

# shiro认证绕过

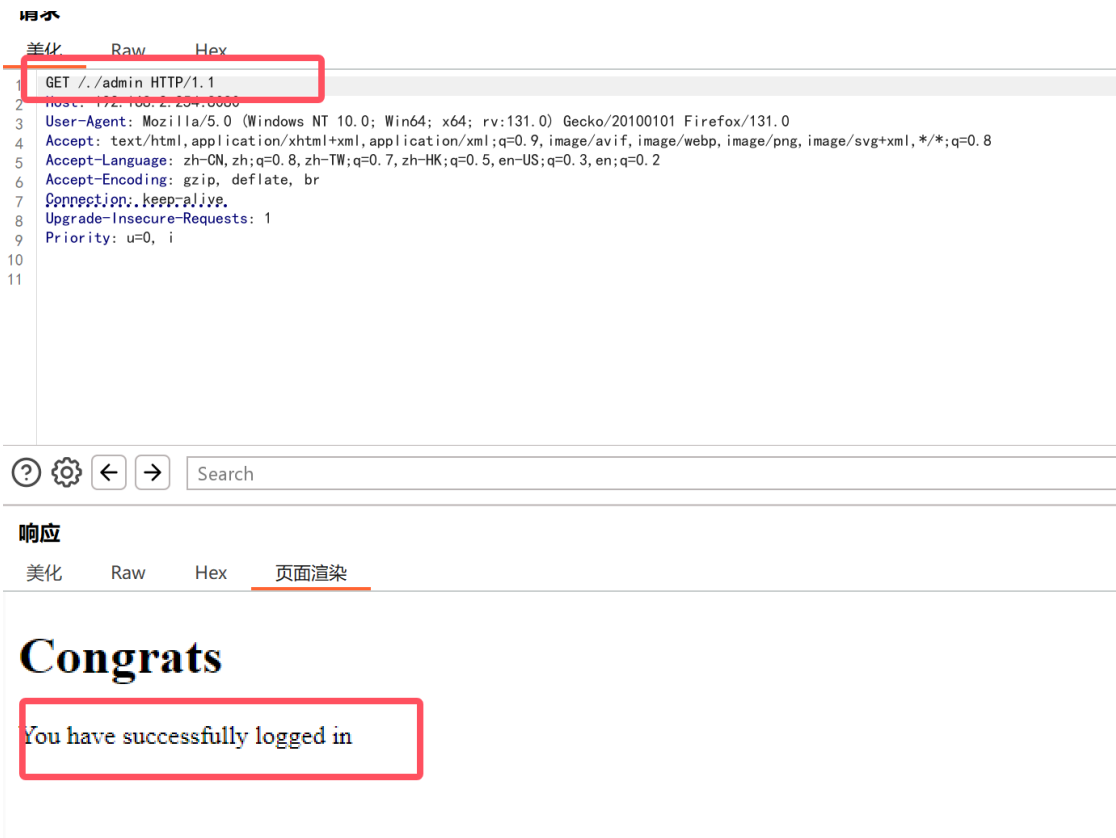
CVE-2010-3863

## 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WARN[0000] /root/.vulhub/shiro/CVE-2010-3863/docker-compose.yml: `version` is obsolete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

```
[root@localhost CVE-2016-4437]# 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WARN[0000] /root/.vulhub/shiro/CVE-2016-4437/docker-compose.yml: 'version' is obsolete
[+] Running 9/9
✔ web Pulled 353.0s
  ✔ 43c265008fae Pull complete 178.4s
  ✔ af36d2c7a148 Pull complete 178.9s
  ✔ 2b7b4d10e1c1 Pull complete 179.0s
  ✔ f264389d8f2f Pull complete 179.1s
  ✔ 1a2c46e93f4a Pull complete 179.2s
  ✔ f9506bb322c0 Pull complete 342.6s
  ✔ 96f5dad14c2c Pull complete 342.7s
  ✔ b6ea9c6684a0 Pull complete 343.0s
[+] Running 2/2
✔ Network cve-2016-4437_default Created 0.2s
✔ Container cve-2016-4437-web-1 Started 1.0s
[root@localhost CVE-2016-4437]#
```

## 开始攻击

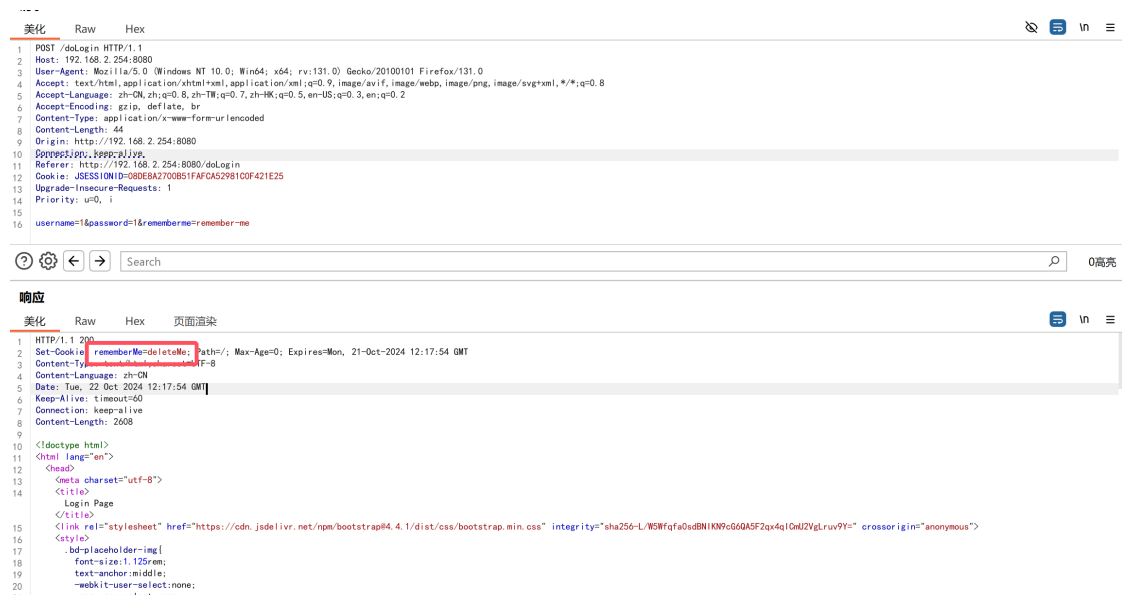
- 输入任意账号密码,勾选 **记住密码**,bp抓包查看

Please sign in

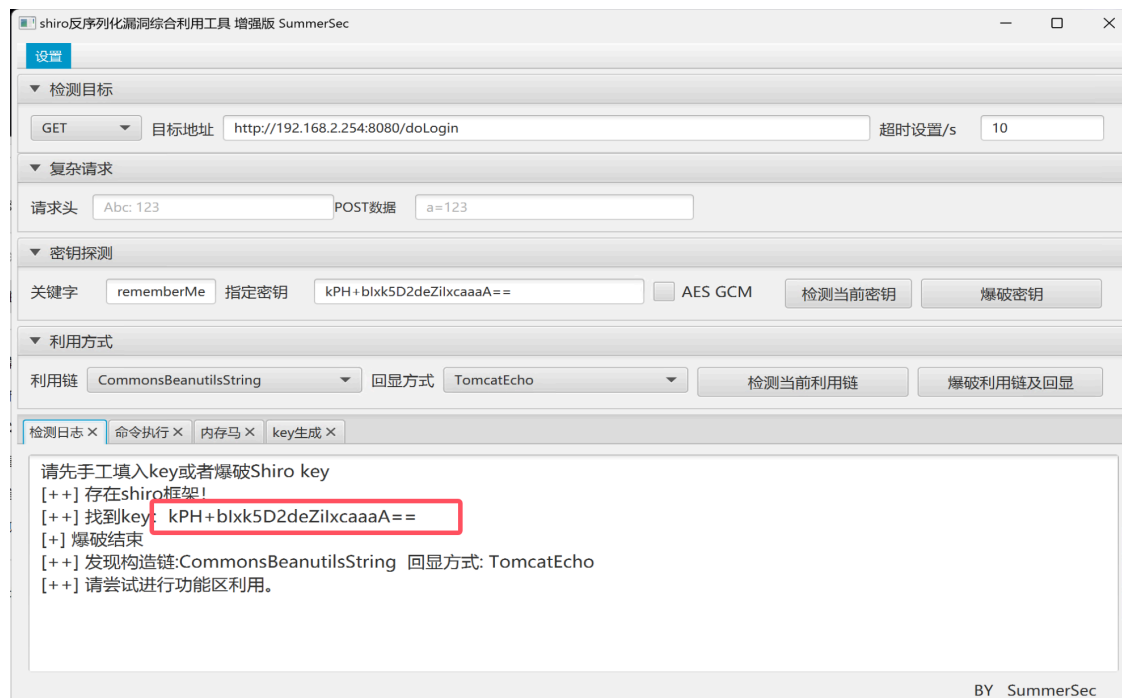
☒ Remember me

Sign in

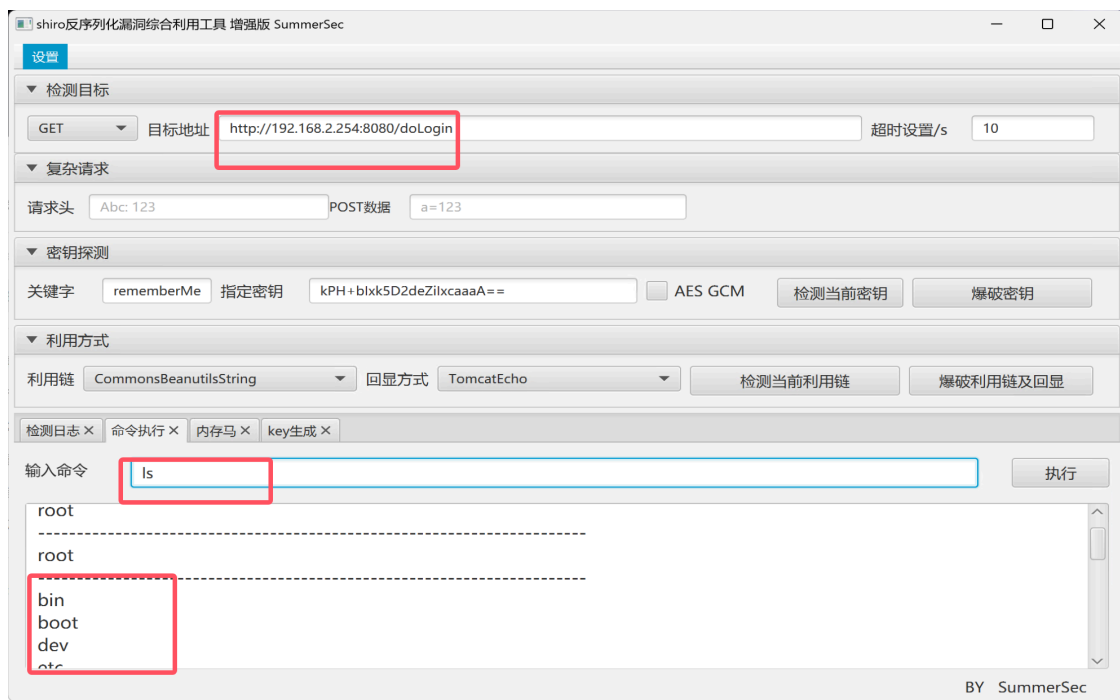
- 发现数据包里有 **rememberme=deleteme** 的字段,说明使用了shiro框架,存在反序列化漏洞



- 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, 在服务端收到 remeberme 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

```
[root@localhost CVE-2020-1957]# 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-2020-1957/docker-compose.yml: 'version' is obsolete
[+] Running 8/8
  ✓ web Pulled                                107.8s
  ✓ b9a857cbf04d Pull complete                 8.3s
  ✓ d557ee20540b Pull complete                 8.7s
  ✓ 3b9ca4f00c2e Pull complete                94.4s
  ✓ 6cee913589ff Pull complete                94.7s
  ✓ 4ce6106adeF3 Pull complete                94.8s
  ✓ 5065f34649a3 Pull complete                96.5s
  ✓ 7977e39076fa Pull complete                96.9s
[+] Running 2/2
  ✓ Network cve-2020-1957_default Created      0.3s
  ✓ Container cve-2020-1957-web-1 Started     1.1s
[root@localhost CVE-2020-1957]#
```

## 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/
```

