

## MODULE

# Wordpress Work The Flow Upload Vulnerability

[TRY SURFACE COMMAND](#)[← BACK TO SEARCH](#)**Disclosed**

Mar 14, 2015

**Created**

May 30, 2018

## Description

This module exploits an arbitrary PHP code upload in the WordPress Work The Flow plugin, version 2.5.2. The vulnerability allows for arbitrary file upload and remote code execution.

## Authors

Claudio Viviani

Roberto Soares Espreto robertoespreto@gmail.com

## Platform

PHP

# Architectures

php

## References

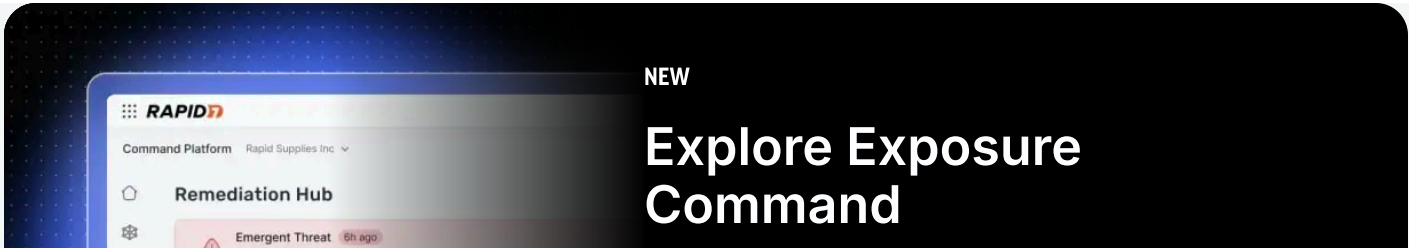
[Source Code](#)

[History](#)

## Module Options

To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

```
msf > use exploit/unix/webapp/wp_worktheflow_upload
msf exploit(wp_worktheflow_upload) > show targets
...targets...
msf exploit(wp_worktheflow_upload) > set TARGET < target-id >
msf exploit(wp_worktheflow_upload) > show options
...show and set options...
msf exploit(wp_worktheflow_upload) > exploit
```



# RAPID7

## GET STARTED

- Command Platform
- Exposure Management
- MDR Services

## TAKE ACTION

- Start a Free Trial
- Take a Product Tour
- Get Breach Support
- Contact Sales

## COMPANY

- About Us
- Leadership
- Newsroom
- Our Customers
- Partner Programs
- Investors
- Careers

## STAY INFORMED

- Blog

[Emergent Threat Response](#)

[Webinars & Events](#)

[Rapid7 Labs Research](#)

[Vulnerability Database](#)

[Security Fundamentals](#)

### FOR CUSTOMERS

[Sign In](#)

[Support Portal](#)

[Product Documentation](#)

[Extension Library](#)

[Rapid7 Academy](#)

[Customer Escalation Portal](#)

### CONTACT SUPPORT

[+1-866-390-8113](tel:+18663908113)

### FOLLOW US

[!\[\]\(c1168d6a8b365d11e842ece304635fa7\_img.jpg\) LinkedIn](#)

[!\[\]\(cbd8541a32dfc32f356f5c6c994b0a21\_img.jpg\) X \(Twitter\)](#)

[!\[\]\(d3e32d099174a7c248ec1f564ee4f69c\_img.jpg\) Facebook](#)

[!\[\]\(40770d9ed6ed4f1222ebf89a1396e8b2\_img.jpg\) Instagram](#)

[!\[\]\(ccd39a0dc6d5afcc151e1371f9462f58\_img.jpg\) Bluesky](#)

© Rapid7

[Legal Terms](#)

[Privacy Policy](#)

[Export Notice](#)

[Trust](#)

[Cookie List](#)

[Accessibility Statement](#)