shiro认证绕过

> CVE-2010-3863

环境准备

```
[root@localhost CVE-2010-3863]# HTTP_PROXY=http://192.168.47.240:7890 HTTPS_PROXY=http://192.168.47.240:7890 docker-compose up -d
WARN[0000] /root/vulhub/shiro/CVE-2010-3863/docker-compose.yml: `version` is obsolete
[+] Running 9/9
 ✓ web Pulled                                                                                                    19.0s
   ✓ 43c265008fae Pull complete                                                                                   9.1s
   ✓ af36d2c7a148 Pull complete                                                                                   9.8s
   ✓ 2b7b4d10e1c1 Pull complete                                                                                   9.9s
   ✓ f264389d8f2f Pull complete                                                                                   9.9s
   ✓ 1a2c46e93f4a Pull complete                                                                                  10.0s
   ✓ f9506bb322c0 Pull complete                                                                                  13.8s
   ✓ 96f5dad14c2c Pull complete                                                                                  13.9s
   ✓ 6e9d37cb5543 Pull complete                                                                                  14.2s
[+] Running 2/2
 ✓ Network cve-2010-3863_default  Created                                                                         0.4s
 ✓ Container cve-2010-3863-web-1  Started                                                                         2.2s
```

攻击

- 构造恶意请求绕过登录认证

漏洞原理

- shiro是一个强大易于使用的`java`安全框架,提供了`认证,授权,加密,会话管理`等
- `Apache Shiro 1.1.0`以前的版本,shiro进行权限认证前未对url做`标准化`处理,攻击者可以利用`/`,`//`,`/./`,`/…/`绕过权限验证

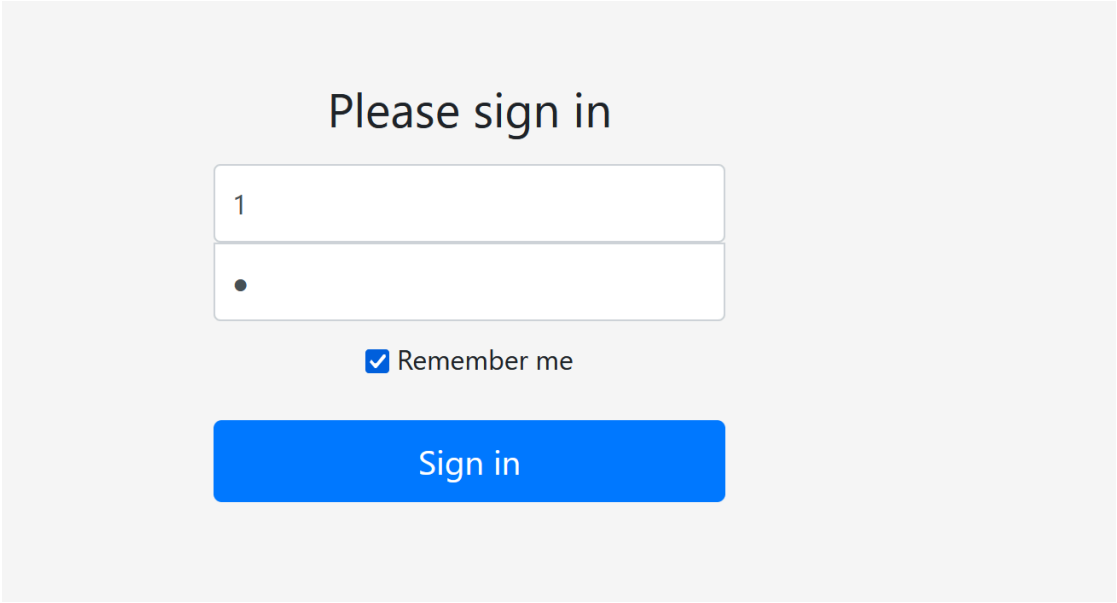
shiro550反序列化

> CVE-2016-4437

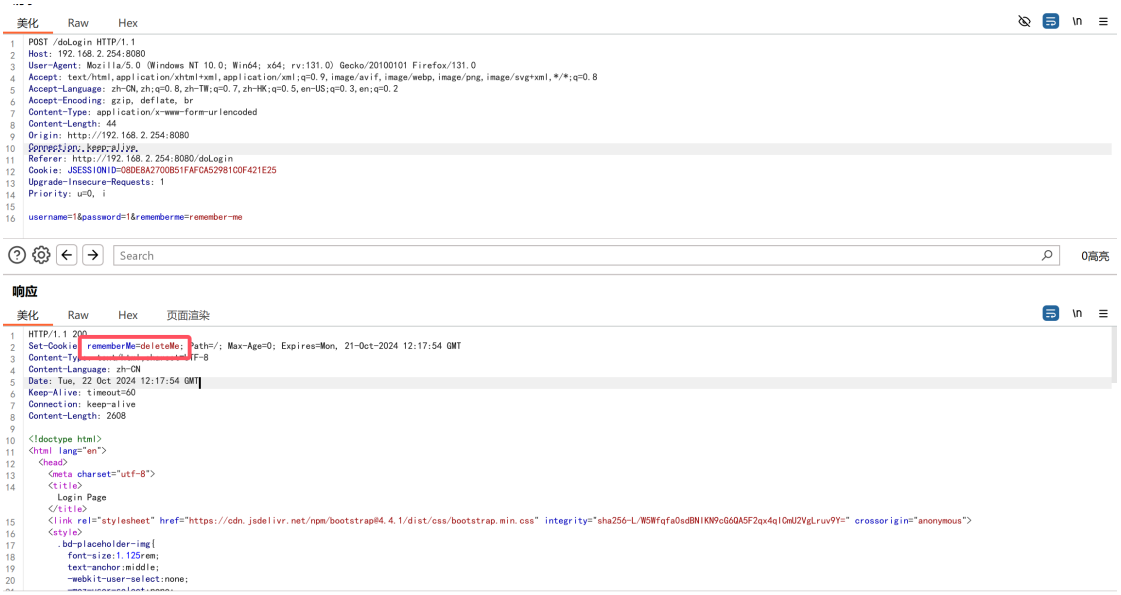
环境准备

开始攻击

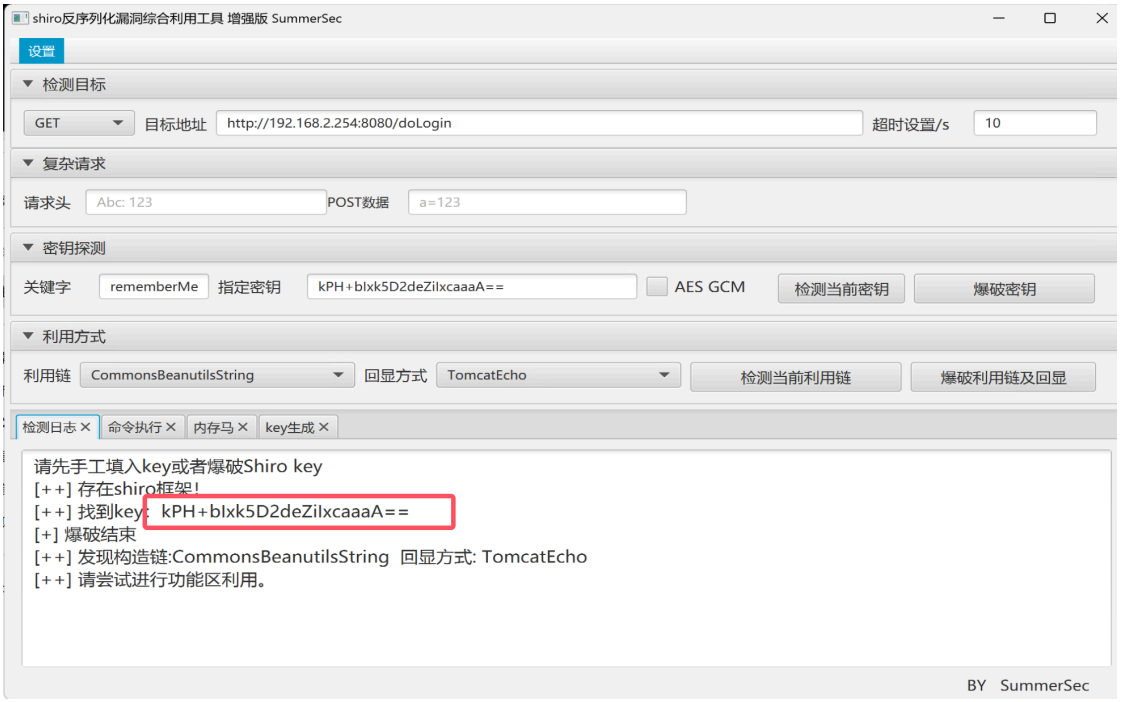
- 输入任意账号密码,勾选`记住密码`,bp抓包查看



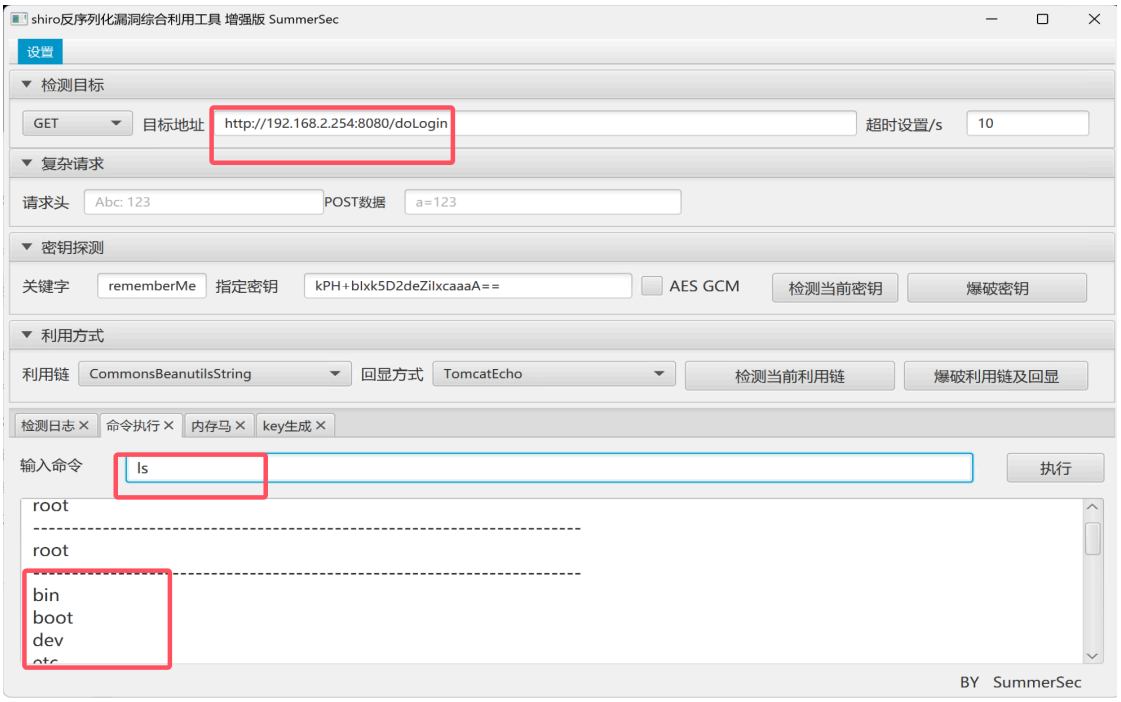
- 发现数据包里有`rememberme=deleteme`的字段,说明使用了shiro框架,存在反序列化漏洞



- 打开shiro反序列化攻击jar



- 利用漏洞



漏洞原理

- `shiro`框架提供了`记住密码`的功能,用户登录成功后会将用户信息进行加密
- 加密过程:`序列化→AES加密→base64编码→remember cookie`
- 如果用户勾选了`记住密码`,那么请求中会`携带cookie`,并且将加密信息存放在cookie的`rememberme`字段里,在服务段收到`rememberme`值先`base64解码`然后再`AES`解密然后`反序列化`,这个过程中如果我们知道AES加密的`密钥`,把用户信息替换成恶意命令就造成了`反序列化远程命令执行漏洞`
- 在`shiro ≤ 1.2.4`版本中使用默认密钥更容易触发

shiro认证绕过

> CVE-2020-1957

环境搭建

攻击手法同上

- 构造恶意请求绕过登录认证

```
1    http://192.168.2.254:8080/xxx/..;/admin/
```