线上ISCC2018 wp 部分writeup解题思路[xueqi]

原创

h2cf 于 2019-04-16 14:52:19 发布 809 收藏 1
分类专栏： CTF

2018年五月份开始的 一年一届的iscc 2018 ctf大赛全国赛区，线上比赛！此为部分解体思路过程

一、WEB

1.Web 比较数字大小

重点在这里，修改为4，提交9999.，拿到flag

2.web01

PHP弱类型 用数组绕过

3.web本地的诱惑

小明扫描了他心爱的小红的电脑，发现开放了一个8013端口，但是当小明去访问的时候却发现只允许从本地访问，可他心爱的小红不敢让这个诡异的小明触碰她的电脑，可小明真的想知道小红电脑的8013端口到底隐藏着什么秘密(key)?

这什么套路！？

4.web你能跨过去吗

Key Words:XSS

如果你对xss了解的话,那你一定知道key是什么了，加油！

```
http://www.test.com/NodeMore.jsp?
id=672613&page=2&pageCounter=32&undefined&callback=%2b/v%2b%20%2bADwAcwBjAHIAaQBwAHQAPgBhAGwAZQByAHQAKAAiAGs
AZQB5ADoALwAlAG4AcwBmAG8AYwB1AHMAWABTAFMAdABlAHMAdAAlAC8AIgApADwALwBzAGMAcgBpAHAAdAA%2bAC0-&_=1302746925413
```

这链接什么意思，看着中间是base64，试试对链接url解码复原

```
http://www.test.com/NodeMore.jsp?id=672613&page=2&pageCounter=32&undefined&callback=+/v+
+ADwAcwBjAHIAaQBwAHQAPgBhAGwAZQByAHQAKAAiAGsAZQB5ADoALwAlAG4AcwBmAG8AYwB1AHMAWABTAFMAdABlAHMAdAAlAC8AIgApADw
ALwBzAGMAcgBpAHAAdAA+AC0-&_=1302746925413
```

选择 base64部分

```
ADwAcwBjAHIAaQBwAHQAPgBhAGwAZQByAHQAKAAiAGsAZQB5ADoALwAlAG4AcwBmAG8AYwB1AHMAWABTAFMAdABlAHMAdAAlAC8AIgApADwA
LwBzAGMAcgBpAHAAdAA+AC0-
```

base64解码 得到

<script>alert("key:/%nsfocusXSStest%/")</script>-

5.Web一切都是套路

手动猜测index.txt / flag.txt .发现存在index.php.txt

变量覆盖漏洞

将$_200的值覆盖为$flag。post提交

二、MISC

1.What is that？ 文件：ISCC-MISC05

什么意思？百度了下图片隐写，实施改图片宽高。

软件：winhex 导入WhatIsThat.png分析

修改高度

为02保存得到flag

2.数字密文

69742773206561737921 看了半天也看不出来是什么加密。

想了半天试试base16吧，然后就得到flag

3.秘密电报

知识就是力量 ABAAAABABBABAAAABABAAABAAABAAABAABAAAABAAAABA

培根密码加密的，解密拿到flag

4.重重谍影

用base64解码多次，解到这样解不下去了

到这个程度，把%0A替换为回车，咨询了大佬，aes了解下，得到

答案就是后面这句但已加密

缽娑遠呐者若奢顛悉呐集梵提梵蒙夢怯倒耶哆般究有栗

佛曰密码,解密网站

未完待更。。。。

2018-07-26 转载请注明作者[Xueqi]与出处！