WeChall CTF Writeup（五）

原创

lmn_ 于 2022-02-27 08:00:00 发布   16 ⭐ 收藏

分类专栏： CTF 文章标签： CTF

本文链接： https://blog.csdn.net/weixin_43211186/article/details/123156295

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]

题目后的三个分值是可以用户自己打分的，可以当作参考

可以看到，使用次网站的人还是遍布非常广的，并且题目思路与国内是有一些差异的

59		Nepal	2	27050	0.93	13529	27050
60		Serbia	7	89626	12.20	12803	89626
61		Lebanon	6	76787	18.61	12797	76787
62		Belarus	4	50292	5.23	12573	50292
63		Cyprus	1	12148	11.02	12148	12148
64		New Zealand	11	124328	29.24	11302	124328
65		Mongolia	37	399786	129.51	10805	399786
66		Benin	1	10088	1.11	10088	10088
67		Estonia	2	19059	14.76	9529	19059
68		Pakistan	7	63992	0.35	9141	63992
69		Colombia	572	5111976	115.64	8937	5111976
70		Costa Rica	2	17769	3.93	8884	17769
71		China	169	1438627	1.08	8512	1438627
72		Bangladesh	4	33061	0.21	8265	33061
73		Hong Kong	6	49561	6.99	8260	49561
74		Ireland	13	96819	20.94	7447	96819
75		Cameroon	1	7351	0.38	7351	7351
76		Chile	13	92302	5.51	7100	92302
77		Trinidad & Tobago	9	62408	50.79	6934	62408
78		Egypt	5	30176	0.37	6035	30176
79		Venezuela	7	40597	1.49	5799	40597
80		Macedonia, Republic of	1	5690	2.75	5690	5690
81		Armenia	2	11343	3.82	5671	11343
82		Denmark	14	71524	12.97	5108	71524
83		Ghana	1	4242	0.17	4242	4242
84		Mexico	12	47397	0.42	3949	47397
85		Myanmar	1	3546	0.07	3546	3546
86		Malaysia	5	14117	0.50	2823	14117
87		Kazakhstan	4	11198	0.72	2799	11198
88		Bolivia	2	5516	0.55	2758	5516
89		Thailand	8	21795	0.32	2724	21795

0x01 2 Training: LSB by Gizmore

Training: LSB (Stegano, Image, Training)

Training: LSB - The least significant bit

This is a very simple, yet spectacular trick.
Can you see the hidden solution?

Note: The solution is bound to your session ID and consists of twelve letters.

Hidden Hint: http://wechall.blogspot.com/2007/11/steganabara-explained.html

Thanks go out to buttmonkey for creating the image :)

The carrier image

Your solution for Training: LSB

Answer

[   ] Submit

题目意思：

这是一个非常简单但非常壮观的技巧。

你能看到隐藏的解决方案吗？

注意：解决方案与您的会话 ID 绑定，由十二个字母组成。

隐藏提示：http://wechall.blogspot.com/2007/11/steganabara-explained.html

点开链接提示了工具

We Chall

I Chall. You Chall. We Chall!!!

🔹 **Wednesday, 14 November 2007**

Steganabara explained

Hey guys,

Contributors

🔹 Gizmore

🔹 Sphinx

Finally I defeated my laziness and created a project page for Steganabara. You can access it from here.

Also included an explanation of the key features: Bit Mask Filter, Color Map Filter, Color Explorer, Histogram and Color Table.

And now a demonstration of the Bit Mask Filter, applying on StenographyOriginal.png, from the wikipedia page about steganography
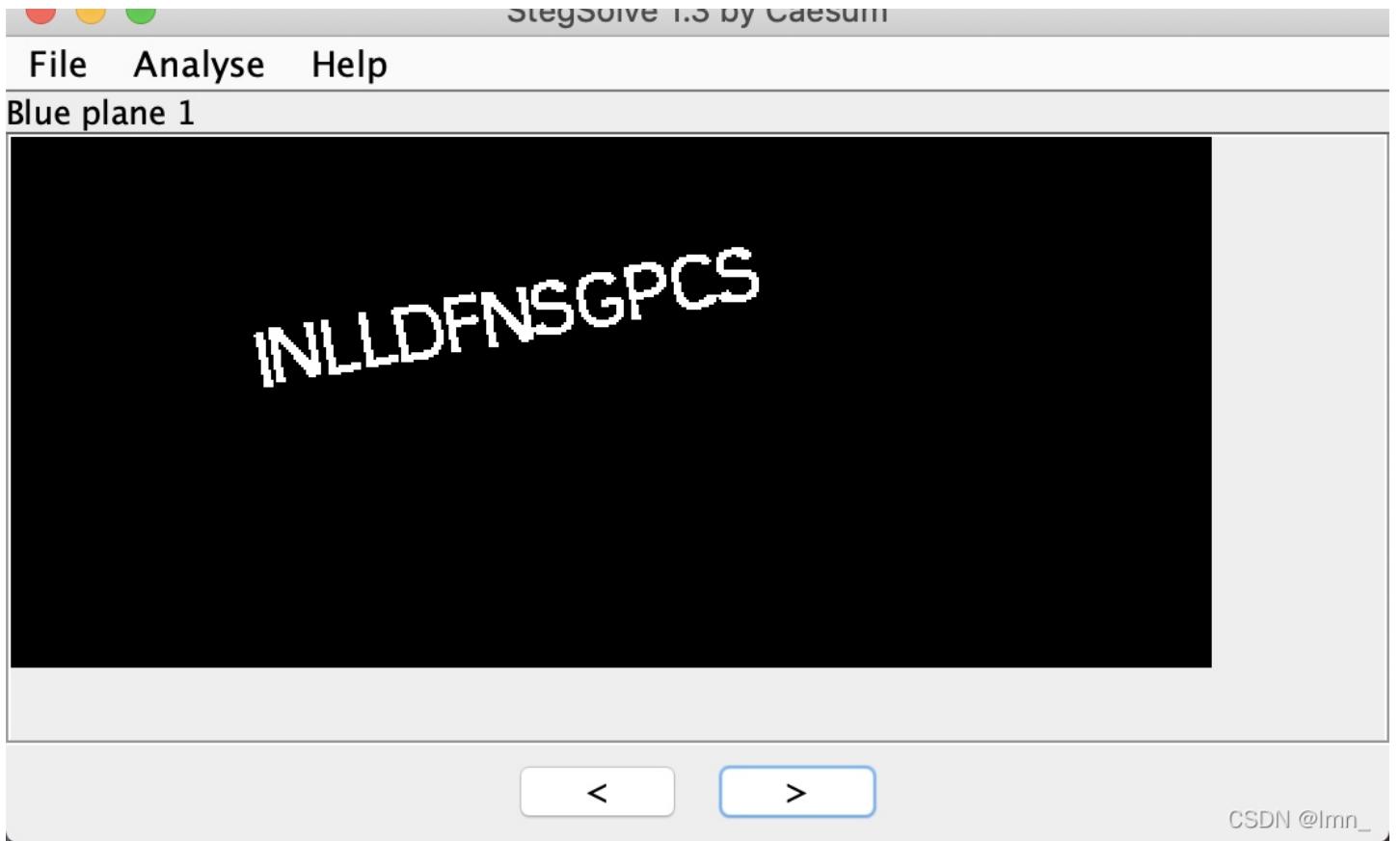
Label Cloud

3564020356 **challenge site**
hackquest rankk electrica
theblacksheep slyfx stegano
challenge ma's reversing omega
project project euler steganabara tbs

不过有一个更好用的被大家公认的工具–

找到答案

其次，LSB全称leastsignificant bit，是一种基于图片最低有效位修改储存信息的隐写方法，即使不提供链接，也可以通过题目名称得到tips！

答案：

INLLDFNSGPCS

0x02 2 Training: GPG by Gizmore

Training: GPG (**Crypto**, **Training**)

Crypto - GPG

In this challenge your goal is to setup gpg encryption for your emails.
To do so, generate your keypairs locally and store your public key on wechall.
Then all your mails sent by wechall are encrypted.
To enable GPG encryption, please goto Your account settings.
When you are done, click the button below to send you a mail.

Happy Challenging!

[Send me encrypted mail please.]

Your solution for Training: GPG
Answer

[   ] [Submit]

题目意思：
在这个挑战中，您的目标是为您的电子邮件设置 gpg 加密。
为此，请在本地生成您的密钥对并将您的公钥存储在Wechall上。
然后您所有通过Wechall发送的邮件都会被加密。
要启用 GPG 加密，请转到您的帐户设置。
完成后，单击下面的按钮向您发送邮件。

首先了解一下什么是GPG加密

背景介绍

加密的一个简单但又实用的任务就是发送加密电子邮件。多年来，为电子邮件进行加密的标准一直是PGP（Pretty Good Privacy）。程序员Phil Zimmermann特别为电子邮件的保密编写的PGP。

这个软件非常好用，迅速流传开来，成了许多程序员的必备工具。但是，它是商业软件，不能自由使用。

作为PGP的替代，如今已经有一个开放源代码的类似产品可供使用。GPG（Gnu Privacy Guard），它不包含专利算法，能够无限制的用于商业应用。

本文将会介绍文件加密，至于GPG的其他用途，比如邮件加密，请参考这个网站

https://help.ubuntu.com

安装GPG软件，安装地址

https://gpgtools.org/

等待生成密钥

导出

访问您的帐户设置

https://www.wechall.net/account
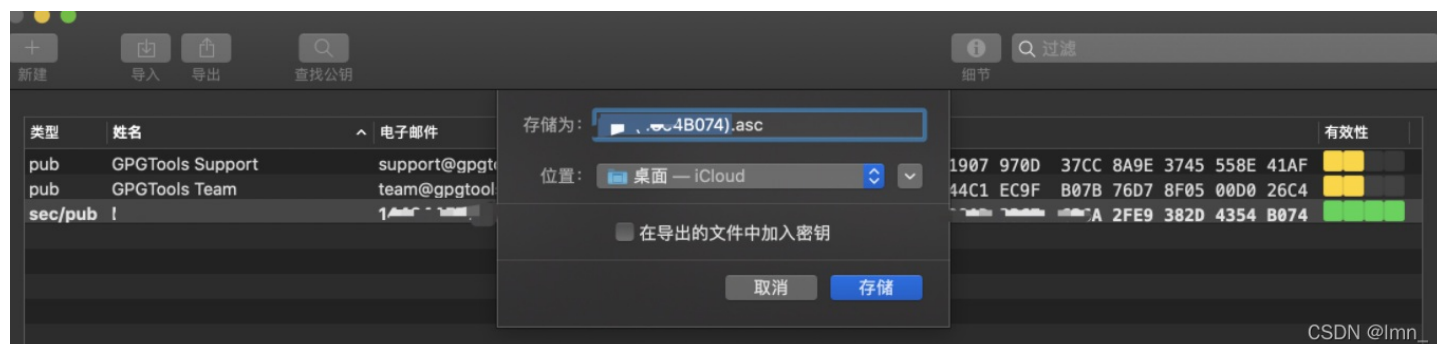
在页面下面会看到这么一个框框，选择文件，上传导出的.asc文件

Setup PGP/GPG Encryption

Upload your public key 💡 [选择文件] 未选择任何文件

Or paste it here

[Upload Key] [Remove Key]

(**Account**)

✅ We have sent you an email to perform the changes. Please follow the instructions in it.

[Linked Sites] [WarBoxes] [View Profile] [Your Stats] [Delete Account]
[WeChall Settings] [Account Settings] [PM Settings] [Forum Settings]
[Edit Profile] [Show Groups] [Guestbook] [Hackerspace]

收到发来的邮件

今天 (1 封)

☐ ✉️ **robot**   **WeChall: Setup GPG Encryption**

上周 (8 封)

WeChall: Setup GPG Encryption ☆

发件人： **robot** <robot@wechall.net> 📧
　　　　（由 wechall@wechall.net 代发）
时　间：2022年1月23日（星期日）下午4：31
收件人： ■ ■■■■■ 📭

🔄 邮件可翻译为中文　立即翻译

-----BEGIN PGP MESSAGE----- Version: GnuPG v2 hQIMA5Xs5ehK6QVxARAAg2tqFYZ3SWqea2PrLV5G+6c0erICqyD1SwLV2+IkwuVD
7jHm3yYkkst4yMm5RslTPL+TSsT9jb9OkuX8NkHw+RcSuwPNUx/RtrBun5tvBcXt T74pUFMQ3eYjjOhk/ADe0o6APbDYupTVj4jB/RF2do+RPg
7jMA5MU5WhNjg0TA3juLclznC1qurvh6oyxlp3qK2YebiEj7lW/0Juo13xERkVmw fakHgVlb3nx+FlzcTImVNIQlJ8st+ebtDmggmHflcMb2KN3W
ttP1vhGblhSK7jksYHQKOExwtrsrUOhDvCxQlGTBomsWecX3o1leHp0icFfVblSz u2sBG5XBQIXvMDHZshmYoJCBxDjYuJNjDMrR4kQbZGdazEAR
AYvC3VQxnQ6yF7mqae5HdSm8MtU+/tNHGMgjF9XbJ7WcwfoGPccEbxVTIpS7/0GB Y8L/mgftzrdUm35gF7jyV0CozC7EYcbsXzWt/wPPw2cKb
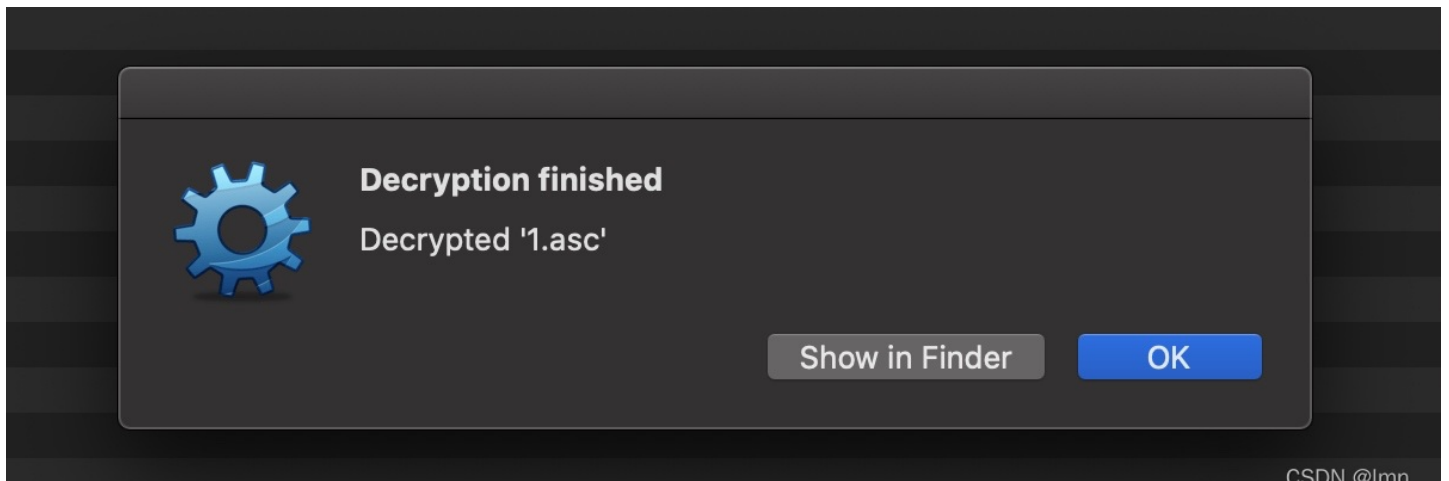
oXUnKVfxwQJBFZrU/oAFD3JL3L6zjrXv6H+uMz+AW4D35bmJWxzLQBB0ZgvV/Kj/ CCjqfNEsddEbTKAXWSy1X+IBnLkwg3rOoKiNEwTvCQdgBl

wM8BG+ekbn0dqmuFn/H4DEmKIDLlM1njR6Zsco8IYE4iBGRY4upUw6dNZPKW7P5h 5pLFLrhrReX/CGR+em/P/GNIbOiOuqalRqdKaW8o9Fs+

QARhkhD5qhQUO8CFH51UrHaeucTv9RIj6xUWIz9cDsPaukSczzu7baeH1zZwQFzn wRXz2CJNqiav5lj7OPCb9QNAWAumtoEFbcoFFG4fKaQOk

6TB+tQSwBKgxXTzCq4h70Qpqw+05/N9bcIcm8qE0Thc7AfwhOHQ13l7fysqdI3Em v3he5t4LLPP5tYxJ//jJIONfVJoCpYVGHifECVfd3D5xUHPu

s9kcYllTy+frJb969YY3vZuhTXPUzgvbAKDsAtmSddTS9PDQYEebecYDwU7samTe sdhfDodIlyBlP453hQT+ZbyQ8q3SAKzv7G+kgtwrdF1eY4n

=QVAW -----END PGP MESSAGE-----

CSDN @lmn_

对比我们导出的邮件□

更改一下我们收到的文件的格式，重命名为.asc文件，之后导入，输入我们新建时候的密码
解密成功

CSDN @lmn_

打开文件

访问链结后应该后会启动wechall的GPG加密功能，但不是直接copy链接！
后果就是这个

修改后缀为.html，访问链接，bling bling～

❓ | score: 2 | **2.89** **6.13** **4.65** | Solved By 1001 People | 61688 views | since Jan 08, 2011 - 16:24:20

Training: GPG (**Crypto**, **Training**)

GPG

✅ We have sent you an encrypted email to ▇.▇▇▇.▇ .com which contains the solution.

Crypto - GPG

In this challenge your goal is to setup gpg encryption for your emails.
To do so, generate your keypairs locally and store your public key on wechall.
Then all your mails sent by wechall are encrypted.
To enable GPG encryption, please goto Your account settings.
When you are done, click the button below to send you a mail.

Happy Challenging!

点击

[Send me encrypted mail please.] ⬅

Your solution for Training: GPG

Answer

[   ] [Submit]

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

进行二次解密

WeChall: GPG Challenge ☆

发件人: **robot** <robot@wechall.net> 📧
　　　　（由 wechall@wechall.net 代发）
时　间：2022年1月23日（星期日）下午5：13
收件人：▇ ▇　　　▇@qq.com>

🈶 邮件可翻译为中文 立即翻译

-----BEGIN PGP MESSAGE----- Version: GnuPG v2 hQIMA5Xs5ehK6QVxARAAiafzdtqa//pSVi6CPuVgi/Iz+ESI64toIrd46GcChLwP
zXAeN9bEEPC4vgHLNgJijTT7AjUfz1Pe4K03UVo3rbdXAemJPZ4oPE1YWLdB3aAM ijQQOfwoUo4l4a6UbINwFx3KeMlvSCd/iLHuBOUlj3FgceKQmUFBHF3PiOsdbUR0
rsZassR3OJSKxZamMKTp3vVTQXJoN66SIaf/mQygF/ZxeI2oExPkCqQFhhkqyvnM IQ8ED7B+54Xea6yE6XuKQaDo4erMWRagxyVrOPLWlvp1NEy8MWLCgms+Iprl+Dwe
Fc8ePrSZXYtkwVHIBVlCq33oitp/o8k2ce9mu6FTOAObHk1whIuKYjqnUThpH/7M 80praMCFjIUjbilK4pSL0sDt0ZPVs/GdIhLyQsaoFbzf3YbMi9fGVp64W84pcd3l
aLmIigJdmWzFxiA0DrjviNbmpH+UGerEgLbh9iDB+sTOW+hTRtBwVA0xpcUnBBS/ eTliy7EuYa0chSk28lpKtnoY+idEUz64JZN0yEwXsXNPW6Ic1FhAq9ufZaDLbnMM
f6a/0XjrEmqf/70eCiFuJBIelxcq/UpqnOLjsRWSVb5kuCmeHuV+VlXkeeYwqCA1 v6Yyow7UU+k5inaUPBSeo6jrKZXfLSpljc/ZSe8dk+m5aKUNJuokYQVuj5/wTTXS
wEMBv9IjF/GPYmWy0YCcFR9zGtQ9E2ZgdDCn8kNolK32x7+n3XG01kaa0WFg6iG8 BT2xEpjGD7/IJtvZOu+dKdBq4A6xTz2CyHwGc3bQ4FVGjSUQNKDAoYHwiIS7F2Dp
e9/K44UWVV1x6y6cQws1lT4UzOsCNgio8/PUNr9fZSHueUBL7D79SK/cDDR18gXU 7NzK4LJAJ6zYbkb2rSVyglwP2OOa+5TtgXmiRJuMte1su6Ecvycu7jF+CkEtt1C1
avBHrKzjWo8TuuVL6tftkI/GHfqsBYojYeFC9GiwsGAq6NxW0gjoqblBpHGlat9H suvDXbVLzJtViIrBR3ulExBE/tD0 =jN3f -----END PGP MESSAGE-----

快捷回复给：robot

■ 12   UNREGISTERED

◀ ▶   1   ×   12   ×   + ▼

1 <html>
2 <head>
3 <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
4 </head>
5 <body>
6 Dear lmn,

```
 7    <br />
 8    I just want to tell you the solution to the GPG challenge.<br />
 9    It is: OECNGSIRHNRI<br />
10    <br />
11    Kind Regards,<br />
12    The WeChall Bot!
13    </body>
14    </html>
15
```

虽然步骤繁多但是分值是2，不是太难，前提是要了解GPG，得到答案

I just want to tell you the solution to the GPG challenge.

It is: OECNGSIRHNRI

0x03 2 Limited Access by wannabe7331

? | score: 2 | **2.68** **4.61** **4.29** | Solved By 2378 People | 117287 views | since Jan 30, 2011 - 18:23:48

Limited Access (**Exploit**, **HTTP**)

Limited Access

I try to secure my pages with .htaccess.
Am I doing it right?

To prove me wrong, please access protected/protected.php.

© 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2021 and 2022 by wannabe7331

题目意思：
我尝试使用.htaccess保护我的页面。 我做对了吗？ 为了证明我错了，请访问 protected/protected.php。

```
GeSHi`ed Plaintext code for .htaccess

AuthUserFile .htpasswd
AuthGroupFile /dev/null
AuthName "Authorization Required for the Limited Access Challenge"
AuthType Basic
<Limit GET>
require valid-user
</Limit>
```

Apache 解决方案

在站点配置文件 .htaccess 中添加如下代码片段

```
<Location />
    <LimitExcept GET POST>
        Order Allow,Deny
        Deny from all
    </LimitExcept>
</Location>
```

为只允许GET/POST请求
为不允许允许GET请求

Request

Raw | Params | Headers | Hex

```
POST /challenge/wannabe7331/limited_access/protected/protected.php HTTP/1.1
Host: www.wechall.net
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:96.0) Gecko/20100101 Firefox/96.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,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
Connection: close
Cookie: WC=16312573-61988-KqvvFuGR8dPcdZy4
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
```

Target: https://www.wechall.net

Response

Raw | Headers | Hex | HTML | Render

```
href="/profile/livinskull">livinskull</a></div><div><a href="/profile/tehron">tehron</a></div><div><a
href="/profile/Donlon">Donlon</a></div><div><a href="/profile/Wyve">Wyve</a></div><div><a
href="/profile/mikeb">mikeb</a></div><div><a
href="/profile/b9e8a462697f9410b">b9e8a462697f9410b</a></div><div><a
href="/profile/dopelilcat23">dopelilcat23</a></div><div><a href="/profile/lordOric">lordOric</a></div><div><a
href="/profile/Silver">Silver</a></div><div><a href="/profile/kourekama">kourekama</a></div><div><a
href="/profile/kael">kael</a></div><div><a href="/profile/thr33go">thr33go</a></div><div><a
href="/profile/Topiary">Topiary</a></div><div><a href="/profile/BenShapiro">BenShapiro</a></div><div><a
href="/profile/shequy">shequy</a></div><div><a href="/profile/wraithax">wraithax</a></div><div><a
href="/users/with/All/by/user_lastactivity/DESC/page-1">more</a></div>
    </div>
</div>

        <div id="page">

<div class="gwf_messages">
        <span class="gwf_msg_t">WeChall</span>
            <ul>
            <li>Your answer is correct. Congratulations you have solved this challenge.<br/>Please <a
href="/challvotes/85/Limited+Access">vote this challenge</a>.<br/>You may also access <a
href="/forum-b181/Solution_Limited_Access.html">the solution board</a> for this challenge now.</li>

            </ul>
</div>
<div class="cl"></div>
<div class="gwf_messages">
        <span class="gwf_msg_t">WeChall</span>
            <ul>
            <li>You gained 0.31% (25 points) on WeChall.</li>

            </ul>
</div>
<div class="cl"></div>
<div class="box box_c">&copy; 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2021 and
```

访问my pages页面，burp抓包修改get为post

https://www.wechall.net/challenge/wannabe7331/limited_access/protected/protected.php

English | News | Links | Sites | Forum[2] | Ranking | Challenges | Account | PM | Downloads | Groups | Logout [lm

We Chall

New Sites
PWN.TN
PromptRiddle
PyDéfis
CryptoHack

247CTF
Énigmes À Thématiques
LordofSQLi
MysteryTwister

New Users
raccoon_fan | NerdBully
Silver | gwonblue
Wyve | daydayup2333
shyW | wwwhu

35 Online
Guest(x22), Donlon, Gr33nL10n(x2), livinskull, lmn(x2), LouisJ, mikeb, N

WeChall

Your answer is correct but you have already solved this challenge.
Did you vote for this challenge yet?

© 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2021 and 2022 by wannabe7331