

Web

Cosmos的博客后台

后台登陆

用户名		
密码		

Submit

看到登录界面,一开始想到的就是sql注入,但是一直写不出,直到后来学长给了hint,才知道这题是本地文件包含漏洞......百度了一堆资料,知道了php://filter可以通过post来执行指定的php代码,一开始一直以为要从username和password传,后来发现原来可以直接通过action来传递(QAQ

二、php://filter

php://filter可以获取指定文件源码。当它与包含函数结合时,php://filter流会被当作php文件执行。所以我们一般对其进行编码,让其不执行。从而导致任意文件读取。

POC1:

?file=php://filter/resource=xxx.php

POC2:

?file=php://filter/read=convert.base64-encode/resource=xxx.php

POC1直接读取xxx.php文件,但大多数时候很多信息无法直接显示在浏览器页面上,所以需要采取POC2中方法将文件内容进行base64编码后显示在浏览器上,再自行解码。

第一步,构造php语句,读取login.php和admin.php的内容

InLnBocCI7CnNlc3Npb25fc3RhcnQoKTsKCi8vT25seSBmb3IqZGVidWcKaWYqKERFQIVHX01PREUpewoqICAqaWYoaXNzZXQoJF9I

base64解码后得到login.php的内容,考察代码审计

分析: 我们需要达成以下条件登录, 而admin password和admin username可以通过GET传入 DEBUG_MODE中的debug变量,匹配了正则表达式后,由eval("var_dump(\$\$debug);输出

```
if ($admin_password == md5($_POST['password']) && $_POST['username'] ===
    $admin_username)
                                                                                                                                                      HTTP/1.1 200 OK
GET /login.php?debug=admin_username HTTP/1.1
                                                                                                                                                       Server: nginx/1.14.0 (Ubuntu)
Host: cosmos-admin.hgame.day-day.work
                                                                                                                                                      Date: Wed, 29 Jan 2020 07:30:48 GMT
Content-Type: text/html; charset=UTF-8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:72.0) Gecko/20100101
Firefox/72.0
Accept: text/html, application/xhtml+xml, application/xml; q=0.9, image/webp, */*; q=0.8
                                                                                                                                                      Content-Length: 1190
Accept-Language: zh-CN, zh;q=0.8, zh-TW;q=0.7, zh-HK;q=0.5, en-US;q=0.3, en;q=0.2 Accept-Encoding: gzip, deflate
                                                                                                                                                      Connection: close
                                                                                                                                                      Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-reval
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
Origin: http://cosmos-admin.hgame.day-day.work
                                                                                                                                                       Pragma: no-cache
                                                                                                                                                      Vary: Accept-Encoding
Connection: close
Referer: http://cosmos-admin.hgame.day-day.work/?action=login.php
Cookie: PHPSESSID=st2a5gtnakrgps1roo8f5vj6rv
                                                                                                                                                      string(7) "Cosmos!
Upgrade-Insecure-Requests: 1
                                                                                                                                                       <! DOCTYPE html
                                                                                                                                                       <html lang="zh-CN">
                                                                                                                                                      <head>
GET /login.php?debug=admin_password HTTP/1.1
Host: cosmos-admin.hgame.day-day.work
                                                                                                                                    HTTP/1.1 200 OK
                                                                                                                                              nginx/1,14,0 (Ubuntu)
Host: cosmos-admin.hgame.day-day.work User-Agent: Mozilla/5.0 (Windows NT 10.0: Win64; x64; rv:72.0) Gecko/20100101 Firefox/72.0 Accept: text/html, application/xhtml+xml, application/xml;q=0.9, image/webp, */*:q=0.8 Accept-Language: zh-CN, zh;q=0.8, zh-TW;q=0.7, zh-HK;q=0.5, en-US;q=0.3, en;q=0.2 Accept-Encoding: gzip, deflate
                                                                                                                                    Server: nginx/1.14.0 (Dbuntu)
Date: Wed, 29 Jan 2020 07:32:09 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 1216
                                                                                                                                    Connection: close
                                                                                                                                    Expires: Thu, 19 Nov 1981 08:52:00 GMT
                                                                                                                                    Cache-Control: no-store, no-cache,
Pragma: no-cache
Vary: Accept-Encoding
                                                                                                                                                                                    must-revalidate
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
```

得到管理员的用户名和密码,密码是0e开头的md5值,刚好查资料的时候看到过(XD,考察的是Hase漏

string(32) "0e114902927253523756713132279690"

<!DOCTYPE html>

漏洞描述

Connection: close

Origin: http://cosmos-admin.hgame.day-day.work

Referer: http://cosmos-admin.hgame.day-day.work/?action=login.php Cookie: PHPSBSSID=st2a5gtnakrgps1roo8f5vj6rv Upgrade-Insecure-Requests: 1

PHP在处理哈希字符串时,会利用"!="或"=="来对哈希值进行比较,它把每一个以"OE"开头的哈希值都解释为O,所以如果两个 不同的密码经过哈希以后, 其哈希值都是以"OE"开头的, 那么PHP将会认为他们相同, 都是O。

攻击者可以利用这一漏洞,通过输入一个经过哈希后以"OE"开头的字符串,即会被PHP解释为O,如果数据库中存在这种哈希值以" OE" 开头的密码的话, 他就可以以这个用户的身份登录进去, 尽管并没有真正的密码。

即:如果md的值是以0e开头的,那么就与其他的0e开头的Md5值是相等的。

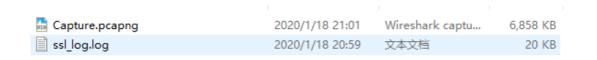
关于解决这个漏洞可参考 http://www.freebuf.com/news/67007.html

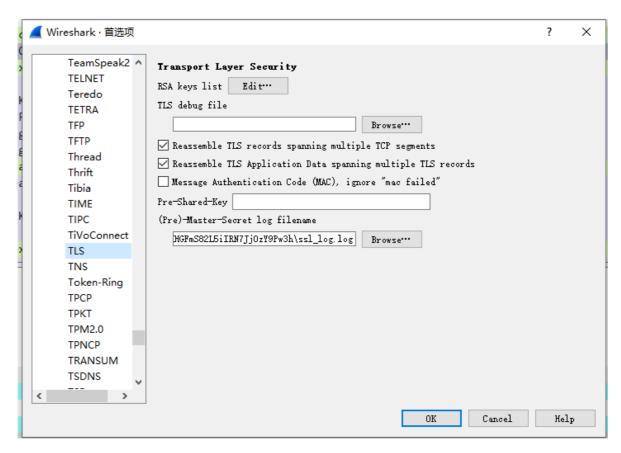
登录后发现可以插入图片url, 考察了SSRF, 题目提示flag在根目录, 通过未过滤的url, 利用file: //得 到flag,这一步一开始我还以为是错的,因为图片无法显示.....结果后面发现源码里给了一串base64, 解密后就是flag



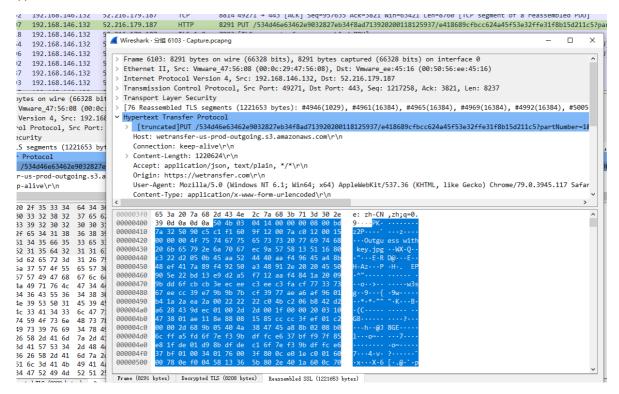
misc

Cosmos的午餐





Firefox和Chrome浏览器都支持用日记文件的方式记录下用来加密TLS数据包对称会话秘钥,导入日志文件



发现一个带有压缩包和jpg的流量包,导出用foremost分离





Outguess with key.jpg

分级 ☆☆☆☆☆ 标记

Key: gUNrbbdR9XhRBDGpzz

来源

备注

作者

拍摄日期

程序名称

得到一个压缩包解压出来一张图片,这里一开始我还以为是从key中找flag,后来发现outguess其实是一种图片隐写的方法,用outguess解密后得到一个txt,里面是一个地址,打开后下载了一个压缩包

root@ubuntu:/home/r4inyni9ht/outguess# outguess -k "gUNrbbdR9XhRBDGpzz" -r '/home/r4inyni9ht/Desktop/Outguess with key.jpg' hidden.txt
Reading /home/r4inyni9ht/Desktop/Outguess with key.jpg....
Extracting usable bits: 1161827 bits
Steg retrieve: seed: 3, len: 24

打开是一个二维码



扫码得到flag, (我还以为还要再来一个二维码的考点XD

所见即为假

output	2020/1/23 21:38	文件夹	
AllFake_XK2ipRXBI3Usi17r57EmawrO	2020/1/23 20:07	ZIP 压缩文件	1,040 KB
FLAG_IN_PICTURE.jpg	2020/1/20 15:28	JPG 文件	1,043 KB
■ foremost.exe	2019/11/24 11:06	应用程序	88 KB

```
PS D:\too1\stegdetect0.4>.\stegdetect.exe -tjopi -s 10.0 1.jpg
Corrupt JPEG data: 69 extraneous bytes before marker 0xd9
1.jpg: negative
PS D:\too1\stegdetect0.4>
```

```
Nicrosoft Windows [MX4、10.0.17763,973]
(c) 2018 Microsoft Corporation。保留所有权利。

C:\Users\HQL>d:

D:\>cd D:\tool\F5-steganography-master

D:\tool\F5-steganography-master>java Extract C:\Users\HQL\Desktop\HGAME2020\WEEK2\MISC2\FLAG_IN_PICTURE.jpg -p N11D7CQon6dBsFLr
Huffman decoding starts

Permutation starts
10911744 indices shuffled
Extraction starts
Length of embedded file: 222 bytes
(1, 127, 7) code used
```

地球上最后的夜晚

解压得到一个加密的压缩包和一个PDF,百度搜PDF隐写,找到了一个工具wbStego4open,从PDF中导出了压缩包密码,解压后得到一个doc,先拖进winhex分析一下

```
21 23 60 00 00 71 00 04
                                     DE 17 EU DI DE UD EU IU
                                                               / HUOM | O/4 U I JUO
00000190
          B3 FF D1 AF 6D 0E 91 BC
                                     BE 57 27 3F 50 4B 03 04
                                                               ³ÿÑ m 14¾W'?PK
000001A0
          14 00 00 00
                      00 00 87 4E
                                     E2 40 00 00 00 00 00 00
                                                                     INâ@
                                00
000001B0
          00 00 00 00
                      00 00 06
                                     00 00 5F
                                              72 65 6C 73 2F
                                                                          _rels/
          50 4B 03 04 14 00 00 00
                                     08 00 87 4E E2 40 01 22
                                                                          INâ@ "
00000100
                                                               PK
                                                               пý
00000100
          22 1F FD OO
                      00 00 E1 02
                                     00 00 0B 00 00 00 5F 72
                                                               els/.rels-'ÝJ 1
000001E0
          65 6C
                73 2F
                       2E 72 65
                                6C
                                     73 AD 92 DD 4A 03 31 10
                      21 CC
                                37
                                                               ∎ï ß!Ì}7Û*"ÒloDè
000001F0
          85 EF 05 DF
                             7D
                                     DB 2A 22 D2 6C
                                                    6F 44 E8
                                                                H}∥!∥Ý Ýü Lμ}{∥
                       21 99 DD OD
                                     DD FC 90 4C B5
                                                    7D 7B 83
00000200
          9D 48 7D 80
00000210
          7F B8 B0 AE
                      BD F0 72
                                32
                                     67 CE 7C 73 C8 7A 73 74
                                                                ∵°®%őr2gÎ|sÈzst
00000220
          83 78 A1 94 6D FO OA 96
                                     55 OD 82 BC OE C6 FA 4E
                                                               IxiImő IU I¼ ÆúN
00000230
          C1 F3 EE 61 71 OB 22 33
                                     7A 83 43 FO A4 EO 44 19
                                                               Áóîaq "3z∎Cð¤àD
00000240
          36 CD E5 C5 FA 89 06 E4
                                     32 94 7B 1B B3 28 2E
                                                               6ꌁú∥ ä2∥{ ³(.>
00000250
          2B E8 99 E3 9D 94 59 F7
                                     E4 30 57 21 92 2F 9D 36
                                                               +è[ã [Y÷ä0W!'/ 6
00000260
          24 87 5C CA D4 C9 88 7A
                                     8F 1D C9 55 5D DF C8 F4
                                                               $∥∖ÊÔÉ∥z ÉU]ßÈô
00000270
          D3 O3 9A 91 A7 D8
                             1A 05
                                     69 6B AE 41 EC 4E B1 6C
                                                               Ó ľ′SØ ik®AìN±l
00000280
          FE DB 3B B4 AD D5 74 1F
                                     F4 C1 91 E7 89 15 72 AC
                                                               þÛ;′-Õt ôÁʻç∥ r¬
                                                               (\hat{I} \cdot b)^{-1} = i \times (I \cdot r)
00000290
          28 CE 98 3A 62 05 AF 21
                                     19 69 3E 07 AB 82 0C 72
000002A0
          9A 66 75 3E CD EF 97 4A
                                     47 8C 06 19 A5 0E 89 16
                                                               |fu>İï|JG| ¥ |
000002B0
          31 95 9C 12 DB 92 EC
                                37
                                     50 61 79 2C CF F9 5D
                                                           31
                                                               1|| Û'ì7Pay,Ïù]1
000002C0
          07 B4 3C
                   1F
                          7C FC
                                54
                                     3C
                                       74 64 F2 86 CC
                                                                ′< h|üT<tdò∥Ì<
                      68
                                                       3C
                                                           12
000002D0
          C6 38 47
                    74 F5 9F 44 FA
                                     90 39 B8 79 9E OF CD
                                                           17
                                                               Æ8Gtõ∥Dú 9,y∥ Í
                                     03 04 14 00 00 00 00
000002E0
          92 1C 7D CC E6 0D 50
                                4B
                                                           00
                                                               ′}Ìæ PK
000002F0
          87 4E E2 40 00 00 00 00
                                     00 00 00 00 00 00 00 00
                                                               INâ@
          OA 00 00 00 63 75 73 74
                                     6F 6D 58 6D 6C 2F 50 4B
00000300
                                                                   customXml/PK
                                     87 4E E2 40 00 00 00
00000310
          03 04 14 00
                      00 00 00
                                nn
                                                                        INA@
                                     10 00 00 00 63 75 73 74
00000320
          nn nn nn nn nn nn
                             nn
                                nn
                                                                            cust
                                72
                                     65 6C 73 2F 50 4B 03 04
00000330
          6F 6D 58 6D 6C
                          2F
                             5F
                                                               omXml/_rels/PK
         | 14 00 00 00 08 00 87 4E
                                    E2 40 74 3F 39 7A BC 00
00000340
                                                                     ∥Nâ@t?9z¼
```

发现多个504B,应该是ZIP文档,把后缀改成zip,解压,翻文件夹,发现一个secret.xml,找到flag

```
<?xml version="1.0" encoding="UTF-8" standalone="true"?>
<flag>hgame{mkLbn8hP2g!p9ezPHqHuBu66SeDA13u1}</flag>
```