度考虑，一是：扫描速度，二是：扫描结果准确度

扫描速度可以通过多线程、高并发、分布式来实现

扫描结果准确度需要平时多收集有关cms注入漏洞的POC，在扫描时通过指纹识别和POC相结合来提高准确度

讲师

白帽子提问1：

Prestatement 和statement 区别？

莫须有：

Prestatement 对批量处理可以提高效率，statement 每次执行SQL语句都要进行编译

白帽子提问2：

预编译能完全防止sql注入吗

莫须有：

一般情况下使用得当是可以防止SQL注入的

白帽子提问3：

Order by，举个例子吧

莫须有：

查询文章标题为“安全”的文章并根据阅读量或者ID排序，select * from article where title = '安全' order by #{readVolume} asc，这里readVolume不是查询参数，无法使用预编译机制，只能这样拼接select * from article where title = '安全' order by ${readVolume} asc。针对这种情况研发人员可以在java层面做映射进行解决。如当在根据阅读量或者ID排序时，我们可以限制用户只能输入0和1，当用户输入0时，我们在代码层面将其映射为readVolume，当用户输入1时，将其映射为id。当用户输入0和1以外的内容时，可以将其转换为默认排序方式。

本期JSRC 安全小课堂到此结束。更多内容请期待下期安全小课堂。如果还有你希望出现在安全小课堂内容暂时未出现，也欢迎留言告诉我们。

安全小课堂的往期内容开通了自助查询，点击菜单栏进入“安全小课堂”即可浏览。

最后，广告时间，京东安全招人，安全开发、运营、风控、安全研究等多个职位虚位以待，招聘内容具体信息请扫描二维码了解。

简历请发送：cv-security@jd.com

微信公众号：jsrc_team

新浪官方微博：京东安全应急响应中心