2019--国赛--第一次参加线上赛的自己的整理

原创

没有任何buff的小菜鸡 于 2019-05-07 15:31:44 发布 382 收藏 1

分类专栏： 比赛

本文链接：https://blog.csdn.net/weixin_44307072/article/details/89922116

比赛 专栏收录该内容

1 篇文章 0 订阅

订阅专栏

misc第一题：签到

打开压缩包，发现一个exe文件和一个txt，要三个人一起站到摄像机，然后等软件识别，就出flag了

但是我发现，你拿手机放一张照片（有三个人或比三人多）上去也可以出flag，所以推测出，该软件是甄别像素点来进行识别的

misc第二题：saleae

下载压缩包，得到一个.logic的程序，都是新东西，没人知道这是用什么软件来打开的，我发现这个特别考百度能力（捂脸）就是需要logicdata软件

下载后，发现其中给的是波形

然后去百度，发现这个软件是与芯片的输入输出有关，（后面是可以利用旁边的软件来读取flag的）

当时的我们没发现这个好办法，只能是0101010101的将flag读出来，然后进行转换成字符串

misc第三题：24C

与第二题类似，但是需要一点脑洞，就是记得改变它的读取顺序就好了

crypto第一题：puzzle

首先是给了一个网站，心想还是不是web+密码，那就有点…舒（zi）适（nue）了吧

让我深深的感受到数学的重要性，三重积分还没学的我，简直看的如痴如醉，第一题的素数来找规律，让我懵逼好久，这是什么题哦

所有的一切都是从0开始的感觉，于是就开启了自学之旅

提示一下：1、question0 记得化简运算，当然网上也有计算器（当时死算到无奈，后面还错了）

```
2、question1就是分组找规律，与素数有关

3、question2是做的最舒服的一道题，简简单单的高数上的计算

4、question4是高中的知识，不过用一下大学的思想就就是大物的东西了，记住公式就没啥大问题了

5、question5是三重积分，与二重积分类似，具体自己去算
```

总而言之，这一道题就是叫你好好的去学习高数，一定要认认真真学习高数

misc第3题：useasp

鬼知道这是东西哦，不过经过昨天的一道题发现，继续使用那个logicdata的软件，就可以了

首先，将文件拖入软件中，然后果然出现了波形

昨天那道题，是对照着题目一道一道念的，010101010101来着，结果，今天发现了一个神奇的地方，在logicdata的右部分中间，可以发现analyzers右边的加号，点进去，有个SPI，根据芯片的一些特性，确定时间线，MOSI和MISO的行，点击确定，就可以得到一个特别长的“flag”

很可惜，这是个陷阱，就是假的flag，flag{you-know-it-can-not-be-such-easy}

于是我们进行了多种尝试，利用这个软件其他的一些工具进行解码，结果一无所获，但是，后来我们决定修改参数，因为之前的配置是可以得出flag的，于是猜测要更改SPI的某个特殊点。

更改SPI的某个特殊点后，进行一个对照，发现只有将setting中最后的一个参数，改成high值，原屏幕的右下角就出现了flag。

web第一题

Just so so

开始时，用伪协议拿到源码，然后就是反序列化利用了

<?php index.php error_reporting(0); $file = $_GET["file"]; $payload = $_GET["payload"]; if(!isset($file)){ echo 'Missing parameter'.' '; } if(preg_match("/flag/",$file)){ die('hack attacked!!!'); } @include($file); if(isset($payload)){ $url = parse_url($_SERVER['REQUEST_URI']); parse_str($url['query'],$query); foreach($query as $value){ if (preg_match("/flag/",$value)) { die('stop hacking!'); exit(); } } $payload = unserialize($payload); }else{ echo "Missing parameters"; } ?> hint.php <?php class Handle{ private $handle; public function __wakeup(){ foreach(get_object_vars($this) as $k => $v) { $this->$k = null; } echo "Waking up\n"; } public function __construct($handle) { $this->handle = $handle; } public function __destruct(){ $this->handle->getFlag(); } }
class Flag{
public $file;
public $token;
public $token_flag;

```
function __construct($file){
 $this->file = $file;
 $this->token_flag = $this->token = md5(rand(1,10000));
}

public function getFlag(){
 $this->token_flag = md5(rand(1,10000));
    if($this->token === $this->token_flag)
 {
  if(isset($this->file)){
   echo @highlight_file($this->file,true);
        }
    }
}
```

}
?>

大佬说： 可以看到Handle类有个__destruct函数，该函数可以触发getFlag函数，但是__wakeup函数会将所有东西清空，这里改下属性个数就能绕过，参考SugerCRM漏洞，然后getFlag函数的条件可以用指针绕过，以前安恒的月赛也考过，最后flag的匹配可以利用parse_url漏洞，三个斜杠就能绕过了

exp

View Code

以上web题参考了琳姐姐的博客，谢谢琳姐姐的指导~~：

https://xi4or0uji.github.io/2019/04/22/2019-4-22-2019-全国大学生信息安全竞赛-writeup/#more

总结：本次比赛只是做了misc的题，web的题目打的也太少了，要继续加油，多进行php的审计，同时多做一些web题总结经验，下次争取多打几道web题