[漏洞预警]泛微e-cology OA Beanshell组件远程代码执行分析

清水川崎 亚信安全网络攻防实验室 6天前

漏洞描述

泛微e-cology OA系统由于某些功能引用BeanShell.jar开发,但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.目前漏洞的安全补丁已由泛微官方发布,可参阅文末.

CVE编号

暂无

漏洞威胁等级

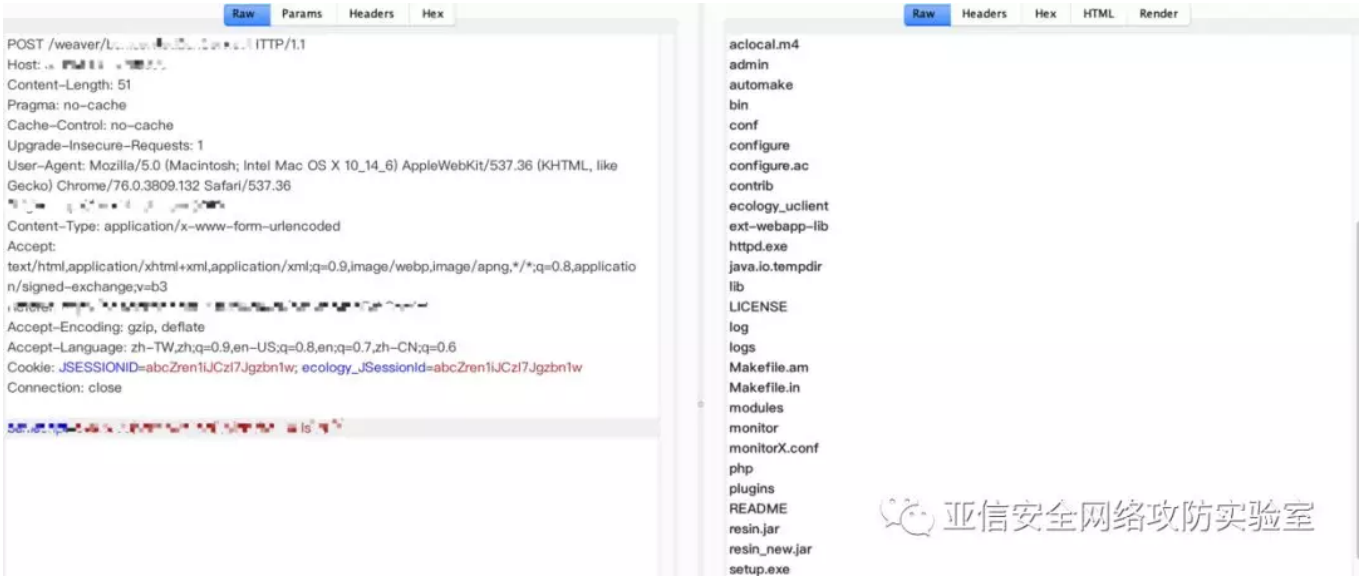
高危

影响范围

包括不限于7.0,8.0,8.1

漏洞复现

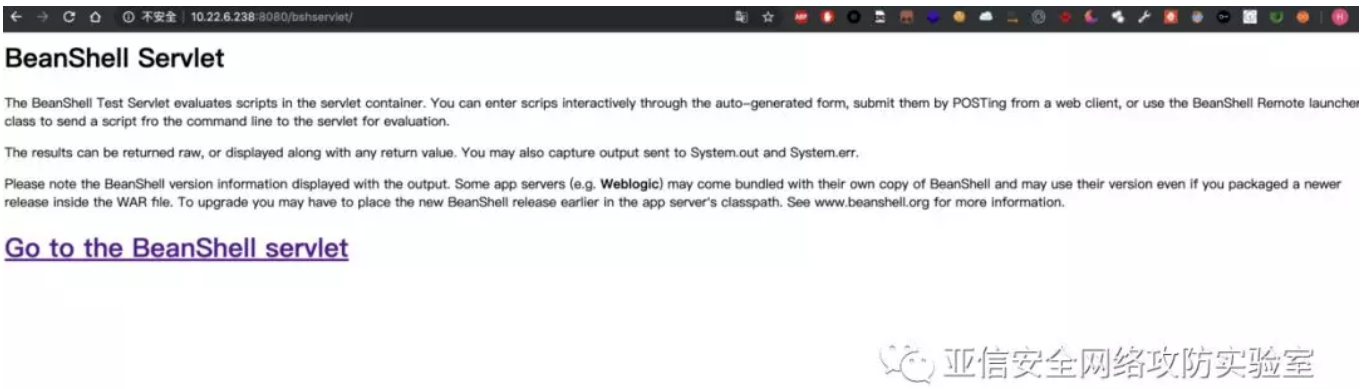
使用payload进行验证

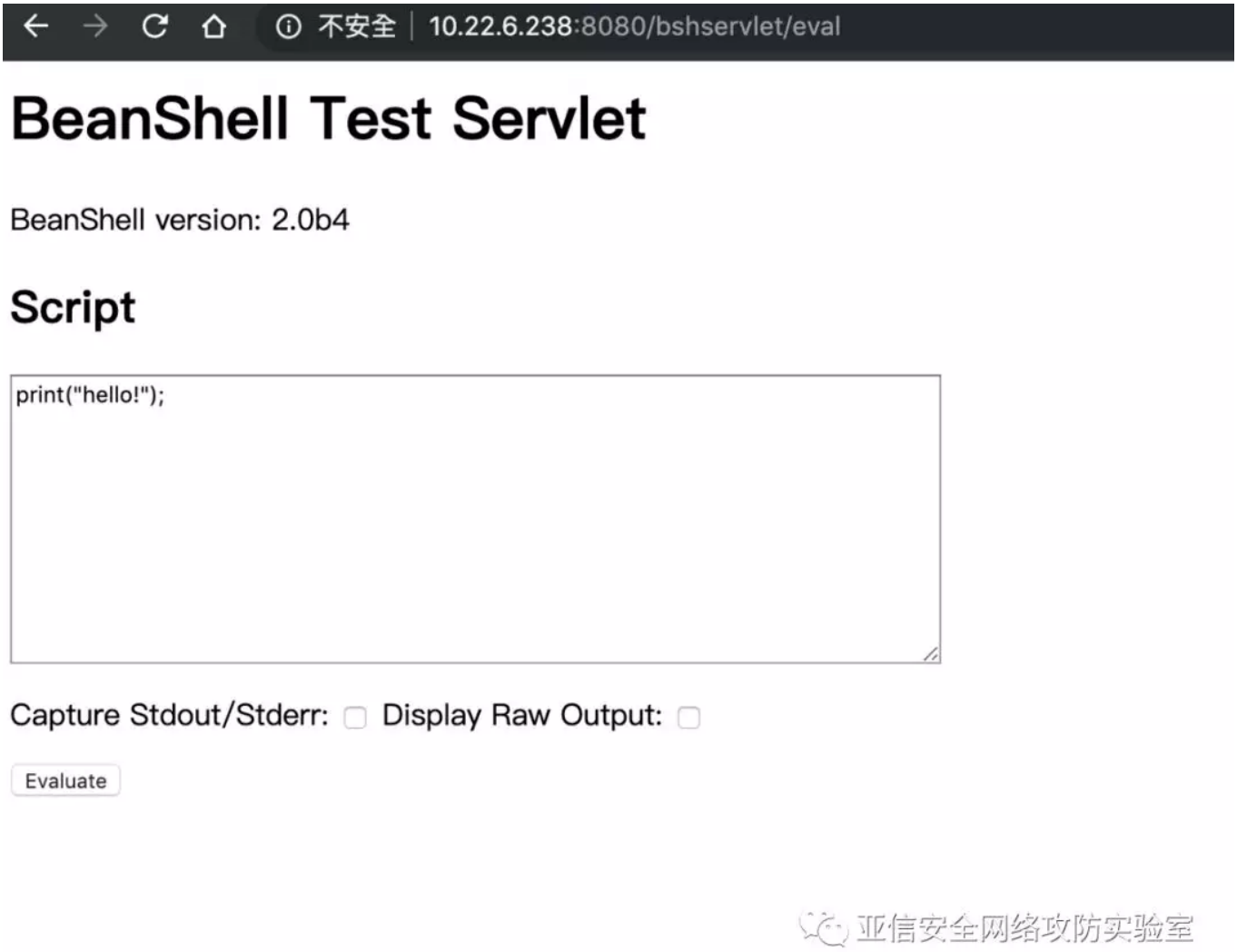


简单分析

由于此次存在漏洞的jar是Beanshell,于是我研究了一下Beanshel.

参阅官方文档,下载了war包在本地搭建





根据官方文档说明,我直接执行一个os命令,得到了回显

```
// Do a loop
for (i=0; i<5; i++)
    print(i);

// Pop up a frame with a button in it
button = new JButton( "My Button" );
frame = new JFrame( "My Frame" );
frame.getContentPane().add( button, "Center" );
frame.pack();
frame.setVisible(true);
```

Jseful BeanShell Commands

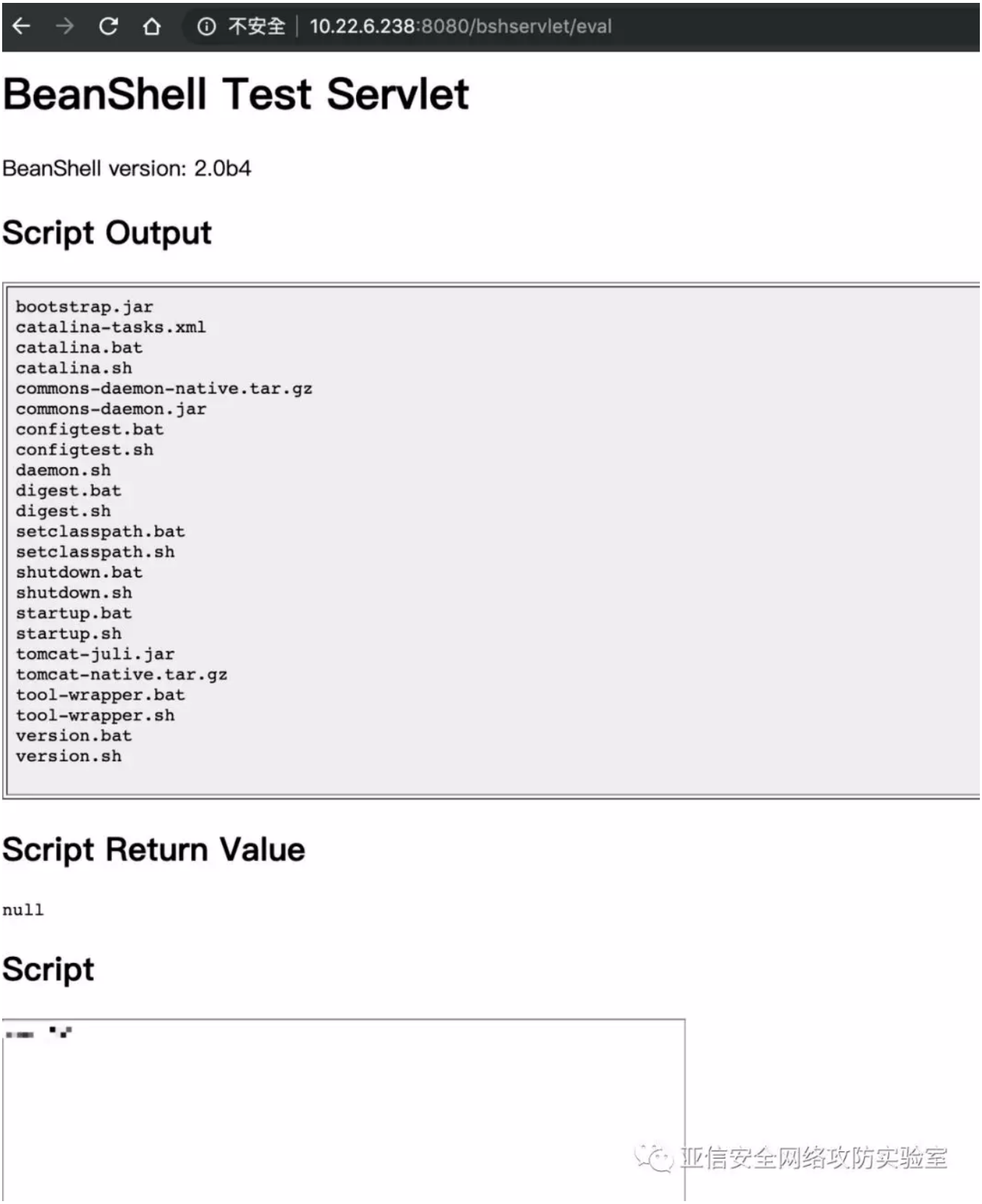
ı the previous example we used a convenient "built-in" BeanShell command called print(), to display values. print() does pretty r
ɔ the command line. print() also displays some types of objects (such as arrays) more verbosely than Java would. Another relate
ou type.

lere are a few other examples of BeanShell commands:

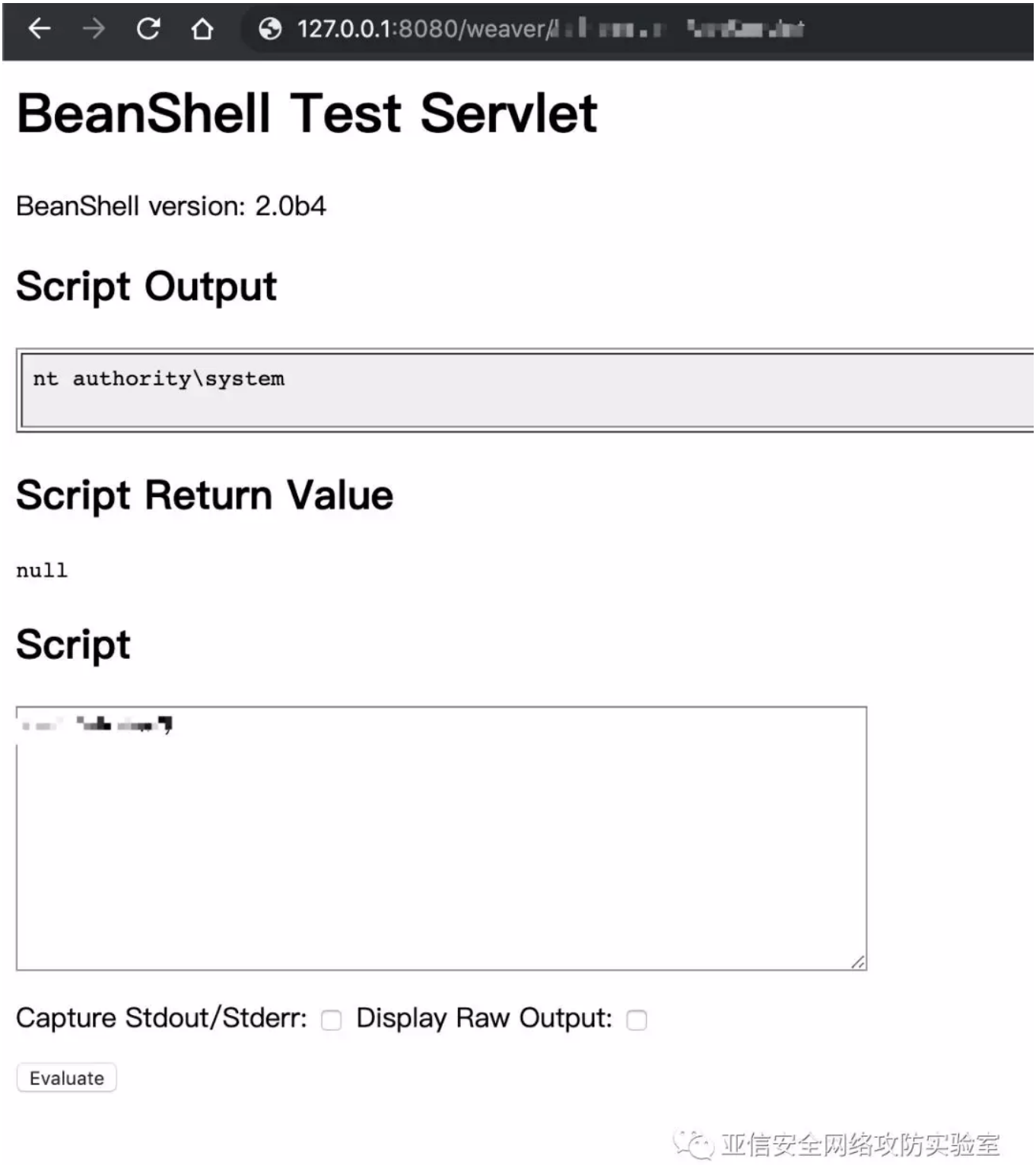
- **source(), run()** – Read a bsh script into this interpreter, or run it in a new interpreter
- **frame()** – Display a GUI component in a Frame or JFrame.
- **load(), save()** – Load or save serializable objects to a file.
- **cd(), cat(), dir(), pwd(), etc.** – Unix-like shell commands
- **exec()** – Run a native application
- **javap()** – Print the methods and fields of an object, similar to the output of the Java javap command.
- **setAccessibility()** – Turn on unrestricted access to private and protected components.

iee the complete list of BeanShell Commands for more information.

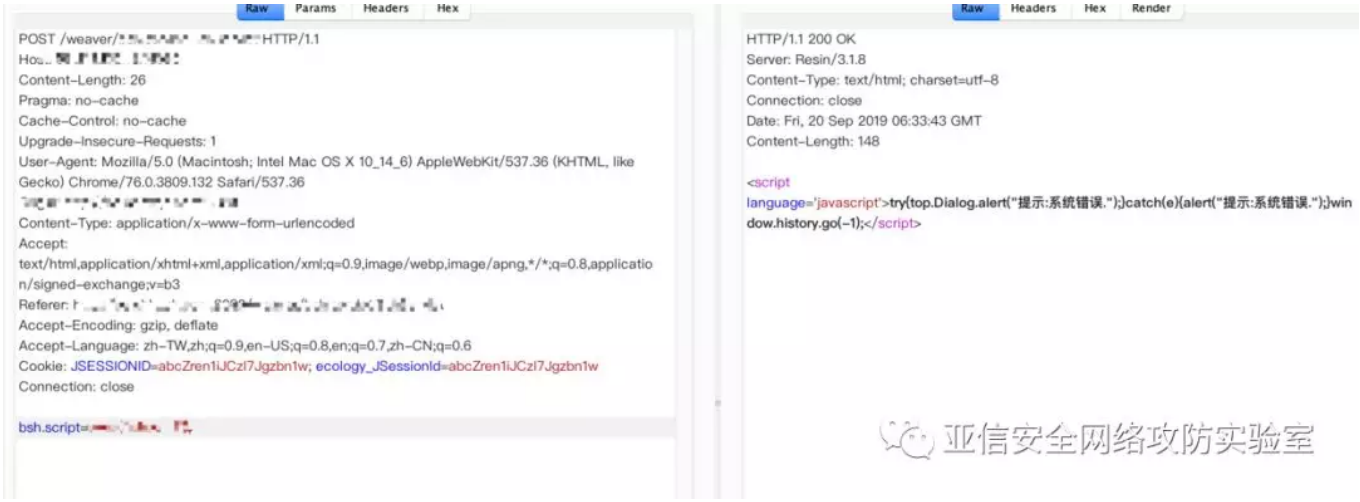
Tip:
BeanShell commands are not really "built-in" but are simply BeanShell scripts that are automatically loaded from the classpath.



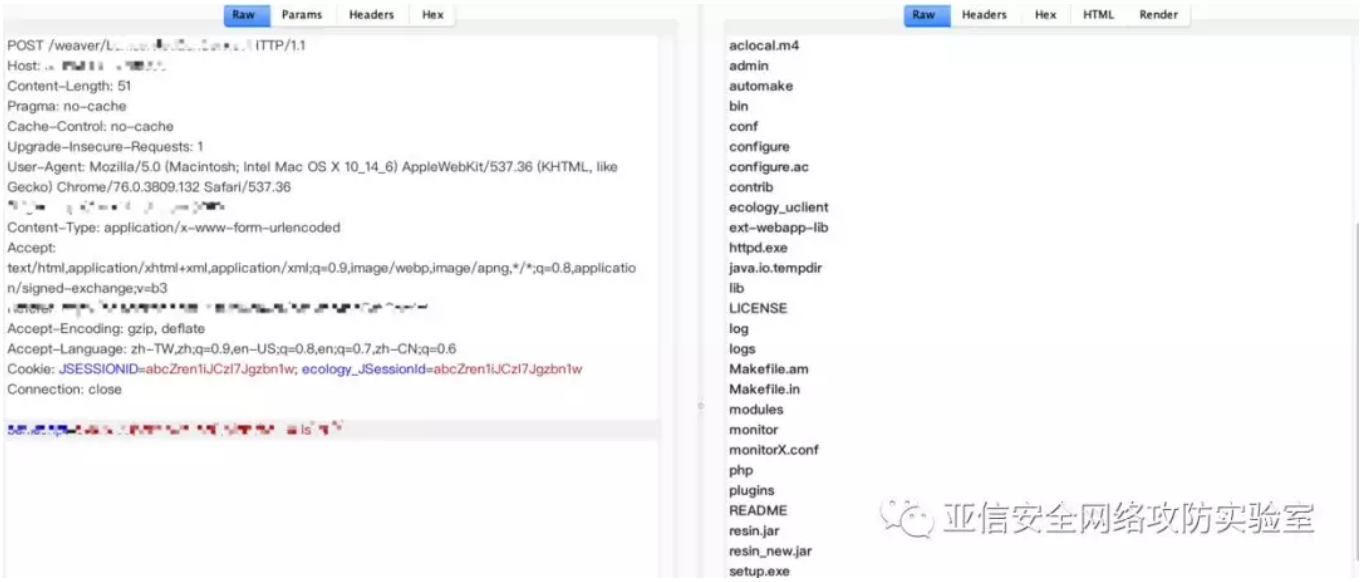
接着我到泛微e-cology OA环境下复现



发现也成功了,但部分版本未成功,因为其做了全局函数过滤,需要绕过



随后在朋友的帮助下,成功绕过了过滤



鸣谢(排名不分先后)

pyn3rd

thesoul(404)

lufei

Reference

Beanshell官方指南:

https://beanshell.github.io/

补丁包下载:

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