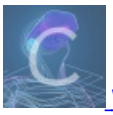
WeChall-writeup-2-11.10

原创

MeliodasC 于 2018-11-13 21:33:33 发布 572 收藏

分类专栏： WeChall 文章标签： WeChall writeup 安全

本文链接：https://blog.csdn.net/Crystal_bing/article/details/84036481



是的，连着上一篇又发了这篇2333也是几天前攒的。我觉得在整个学习过程中，与同伴的交流还是很重要的，如果你的身边没有可以讨论的小伙伴，那就借助互联网的力量来进行思维的碰撞吧~我写的解法也不一定是唯一正确的，如果有更好的方式请来告诉我鸭！上正题。

Training: Programming 1

题目很明确，在链接种获得一个message，然后提交这个message。但是题目中给了限时，不可能用人工的方式去做。所以借助python来完成这个过程。直接Python访问的话需要登陆。所以要先拿到浏览器的Cookie，再利用这个Cookie访问url_1。

```
import requests

url_1 = "http://www.wechall.net/challenge/training/programming1/index.php?action=request"
url_2 = "http://www.wechall.net/challenge/training/programming1/index.php?answer="
c = {"WC":"10953709-43921-CeH3AfwZyWHsqBHU"}
a = requests.get(url_1 , cookies = c)
key = a.text
requests.get(url_2 + key , cookies = c)
```

友情链接：
PyCharm 安装教程（Windows）：
http://www.runoob.com/w3cnote/pycharm-windows-install.html

Training: Regex（Level 1）

首尾直接相连即为空。

Training: Regex（Level 2）

匹配wechall。

Training: Regex（Level 3）

. -> 转义
(?:pattern) -> 非获取匹配
匹配pattern但不获取匹配结果，不进行存储供以后使用。这在使用或字符“(|)”来组合一个模式的各个部分时很有用。例如“industr(?:y|ies)”就是一个比“industry|industries”更简略的表达式。

Training: Regex（Level 4）

捕获文件名，没有扩展名。

Training: PHP LFI

（首先学习一下LFI漏洞）本地文件包含漏洞（Local File Include），是php的include()函数存在设计缺陷.
回到题目，尝试直接打开给的链接发现没有权限去打开这个PHP文件。所以需要依靠把…/solution.php传到 index.php?file=，通过index.php来做打开文件的操作。
发现是传参以后会被加上.html导致错误，结合作者的提示（灰色的注释），在最后加上%00（在URL中）
尝试 ?file=…/solution.php%00，不通过。
再向上一级 ?file=…/…/solution.php%00，通过。

PHP 0817

观察给出的代码，case0和1中都没有给出。给出的任务是访问solution.php。尝试直接把参数赋为solution，通过。

Training: Math Pyramid

首先算出这个数学题的公式，如果按照我最初写的公式结合提示，答案会是这样：sqrt(2)/3*a^3。从数学界角度上来说没有什么问题，但是不符合题目的要求：9个字符以内。
经过化简和不听题目的提示【误】，我最终化出了这样的式子：(哈哈自己尝试化一下啦)

有趣的链接：师傅们写的各种式子(可以去找灵感喔）