####################################################################

# Exploit Title : WordPress 5.2.1 DingTalk Themes LTS 4.6 Open Redirection

# Author [ Discovered By ] : steven-jiangsutianwangjisuanjijishuyouxiangongsi

# Team : jiangsutianwangjisuanjijishuyouxiangongsi

# Date : 25/05/2019

# Vendor Homepage : zmingcx.com - dingfen.net

# Information Link : zmingcx.com/begin.html

# WordPress Version : 5.2.1

# Theme Version : LTS 4.6

# Tested On : Windows and Linux

# Category : WebApps

# Exploit Risk : Medium

# Google Dorks : inurl:/wp-content/themes/dingtalk/

# Vulnerability Type : CWE-601 [ URL Redirection to Untrusted Site ('Open Redirect') ]

####################################################################

# Impact :

\*\*\*\*\*\*\*\*\*\*\*

WordPress DingTalk Themes accepts a user-controlled input that specifies

a link to an external site, and uses that link in a Redirect. This simplifies phishing

attacks. An http parameter may contain a URL value and could cause the web

application to redirect the request to the specified URL. By modifying the URL

value to a malicious site, an attacker may successfully launch a phishing scam and

steal user credentials. Because the server name in the modified link is identical to the

original site, phishing attempts have a more trustworthy appearance. Open redirect is a

failure in that process that makes it possible for attackers to steer users to malicious

websites. This vulnerability is used in phishing attacks to get users to visit malicious

sites without realizing it. Web users often encounter redirection when they visit the

Web site of a company whose name has been changed or which has been acquired by

another company. Visiting unreal web page user's computer becomes affected

by malware the task of which is to deceive the valid actor and steal his personal data.

####################################################################

# Vulnerable File :

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

/go.php

# Vulnerable Parameters :

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

?url=

# Open Redirection Exploit :

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

/wp-content/themes/dingtalk/go.php?url=[BASE64 Encoded URL]

/wp-content/themes/dingtalk/go.php?url=aHR0cHM6Ly9jeHNlY3VyaXR5LmNvbS8=

Note : Convert any random desired redirection address into the Base64 Encoded Link.

Example 1 => aHR0cHM6Ly9jeHNlY3VyaXR5LmNvbS8= stands for cxsecurity.com

Example 2 => aHR0cHM6Ly93d3cuY3liZXJpem0ub3JnLw== stands for cyberizm.org

Example 3 => aHR0cDovL2V4cGxvaXQ0YXJhYi5vcmcv stands for exploit4arab.org

Example 4 => aHR0cHM6Ly9wYWNrZXRzdG9ybXNlY3VyaXR5LmNvbS8= stands for packetstormsecurity.com

Useable Base64 Encoder - Decoder Links :

base64decode.org

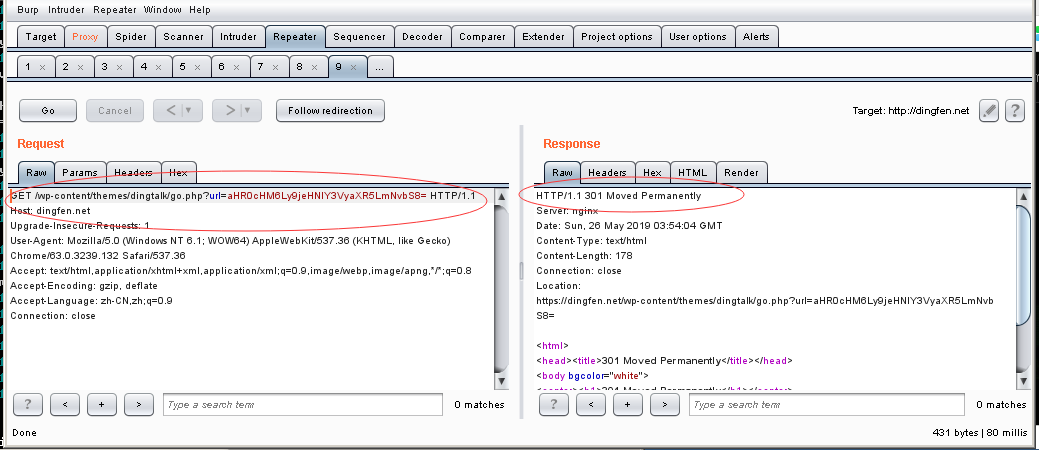
base64encode.org

####################################################################

# Example Vulnerable Sites :

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

[+] dingfen.net/wp-content/themes/dingtalk/go.php?url=aHR0cHM6Ly9jeHNlY3VyaXR5LmNvbS8=



####################################################################