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]

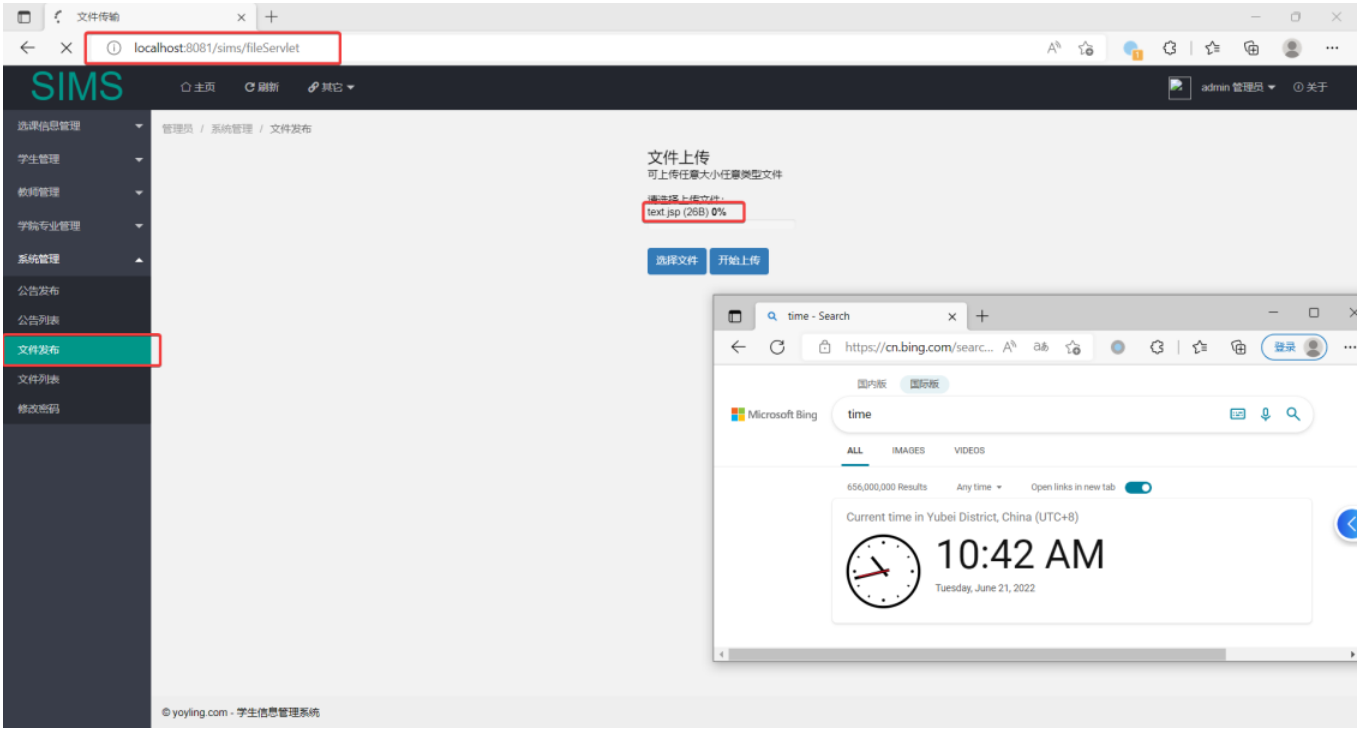
Remote

[Impact Code execution]

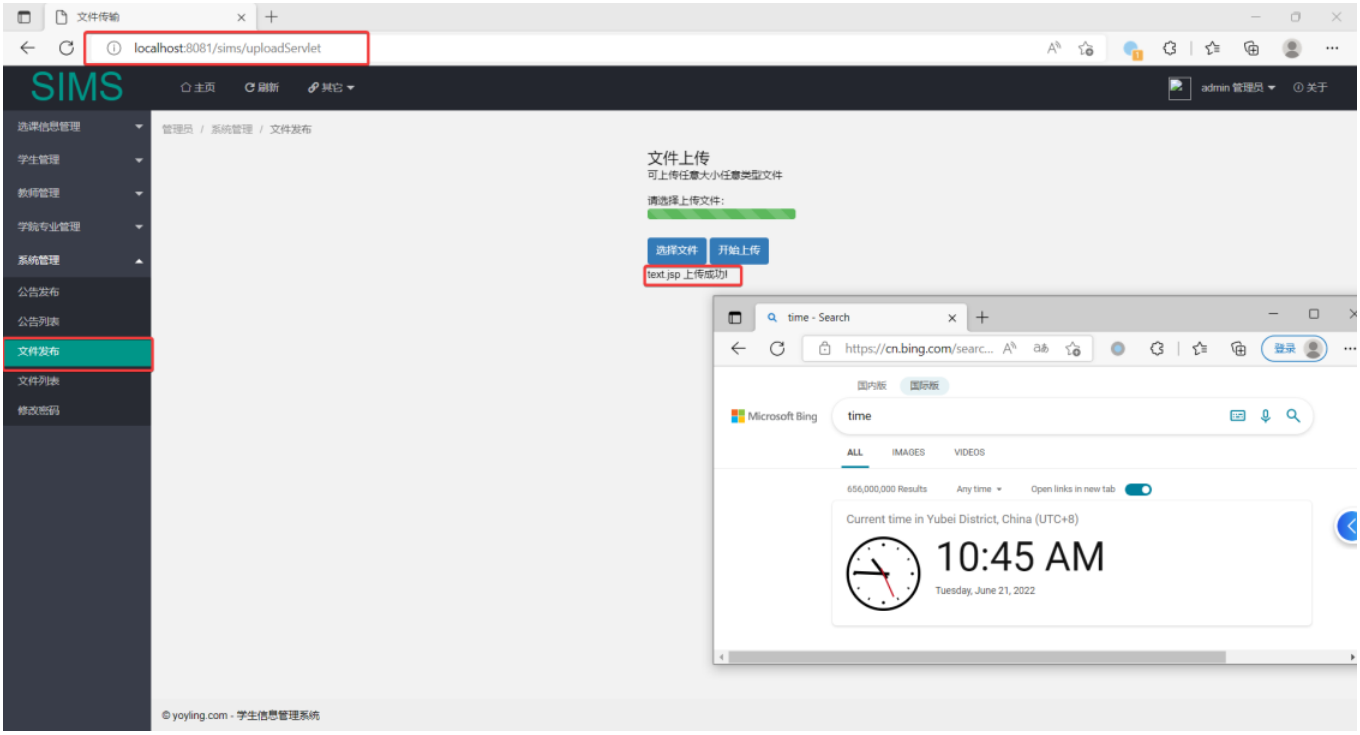
False

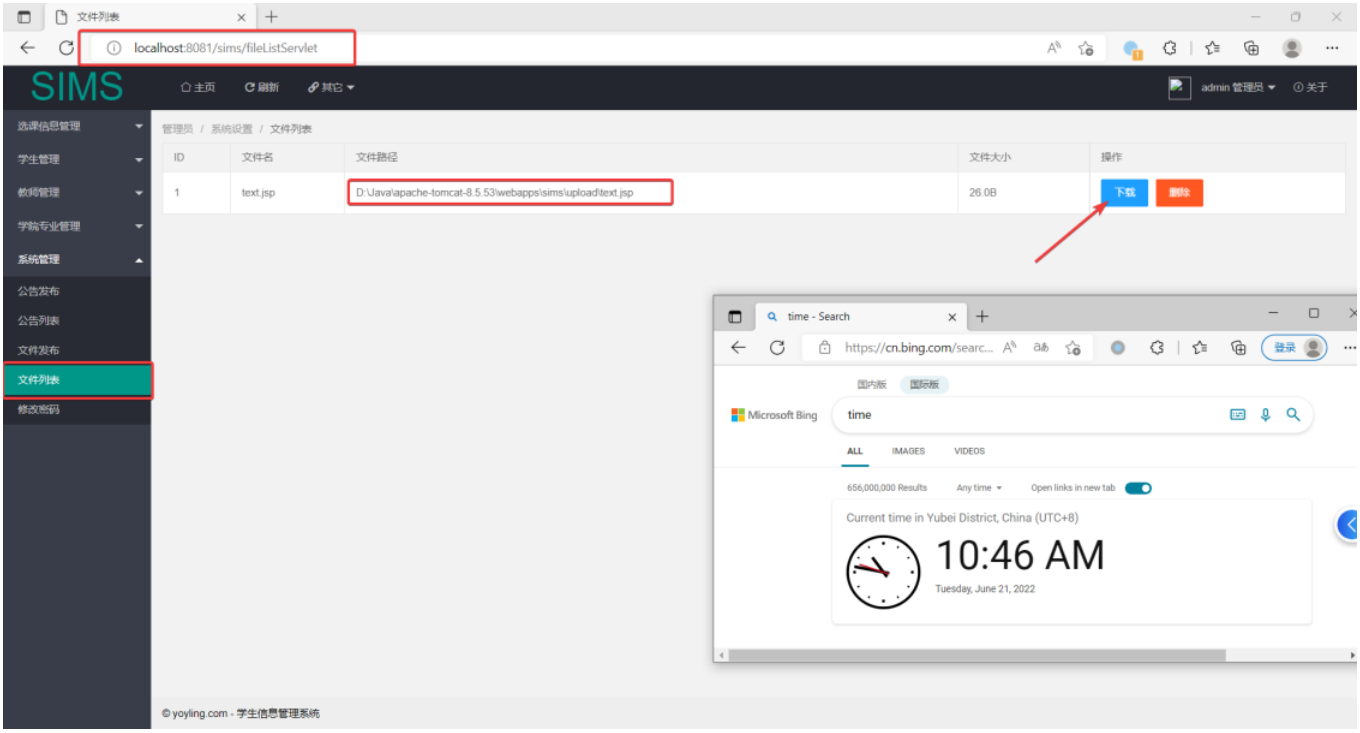
[Proof of concept]

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

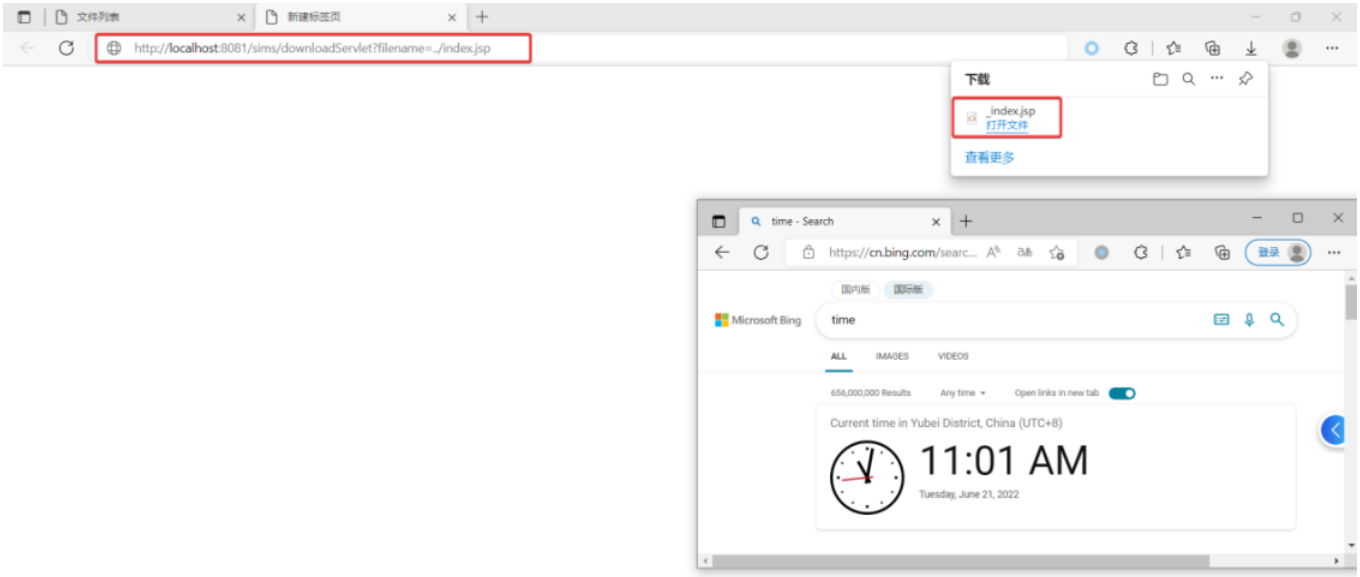


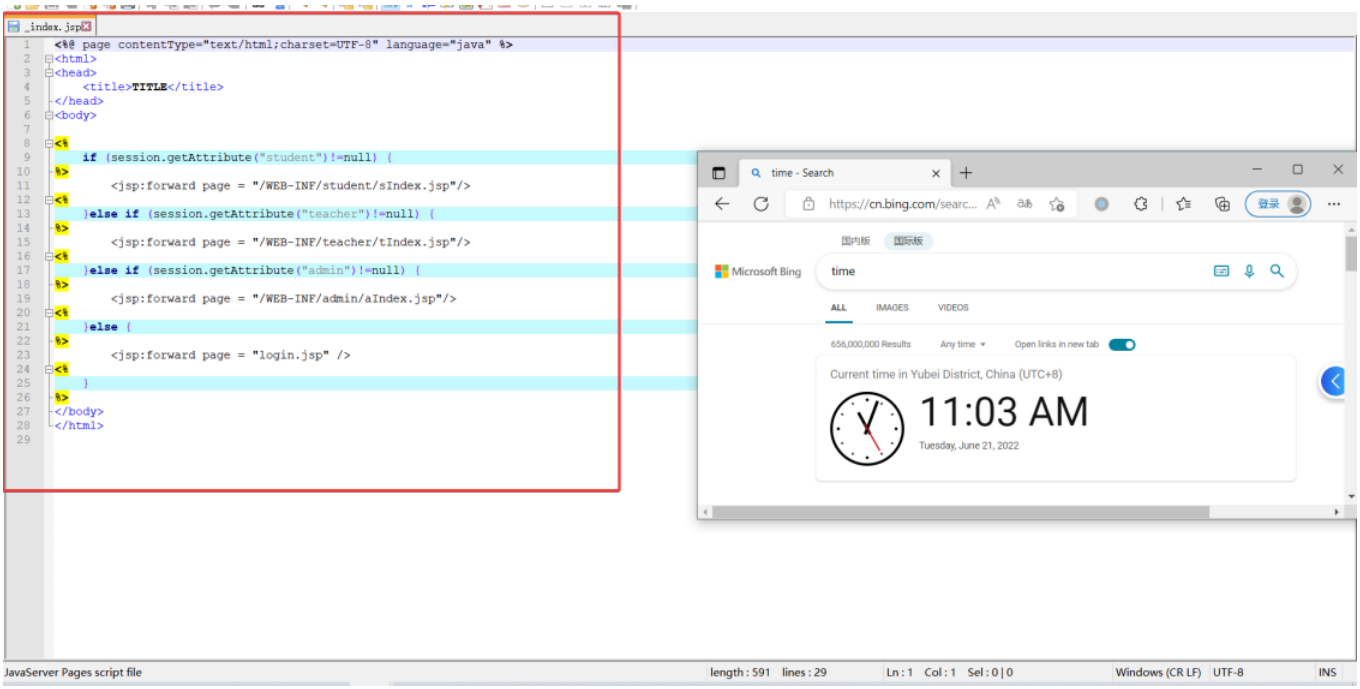
Step2: The upload is successful, and under the "System Management" tab, select "File List" and click the "Download" button to obtain the download interface.





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





[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