

接头霸王



You need to come from <https://vidar.club/>.

© HGAME 2020

打开。点击链接，没毛病

再看源码，没有问题。

抓包，结合hint，应该是要添加访问来源referer

Burp Suite Community Edition v2.1.07 - Temporary Project

DashboardTargetProxyIntruderRepeaterSequencerDecoderComparerExtenderProject optionsUser options

5 × 6 × 7 × 8 × 9 × 10 × 11 × 12 × 13 × 15 × 17 × 18 × ...

SendCancel<>

Request

RawHeadersHex

GET / HTTP/1.1
Host: kyaruhgame.n3ko.co
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
Referer: https://vidar.club/
Connection: close
Upgrade-Insecure-Requests: 1

Response

RawHeadersHexHTMLRender

<meta name="viewport" content="width=device-width, initial-scale=1">
<title> </title>
<!-- Bootstrap core CSS -->
<link href="/static/css/bootstrap.min.css" rel="stylesheet">
<!-- Custom styles for this template -->
<link href="/static/css/jumbotron-narrow.css" rel="stylesheet">
<!-- HTML5 shim and Respond.js for IE8 support of HTML5 elements and media queries -->
<!--[if lt IE 9]>
<script src="/static/js/html5shiv.min.js"></script>
<script src="/static/js/respond.min.js"></script>
<![endif]-->
</head>
<body>
<div class="container">
<div class="header clearfix">
<h3 class="text-muted"> </h3>
</div>
<div class="jumbotron">

<p class="lead">
You need to come from https://vidar.club. </p>
</div>
<footer class="footer">
<p>© HGAME 2020</p>
</footer>
</div>
</body>
</html>

Target: http://kyaru.hgame.n3ko.co

Done1,451 bytes | 41 milli

Burp Suite Community Edition v2.1.07 - Temporary Project

DashboardTargetProxyIntruderRepeaterSequencerDecoderComparerExtenderProject optionsUser options

5 × 6 × 7 × 8 × 9 × 10 × 11 × 12 × 13 × 15 × 17 × 18 × ...

SendCancel<>

Request

RawHeadersHex

GET / HTTP/1.1
Host: kyaruhgame.n3ko.co
X-Forwarded-For: 127.0.0.1
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
Referer: https://vidar.club/
Connection: close
Upgrade-Insecure-Requests: 1

Response

RawHeadersHexHTMLRender

<meta name="viewport" content="width=device-width, initial-scale=1">
<title> </title>
<!-- Bootstrap core CSS -->
<link href="/static/css/bootstrap.min.css" rel="stylesheet">
<!-- Custom styles for this template -->
<link href="/static/css/jumbotron-narrow.css" rel="stylesheet">
<!-- HTML5 shim and Respond.js for IE8 support of HTML5 elements and media queries -->
<!--[if lt IE 9]>
<script src="/static/js/html5shiv.min.js"></script>
<script src="/static/js/respond.min.js"></script>
<![endif]-->
</head>
<body>
<div class="container">
<div class="header clearfix">
<h3 class="text-muted"> </h3>
</div>
<div class="jumbotron">

<p class="lead">
You need to visit it locally. </p>
</div>
<footer class="footer">
<p>© HGAME 2020</p>
</footer>
</div>
</body>
</html>

Target: http://kyaru.hgame.n3ko.co

Done1,404 bytes | 40 milli

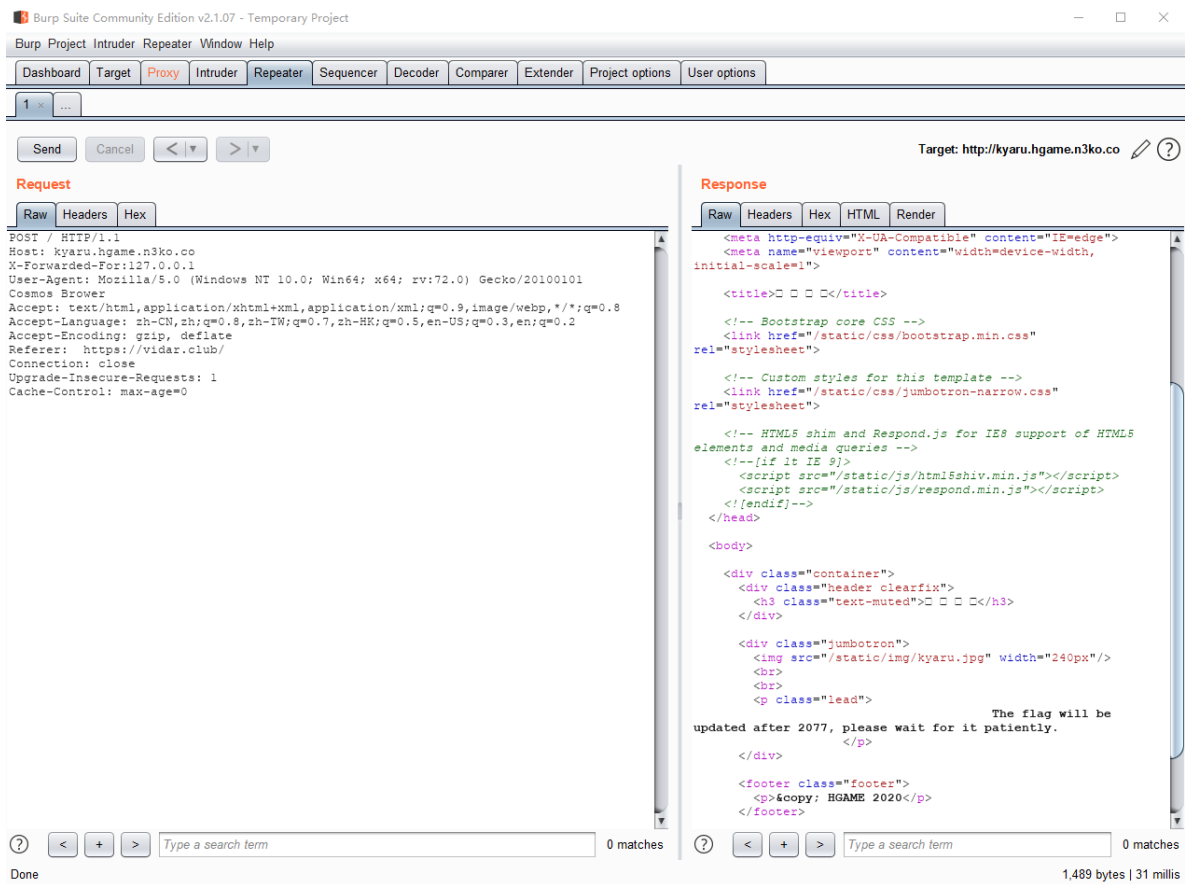
send后, 结合提示, 本地访问, 就填写伪造地址X-Forwarded-For:127.0.0.1

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. The 'Request' pane on the left displays a GET request to `http://kyaru.hgame.n3ko.co` with headers including `X-Forwarded-For:127.0.0.1` and `Gecko/20100101 Cosmos Brower`. The 'Response' pane on the right shows the HTML response, which includes a message: "You need to use Cosmos Brower to visit." The status bar at the bottom indicates "Done" and "1,400 bytes | 40 milis".

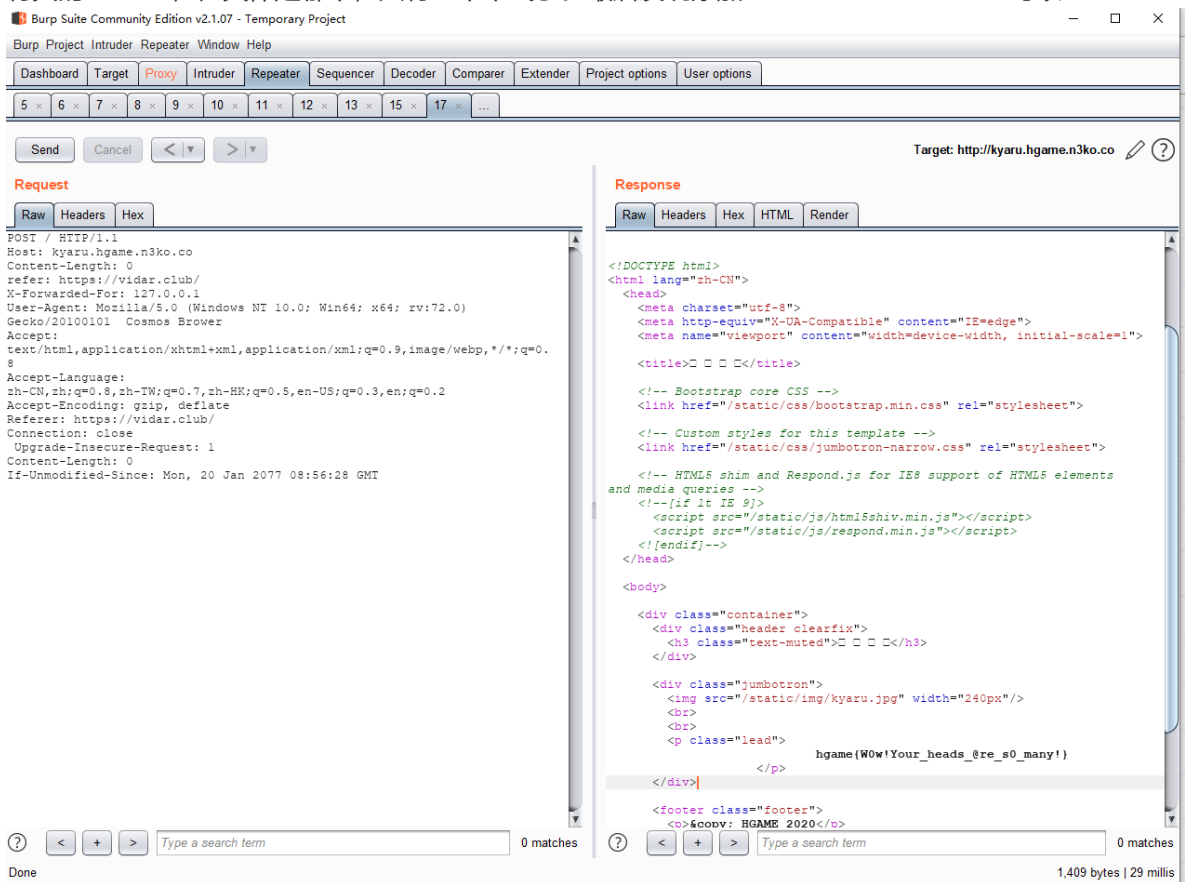
send后结合提示, 改浏览器, 就把之前的火狐改成给的cosmos brower

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. The 'Request' pane on the left displays a POST request to `http://kyaru.hgame.n3ko.co` with headers including `X-Forwarded-For:127.0.0.1` and `Gecko/20100101 Cosmos Brower`. The 'Response' pane on the right shows the HTML response, which includes a message: "Your should use POST method :)". The status bar at the bottom indicates "Done" and "1,405 bytes | 40 m".

结合提示, 要用post请求, 就把get改成post



这个提示，无从下手了。看看last-modified是2077年，结合题目的接头霸王，估计是添加一个和时间有关的header，但具体是哪个，只有一个个试了。最后发现添加 If-Unmodified-Since: 可以

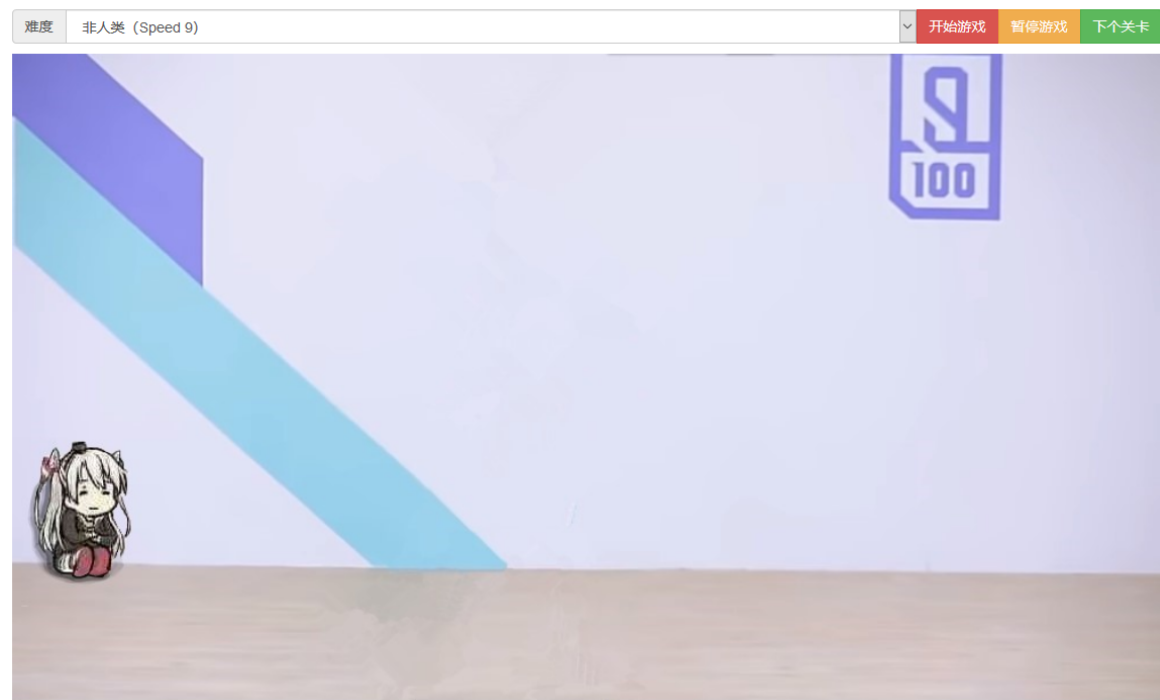


得到flag!

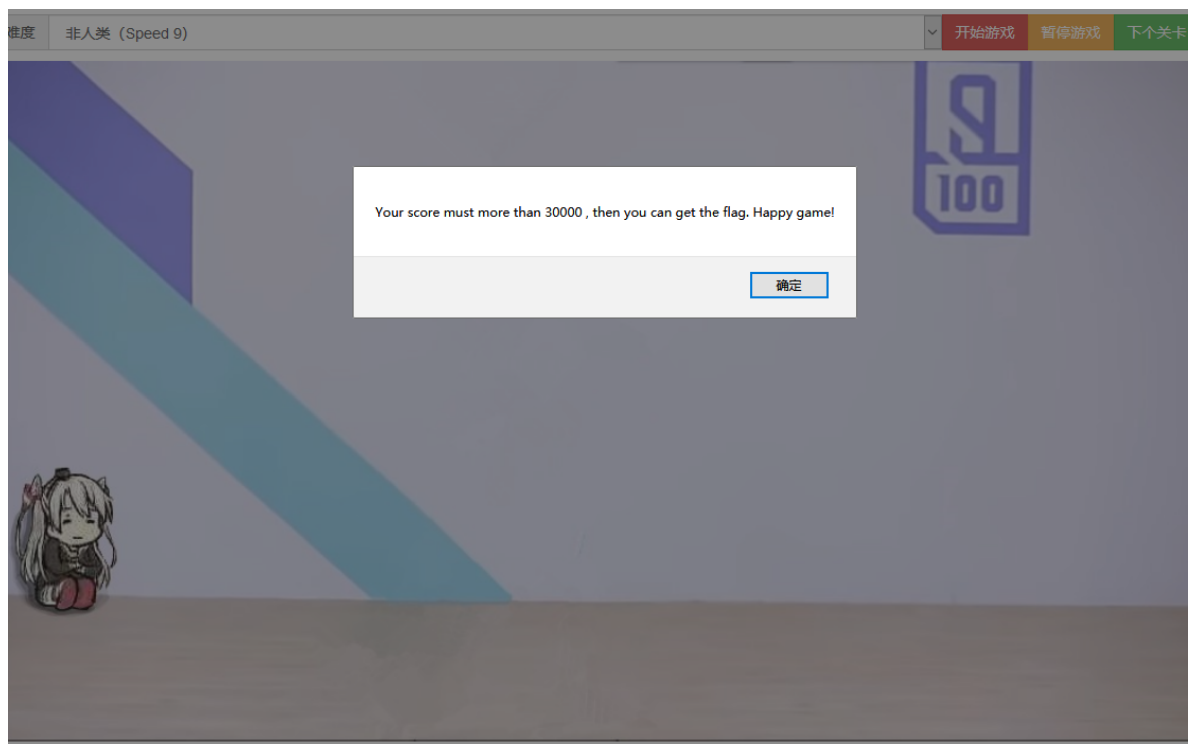
web4 鸡你太美

CXK 打篮球

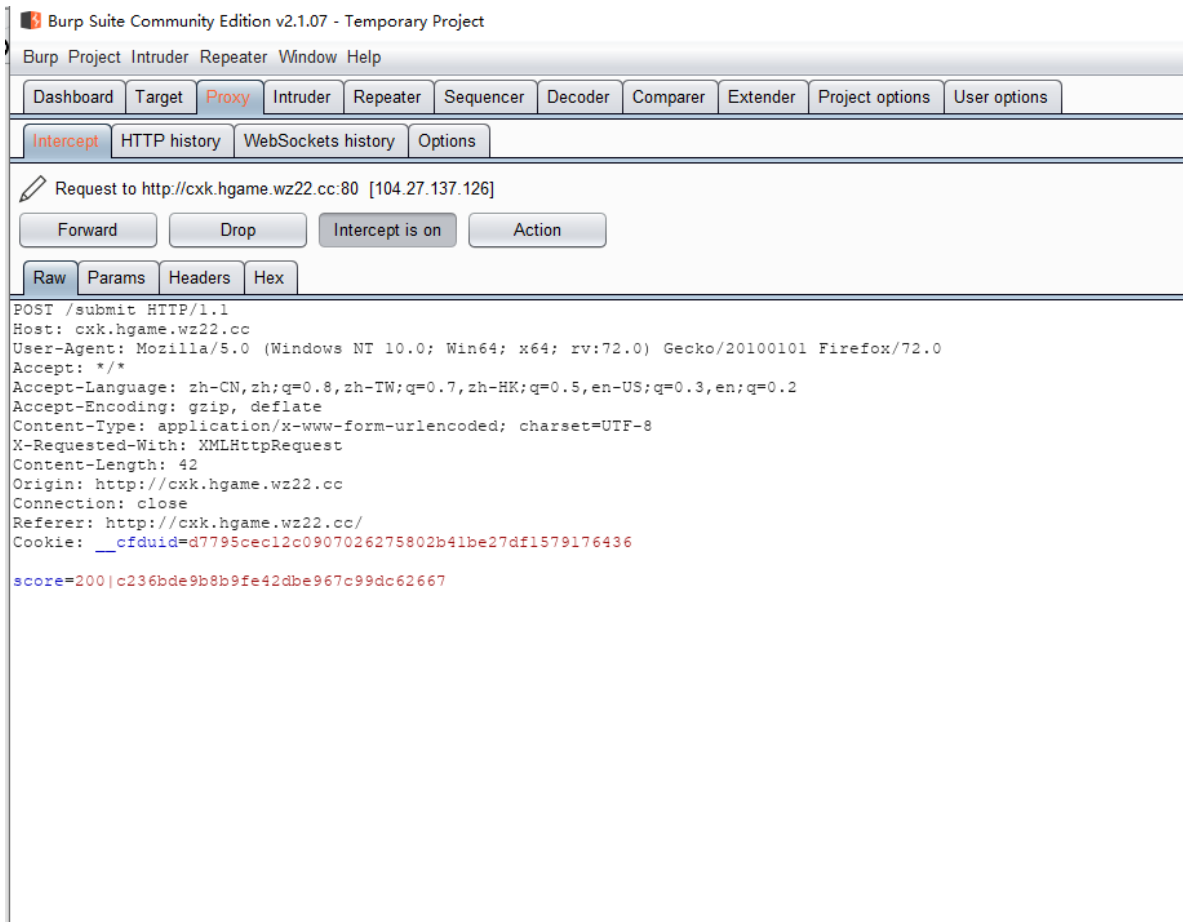
CXK, 出来打球!



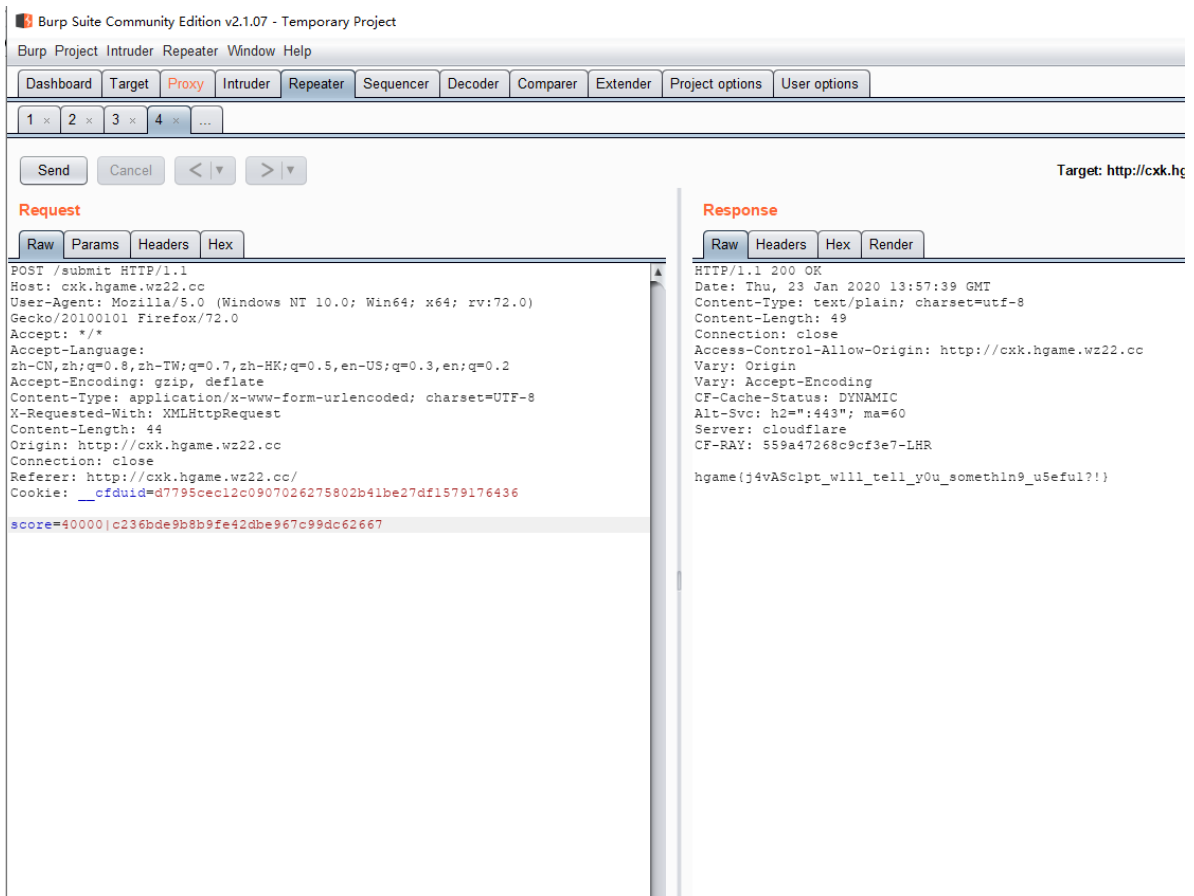
先玩一下呗。



死了。。。得到提示，要拿到三万分。那就试试抓包能不能该分数吧



有score, 试试看改一下然后发出去



得到flag!

crypto1

InfantRSA[SOLVED]

Description

真*签到题

$p = 681782737450022065655472455411;$

$q = 675274897132088253519831953441;$

$e = 13;$

$c = \text{pow}(m, e, p \cdot q) = 275698465082361070145173688411496311542172902608559859019841$

Challenge Address <https://paste.ubuntu.com/p/9hVzhnxqPc/>

Base Score 50

Now Score 50

User solved 183

百度之后，应该是RSA解密的问题

ubuntu^Qpas

Paste from Lurkrul at Thu, 16 Jan 2020

Download as text

```
1 #!/usr/bin/env python3
2 from secret import flag
3 assert flag.startswith(b'hgame(') and flag.endswith(b')')
4
5 m = int.from_bytes(flag, byteorder='big')
6
7 p = 681782737450022065655472455411
8 q = 675274897132088253519831953441
9 e = 13
10 c = pow(m, e, p*q)
11
12 assert c == 275698465082361070145173688411496311542172902608559859019841
```

Download as text

结合给的网址的代码，m就是flag以正序被转成的整数形式，所以要解m然后转成bytes。

The screenshot displays the PyCharm IDE interface. The main editor window shows a Python script named `hello world.py` with the following code:

```
1 def ext_euclid(a, b):
2     if b == 0:
3         return 1, 0, a
4     else:
5         x, y, g = ext_euclid(b, a % b) # q = gcd(a, b) = gcd(b, a % b)
6         x, y = y, (x - (a // b) * y)
7         return x, y, g
8     p = 681782737458022865655472455411
9     q = 675274897132888253519831953441
10    e = 13
11    c = 275698465982361070145173688411496311542172902608559659919641
12    print(ext_euclid(e, (p-1)*(q-1)))
13
14    #m = pow(cxd,p,q)
15    #text = '39062110472669388914389428064807335236334031991333245'
16    print(len(text))
17    print(int.to_bytes(m,53,byteorder.'big',signed=True))
```

Below the editor, the **运行** (Run) tab is active, showing the execution command and output:

运行: `C:\Users\ytz\venv\untitled\Scripts\python.exe "C:\Users\ytz\PycharmProjects\untitled\hello world.py"`
(141658697814768364339375366617699419709389378231351875726277, -4, 1)

The output indicates that the program has completed execution: **进程已结束,退出代码0** (Process finished, exit code 0).

The bottom status bar shows the current file encoding as **UTF-8** and the Python version as **Python 3.7**.

[illegible]

Misc1

欢迎参加HGame! [SOLVED]

User solved 431

请将要加密或解密的内容复制到以下区域

BASE64加密

BASE64解密

[翻译器](#)
[JavaScript代码压缩](#)
[CSS代码格式化和加密化](#)
[CSS格式整理与压缩](#)
[Html转化为Js](#)
[JS代码混淆在线工](#)

W...-LC----ME...-TO...-...-...-...-...-...-...-HGAM...-

字符	电码符号	字符	电码符号	字符	电码符号
A	• —	N	— •	1	• — — — —
B	— • • •	O	— — —	2	• • — — —
C	— • — •	P	• — — •	3	• • • — —
D	— • •	Q	— — • —	4	• • • • —
E	•	R	• — •	5	• • • • •
F	• • — •	S	• • •	6	— • • • •
G	— — •	T	—	7	— — • • •
H	• • • •	U	• • —	8	— — — • •
I	• •	V	• • • —	9	— — — — •
J	• — — —	W	• — —	0	— — — — —
K	— • —	X	— • • —	?	• • — — • •
L	• — • •	Y	— • — —	/	— • • — •
M	— —	Z	— — • •	()	— • — — • —
				—	— • • • • —
				•	• • — — • —

换成大写，提交，正确！

