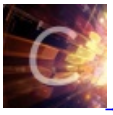
CTF【每日一题20160608】

转载

hhhparty 于 2016-06-10 11:26:41 发布 2387 收藏 1
分类专栏： CTF 文章标签： ctf编程


CTF 专栏收录该内容
20 篇文章 0 订阅
订阅专栏

简单编程-字符统计

点这个链接 → http://ctf.idf.cn/game/pro/37

你会看到题目，要快速提交答案哦，刷新后内容会变，所以编个程序读网页，再计算。

分析：

发现网上有人解决的不错，我就不多言了。

网上的解法1：【java程序实现】

一开始以为只要简单统计好了，后来一看，发现竟然写着要2秒内提交。。。好吧，没注意到，于是决定用HttpWebRequest来完成。用httpwatch抓包，出来个post提交的数据是answer=？，怪我功底不好，不论怎么改代码，数据都post不上去啊。。。郁闷了

想到之前做过一个软件，用的是webBrowser，试试看吧，代码如下：

```
<pre name="code" class="java">using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Text;
using System.Windows.Forms;
using System.Web;
using System.Net;
using System.IO;

namespace 简单字符统计
{
 public partial class Form1 : Form
 {
  public Form1()
  {
   InitializeComponent();
  }

  public string getWord(string str)
  {
   int w = 0, o = 0, l = 0, d = 0, y = 0;
   char[] ch = str.ToCharArray();
   for(int i = 0; i < str.Length; i++)
```

```
   for(int i = 0; i < ch.Length; i++)
   {
    if (ch[i] == 'w') w++;
    if (ch[i] == 'o') o++;
    if (ch[i] == 'l') l++;
    if (ch[i] == 'd') d++;
    if (ch[i] == 'y') y++;
   }
   return w + "" + o + "" + l + "" + d + "" + y;
  }

  private void button2_Click(object sender, EventArgs e)
  {
   webBrowser1.Navigate("http://ctf.idf.cn/game/pro/37/index.php");
  }

  public int flag = 1;
  private void webBrowser1_DocumentCompleted(object sender, WebBrowserDocumentCompletedEventArgs e)
  {
   StreamReader getReader = new StreamReader(this.webBrowser1.DocumentStream, System.Text.Encoding.GetEncod
   string gethtml = getReader.ReadToEnd();
   int a = gethtml.IndexOf("<hr />");
   int b = gethtml.LastIndexOf("<hr />");
   gethtml = gethtml.Substring(a + 6, b - a - 6);

   HtmlDocument web = webBrowser1.Document;
   //获取web页面控件
   HtmlElement Anwser = web.All["anwser"];
   Anwser.SetAttribute("value", getWord(gethtml));

   HtmlElementCollection bn = webBrowser1.Document.GetElementsByTagName("input");//填充
   foreach (HtmlElement btn in bn)//接管按钮
   {
    if (btn.GetAttribute("value") == "走你! " && flag==1)
    {
     btn.InvokeMember("click");
     flag = 0;
    }
   }
  }
 }
}
```

成功了，感动得作者热泪盈眶。

提交，通过！

解法2，用python程序计算

参考http://blog.csdn.net/u012241633/article/details/45766281的解法，小改一了下。

这个程序不仅要抓网页内容、用post方法提交request、获取response，还特别要注意cookie的使用，服务器用cookie来区别用户，所以提交时要验证cookie的，不匹配的任务不是你做的。

```
# -*- coding: utf-8 -*-

import urllib
import urllib2
import string
import re
import cookielib
#需要提交post的url
TARGET_URL = "http://ctf.idf.cn/game/pro/37/"
'''
不拿cookie不行
wp = urllib.urlopen(TARGET_URL)
content = wp.read()
'''
# 设置一个cookie处理器
req = urllib2.Request(TARGET_URL)
cj = cookielib.CookieJar()
opener = urllib2.build_opener(urllib2.HTTPCookieProcessor(cj))
res = opener.open(req)
content = res.read()



ct = re.findall(r'<hr />(.*)<hr />',content,re.S)[0]
print ct #看看抓到的内容对不对
#计算ct中的w,o,l,d,y
wn = ct.count('w')
on = ct.count('o')
ln = ct.count('l')
dn = ct.count('d')
yn = ct.count('y')
result = str(wn)+str(on)+str(ln)+str(dn)+str(yn)
print result
# 提交
'''
网页提交处源代码
<form action="" method="post">
 <p>答案: <input type="text" name="anwser" /></p>
 <input type="submit" value="走你! " />
</form>

'''
value = {'anwser': result} #input name is 'anwser'
data = urllib.urlencode(value)
request = urllib2.Request(TARGET_URL,data)
response = opener.open(request)  #urllib2.urlopen(request)#
r = response.read()

f=file('response.html','w+')
print >> f,r
#之后看response.html中的key，提交即可
```