2021-3-15 misc+web

原创

ProbeN1 于 2021-03-15 22:09:23 发布 152 收藏

分类专栏： CTF

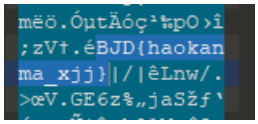
本文链接：https://blog.csdn.net/m0_51792282/article/details/114851955

[BJDCTF 2nd]小姐姐-y1ng

是这样的，馋她身子，但是为什么，这里被切了一刀

。。。一千年以后。。。

是我多虑了



以后不要只搜索flag了

呜呜呜

[BJDCTF 2nd]圣火昭昭-y1ng

我去，在属性里
找得我猝不及防

与佛论禅，没参透。。。
搜了半天找到个新佛曰的，这回参透了
http://hi.pcmoe.net/buddha.html
解密出gemlovecom，按提示去掉com，交flag
失败，知道为啥失败吗？
因为太菜了（笑哭）
有一款隐写工具outguess

这里是安装
https://www.cnblogs.com/2f28/p/9740347.html
-r 解密
-k '密码'
1.txt 输出文件

```
root@kali:~/桌面# outguess -r 1.jpg -t 1.txt
Reading 1.jpg....
```

> wdnmd_misc_1s_so_Fuck1ng_e@sy

[GKCTF2020]cve版签到

也就会做个签到题了
在题目上hint1：cve-2020-7066
查？
查！
卧槽直接查到了writeup。。。
）（略过）（

> PHP
> 7.2.29之前的7.2.x版本、7.3.16之前的7.3.x版本和7.4.4之前的7.4.x版本中的'get_headers()'函数存在安全漏洞。攻击者可利用该漏洞造成信息泄露。

一个有关这个复现的博客
https://www.cnblogs.com/Ky1226/p/14332110.html

> ?url=http://127.0.0.1%00www.ctfhub.com

提示必须以123结尾
那就改！

> ?url=http://127.0.0.123%00www.ctfhub.com

Ohhhhhh

[GKCTF2020]CheckIN

```
<title>Check_In</title>
<?php
highlight_file(__FILE__);
class ClassName
{
        public $code = null;
        public $decode = null;
        function __construct()
        {
                $this->code = @$this->x()['Ginkgo'];
                $this->decode = @base64_decode( $this->code );
                @Eval($this->decode);
        }

        public function x()
        {
                return $_REQUEST;
        }
}
new ClassName();
```

构造函数

__construct()

```
function __construct( $par1, $par2 ) {
   $this->url = $par1;
   $this->title = $par2;
}
```

> $runoob = new Site('www.runoob.com', '菜鸟教程');

主要用来在创建对象时初始化对象， 即为对象成员变量赋初始值，在创建对象的语句中与 new 运算符一起使用。

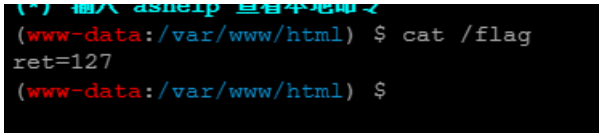
传参Ginkgo，值为base64化的php语句

来个一句话

> ZXZhbCgkX1BPU1RbYV0pOw==

直接连，成功！

个锤子！



这是什么？？？

> 这是一个没有找到命令的错误返回值

大意。。。权限不够

wdnmd，睡觉

晚安