New issue

Jump to bottom

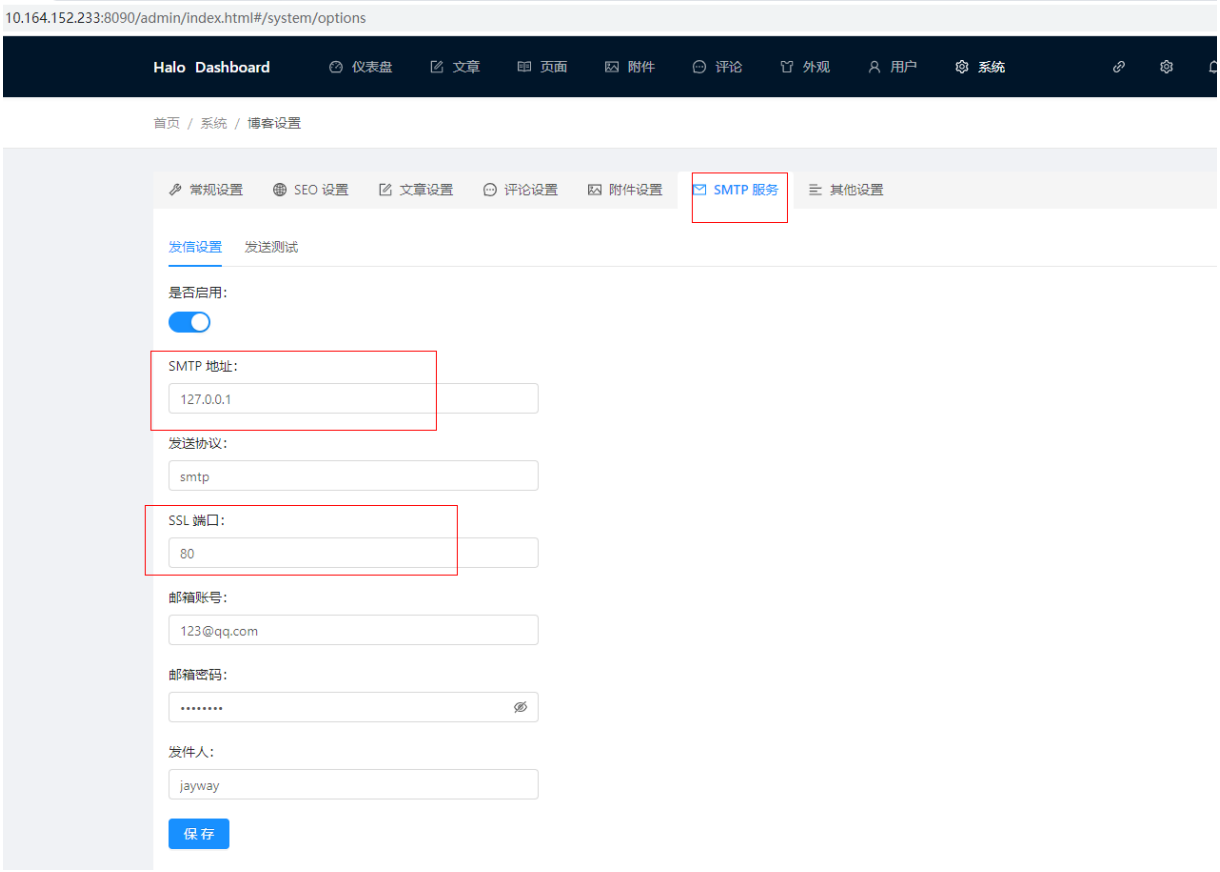
# SSRF vulnerability exists at the SMTP configuration, which can detect the server intranet #806

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




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

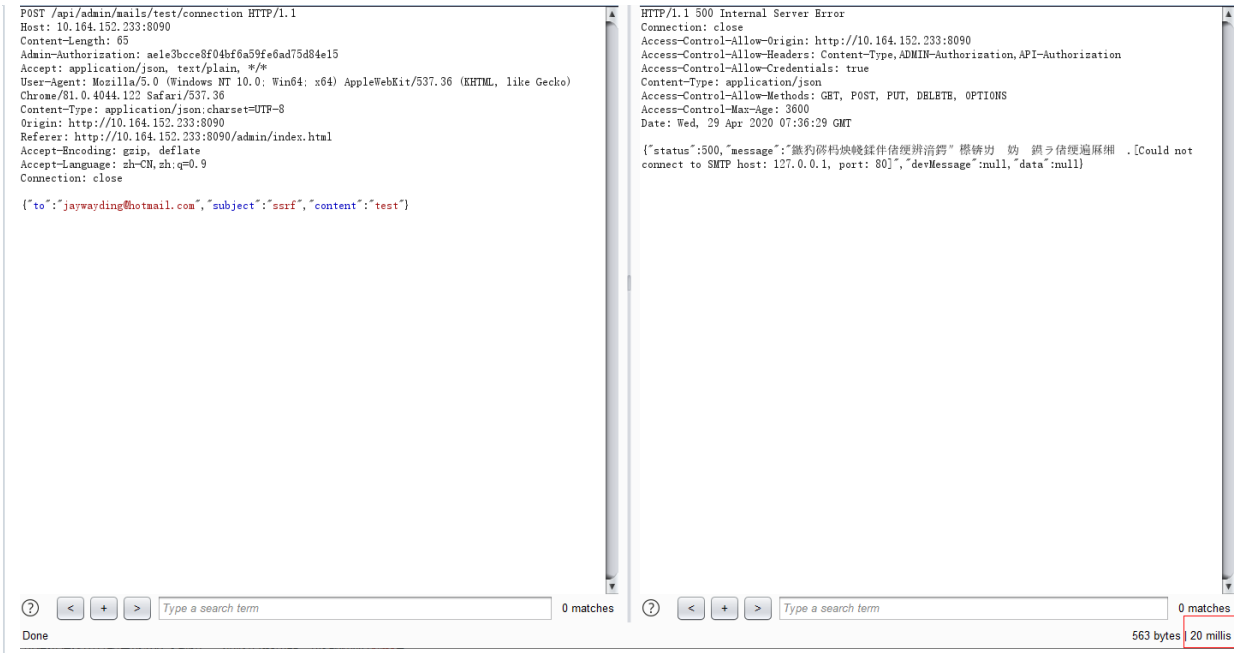
```
    @PostMapping("test/connection")
    @ApiOperation("Test connection with email server")
    @DisableOnCondition
    public BaseResponse<String> testConnection() {
        mailService.testConnection();
        return BaseResponse.ok("您和邮箱服务器的连接通畅");
    }

}
```

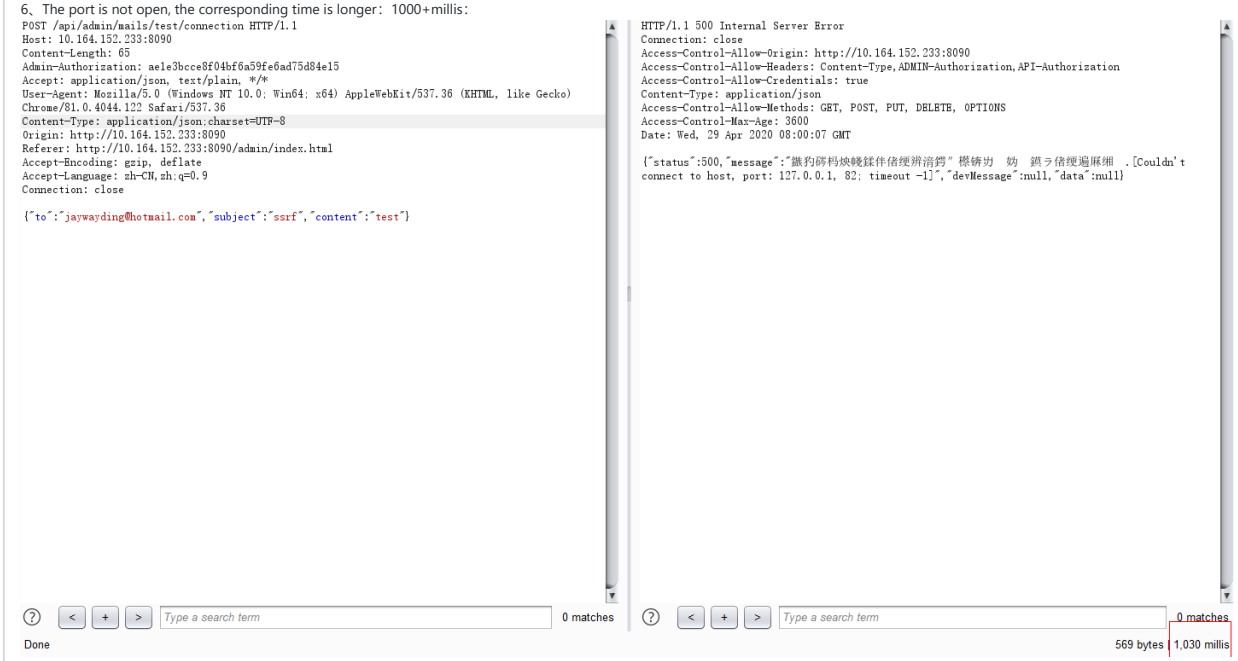
4、It is a javaMailSender that depends on springframework：

```
     */
    @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：




6、The port is not open, the corresponding time is longer：1000+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