链滴

大家一起讨论一下 SQL 注入的防范姿势

作者：junze

原文链接：https://ld246.com/article/1465610855497

来源网站：链滴

1. 昨天晚上已经11点多的时间，一个朋友突然找我说她们公司的网站的漏洞被提交到wooyun了。（后就跟妹子大概了解了一下漏洞的情况 PS：妹子是php程序员）

2. wooyun上提交了两处漏洞,1处是SQL注入 (经过了解,她们公司的用的框架是11年的老框架,还是mysql_query()这些老的mysql函数) 另一处就是cookie的问题,妹子把用户的uid,等敏感信息都写进cooki了,2333。然后php处理业务逻辑的uid也是从cookie里面拿的,233333 (导致修改cookie后可以伪装任意用户)

3.我给她说了SQL注入的解决方案(第一种治标不治本的,用正则匹配SQL语句,过滤危险字符,关键字,转符号,第二种方案,弃用mysql老函数,用PDO或者mysqli)(cookie那个地方的漏洞,我建议她把uid等敏信息存在session里面,然后把sessionID加密后放在cookie里面)

4.妹子最后说,她大概听懂了.改公司框架的mysql驱动是不太现实的,公司不会让她改的,那就只好用正匹配SQL语句,过滤非法字符串了!

5.我就去网上找了一些SQL语句过滤的函数 号称很好用的SQL过滤函数

知乎大婶们的回答

想跟大家讨论一下 SQL注入防范的姿势，大家有没有比较好用的SQL入 过滤SQL语句的函数,分享一下,谢谢!