GDUFS-CTF新手赛划水记录

原创

Cymbals 于 2018-11-12 13:24:58 发布 394 收藏
分类专栏： 瞎写 文章标签： ctf

昵称：后缀自动机Parent树上启发式合并

Solves

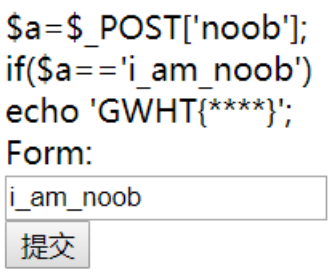
Challenge	Category	Value	Time
Web1水题	Web	20	November 11th, 2:00:55 PM
Web水题2	Web	20	November 11th, 2:21:46 PM
水题Web5	Web	20	November 11th, 3:27:29 PM
W水题eb4	Web	20	November 11th, 3:33:39 PM
We水题b3	Web	20	November 11th, 3:36:27 PM
贝斯	Misc	50	November 11th, 4:35:10 PM
你是萌新吗?	Misc	200	November 11th, 10:34:24 PM
RE1	RE	50	November 12th, 12:08:23 AM
simple_re	RE	250	November 12th, 2:09:35 AM

650分签到。
ctf也太快乐了吧！

应主办方要求写WriteUp。

web水题1：
右键查看源代码，flag get。

web水题2：
看到了一段接收表单就echo flag的php代码。写了个表单，填了个叫noob的参数，提交，flag get。



web水题3：
给了一张饼干图。第一反应下载下来后缀改成rar打开，然后打开失败了。然后才反应过来是cookie。查看cookie看到一条…乱码？由于没有其他线索猜测要解密，百度了一下觉得可能是Base64。找了个在线解密，结果提示解密失败，并且输出一堆乱码，差点以为凉了，叉出去之前在乱码里看到了flag，get。

web水题4：
点开之后跳转到了比赛首页…懵逼之后猜测这一定是假的网站，查看源码后发现卧槽，这是真的。回头去查看了点进来那个按钮的源码，发现并不是我打开的那个网站。再开一次，卧槽，竟然是跳转。然后再开了一次快速点下了浏览器的停止加载阻止了跳转。查看源码，flag get。

web水题5：
又是一段php代码。仔细看了一下，好像是个登录界面，感觉突破口应该在哈希算法上。于是百度sha1漏洞，然后就找到了原题…
原来可以用数组撞破，把链接后面加上：

```
/?name[]=1&password[]=2
```

flag get。

RE1：
下载下来一个exe，双击执行，执行失败，？？？？
右键edit with notepad++，卧槽，flag get。

simple_re：
又下载下来一个exe，双击运行，让我输入flag？没有啊，告辞。
然后发现这是一个C#窗体…想起来昨天忽然有人问我C#怎么反编译，然而他并不告诉我为啥他要问这个，好的，现在我知道了，ilspy启动！
找到窗体主程序部分，发现一个意☆义☆不☆明的Hash函数，找到了获取flag的方法，hash结果逆向可以求出flag。
感觉他在前面疯狂暗示我用md5，然而解密失败，只好自己去写程序暴力破解。
想了一下好像可以写个dfs枚举，但是太晚了懒得思考，先敲个暴力再说。我猜flag的前面肯定是“GWHT{”，所以先填上这些，然后$O(n^3)$在ASKII可见字符范围内暴力枚举，一次枚举3位，然后从中取两位有效的，每求出两位就终止程序，改改代码调调参继续枚举下一个。

```
for(int i = 32; i <= 126; i++) {
 get.push_back((char)i);
 for(int j = 32; j <= 126; j++) {
  get.push_back((char) j);
  for(int k = 32; k <= 126; k++) {
   get.push_back((char) k);
   string h = hash(get);
   cout << h << endl;
   if(h.find("LEGV") != string::npos) {
    cout << "find:" << h << endl;
    cout << (char)i << (char)j << (char)k <<endl;
    return 0;
   }
   get.pop_back();
  }
  get.pop_back();
 }
 get.pop_back();
}
```

我感觉枚举的差不多了就直接在最后填上了“}”，测试，完美，flag get！

贝斯：
根据hint，base系列乱搞，我也不知道怎么搞的，解码来解码去就有了flag。

你是萌新吗？：

我是哦。

下载下来一张图。右键后缀改成rar，哇，这次打开了。发现压缩包x1，解压，卧槽居然有密码，找了一圈没有哪有密码提示，百度了一下，用winhex炸掉密码，成功解压。

然后解压出来一堆文本文档。

我猜肯定是做匹配找不同啦，~~赶紧写个后缀自动机~~ 暴力匹配就完事了。

Eclipse启动，写了以第一个文件为母本，其他的跟他匹配的程序（为什么会这么做…？因为第一个文件没加编号我不能用for循环一次读入只能单独读入就这么搞了），遇到不同的字符就输出，感觉flag大概就只有这么长，不会有多的不同字符吧。

程序没有bug，运行之后立马出flag，非常舒服。

```
        }

        for (int i = 1; i <= 23; i++) {
            String fileName = "E:/miao/hacker" + i + ".txt";
            File f2 = new File(fileName);
            StringBuilder input = new StringBuilder();
            BufferedReader reader2 = new BufferedReader(new FileReader(f2));
            try {
                String temp = "";
                while ((temp = reader2.readLine()) != null) {
                    input.append(temp);
                }
                reader2.close();
            } catch (Exception e) {
                e.printStackTrace();
            }
            check(input.toString());
        }
    }

    public static void check(String e) {
        for (int i = 0; i < e.length(); i++) {
            if(e.charAt(i) != input.charAt(i)) {
                System.out.print(e.charAt(i));
                return;
            }
        }
    }
```

```
Console × Problems Javadoc Declaration Search P3C Results Rule Detail
<terminated> Main (1) [Java Application] C:\Program Files\Java\jre1.8.0_151\bin\javaw.exe (2018年11月12日 上午1:04:05)
GWHT{h4cK3r_twings_666}
```