seabird1992 Add files via upload History

1 contributor

566 KB

Code view：

1.Open ZZCMS system file，view admin/template_user.php,this code show that it first get parameter “ml”，if parameter ml is not nuhll，then open /skin/ system file:

```
<?php
include("admin.php");
?>
<!DOCTYPE html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<link href="style.css" rel="stylesheet" type="text/css">
<?php
checkadminisdo("label");
$action = isset($_REQUEST['action'])?$_REQUEST['action']:"";
$ml = isset($_GET['ml'])?$_GET['ml']:"";
if ($ml==""){
$ml = isset($_POST['ml'])?$_POST['ml']:"";
}

if ($ml!=""){
$dirs="";
$dirskin = opendir("../skin");
while(($dir = readdir($dirskin))!=false){
        if ($dir!="." && $dir!="..") { //不读取. ..
                $dirs=$dirs.$dir."#";
        }
}
closedir($dirskin);
$dirs=substr($dirs,0,strlen($dirs)-1);//去除最后面的"#"
//echo $dirs;
if (str_is_inarr($dirs,$ml)=='no'){
showmsg($ml.'参数有误');
}

}

if ($action=="add") {
checkadminisdo("label_add");

$title=nostr($_POST["title"]);
$title_old=$_POST["title_old"];
if (substr($title,-3)!='css' and substr($title,-3)!='htm'){
showmsg('只能是html或css这两种格式,模板名称：后面加上.html或.css');
}
```

2.view template_user.php code，it shows that this code write file using parameter “title”，and this file also allows to write php template file,in this case it can be written

Php code using parameter title.

```
                        echo "<li> <a href='?ml=".$dir."'>".$dir."</a> </li>";
                        }
                }
}
closedir($dirskin);
?>
    </div></td>
    </tr>
<?php
if ($ml<>''){
?>
    <tr>
      <td align="right" class="border" >模板文件：  </td>
      <td class="border" ><div class="boxlink">
        <?php
$title="";
$fcontent="";
if (isset($_GET['title'])){
$title=$_GET['title'];
if (substr($title,-3)!='css' and substr($title,-3)!='htm'){
showmsg('只能是html或css这两种格式');//防止直接输入php 文件地址显示PHP代码
}
}
        $dir2 = opendir("../skin/".$ml);
        while(($file = readdir($dir2))!=false){
                if ($file!="." && $file!=".." && $file!='image') { //不读取. ..
                        if ($title==$file){
                        echo "<li><a href='?ml=".$ml."&title=".$file."' style='color:#000000;background-color:#FFFFFF'>".$file."</a></li>";
                        }else{
                        echo "<li> <a href='?ml=".$ml."&title=".$file."'>".$file."</a> </li>";
                        }
                }
        }
        closedir($dir2);
        //读取现有标签中的内容
        if ($title!=''){
        $fp='../skin/'.$ml.'/'.$title;
        $f=fopen($fp,'r');
        $fcontent=fread($f,filesize($fp));
        fclose($f);
        }
```

PAYLOAD:

1.Install ZZCMS

2.login to admin page: