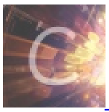
# WeChall CTF Writeup（八）

lmn_ 于 2022-02-28 05:00:00 发布 150 收藏

分类专栏： CTF 文章标签： CTF

本文链接：https://blog.csdn.net/weixin_43211186/article/details/123156621

版权

 CTF 专栏收录该内容

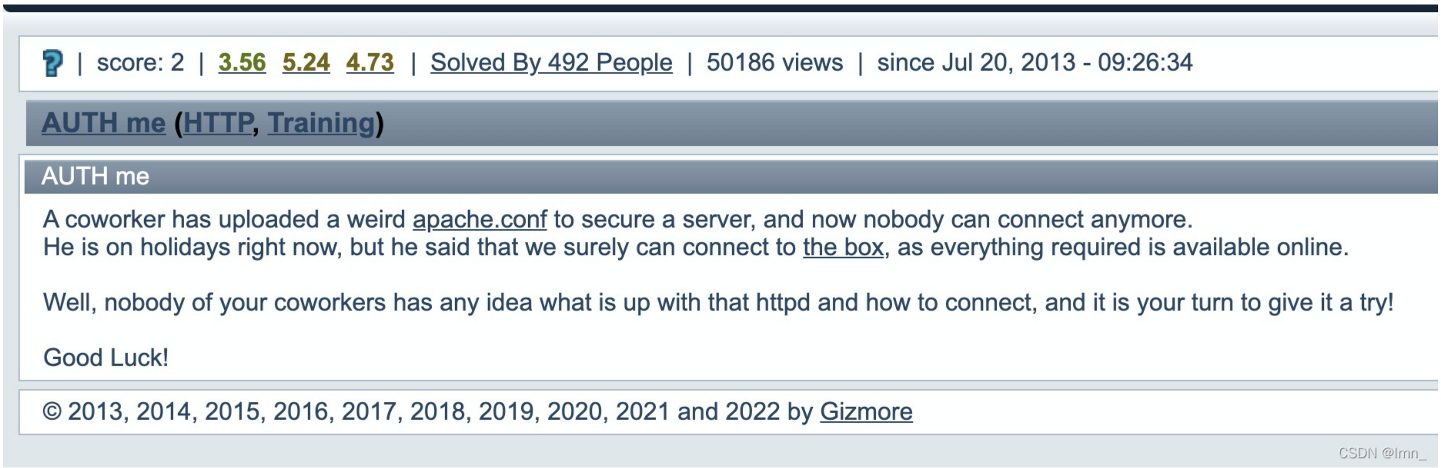
15 篇文章 0 订阅

订阅专栏

## 文章目录

以下题目标题组成：
[Score] [Title] [Author]

## 0x10 2 AUTH me by Gizmore



| score: 2 | 3.56 5.24 4.73 | Solved By 492 People | 50186 views | since Jul 20, 2013 - 09:26:34

AUTH me (HTTP, Training)

AUTH me

A coworker has uploaded a weird apache.conf to secure a server, and now nobody can connect anymore.
He is on holidays right now, but he said that we surely can connect to the box, as everything required is available online.

Well, nobody of your coworkers has any idea what is up with that httpd and how to connect, and it is your turn to give it a try!

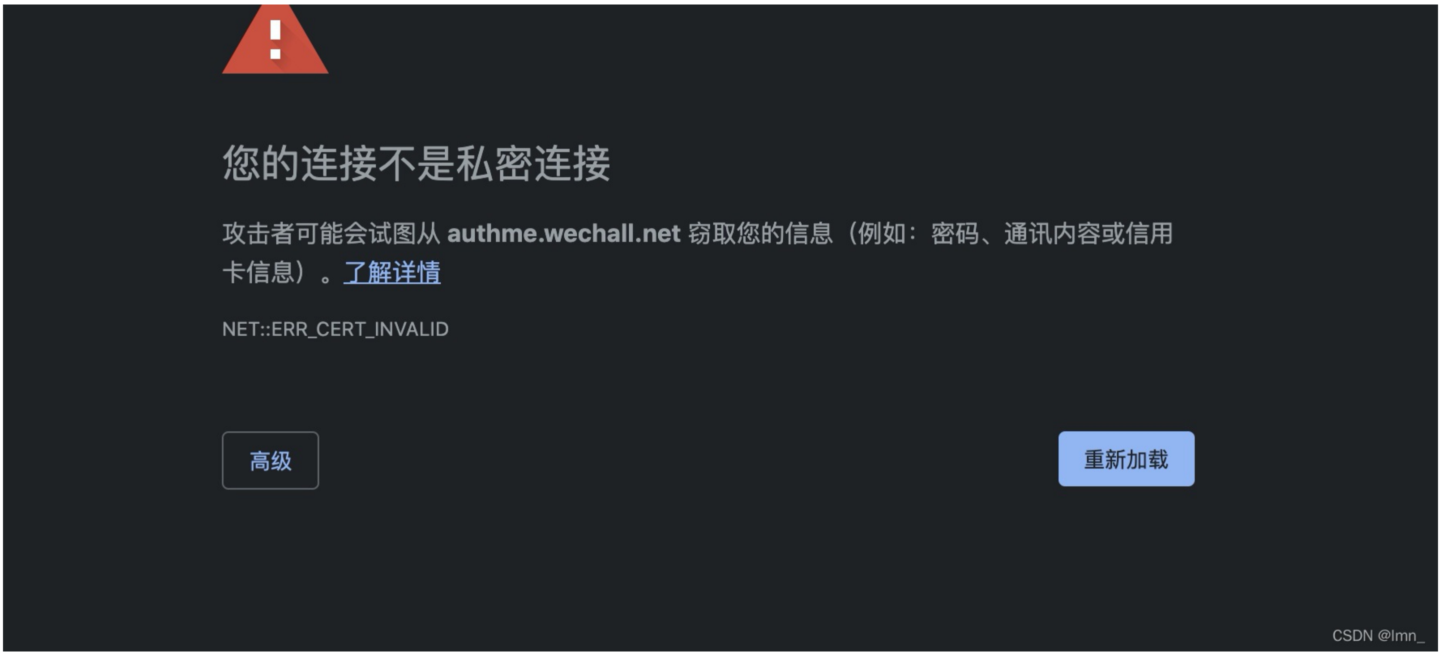
Good Luck!

© 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2021 and 2022 by Gizmore

题目意思：
一位同事上传了一个奇怪的apache.conf来保护服务器，现在没有人可以连接了。
他现在正在度假，但他说我们肯定可以连接到盒子，因为所需的一切都可以在线获得。

好吧，您的同事中没有人知道该 httpd 发生了什么以及如何连接，现在轮到您试一试了！

访问the box

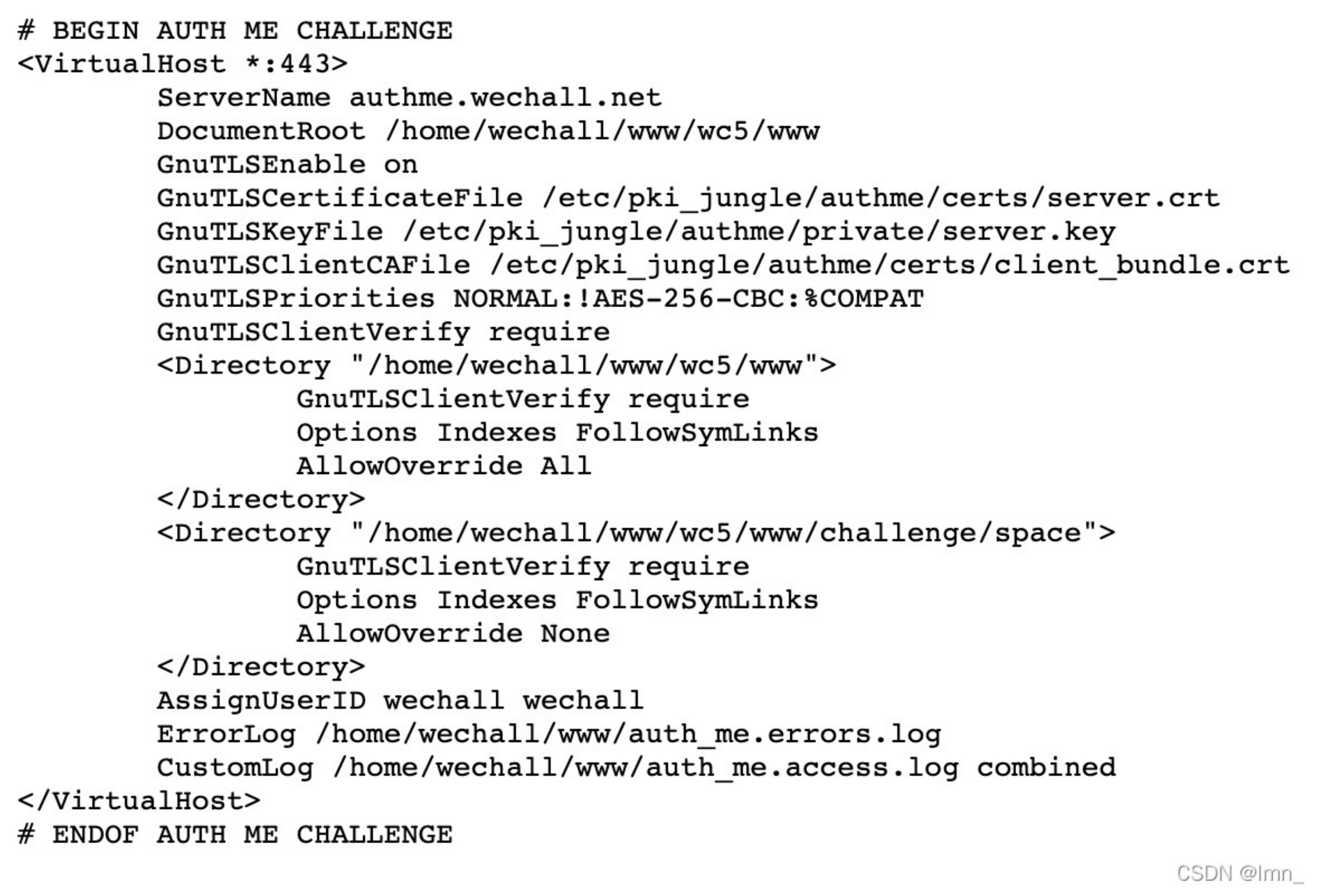


您的连接不是私密连接

攻击者可能会试图从 **authme.wechall.net** 窃取您的信息（例如：密码、通讯内容或信用卡信息）。了解详情

NET::ERR_CERT_INVALID

访问不了因为没有证书



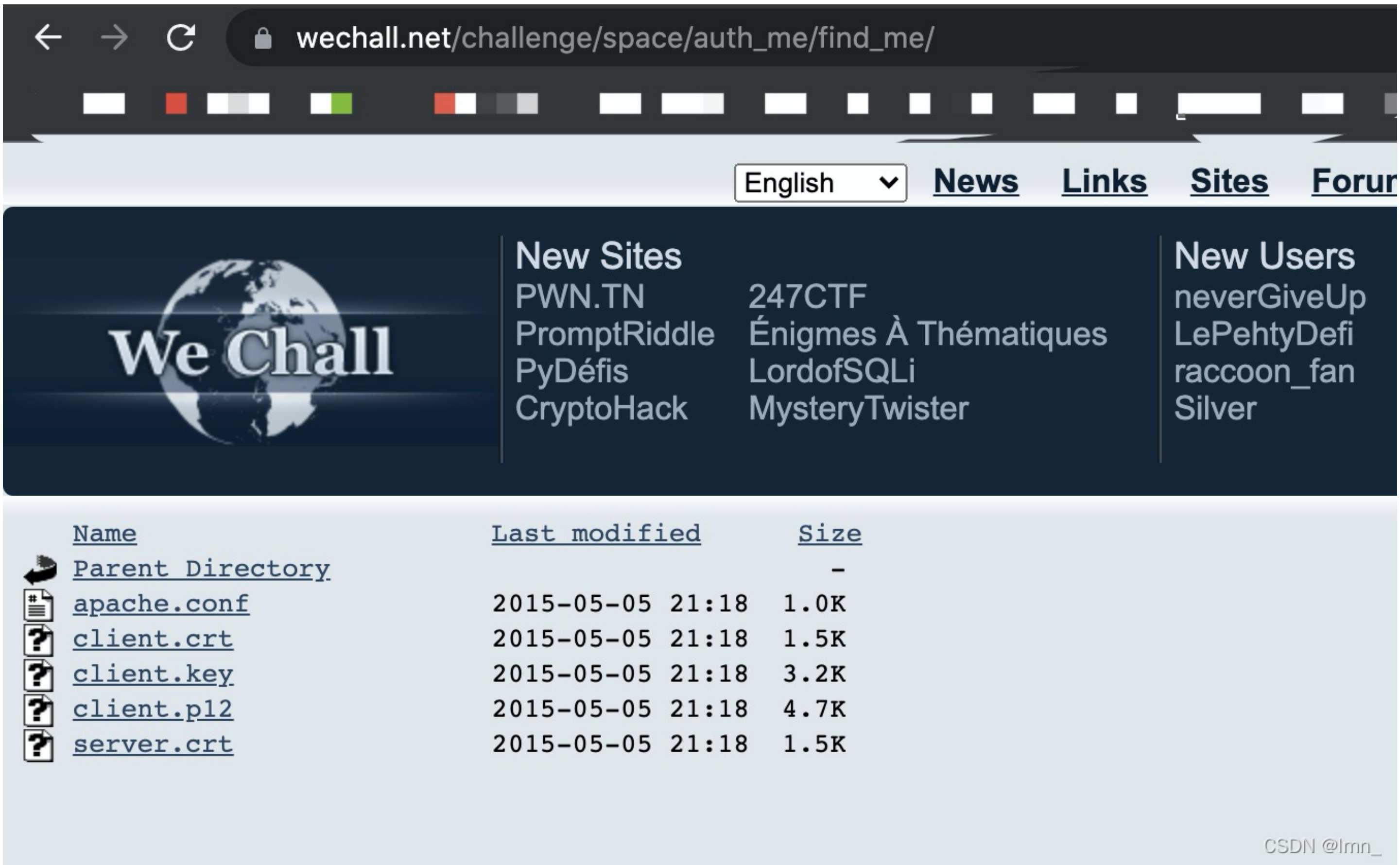
```
# BEGIN AUTH ME CHALLENGE
<VirtualHost *:443>
        ServerName authme.wechall.net
        DocumentRoot /home/wechall/www/wc5/www
        GnuTLSEnable on
        GnuTLSCertificateFile /etc/pki_jungle/authme/certs/server.crt
        GnuTLSKeyFile /etc/pki_jungle/authme/private/server.key
        GnuTLSClientCAFile /etc/pki_jungle/authme/certs/client_bundle.crt
        GnuTLSPriorities NORMAL:!AES-256-CBC:%COMPAT
        GnuTLSClientVerify require
        <Directory "/home/wechall/www/wc5/www">
                GnuTLSClientVerify require
                Options Indexes FollowSymLinks
                AllowOverride All
        </Directory>
        <Directory "/home/wechall/www/wc5/www/challenge/space">
                GnuTLSClientVerify require
                Options Indexes FollowSymLinks
                AllowOverride None
        </Directory>
        AssignUserID wechall wechall
        ErrorLog /home/wechall/www/auth_me.errors.log
        CustomLog /home/wechall/www/auth_me.access.log combined
</VirtualHost>
# ENDOF AUTH ME CHALLENGE
```

ServerName：设置服务器用于辨识自己的主机名和端口号。
DocumentRoot：设置Web文档根目录。
GnuTLS是传输层安全的 LGPL 许可实现。
GnuTLSCertificateFile：整数文件。

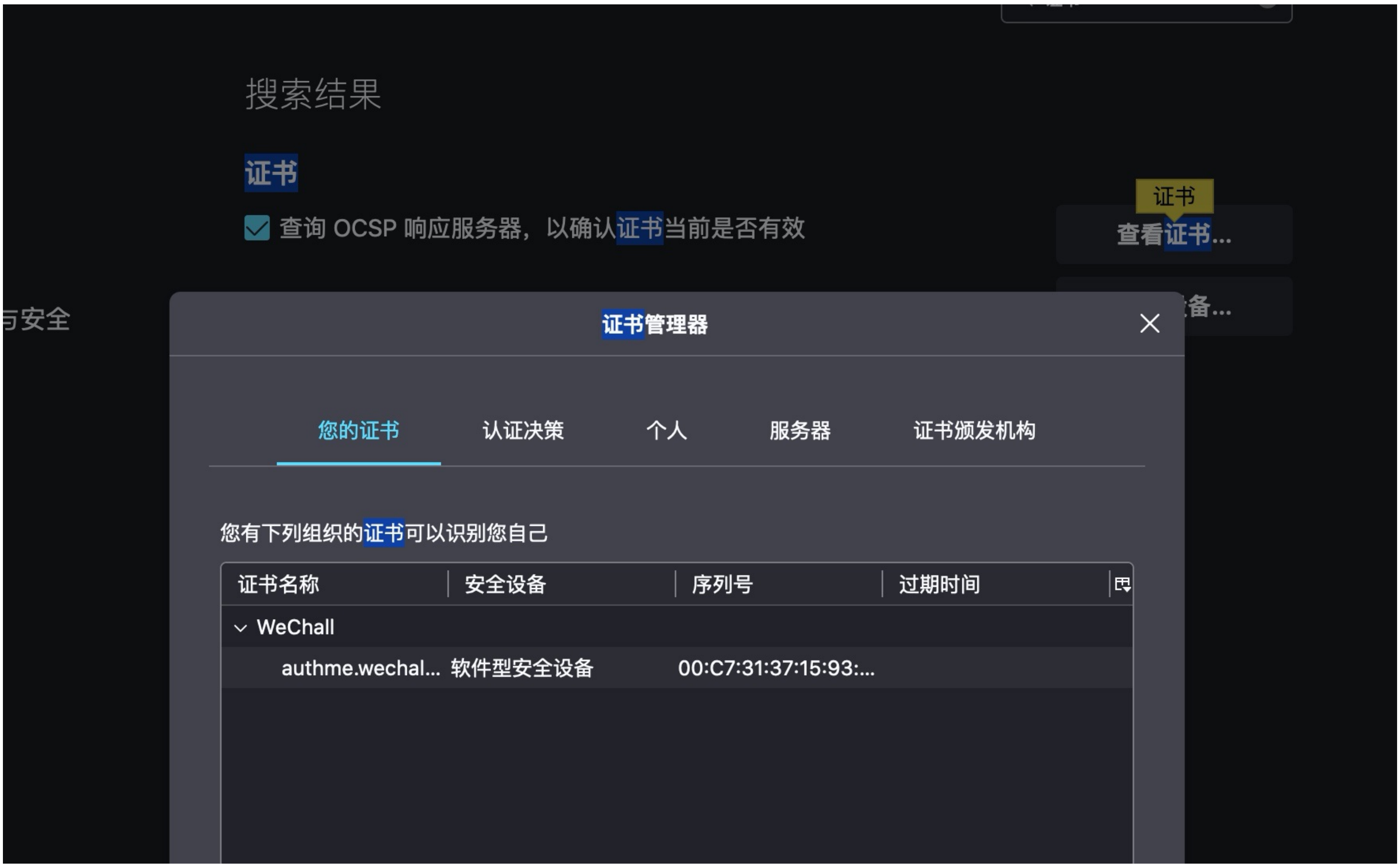
我们需要的是客户端证书文件

```
GnuTLSClientCAFile /etc/pki_jungle/authme/certs/client_bundle.crt
```

题目给了暗示“因为所需的一切都可以在线获得”
在上一级地址获得：
https://www.wechall.net/challenge/space/auth_me/find_me/



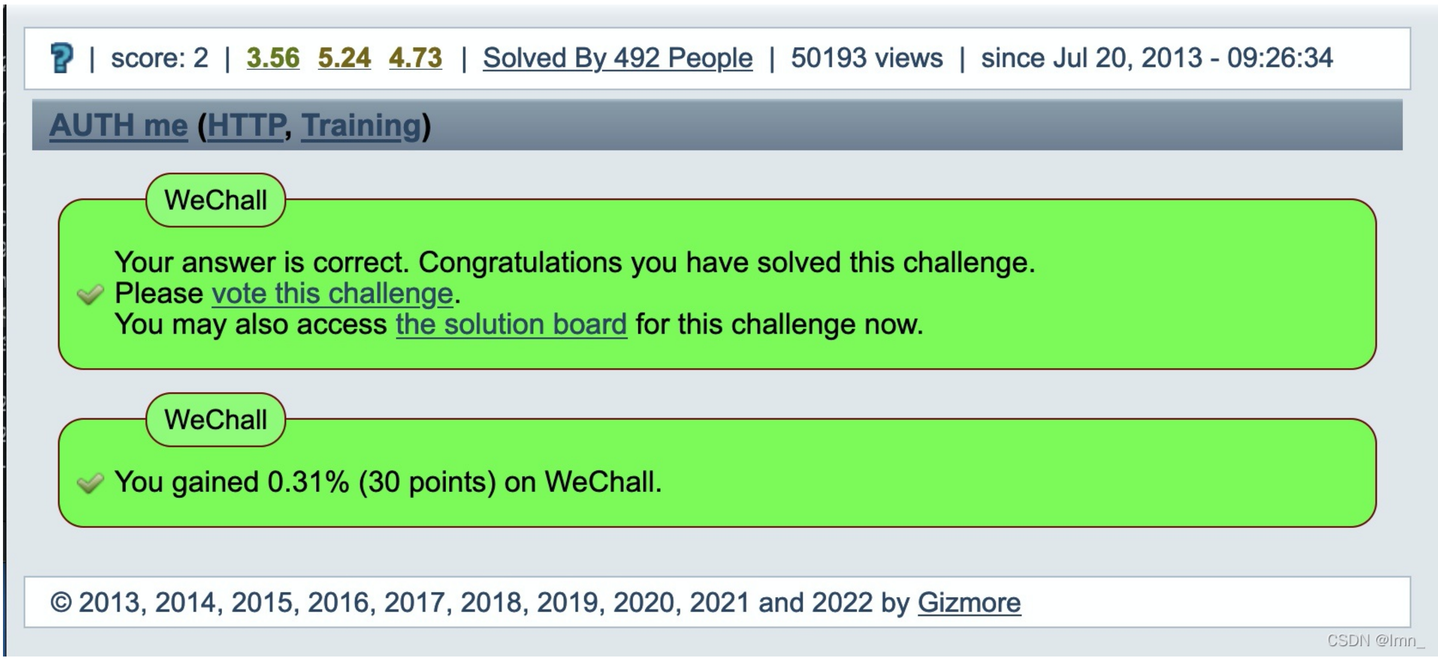
```
Name                  Last modified      Size
Parent Directory                           -
apache.conf           2015-05-05 21:18  1.0K
client.crt            2015-05-05 21:18  1.5K
client.key            2015-05-05 21:18  3.2K
client.p12            2015-05-05 21:18  4.7K
server.crt            2015-05-05 21:18  1.5K
```



☑ 查询 OCSP 响应服务器，以确认证书当前是否有效

您有下列组织的证书可以识别您自己

| 证书名称 | 安全设备 | 序列号 | 过期时间 |
|---|---|---|---|
| ⌄ WeChall | | | |
| authme.wechal... | 软件型安全设备 | 00:C7:31:37:15:93:... | |


? | score: 2 | 3.56 5.24 4.73 | Solved By 492 People | 50193 views | since Jul 20, 2013 - 09:26:34

AUTH me (HTTP, Training)

WeChall

✓ Your answer is correct. Congratulations you have solved this challenge.
Please vote this challenge.
You may also access the solution board for this challenge now.

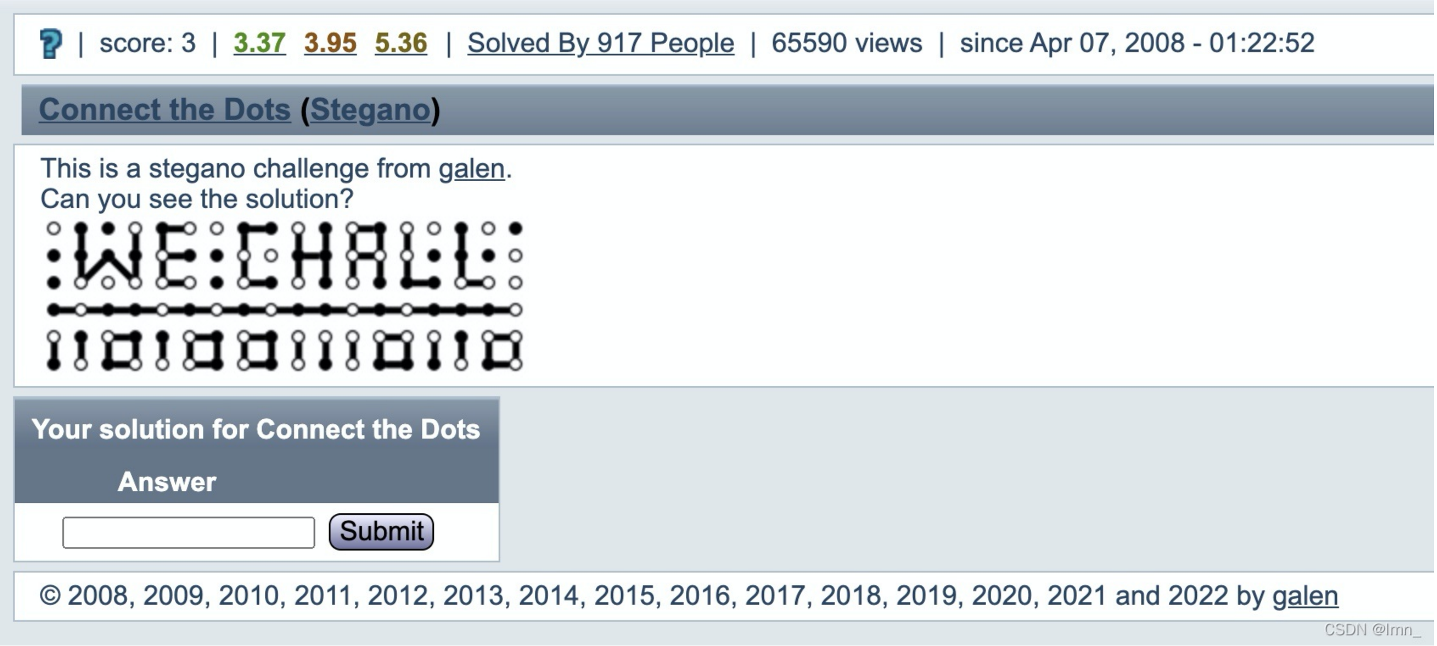
WeChall

✓ You gained 0.31% (30 points) on WeChall.

© 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2021 and 2022 by Gizmore

bingo!

## 0x11 3 Connect the Dots by galen



| score: 3 | 3.37 3.95 5.36 | Solved By 917 People | 65590 views | since Apr 07, 2008 - 01:22:52

Connect the Dots (Stegano)

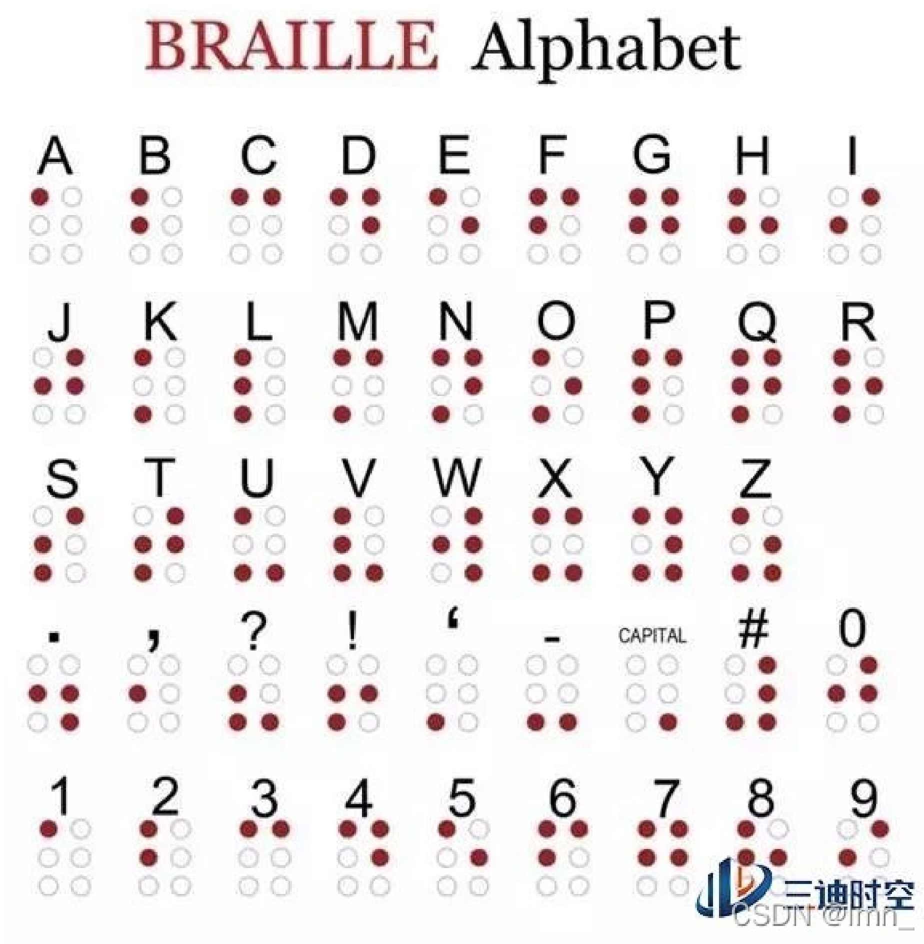
This is a stegano challenge from galen.
Can you see the solution?

Your solution for Connect the Dots

Answer

© 2008, 2009, 2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2021 and 2022 by galen

可以很快看出来像是盲文，找一张盲文表对照一下



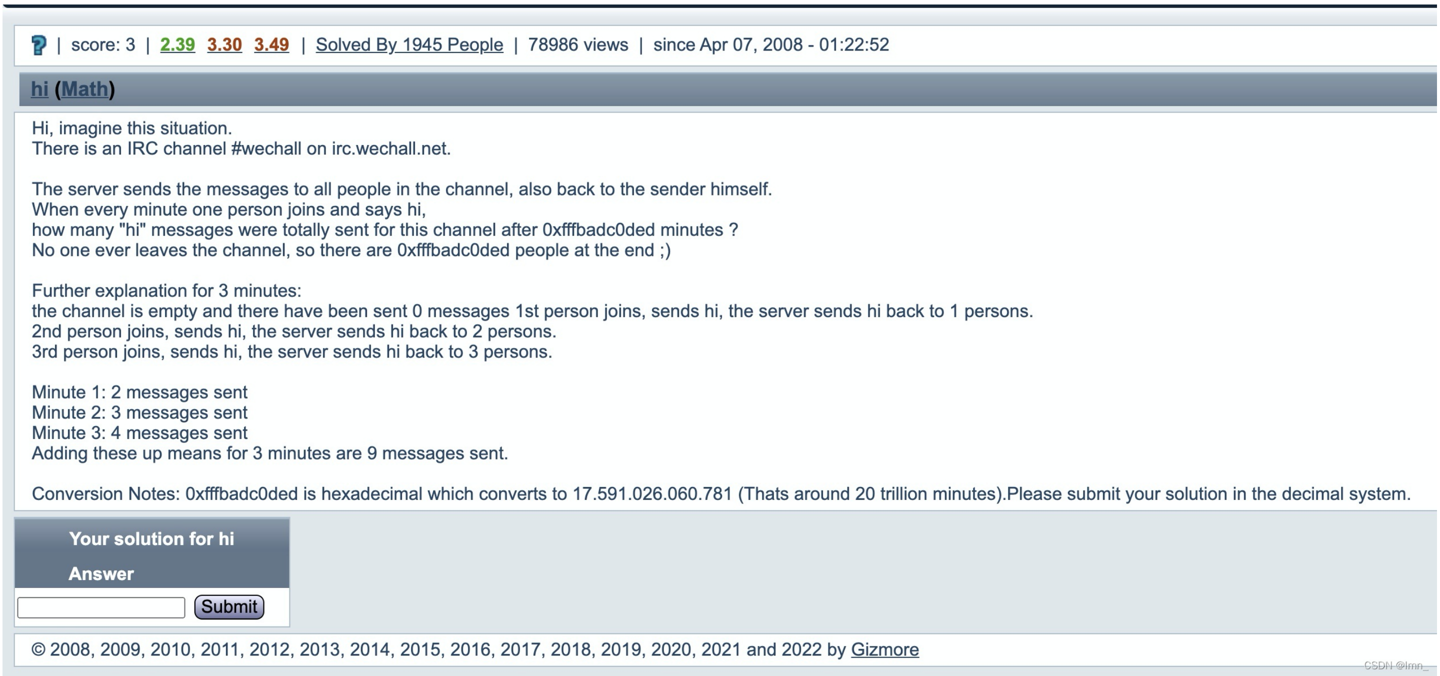
两行的答案分别是：

THESOLUTI

ONISSKUNK

提交：skunk

## 0x12 3 hi by Gizmore



| score: 3 | 2.39 3.30 3.49 | Solved By 1945 People | 78986 views | since Apr 07, 2008 - 01:22:52

**hi (Math)**

Hi, imagine this situation.
There is an IRC channel #wechall on irc.wechall.net.

The server sends the messages to all people in the channel, also back to the sender himself.
When every minute one person joins and says hi,
how many "hi" messages were totally sent for this channel after 0xfffbadc0ded minutes ?
No one ever leaves the channel, so there are 0xfffbadc0ded people at the end ;)

Further explanation for 3 minutes:
the channel is empty and there have been sent 0 messages 1st person joins, sends hi, the server sends hi back to 1 persons.
2nd person joins, sends hi, the server sends hi back to 2 persons.
3rd person joins, sends hi, the server sends hi back to 3 persons.

Minute 1: 2 messages sent
Minute 2: 3 messages sent
Minute 3: 4 messages sent
Adding these up means for 3 minutes are 9 messages sent.

Conversion Notes: 0xfffbadc0ded is hexadecimal which converts to 17.591.026.060.781 (Thats around 20 trillion minutes).Please submit your solution in the decimal system.

© 2008, 2009, 2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2021 and 2022 by Gizmore

题目意思：
嗨，想象一下这种情况。
irc.wechall.net 上有一个 IRC 频道#wechall。

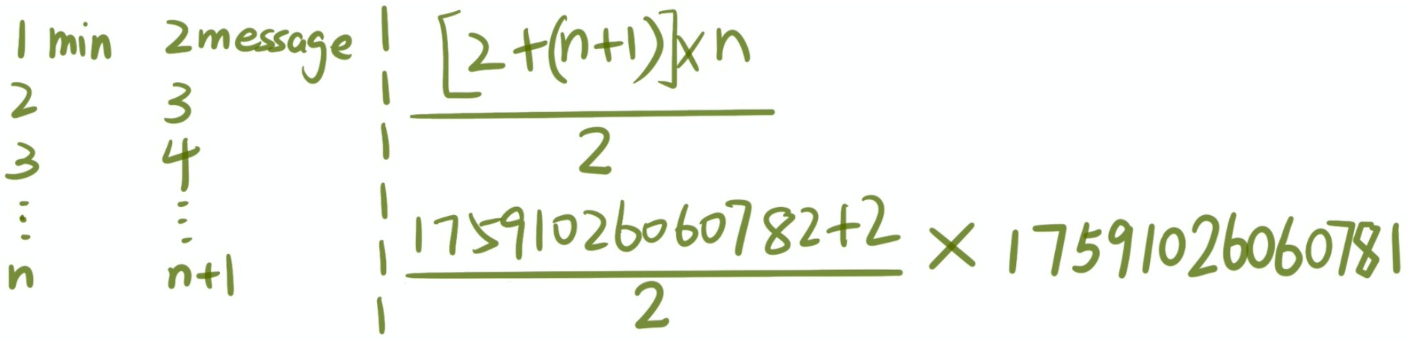
服务器将消息发送给频道中的所有人，同时也返回给发送者本人。
当每分钟一个人加入并打招呼时，
在 0xfffbadc0ded 分钟后，该频道总共发送了多少条“hi”消息？
没有人离开频道，所以最后有 0xfffbadc0ded 人；）

3 分钟的进一步解释：
频道是空的，已经发送了 0 条消息 1 人加入，发送 hi，服务器将 hi 发送回 1 人。
第 2 个人加入，发送 hi，服务器将 hi 发送回 2 个人。
第 3 个人加入，发送 hi，服务器将 hi 发送回 3 个人。

第 1 分钟：发送了 2 条消息
第 2 分钟：发送了 3 条消息
第 3 分钟：发送了 4 条消息
将这些相加意味着 3 分钟发送了 9 条消息。

转换说明：0xfffbadc0ded 是十六进制，转换为 17.591.026.060.781（大约 20 万亿分钟）。请以十进制提交您的解决方案。

问题是：在 0xfffbadc0ded 分钟后，该频道总共发送了多少条“hi”消息？
构造一个表达式（有点丑意思对了）

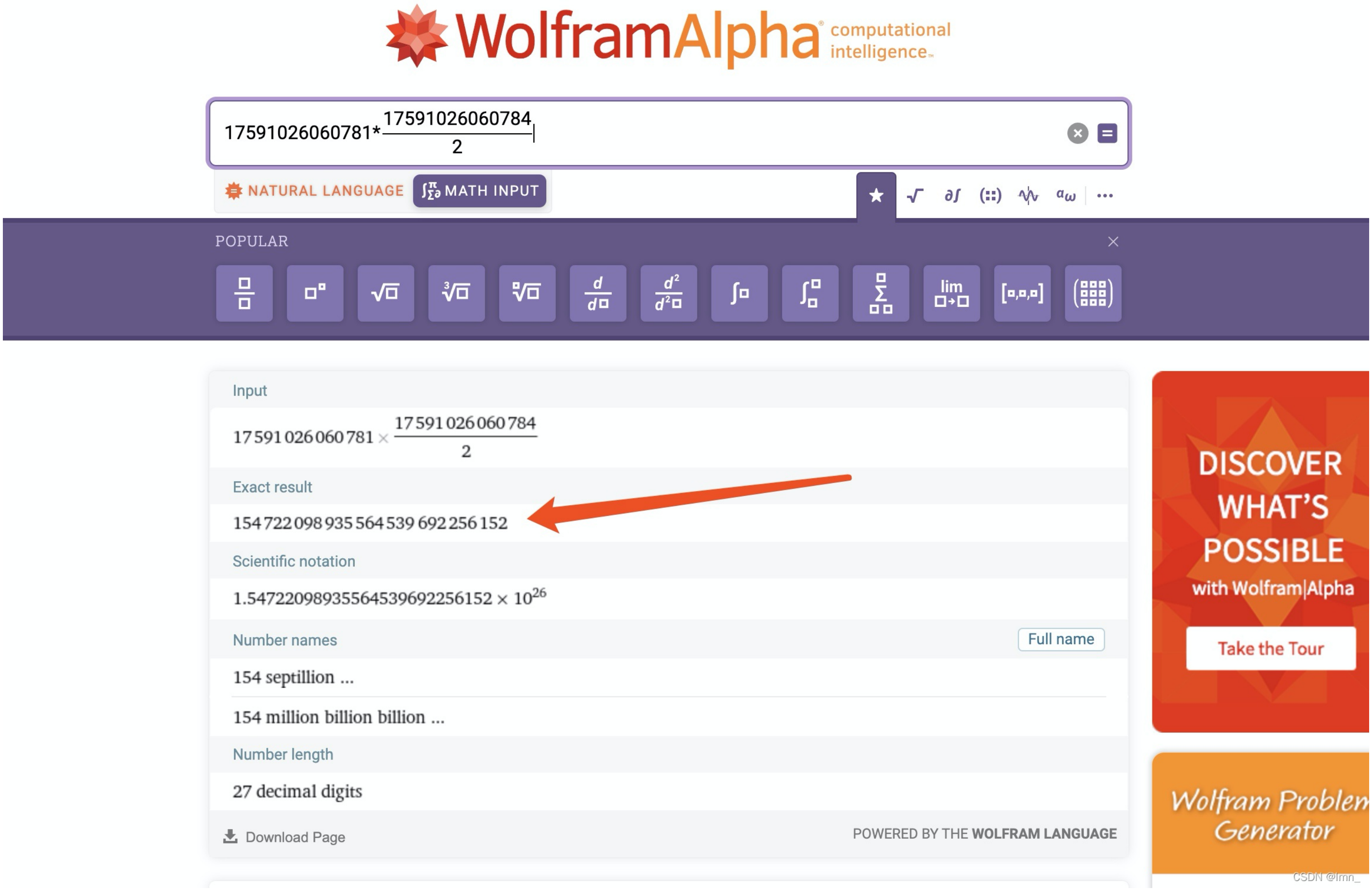


| | |
|---|---|
| 1 min | 2message |
| 2 | 3 |
| 3 | 4 |
| ⋮ | ⋮ |
| n | n+1 |

$$\frac{[2+(n+1)]\times n}{2}$$

$$\frac{17591026060782+2}{2}\times 17591026060781$$

网站地址：
https://www.wolframalpha.com/input/?i=17591026060781*17591026060784%2F2



WolframAlpha computational intelligence.
NATURAL LANGUAGE
MATH INPUT
POPULAR
Full name
Download Page
POWERED BY THE WOLFRAM LANGUAGE
DISCOVER WHAT'S POSSIBLE with Wolfram|Alpha
Take the Tour
Wolfram Problem Generator

$17591026060781*\frac{17591026060784}{2}$

Input

$17\,591\,026\,060\,781\times\frac{17\,591\,026\,060\,784}{2}$

Exact result

154 722 098 935 564 539 692 256 152

Scientific notation

$1.54722098935564539692256152\times 10^{26}$

Number names

154 septillion ...

154 million billion billion ...

Number length

27 decimal digits

答案：
154722098935564539692256152