




WeChall CTF Writeup (七)

原创

[lmn_](#)  于 2022-02-27 21:30:00 发布  172  收藏

分类专栏: [CTF](#) 文章标签: [CTF](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/weixin_43211186/article/details/123156534

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

[0x07 2 Repeating History by space and Gizmore](#)

[0x08 2 PHP My Admin by Gizmore](#)

[0x09 2 Training: Caterpillar by Gizmore](#)

以下题目标题组成:

[Score] [Title] [Author]

0x07 2 Repeating History by space and Gizmore

Repeating History (Research)

Repeating History

This challenge is about researching the [WeChall challenges](#) and the [GWF3 codebase](#).

I have put 2 passwords somewhere, but

where the hack did I put them?!

The first password is obvious and the second is very subversive. Both are near. Combine them without any separator.

Good luck on your research!

space and gizmore

Greets to [kwisatz](#). Thank you for motivation :)

Your solution for Repeating History

Answer

Submit

© 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2021 and 2022 by [space](#) and [Gizmore](#)

CSDN @lrmn_

题目意思：

这个挑战是关于研究WeChall 挑战和GWF3 代码库。

我在某个地方放了 2 个密码，但是...

我把它放在哪里了？！

第一个密码很明显，第二个很颠覆。两个都在附近。将它们组合在一起，无需任何分隔符。

WeChall challenges

Name	Last modified	Size
Parent Directory		-
addslashes/	2015-05-05 21:18	-
anto/	2015-05-06 01:44	-
are_you_serial/	2015-05-05 21:18	-
B.AiM/	2019-05-29 18:33	-
blind_light/	2019-02-21 18:03	-
blind_lighter/	2019-02-21 18:03	-
brainfucked/	2013-10-11 16:35	-
britcoin/	2018-03-20 12:25	-
bsdhell/	2015-05-06 01:44	-
burning_fox/	2015-05-05 21:18	-
can_you_readme/	2012-06-03 01:40	-
christmas2021/	2021-12-21 02:34	-
connect_the_dots/	2015-05-05 21:18	-
contribute/	2021-03-31 21:37	-
count_dont_wonder/	2012-06-03 01:38	-
crackcha/	2015-05-05 21:18	-
crappysshare/	2015-05-05 21:18	-
dloser/	2015-05-06 01:44	-
fixus/	2012-06-03 01:38	-
FREMES/	2015-05-05 21:18	-
gizcrypt/	2012-06-03 01:40	-
gizmore/	2021-01-02 20:07	-
guesswork/	2012-06-03 01:38	-
guestbook/	2012-06-03 01:40	-
hashgame/	2015-05-05 21:18	-
hi/	2012-06-03 01:38	-
Hirsch/	2015-05-06 01:44	-
hsec/	2011-12-29 23:42	-
htmlspecialchars/	2012-06-03 01:38	-
identity/	2015-05-05 21:18	-
illuminati/	2016-12-10 04:52	-
impossible/	2012-06-03 01:40	-

inka/	2020-09-07	23:59	-
interesting/	2014-04-19	18:47	-
Jander/	2015-05-06	01:44	-
Jinx/	2015-05-06	01:44	-
lamb/	2015-05-06	01:44	-
lettergrid/	2015-05-05	21:18	-
letterworm/	2015-05-05	21:18	-
livinskull/	2015-05-06	01:44	-
ludde/	2015-05-06	01:44	-
Mawekl/	2017-10-15	21:39	-
MD5.SALT/	2012-06-03	01:41	-
memorized/	2021-01-13	14:20	-
morsed/	2012-06-03	01:40	-
nippon/	2016-12-10	04:55	-
no_escape/	2015-05-14	22:54	-

CSDN @lrm_

GWF3 codebase

gizmore / gwf3 (Public)

Search or jump to... Pull requests 36 Issues 16 Actions Projects Wiki Security Insights

master 3 branches 0 tags

Go to file Add file Code

About
Gizmore Website Framework
Readme
27 stars
8 watching
19 forks

Releases
No releases published

Packages
No packages published

Contributors 8

Languages

猜测有一个答案可能放在那些目录下，看到uri已经告诉了该题的目录

[3][WeChall] Repeating History x [WeChall] WeChall x gizmore/gwf3: Gizmore Website x

wechall.net/challenge/subversive/history/index.php

应用 Gmail

English News Links Sites Forum[3]

We Chall

New Sites	New Users	New Users
WN.TN	247CTF	LePehtyDefi shyW
PromptRiddle	Énigmes À Thématiques	raccoon_fan NerdB
PyDéfis	LordofSQLi	Silver gwont
CryptoHack	MysteryTwister	Wyve dayda

? | score: 2 | 3.55 3.53 4.58 | Solved By 610 People | 62284 views | since Mar 13, 2012 -

Repeating History (Research)

Repeating History

This challenge is about researching the [WeChall challenges](#) and the [GWF3 codebase](#).

I have put 2 passwords somewhere, but

where the hack did I put them?!

The first password is obvious and the second is very subversive. Both are near. Combine them wi

Good luck on your research!
space and gizmore

Greets to [kwisatz](#). Thank you for motivation :)


Your solution for Repeating History

CSDN @Imn_

Oh right... the solution to part one is " without the PHP comments and singlequotes.

CSDN @Imn_

从github查看源码



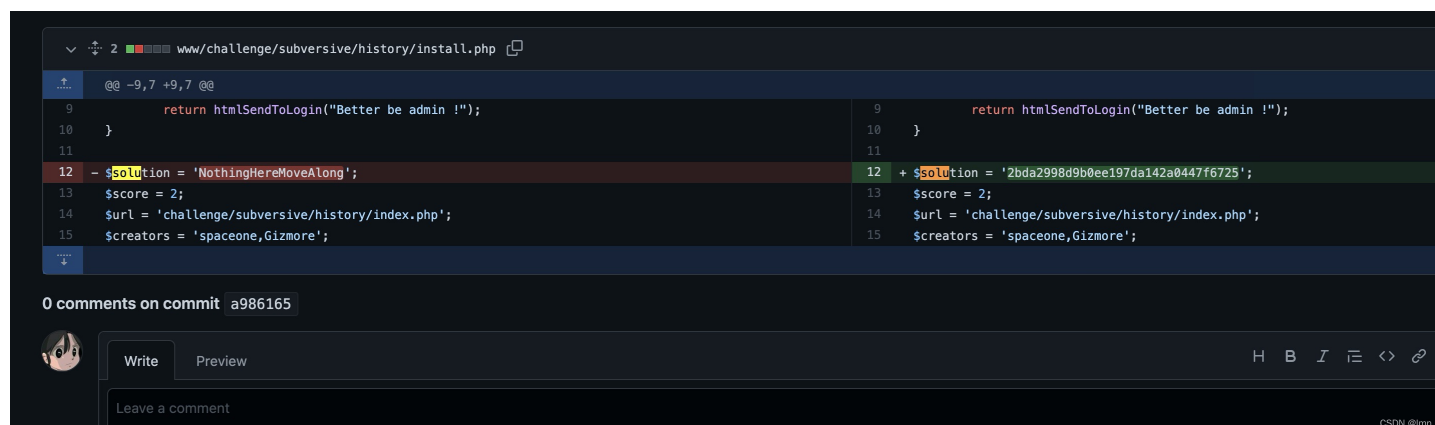
The screenshot shows a GitHub file view for the file `what_do_you_want_here.php` located at `gwf3 / www / challenge / subversive / repeating /`. The file is owned by `ricerbot` (Shadowlamb) and was last committed on 13 Mar 2012. It has 1 contributor. The file size is 115 Bytes and contains 1 line of code. The code content is: `<h1>Oh right... the solution to part one is '<?php /*InDaxIn*/ ?>' without the PHP comments and singlequotes.</h1>`. The interface includes a search bar, a 'Go to file' button, and a 'History' link.

第一部分：InDaxIn

题目叫Repeating History，那我们就从history里找另一个

搜索关键词：solution

因为第一部分为InDaxIn，是可以读懂的，第二部分也应该是可以读懂的



```
9         return htmlSendToLogin("Better be admin !");
10     }
11
12 - $solution = 'NothingHereMoveAlong';
13     $score = 2;
14     $url = 'challenge/subversive/history/index.php';
15     $creators = 'spaceone,Gizmore';
16
17 + $solution = '2bda2998d9b0ee197da142a0447f6725';
18     $score = 2;
19     $url = 'challenge/subversive/history/index.php';
20     $creators = 'spaceone,Gizmore';
```

第二部分：NothingHereMoveAlong

complete solution: InDaxInNothingHereMoveAlong

0x08 2 PHP My Admin by Gizmore



? | score: 2 | **3.47 2.97 3.00** | Solved By 613 People | 137127 views | since Mar 18, 2012 - 15:43:05

PHP My Admin (Research)

PHP My Admin

Your mission here is easily explained:
Find the hidden PHPMyAdmin page which is used by the admins to maintain the database on the wechall server.

We are awaiting your success.
Good Luck!

© 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2021 and 2022 by [Gizmore](#)

题目意思：

找到隐藏的 PHPMyAdmin 页面，管理员使用该页面来维护微信服务器上的数据库。

就很巧，突然时候发现一句

 | score: 2 | **3.47** **2.97** **3.00** | [Solved By 613 People](#) | 137127 views | since Mar 18, 2012 - 15:43:05

PHP My Admin (Research)

 My Admin

Your mission here is easily explained:

Find the hidden PHPMyAdmin page which is used by the admins to maintain the database on the wechall server.

You don't need a hint, do you?

We are awaiting your success.

Good Luck!

© 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2021 and 2022 by [Gizmore](#)

CSDN @lmm_

Don't need? I need hint more than anyone else!

根据大佬的思路，在Forums里面看到Evil的留言

WeChall Forums Polls

WeChall -> Challenges -> Challenge: PHP My Admin

Title	Creator	Posts	Reply From	Last Post	Thx	VoteUp	Views
Test	ConstantinHaxx	1	ConstantinHaxx	Jul 14, 2020 - 21:05:53	1	1	743
Hint	GroM	1	GroM	Jun 03, 2020 - 14:28:39	1	1	1030
Evil	kkoliver	10	l3st3r	Aug 13, 2018 - 12:57:54	19	17	22608
zentinel	zentinel	1	zentinel	May 31, 2016 - 04:43:24	1	1	4914

Subscribe

CSDN @lmm_

Here you got it!

gizmore
Global Rank: 238
Totalscore: 86235
Posts: 1456
Thanks: 1268
UpVotes: 788
Registered: 13y 343d

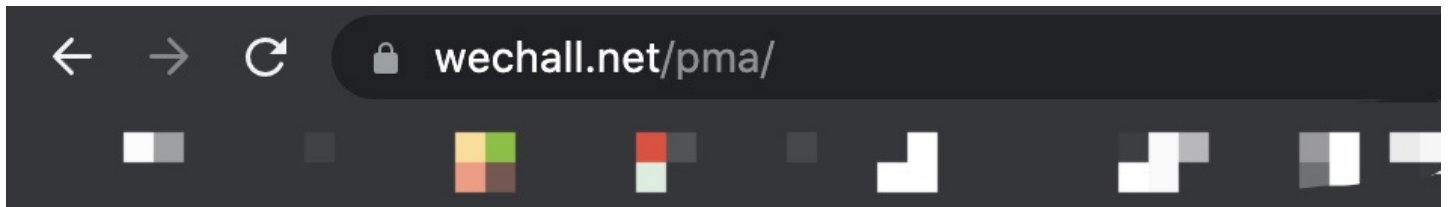
RE: Evil
Dec 28, 2012 - 20:22:10 (9y 28d)

Not really, but it's very obvious with the hint.
I chose a very common name, and there might be little quirk/gotcha... but many people got it straight away.
It actually was the real setup i chose when there was a **pma** on this box a few months ago 😊

Happy Holidays!
gizmore

The geeks shall inherit the properties and methods of object earth.

CSDN @lmm_



You are searching for PMA?
Not on this subdomain, buddy!

CSDN @lmm_

不在这个子网域，然后，you got it

[WeChall] Challenge(s) Overview [WeChall] Training: Caterpillar https://pma.wechall.net

不安全 | https://pma.wechall.net

```
<html>
<body>
1:266:Your answer is correct. Congratulations you have solved this challenge.<br/>Please <a href="/challengevotes/113/PHP+My+Admin">vote this challenge</a>.<br/>You may also access <a href="/forum-b241/Solution_PHP_My_Admin.html">the solution board</a> for this challenge now.
1:40:You gained 0.31% (29 points) on WeChall.
</body>
</html>
```

CSDN @lmm_

0x09 2 Training: Caterpillar by Gizmore

? | score: 2 | [4.49](#) [3.62](#) [3.36](#) | [Solved By 349 People](#) | 52214 views | since Apr 01, 2012 - 17:27:13

Training: Caterpillar (Stegano)

Caterpillar

I have drawn a picture of an caterpillar and hid some text in it.
I am sure you can figure it out, as it is not too hard :)



Happy Challenging!

Your solution for Training: Caterpillar

Answer

Submit

© 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2021 and 2022 by [Gizmore](#)

CSDN@lmm_

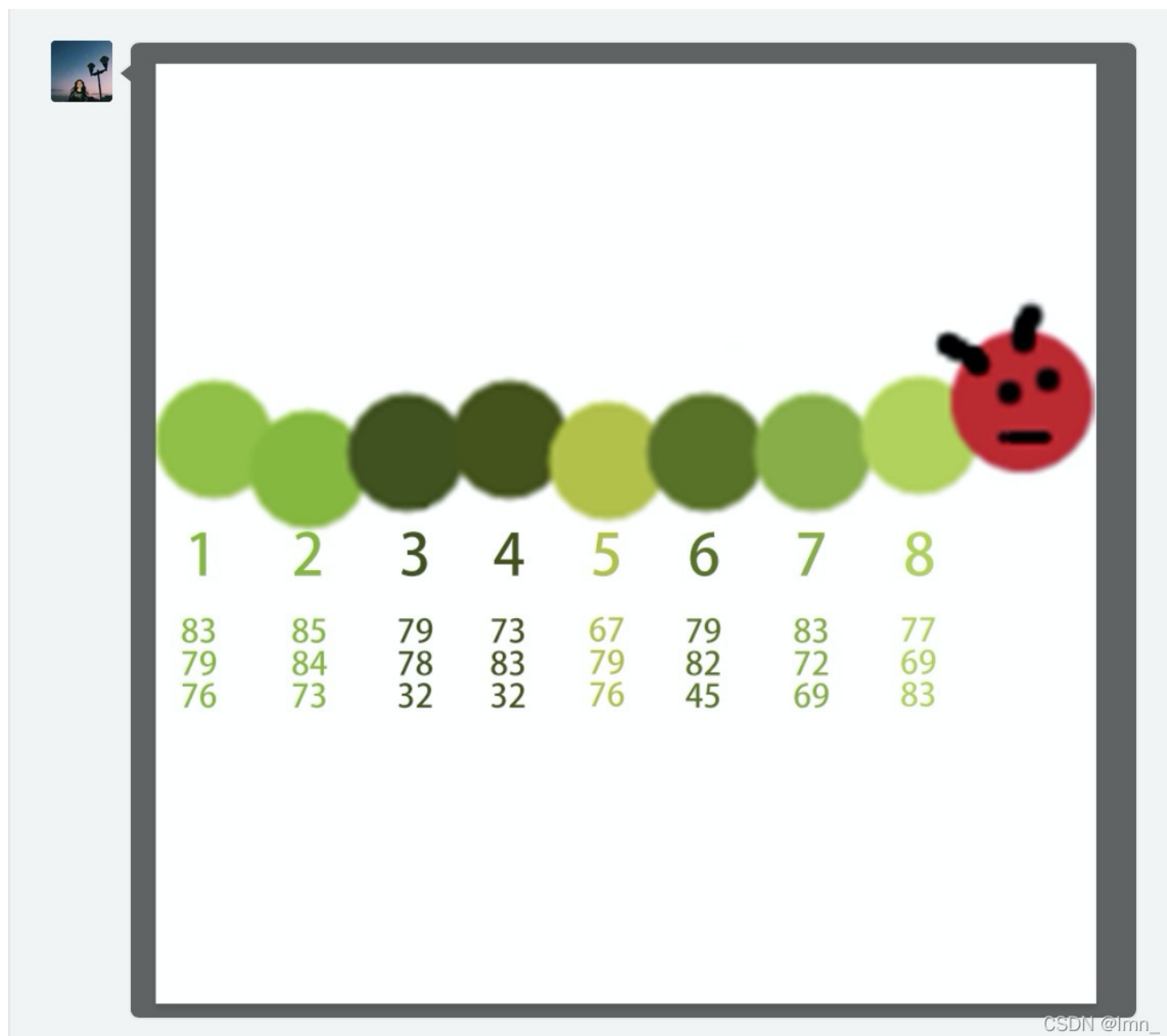
题目意思:

我画了一张毛毛虫的照片，并在其中隐藏了一些文字。

我相信你能弄明白，因为它不是太难:)

因为没有思路，借鉴了一下https://blog.csdn.net/qq_34626094/article/details/113127312的wp

找到图片8个球的HSB值（可惜我没有photoshop，找闺蜜一把梭哈）



```
what_do_you_want_here.php x 1.py x
1 HSB = [83,79,76,85,84,73,79,78,32,73,83,32,67,79,76,79,82,45,83,72,69,77,69,83]
2 ans = ''
3 for c in HSB:
4     ans+=chr(c)
5 print(ans)

SOLUTION IS COLOR-SHEMES
[Finished in 136ms]
```

CSDN @Imn_

solution: COLOR-SHEMES