Some SQL injection vulnerabilities exists in JFinal CMS 5.1.0 #51

Open **So4ms** opened this issue on Aug 9 · 0 comments

So4ms commented on Aug 9 • edited

Administrator login is required. The default account password is admin:admin123

admin/article/list

There is a SQLI vul in background mode.The route is as following

```java
@ControllerBind(controllerKey = "/admin/article")
public class ArticleController extends BaseProjectController {

    10 usages
    private static final String path = "/pages/admin/article/article_";

    public void index() { list(); }

    public void list() {
        TbArticle model = getModelByAttr(TbArticle.class);

        SQLUtils sql = new SQLUtils(" from tb_article t " //
                + " left join tb_folder f on f.id = t.folder_id " //
                + " where 1 = 1 ");
        if (model.getAttrValues().length != 0) {
            sql.setAlias("t");
            sql.whereLike( attrName: "title", model.getStr( attr: "title"));
            sql.whereEquals( attrName: "folder_id", model.getInt( attr: "folder_id"));
            sql.whereEquals( attrName: "status", model.getInt( attr: "status"));
        }
        // 站点设置
        int siteId = getSessionUser().getBackSiteId();
        sql.append(" and site_id = " + siteId);

        // 排序
        String orderBy = getBaseForm().getOrderBy();
        if (StrUtils.isEmpty(orderBy)) {
            sql.append(" order by t.folder_id,t.sort,t.create_time desc ");
        } else {
            sql.append(" order by t.").append(orderBy);
        }
```

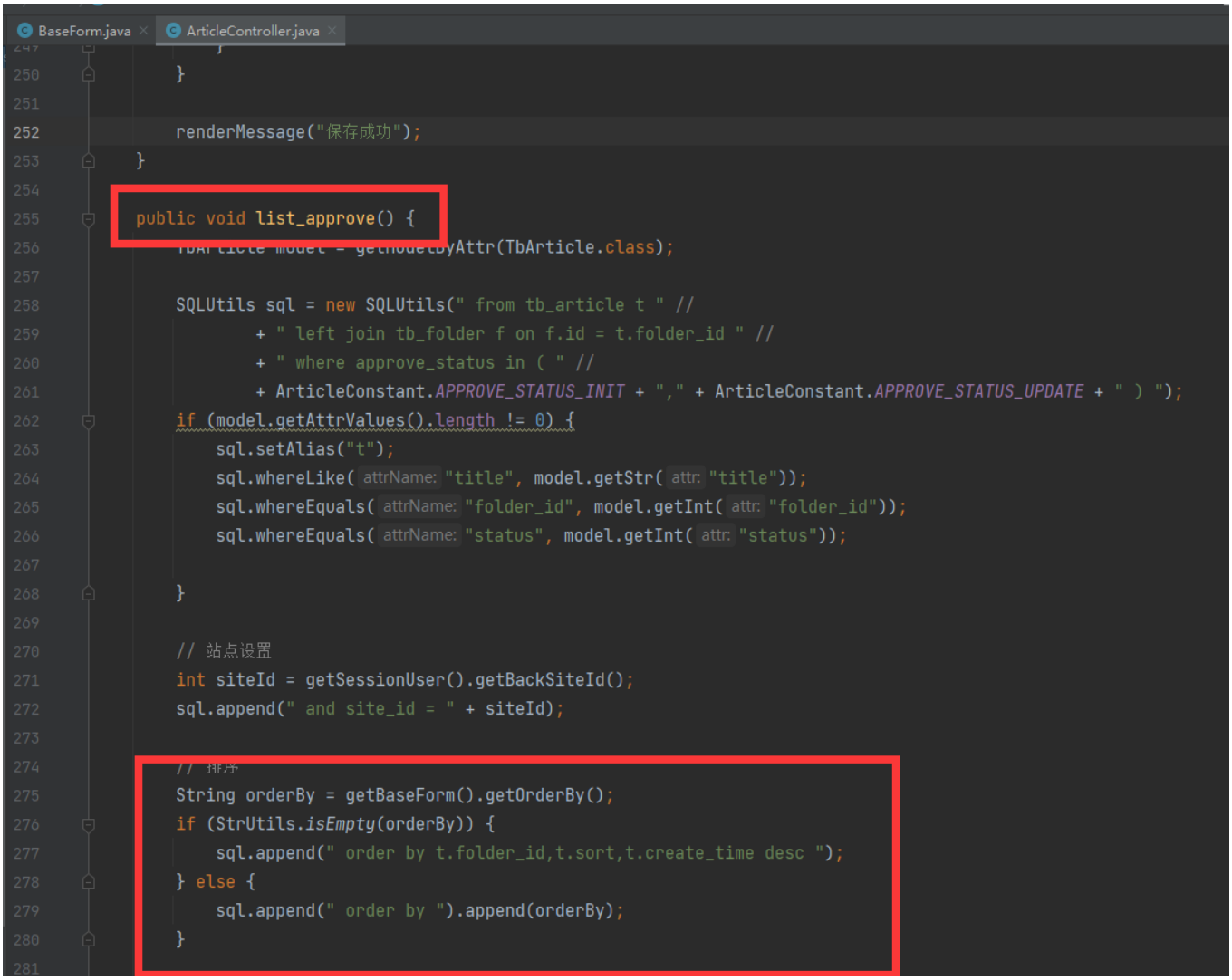
vulnerable argument passing is as following

```java
BaseForm.java  ArticleController.java
53      public boolean isShowCondition() { return showCondition; }
56
57      public void setShowCondition(boolean showCondition) { this.showCondition = showCondition;
60
61      public Paginator getPaginator() { return paginator; }
64
65      public void setPaginator(Paginator paginator) { this.paginator = paginator; }
68
69      public String getOrderBy() {
70          if (StrUtils.isEmpty(getOrderColumn())) {
71              return "";
72          }
73          return " " + getOrderColumn() + " " + getOrderAsc() + " ";
74      }
75
76      public String getOrderColumn() { return orderColumn; }
```

Successful injection at route `admin/article/list`

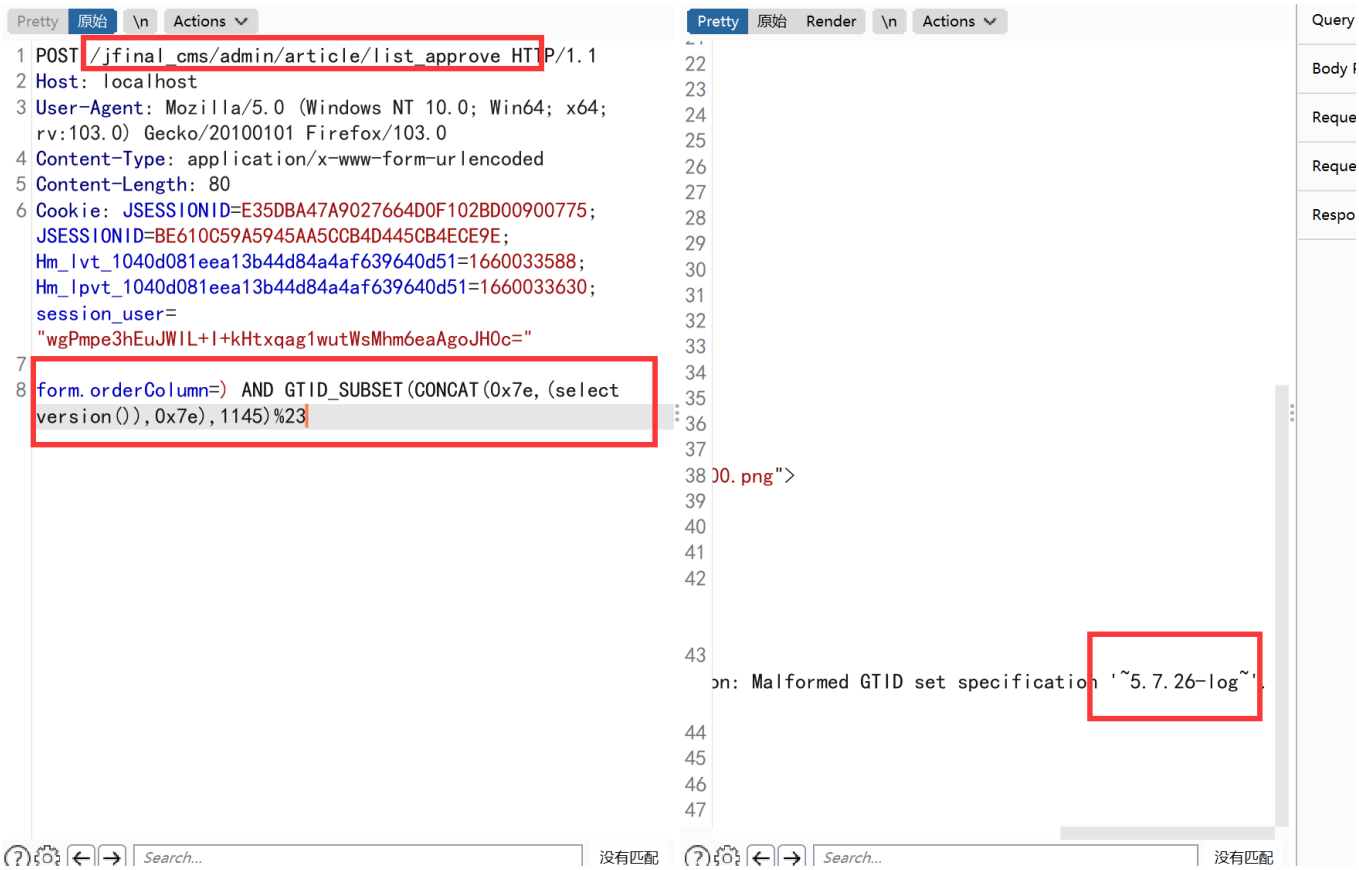
admin/article/list_approve

There is a SQLI vul in background mode.The route is as following



vulnerable argument passing is as following

Successfully injected at route `admin/article/list_approve`



admin/comment

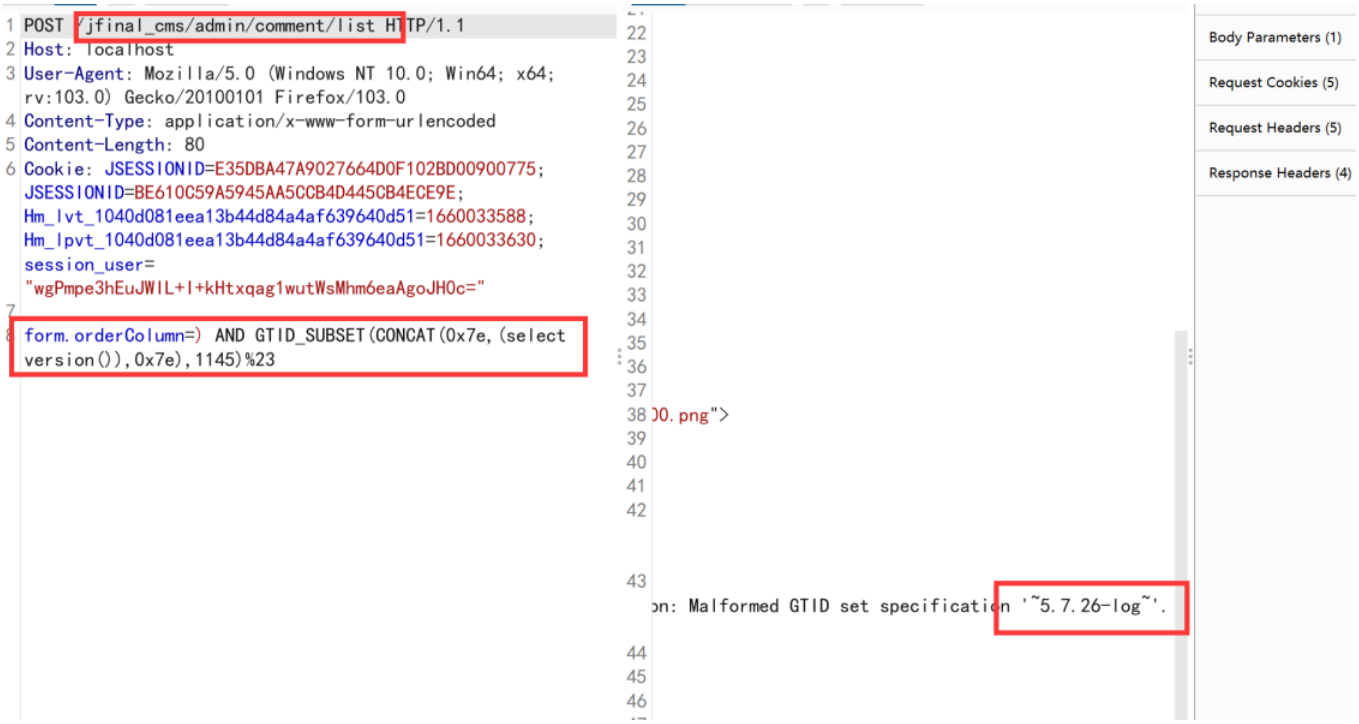
There is a SQLI vul in background mode.The route is as following

```java
@ControllerBind(controllerKe = "/admin/comment")
public class CommentController extends BaseProjectController {

    4 usages
    private static final String path = "/pages/admin/comment/comment_";

    public void list() {
        TbComment model = getModelByAttr(TbComment.class);

        SQLUtils sql = new SQLUtils(" from tb_comment t " //
                + " left join tb_article a on a.id = t.article_id where 1=1 ");
        if (model.getAttrValues().length != 0) {
            sql.setAlias("t");
            // 查询条件
            sql.whereLike( attrName: "content", model.getStr( attr: "content"));

            sql.whereEquals( attrName: "article_id", model.getInt( attr: "article_id"));
        }

        // 排序
        String orderBy = getBaseForm().getOrderBy();
        if (StrUtils.isEmpty(orderBy)) {
            sql.append(" order by t.id desc ");
        } else {
            sql.append(" order by ").append(orderBy);
        }

```

vulnerable argument passing is as following

```java
BaseForm.java  ArticleController.java
public boolean isShowCondition() { return showCondition; }

public void setShowCondition(boolean showCondition) { this.showCondition = showCondition;

public Paginator getPaginator() { return paginator; }

public void setPaginator(Paginator paginator) { this.paginator = paginator; }

    public String getOrderBy() {
        if (StrUtils.isEmpty(getOrderColumn())) {
            return "";
        }
        return " " + getOrderColumn() + " " + getOrderAsc() + " ";
    }

public String getOrderColumn() { return orderColumn; }
```

Successfully injected at route `admin/comment/list`



admin/contact/list

There is a SQLI vul in background mode.The route is as following

```java
@ControllerBind(controllerKey = "/admin/contact")
public class ContactController extends BaseProjectController {

    4 usages
    private static final String path = "/pages/admin/contact/contact_";

    public void list() {
        TbContact model = getModelByAttr(TbContact.class);

        SQLUtils sql = new SQLUtils(" from tb_contact t where 1=1 ");
        if (model.getAttrValues().length != 0) {
            sql.setAlias("t");
            sql.whereLike( attrName: "name", model.getStr( attr: "name"));
            sql.whereEquals( attrName: "type", model.getStr( attr: "type"));
        }

        // 排序
        String orderBy = getBaseForm().getOrderBy();
        if (StrUtils.isEmpty(orderBy)) {
            sql.append(" order by id desc ");
        } else {
            sql.append(" order by ").append(orderBy);
        }

        Page<TbContact> page = TbContact.dao.paginate(getPaginator(), select: "select t.* ", //
                sql.toString().toString());
```

vulnerable argument passing is as following

```java
BaseForm.java  ArticleController.java
    public boolean isShowCondition() { return showCondition; }

    public void setShowCondition(boolean showCondition) { this.showCondition = showCondition;

    public Paginator getPaginator() { return paginator; }

    public void setPaginator(Paginator paginator) { this.paginator = paginator; }

    public String getOrderBy() {
        if (StrUtils.isEmpty(getOrderColumn())) {
            return "";
        }
        return " " + getOrderColumn() + " " + getOrderAsc() + " ";
    }

    public String getOrderColumn() { return orderColumn; }
```

Successfully injected at route `admin/contact/list`

admin/foldernotice/list

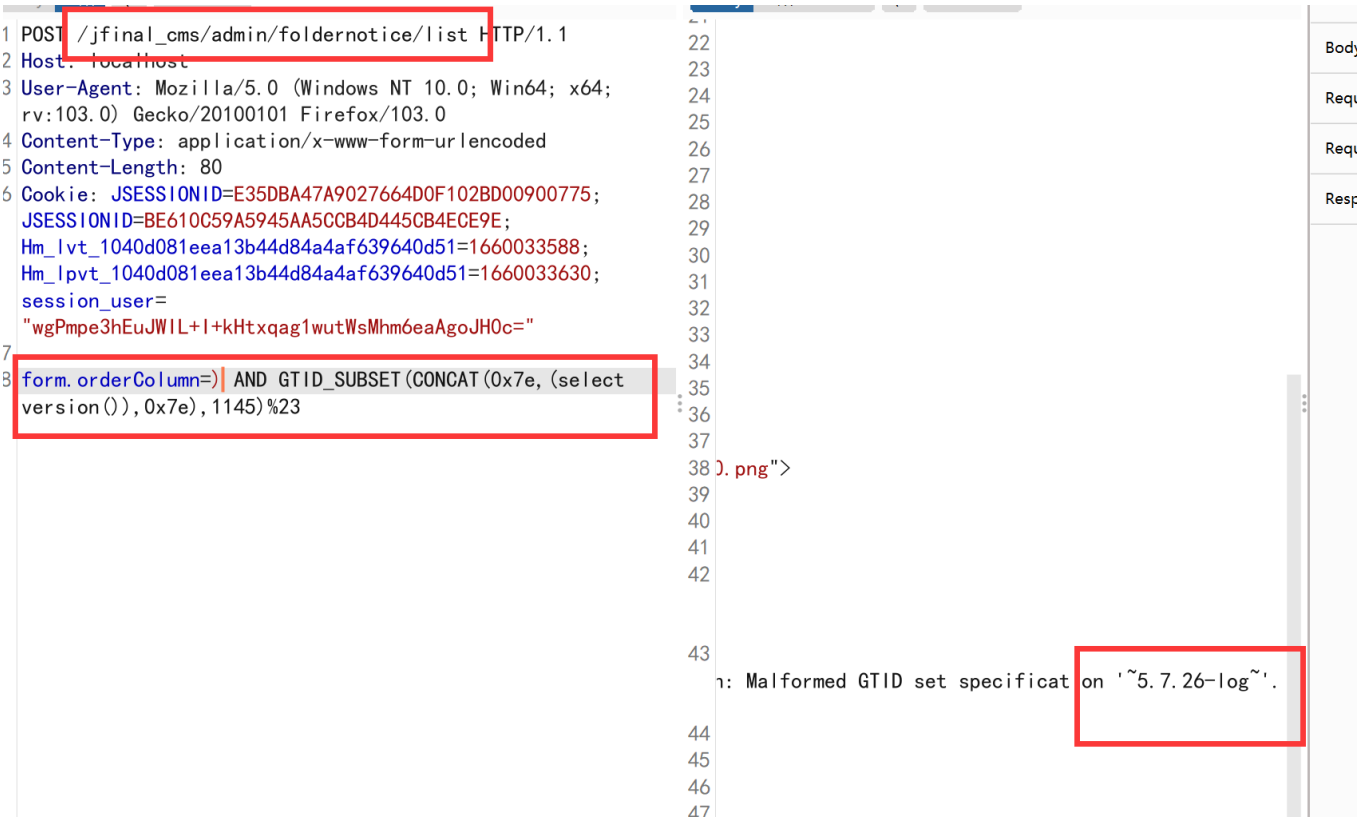
There is a SQLI vul in background mode.The route is as following

```
栏目公告
Author: flyfox 2014-4-24
@ControllerBind(controllerKey = "/admin/foldernotice")
public class FoldernoticeController extends BaseProjectController {

    4 usages
    private static final String path = "/pages/admin/foldernotice/foldernotice_";

    public void list() {
        TbFolderNotice model = getModelByAttr(TbFolderNotice.class);

        SQLUtils sql = new SQLUtils(" from tb_folder_notice t " //
                + " left join tb_folder f on f.id = t.folder_id " //
                + " where is_deleted = " + JFlyFoxUtils.IS_DELETED_NO + " ");
        if (model.getAttrValues().length != 0) {
            sql.setAlias("t");
            // 查询条件
            sql.whereEquals( attrName: "folder_id", model.getInt( attr: "folder_id"));
        }
        // 站点设置
        sql.append(" and site_id = " + getSessionUser().getBackSiteId());

        // 排序
        String orderBy = getBaseForm().getOrderBy();
        if (StrUtils.isEmpty(orderBy)) {
            sql.append(" order by t.folder_id,t.sort,t.id desc ");
        } else {
            sql.append(" order by ").append(orderBy);
        }
```

vulnerable argument passing is as following

```
BaseForm.java  ArticleController.java
53      public boolean isShowCondition() { return showCondition; }
56
57      public void setShowCondition(boolean showCondition) { this.showCondition = showCondition;
60
61      public Paginator getPaginator() { return paginator; }
64
65      public void setPaginator(Paginator paginator) { this.paginator = paginator; }
68
69          public String getOrderBy() {
70              if (StrUtils.isEmpty(getOrderColumn())) {
71                  return "";
72              }
73              return " " + getOrderColumn() + " " + getOrderAsc() + " ";
74          }
75
76      public String getOrderColumn() { return orderColumn; }
```

Successfully injected at route `admin/foldernotice/list`



admin/folderrollpicture/list

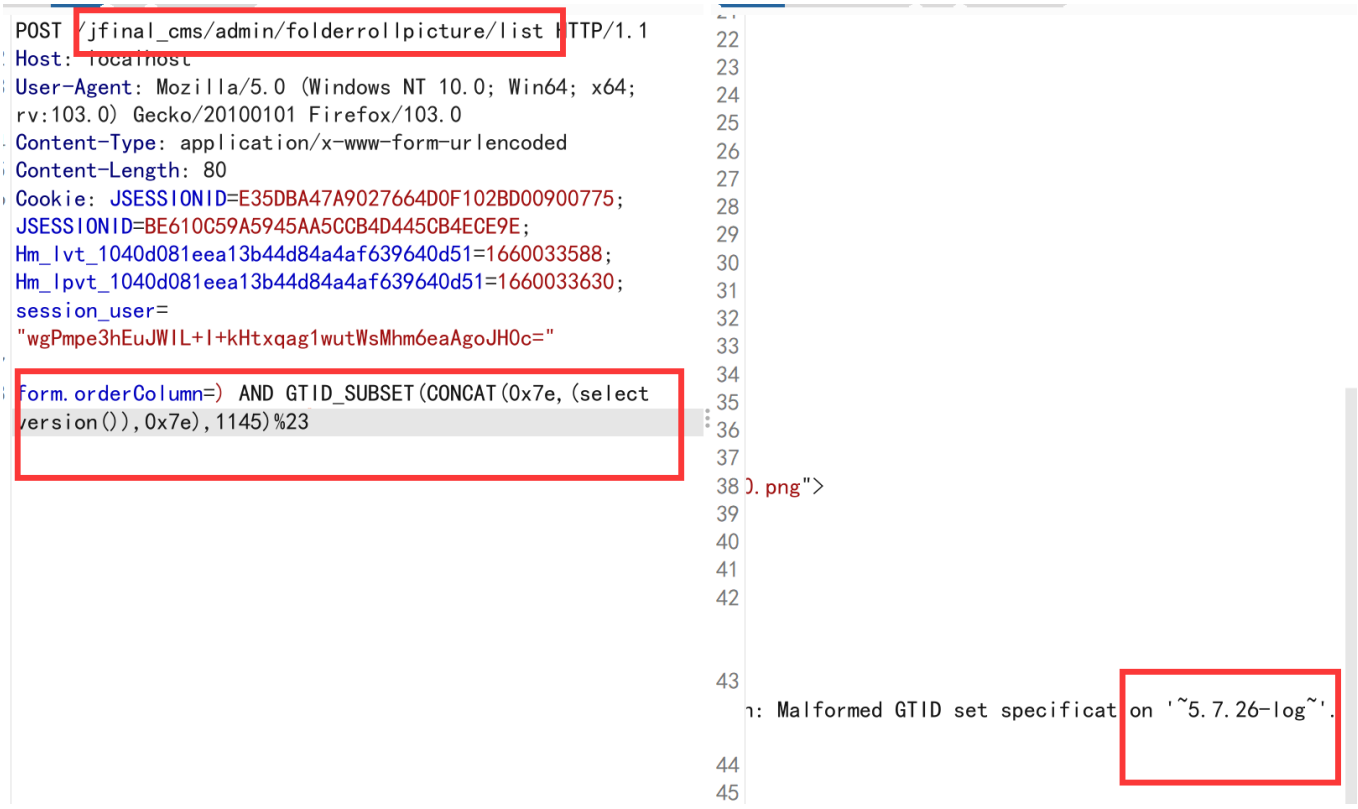
There is a SQLI vul in background mode.The route is as following

```java
@ControllerBind(controllerKey = "/admin/folderrollpicture")
public class FolderrollpictureController extends BaseProjectController {

    4 usages
    private static final String path = "/pages/admin/folderrollpicture/folderrollpicture_";

    public void list() {
        TbFolderRollPicture model = getModelByAttr(TbFolderRollPicture.class);

        SQLUtils sql = new SQLUtils(" from tb_folder_roll_picture t " //
                + " left join tb_folder f on f.id = t.folder_id " //
                + " where is_deleted = " + JFlyFoxUtils.IS_DELETED_NO + " ");
        if (model.getAttrValues().length != 0) {
            sql.setAlias("t");
            // 查询条件
            sql.whereEquals( attrName: "folder_id", model.getInt( attr: "folder_id"));
        }
        // 站点设置
        sql.append(" and site_id = " + getSessionUser().getBackSiteId());

        // 排序
        String orderBy = getBaseForm().getOrderBy();
        if (StrUtils.isEmpty(orderBy)) {
            sql.append(" order by t.folder_id,t.sort,t.id desc ");
        } else {
            sql.append(" order by ").append(orderBy);
        }
```

vulnerable argument passing is as following

```java
BaseForm.java  ArticleController.java
53      public boolean isShowCondition() { return showCondition; }
56
57      public void setShowCondition(boolean showCondition) { this.showCondition = showCondition;
60
61      public Paginator getPaginator() { return paginator; }
64
65      public void setPaginator(Paginator paginator) { this.paginator = paginator; }
68
69      public String getOrderBy() {
70          if (StrUtils.isEmpty(getOrderColumn())) {
71              return "";
72          }
73          return " " + getOrderColumn() + " " + getOrderAsc() + " ";
74      }
75
76      public String getOrderColumn() { return orderColumn; }
```

Successfully injected at route `admin/folderrollpicture/list`



admin/friendlylink/list

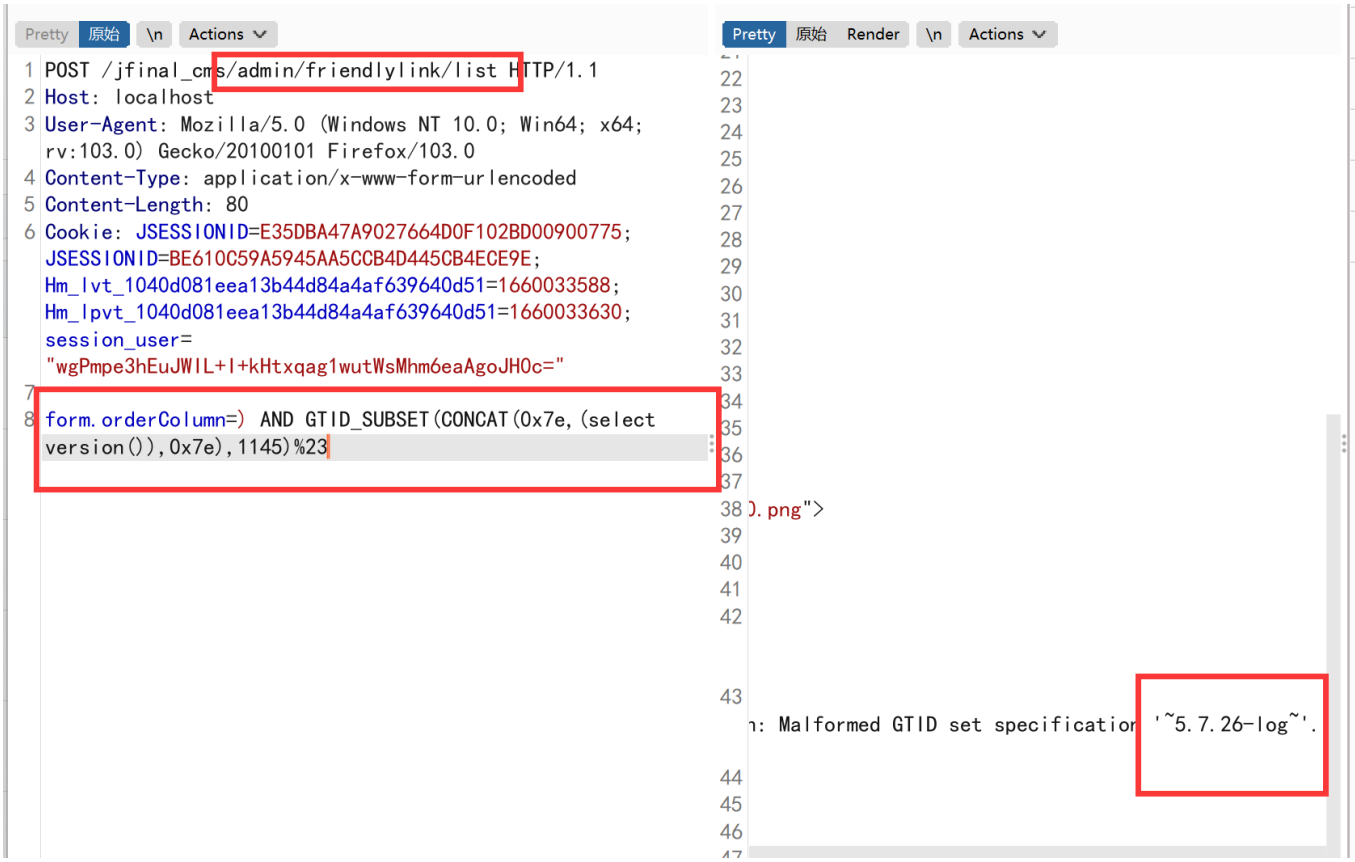
There is a SQLI vul in background mode.The route is as following

```java
@ControllerBind(controllerKey = "/admin/friendlylink")
public class FriendlylinkCont ller {

    4 usages
    private static final String path = "/pages/admin/friendlylink/friendlylink_";

    public void list() {
        TbFriendlylink model = getModelByAttr(TbFriendlylink.class);

        SQLUtils sql = new SQLUtils(" from tb_friendlylink t"
                + " left join tb_site s on s.id = t.site_id where 1=1 ");
        if (model.getAttrValues().length != 0) {
            sql.setAlias("t");
            sql.whereLike( attrName: "name", model.getStr( attr: "name"));
        }

        // 排序
        String orderBy = getBaseForm().getOrderBy();
        if (StrUtils.isEmpty(orderBy)) {
            sql.append(" order by t.sort,t.id ");
        } else {
            sql.append(" order by ").append(orderBy);
        }

        nate(getPaginator(), select: "select t.*,s
```

vulnerable argument passing is as following

```java
BaseForm.java  ArticleController.java
53      public boolean isShowCondition() { return showCondition; }
56
57      public void setShowCondition(boolean showCondition) { this.showCondition = showCondition;
60
61      public Paginator getPaginator() { return paginator; }
64
65      public void setPaginator(Paginator paginator) { this.paginator = paginator; }
68
69      public String getOrderBy() {
70          if (StrUtils.isEmpty(getOrderColumn())) {
71              return "";
72          }
73          return " " + getOrderColumn() + " " + getOrderAsc() + " ";
74      }
75
76      public String getOrderColumn() { return orderColumn; }
```

Successfully injected at route `admin/friendlylink/list`



admin/imagealbum/list

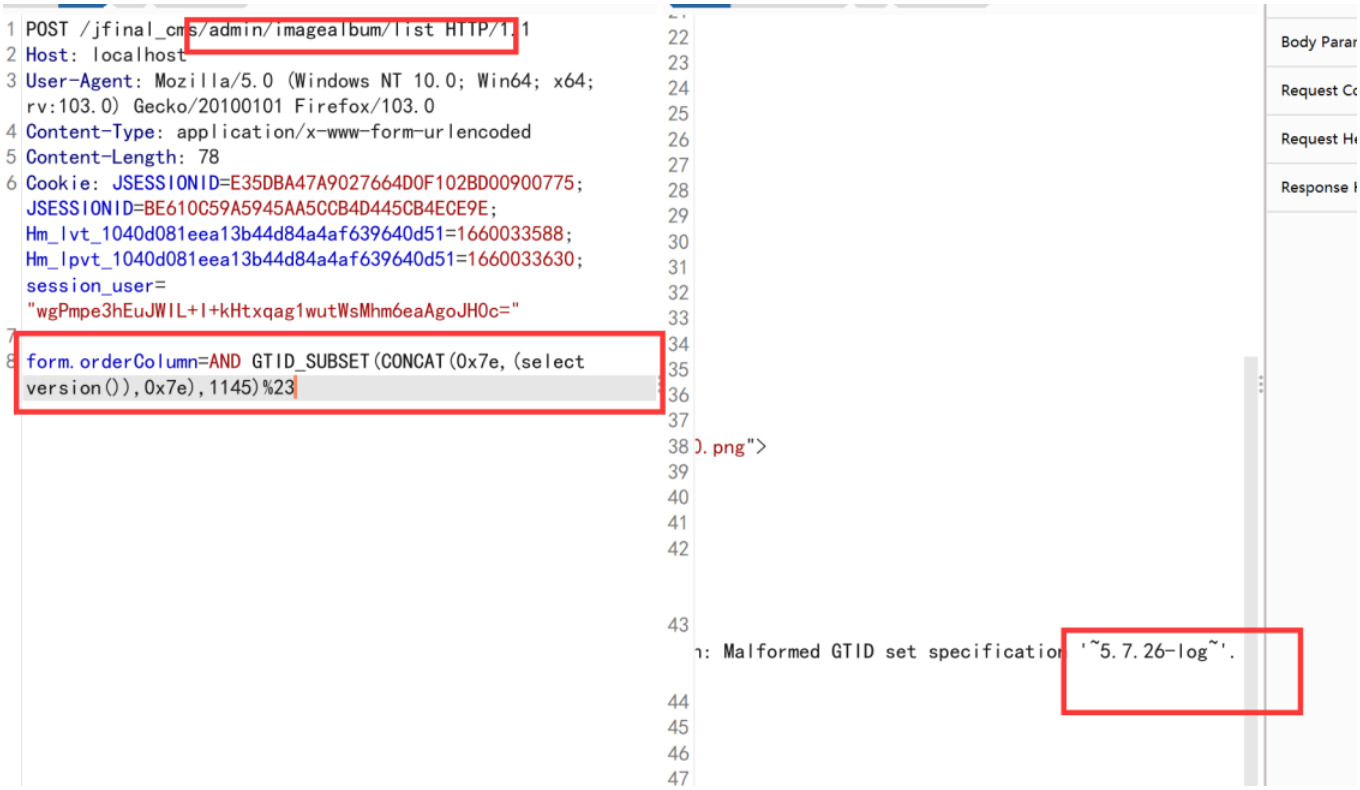
There is a SQLI vul in background mode.The route is as following

```java
@ControllerBind(controllerKey = "/admin/imagealbum")
public class ImagealbumControl... extends ...troller {

    4 usages
    private static final String path = "/pages/admin/imagealbum/imagealbum_";

    public void list() {
        TbImageAlbum model = getModelByAttr(TbImageAlbum.class);

        SQLUtils sql = new SQLUtils(" from tb_image_album t "
                + " left join tb_image_album f  on f.id = t.parent_id  where 1=1 ");
        if (model.getAttrValues().length != 0) {
            sql.setAlias("t");
            sql.whereLike( attrName: "name", model.getStr( attr: "name"));
            sql.whereEquals( attrName: "status", model.getInt( attr: "status"));
        }

        // 排序
        String orderBy = getBaseForm().getOrderBy();
        if (StrUtils.isEmpty(orderBy)) {
            sql.append(" order by t.sort,t.id desc");
        } else {
            sql.append(" order by t.").append(orderBy);
        }
```

vulnerable argument passing is as following

```
BaseForm.java  ArticleController.java
53      public boolean isShowCondition() { return showCondition; }
56
57      public void setShowCondition(boolean showCondition) { this.showCondition = showCondition;
60
61      public Paginator getPaginator() { return paginator; }
64
65      public void setPaginator(Paginator paginator) { this.paginator = paginator; }
68
69      public String getOrderBy() {
70          if (StrUtils.isEmpty(getOrderColumn())) {
71              return "";
72          }
73          return " " + getOrderColumn() + " " + getOrderAsc() + " ";
74      }
75
76      public String getOrderColumn() { return orderColumn; }
```

Successfully injected at route `admin/imagealbum/list`



admin/image/list

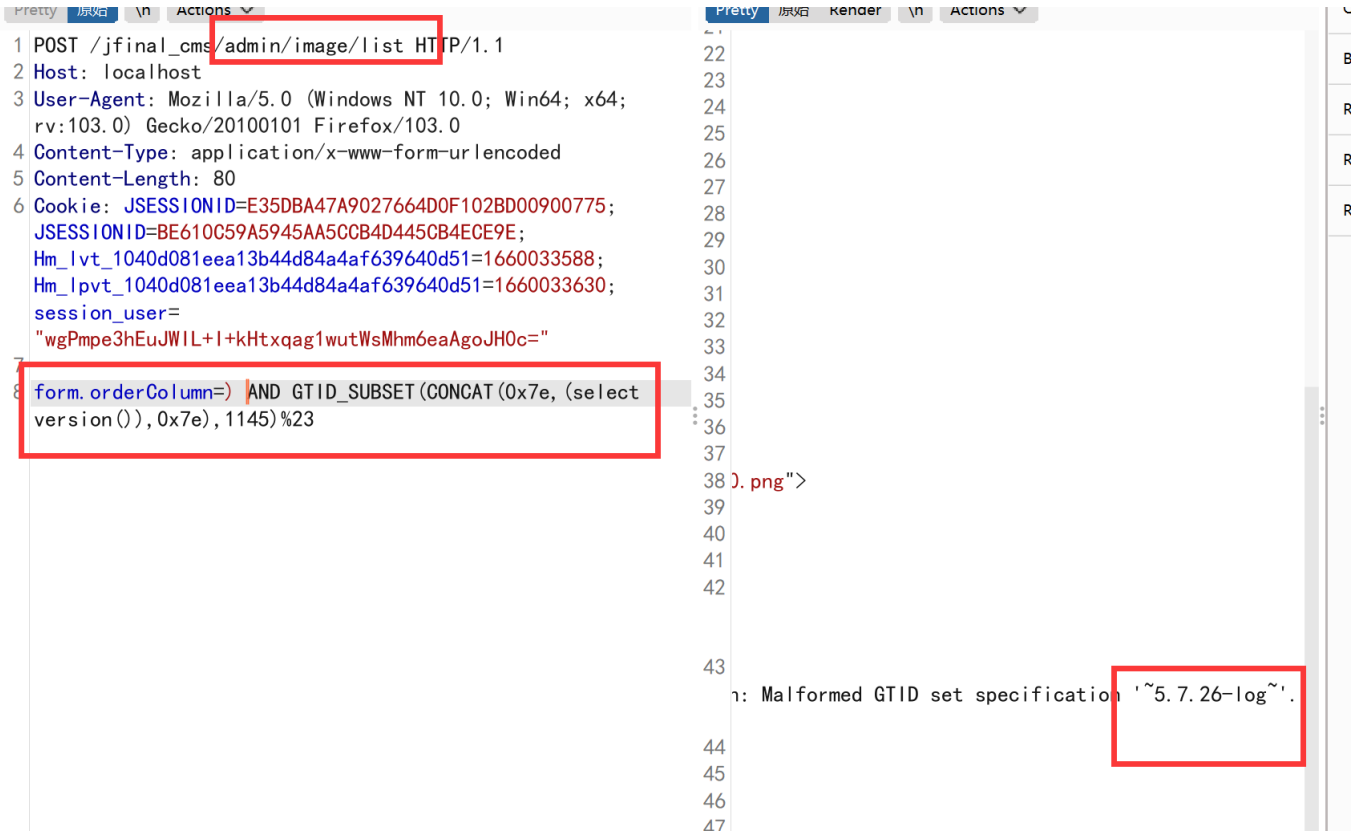
There is a SQLI vul in background mode.The route is as following

```java
@ControllerBind(controllerKey = "/admin/image")
public class ImageController extends BaseProjectController {

    4 usages
    private static final String path = "/pages/admin/image/image_";

    public void list() {
        TbImage model = getModelByAttr(TbImage.class);

        SQLUtils sql = new SQLUtils(" from tb_image t where 1=1 ");
        if (model.getAttrValues().length != 0) {
            sql.setAlias("t");
            sql.whereEquals( attrName: "album_id", model.getAlbumId());
            sql.whereLike( attrName: "name", model.getStr( attr: "name"));
            sql.whereEquals( attrName: "status", model.getInt( attr: "status"));
        }

        // 排序
        String orderBy = getBaseForm().getOrderBy();
        if (StrUtils.isEmpty(orderBy)) {
            sql.append(" order by sort,id desc");
        } else {
            sql.append(" order by ").append(orderBy);
        }
```

vulnerable argument passing is as following

```java
BaseForm.java  ArticleController.java
    public boolean isShowCondition() { return showCondition; }

    public void setShowCondition(boolean showCondition) { this.showCondition = showCondition;

    public Paginator getPaginator() { return paginator; }

    public void setPaginator(Paginator paginator) { this.paginator = paginator; }

    public String getOrderBy() {
        if (StrUtils.isEmpty(getOrderColumn())) {
            return "";
        }
        return " " + getOrderColumn() + " " + getOrderAsc() + " ";
    }

    public String getOrderColumn() { return orderColumn; }
```

Successfully injected at route `admin/image/list`



admin/site/list

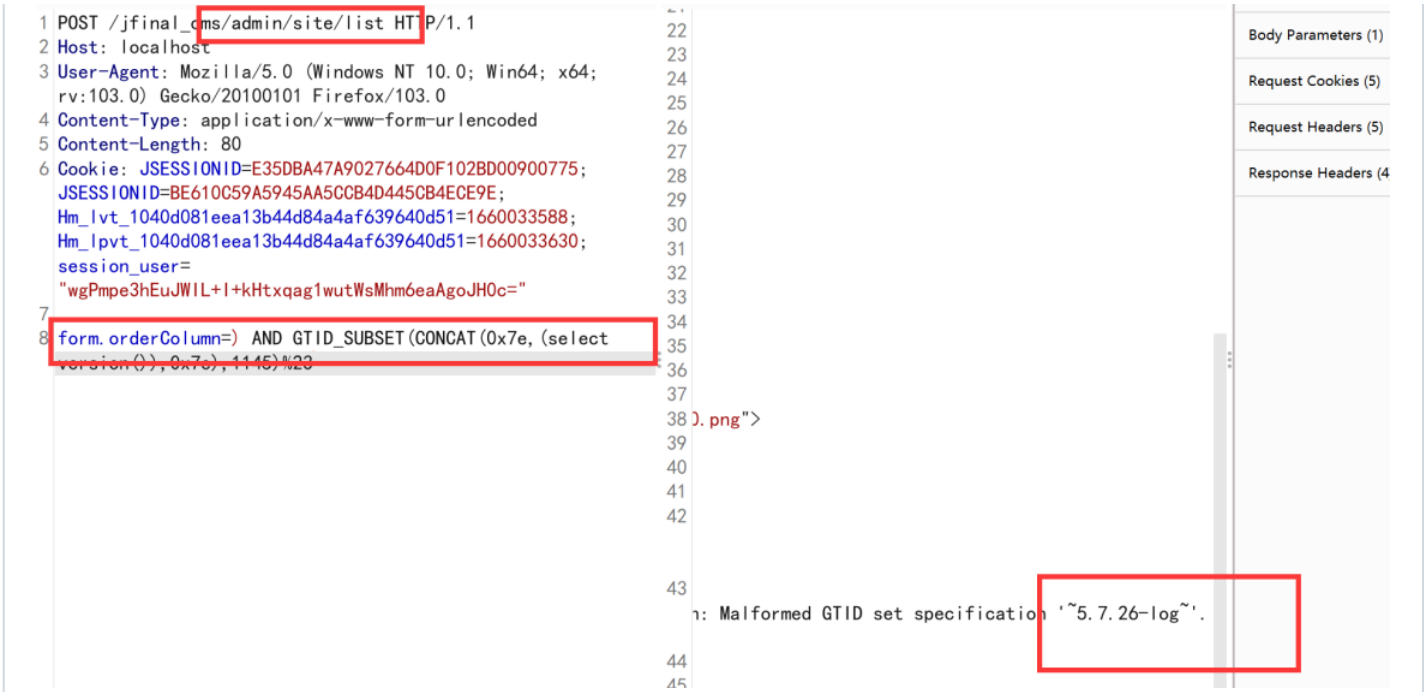
There is a SQLI vul in background mode.The route is as following

```java
@ControllerBind(controllerKey = "/admin/site")
public class SiteController extends BaseProjectController {

    4 usages
    private static final String path = "/pages/admin/site/site_";

    public void index() { list(); }

    public void list() {
        TbSite model = getModelByAttr(TbSite.class);

        SQLUtils sql = new SQLUtils(" from tb_site t where 1=1 ");
        if (model.getAttrValues().length != 0) {
            sql.setAlias("t");
            // 查询条件
            sql.whereLike( attrName: "name", model.getStr( attr: "name"));
        }
        String orderBy = getBaseForm().getOrderBy();
        if (StrUtils.isEmpty(orderBy)) {
            sql.append(" order by t.sort,t.id ");
        } else {
            sql.append(" order by ").append(orderBy);
        }

        Page<TbSite> page = TbSite.dao.paginate(getPaginator(),  select: "select t.* ", //
```

vulnerable argument passing is as following

```java
BaseForm.java  ArticleController.java
    public boolean isShowCondition() { return showCondition; }

    public void setShowCondition(boolean showCondition) { this.showCondition = showCondition;

    public Paginator getPaginator() { return paginator; }

    public void setPaginator(Paginator paginator) { this.paginator = paginator; }

    public String getOrderBy() {
        if (StrUtils.isEmpty(getOrderColumn())) {
            return "";
        }
        return " " + getOrderColumn() + " " + getOrderAsc() + " ";
    }

    public String getOrderColumn() { return orderColumn; }
```

Successfully injected at route `admin/site/list`



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant