



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 Plugin Responsive Thumbnail Slider 1.0 - Arbitrary File Upload

EDB-ID:

37998

CVE:

EDB Verified: 

Author:

[ARASH KHAZAEI](#)

Type:

[WEBAPPS](#)

Exploit:  

Platform:

[PHP](#)

Date:

2015-08-28

Vulnerable App: 



 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

```
# Exploit Title: Wordpress Responsive Thumbnail Slider Arbitrary File
Upload
# Date: 2015/8/29
# Exploit Author: Arash Khazaei
# Vendor Homepage:
https://wordpress.org/plugins/wp-responsive-thumbnail-slider/
# Software Link:
https://downloads.wordpress.org/plugin/wp-responsive-thumbnail-slider.zip
# Version: 1.0
# Tested on: Kali , Iceweasel Browser
# CVE : N/A
# Contact : http://twitter.com/0xClay
# Email : 0xclay@gmail.com
# Site : http://bhunter.ir

# Intrduction :

# Wordpress Responsive Thumbnail Slider Plugin iS A With 6000+ Active
Install
# And Suffer From A File Upload Vulnerability Allow Attacker Upload Shell
As A Image .
# Authors , Editors And Of Course Administrators This Vulnerability To Harm
WebSite .

# POC :

# For Exploiting This Vulnerability :

# Go To Add Image Section And Upload File By Self Plugin Uploader
# Then Upload File With Double Extension Image
# And By Using A BurpSuite Or Tamper Data Change The File Name From
Shell.php.jpg To Shell.php
# And Shell Is Uploaded . :)

<!-- Discovered By Arash Khazaei (Aka JunkyBoy) -->
```

Tags: [WordPress Plugin](#)

Advisory/Source: [Link](#)



Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

[TERMS](#)

[PRIVACY](#)

[ABOUT US](#)

[FAQ](#)

[COOKIES](#)



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