IDF实验室WriteUp

原创

Turisla 于 2015-05-12 11:09:09 发布 7376 收藏
分类专栏： 非安全 文章标签： idf实验室

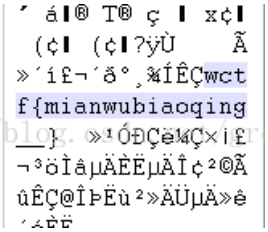
----------小试牛刀----------

第一题 被改错的密码

题目给出一个类似于MD5码的字符串，cca9cc444e64c8116a30la00559c042b4。熟悉MD5的童鞋应该很容易就能看出其中的猫腻，中间有一个怪异的l。再数一下字串的长度是33，刚好比标准MD5的长度多一。去掉l以后将MD5转化为明文。得解。

第二题 啥？

题目只给出一个图片，下载之。用WinHex打开，搜索“ctf”发现



得解。

第三题 ASCII码而已

打开题目发现是一堆Unicode码。使用python转换一下：

```
>>> string =  u'\u5927\u5bb6\u597d\uff0c\u6211\u662f\u0040\u65e0\u6240\u4e0d\u80
fd\u7684\u9b42\u5927\u4eba\uff01\u8bdd\u8bf4\u5fae\u535a\u7c89\u4e1d\u8fc7\u767e
\u771f\u7684\u597d\u96be\u3002\u3002\u0077\u0063\u0074\u0066\u007b\u006d\u006f\u
0072\u0065\u006d\u006f\u0072\u0065\u005f\u0077\u0065\u0069\u0062\u006f\u005f\u00
66\u0061\u006e\u0073\u007d'
>>> print string
大家好，我是@无所不能的魂大人！话说微博粉丝过百真的好难。。wctf{moremore_weibo_fans}
>>>
```


得解。

第四题 摩斯密码

题目已经说的很清楚了，就是摩斯码。可以找对照表自己解码，也可以去网上找一个在线破解。得到两个单词。按照题目要求的格式提交，得解。

第五题 聪明的小羊

从题目中提示中多次出现的“栅栏”一词可以猜测是栅栏密码。

用java写了一段解码：

```
String string = "tn c0afsiwal kes,hwit1r  g,npt  ttessfu}ua u  hmqik e {m,  n huiouosarwCniibecesnren.";
  int len = string.length();
  for (int i = 0; i < 17; i++) {
   for (int j = 0; j < 5; j++) {
    System.out.print(string.charAt(j * 17 + i));
   }
  }
```

得解。

----------天罗地网----------

超简单的js：

二话不说，查看网页源代码。发现变量用url加密过。使用unescape解码并输出，可以看到简单逻辑。

```
function checkSubmit(){var a=document.getElementById("password");if("undefined"!=typeof a)
{if("4a33f9960a70cf7f947b249fea845d0c"==a.value)return!0;alert("Error");a.focus();return!1}}document.getElementById("levelQuest").onsubmit=checkSubmit;
```

由此可知，密码为4a33f9960a70cf7f947b249fea845d0c，输入后得到flag。

古老邮件：

详见：http://blog.csdn.net/greyfreedom/article/details/45061851

一种编码而已：

打开题目发现给的是一坨编码，很明显是jother编码。在网上找一个在线解码网站解码即可。

jother编码详见：http://blog.csdn.net/greyfreedom/article/details/45070667

你关注最新的漏洞吗：

题目给出一个文件，使用wireshark打开后发现是用了kerberos。于是去百度一下kerberos最新的漏洞。得知漏洞名为MS14-068。得解。

简单的js加密：

打开给的题目链接，照例先看源代码。发现源代码中有个伪MD5加密函数，其实就是以ascii码128位界，把两边的调换了一下而已。把脚本拿到本地，并且补充解密函数。根据加密函数来写解密函数并不难。以下是完整的加解密函数。

```
<script>
/**
 * Pseudo md5 hash function
 * @param {string} string
 * @param {string} method The function method, can be 'ENCRYPT' or 'DECRYPT'
 * @return {string}
 */
function pseudoHash(string, method) {
  // Default method is encryption
  if (!('ENCRYPT' == method || 'DECRYPT' == method)) {
    method = 'ENCRYPT';
  }
  // Run algorithm with the right method
  if ('ENCRYPT' == method) {
    // Variable for output string
    var output = '';
    // Algorithm to encrypt
    for (var x = 0, y = string.length, charCode, hexCode; x < y; ++x) {
      charCode = string.charCodeAt(x);
      if (128 > charCode) {
        charCode += 128;
      } else if (127 < charCode) {
        charCode -= 128;
      }
      charCode = 255 - charCode;
      hexCode = charCode.toString(16);
      if (2 > hexCode.length) {
        hexCode = '0' + hexCode;
      }

      output += hexCode;
    }
    // Return output
    return output;
  }
//----------------------------------------以下是解密部分-----------------------------------------
  else if ('DECRYPT' == method) {
    var destring = '';
    for (var i = 0; i < string.length - 1; i=i+2) {
      strCode = string.substring(i,i+2);
      var strInt = parseInt(strCode,16);
      strInt = 255 - strInt;
      if (strInt > 127) {
        strInt -= 128;
      }else if (strInt < 128) {
        strInt += 128;
      }
      destring += String.fromCharCode(strInt);
    }
    return destring;
  }
}
document.write(pseudoHash('4a191b4f4d4b4a19491c461b1b1d1b194c1a19194f194a4f4a46484a1d491e48','DECRYPT'));
// document.getElementById('password').value = pseudoHash('4a191b4f4d4b4a19491c461b1b1d1b194c1a19194f194a4f

</script>
```

将题目给的那段4a191b4f4d4b4a19491c461b1b1d1b194c1a19194f194a4f4a46484a1d491e48 解密后为

5fd0245f6c9ddbdf3eff0f505975b6a7。提交，得解。

----------**包罗万象**----------

图片里的英语：

从题目中可以看出，在图片中包含有东西。到底是啥东西呢，还得一步一步解开。首先用WinHex打开图片，找了半天发现并没有什么。。。。。于是乎只能将图片后缀名改为.rar。结果得到另一张图片。打开一看，是本山大叔《大笑江湖》的剧照。。自然那句英语就是May the force be with you.得解。

如何将压缩文件放入图片中，详情请看压缩文件放入图片，点我