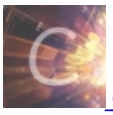
梦之光芒/Monyer game1 Writeup

原创

果光 于 2020-01-15 12:53:35 发布 2824 收藏 2

分类专栏： CTF 文章标签： ctf



- A homework of NEFU NSI
- 好久没发现这种好玩的东西了 ヾ(•ω•`)o
- So I write down a writeup here.

Level 0

http://monyer.com/game/game1/

欢迎来到梦之光芒的小游戏。

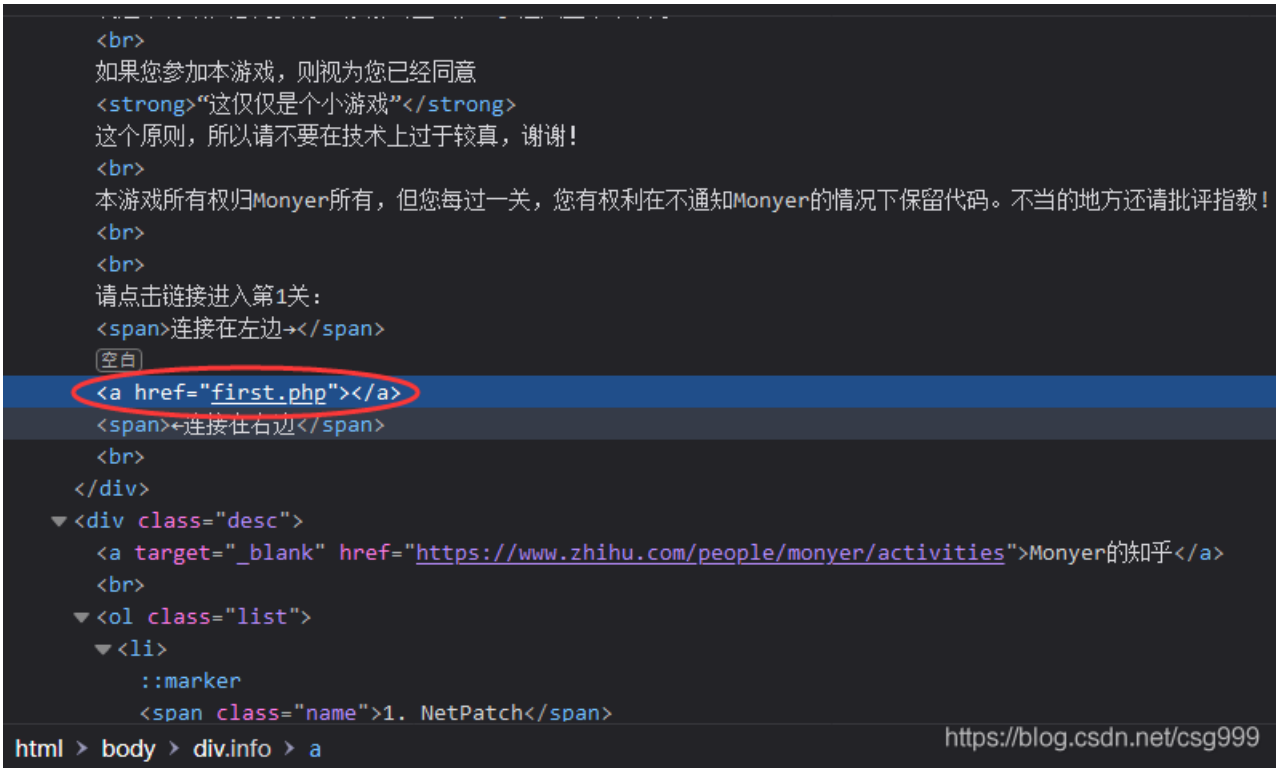
玩这个游戏，您需要有JS加解密基础，SQL注入基本常识等...

如果您参加本游戏，则视为您已经同意**“这仅仅是个小游戏”**这个原则，所以请不要在技术上过于较真，谢谢！

本游戏所有权归Monyer所有，但您每过一关，您有权利在不通知Monyer的情况下保留代码。不当的地方还请批评指教!

请点击链接进入第1关： 连接在左边→ ←连接在右边

开始很简单，直接 F12 查看元素找到中间的 first.php 就可以进入第一关了



Level 1

http://monyer.com/game/game1/first.php

欢迎您来到第1关

请输入密码进入第2关： 提交

观察 JS 发现密码就是两个空格

first.php

```
<!DOCTYPE HTML>
<html>
<head>
<meta http-equiv="content-type" content="text/html; charset=UTF-8">
<meta name="robots" content="noindex,nofollow">
<title>梦之光芒/Monyer——Monyer's Game(第1关)</title>
</head>
<body>
<script type="text/javascript">
    function check(){
        if(document.getElementById('txt').value=="  "){
            window.location.href="hello.php";
        }else{
            alert("密码错误");
        }
    }
</script>
<div align="center">
    <p>欢迎您来到第1关</p>
    <p>请输入密码进入第2关:
        <input type="text" id="txt" value="">
        <input type="button" onClick="check()" value="提交">
    </p>
</div>
</body>
</html>
```


Level 2

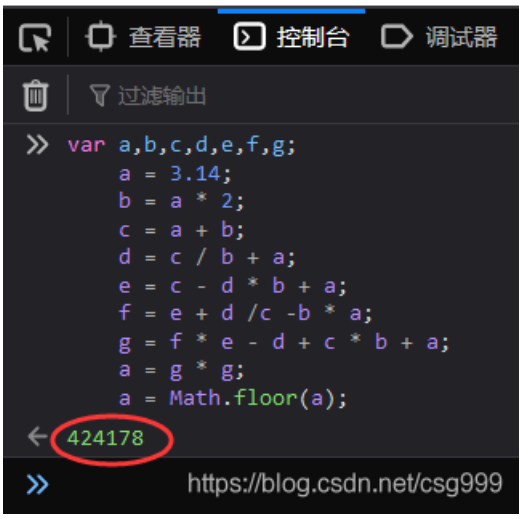
http://monyer.com/game/game1/hello.php

欢迎您来到第2关

请输入密码进入第3关： 提交

可以看到一段代码，把代码扔到控制台里跑一下就出结果了

```
<script type="text/javascript">
    document.oncontextmenu=function(){return false};

    var a,b,c,d,e,f,g;
    a = 3.14;
    b = a * 2;
    c = a + b;
    d = c / b + a;
    e = c - d * b + a;
    f = e + d /c -b * a;
    g = f * e - d + c * b + a;
    a = g * g;
    a = Math.floor(a);

    function check(){
        if(document.getElementById("txt").value==a){
            window.location.href=a + ".php";
        }else{
            alert("密码错误");
            return false;
        }
    }
</script>
```

Level 3

http://monyer.com/game/game1/424178.php

欢迎您来到第3关

请输入密码进入第4关： 提交

恭喜恭喜！顺便问一下：第2关有多少人是用计算器算出来的？嘿嘿

查看源码可以看到脚本被转化成ASCII码了
把eval里面的内容全都扔进控制台跑一下就看到真正脚本中的密码了

424178.php

```
<!DOCTYPE HTML>
<html>
<head>
<meta http-equiv="content-type" content="text/html; charset=UTF-8">
<meta name="robots" content="noindex,nofollow">
<title>梦之光芒/Monyer——Monyer's Game(第3关)</title>
<script type="text/javascript">
    eval(String.fromCharCode(102,117,110,99,116,105,111,110,32,99,104,101,99,107,40,41,123,13,10,09,118,97,114,32,97,32,61,32,39,100,52,10
</script>
</head>
<body>
<div align="center">
    <p>欢迎您来到第3关</p>
    <p>请输入密码进入第4关:
        <input type="text" id="txt" value="">
        <input type="button" onClick="check()" value="提交">
    </p>
    <p>恭喜恭喜！顺便问一下：第2关有多少人是用计算器算出来的？嘿嘿</p>
</div>
</body>
</html>
```


查看器 控制台 调试器 网络 样式编辑器 性能 内存 存储

过滤输出

```
String.fromCharCode(102,117,110,99,116,105,111,110,32,99,104,101,99,107,40,41,123,13,10,09
121,73,100,40,39,116,120,116,39,41,46,118,97,108,117,101,61,61,97,41,123,13,10,09,09,119,1
09,09,97,108,101,114,116,40,34,23494,30721,38169,35823,34,41,59,13,10,09,125,13,10,125)
"function check(){
        var a = 'd4g';
        if(document.getElementById('txt').value==a){
                window.location.href=a+\".php\";
        }else{
                alert(\"密码错误\");
        }
}"
```

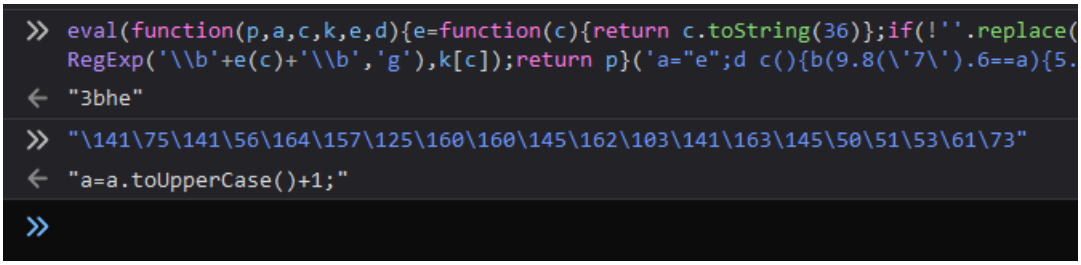

Level 4

http://monyer.com/game/game1/d4g.php

本关卡会自动跳转回 Level 3 所以可以直接查看源码

直接把两段代码扔进控制台试试

一个是 `3bhe` 另一个是 `a=a.toUpperCase()+1;`



把上面的代码格式化一下，可以发现函数返回的p就是真正的代码

所以输出一下p再扔控制台，得到真实 js

a=3bhe，再结合第二段代码a又变大写+1

所以最后密码就是 3BHE1

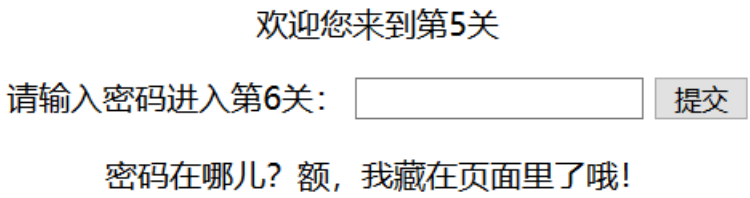
直接打开 http://monyer.com/game/game1/3BHE1.php 即可

```
eval(function(p, a, c, k, e, d) {
    e = function(c) {
        return c.toString(36)
    };
    if (!''.replace(/^/, String)) {
        while (c--) d[c.toString(a)] = k[c] || c.toString(a);
        k = [function(e) {
            return d[e]
        }];
        e = function() {
            return '\\w+'
        };
        c = 1
    };
    while (c--) if (k[c]) p = p.replace(new RegExp('\\b' + e(c) + '\\b', 'g'), k[c]);
    console.log(p) //加一个输出
    return p
} ('a="e";d c(){b(9.8(\'7\').6==a){5.4.3=a+".2"}1{0("密码错误")}}', 15, 15, 'alert|else|php|href|location|window|
value|txt|getElementById|document||if|check|function|3bhe'.split('|'), 0, {}))

//输出的内容再格式化一下
a = "3bhe";
function check() {
    if (document.getElementById('txt').value == a) {
        window.location.href = a + ".php"
    } else {
        alert("密码错误")
    }
}
```

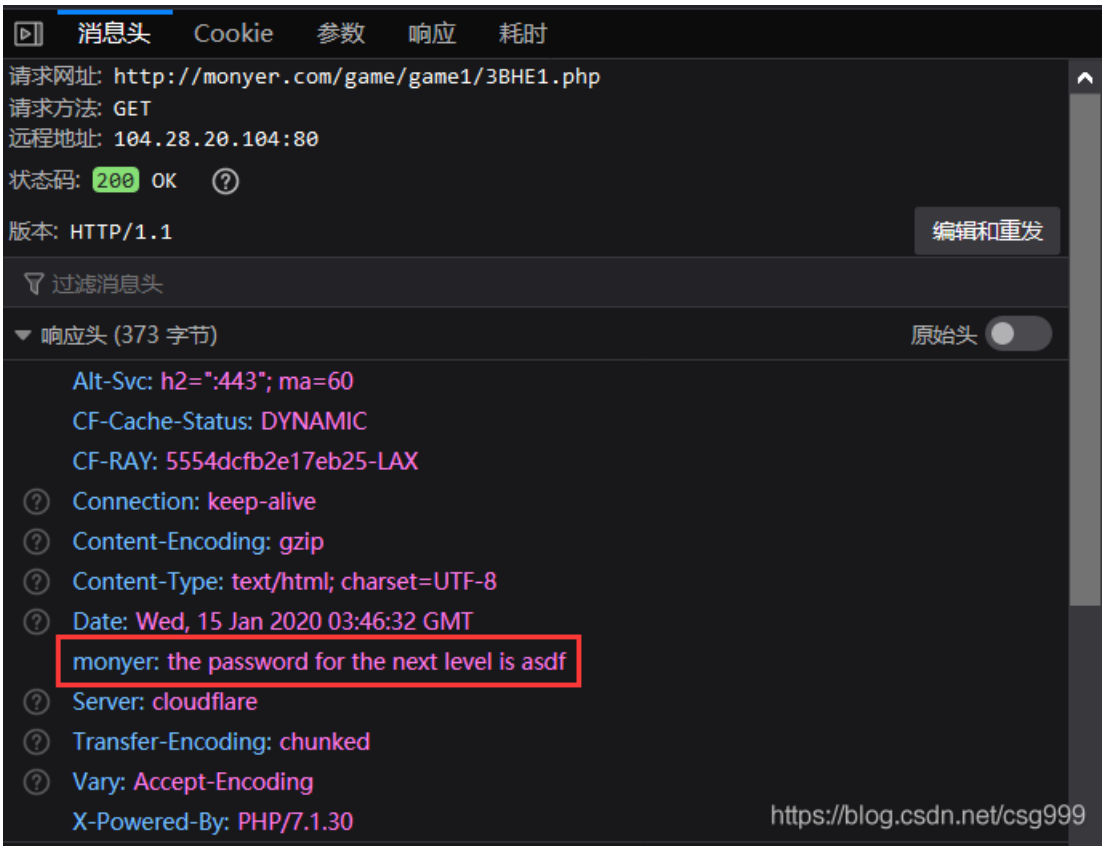
Level 5

---

http://monyer.com/game/game1/3BHE1.php



翻一翻 源码和里面的 js 发现啥也没有
又看了看消息头找到了密码



Level 6

http://monyer.com/game/game1/asdf.php

欢迎您来到第6关

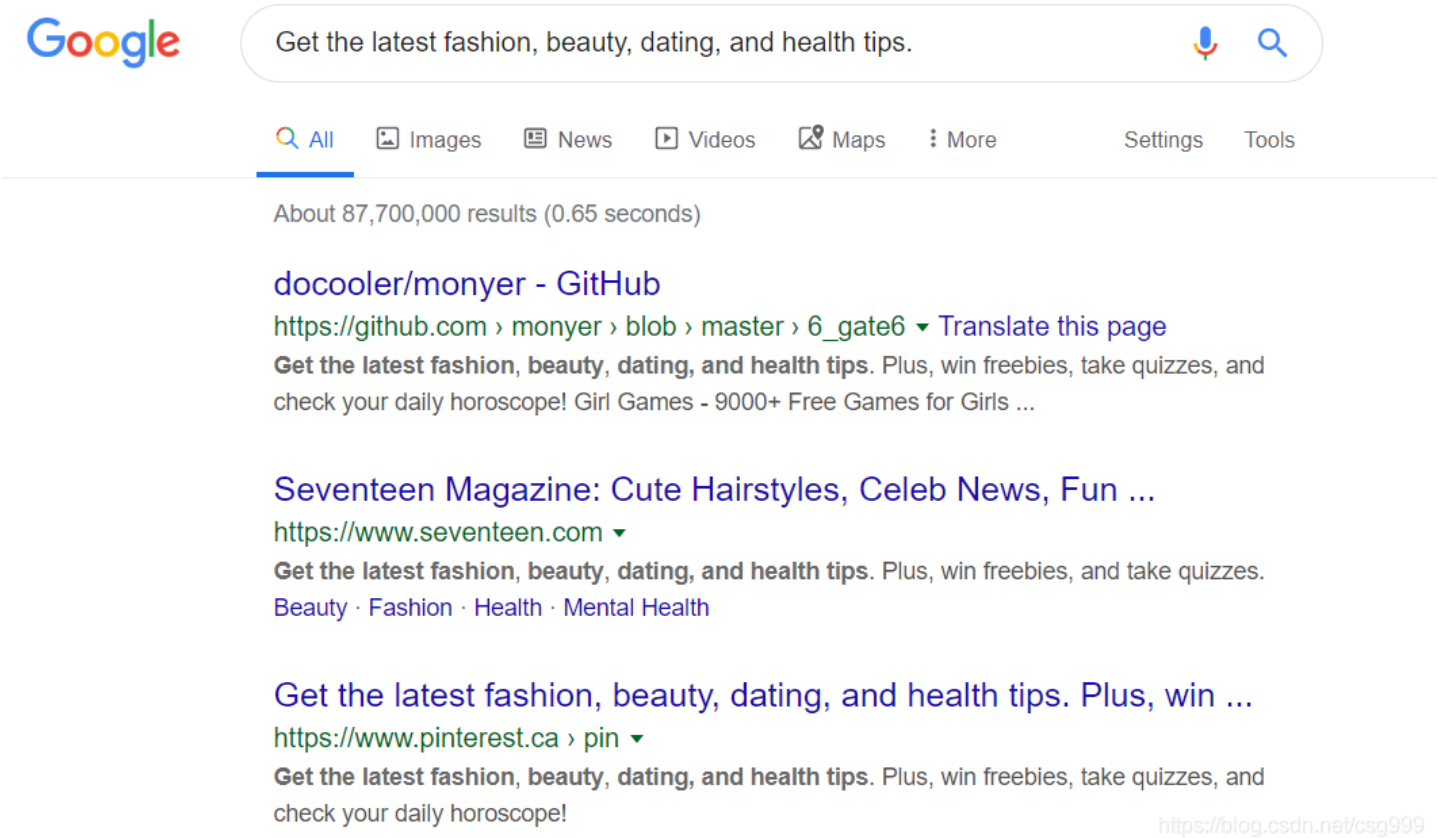
请输入密码进入第7关： 提交

一张被盖住的残缺谷歌图片

发现没藏什么信息，binwalk 也没 walk 出来啥，winhex 也没啥

架上梯子搜一下上面的 Get the latest…

发现被盖住的是 seventeen，输进去试一下还真对了



Level 7

http://monyer.com/game/game1/seventeen7.php

欢迎您来到第7关

请输入密码进入第8关： 提交

提示1：这关需要简单的社会工程学，请联想本关特点进入下一关。

提示2：不要被你的所见、经验及习惯蒙蔽了你的双眼，看不到的正是你想要的。

提示3：与社会工程学相仿的是暴力破解，所以Monyer给你MD5：5e023995fb3f5e840ee684784f8f0799（小于10的数字+字母）

看到 MD5 就直接去查了一下，还真查出来了

MD5 查询网站

Level 8

http://monyer.com/game/game1/eighteen8.php

Not Found

The requested URL /eighteen8.php was not found on this server.

Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request.

上来就一个 404 最开始以为上一关过的不对
后来发现这个网站真正的 404 是这样的

404 Not Found

nginx

查看源码发现下面有说明，求10000以内素数和
也可以把元素样式中的 `display:none;` 勾掉在上面显示

Not Found

The requested URL /eighteen8.php was not found on this server.

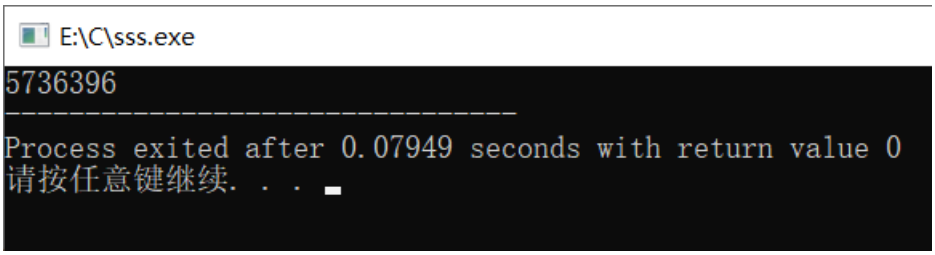
Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request.

第8关朋友您好，第8关欢迎您！我对您的聪明才智感到惊讶！相信我，现在世界上85%以上的人都在你之下，所以你可以大步向前，义无反顾地进行你的事业了。因为只
倒你的事。那么继续我们的约定，我将告诉你第9关的入口： 10000以内所有质数和.php

抄上前几天刚研究的素数筛 C/C++ 素数筛 ACM算法 φ(˚▽ ˚*)♪

```
#include <bits/stdc++.h>
using namespace std;
#define MAXN 10000
char prime[MAXN];
int primeList[MAXN],num=0;
void getPrime()
{
 memset(prime,1,sizeof(prime));
 prime[0]=prime[1]=0;
    for(int i=2;i<MAXN;i++)
    {
     if(prime[i])primeList[num++]=i;
     for (int j=0;j<num&&i*primeList[j]<MAXN;j++)
  {
            prime[i*primeList[j]]=0;
            if (i%primeList[j]==0)break;
        }
    }
}

int main()
{
 int sum=0;
 getPrime();
 for(int i=1;i<MAXN;i++)
 {
  if(prime[i])sum+=i;
 }
 cout<<sum;
}
```

输出结果即为本关密码



Level 9

http://monyer.com/game/game1/5736396.php

欢迎您来到第9关

请输入密码进入第10关： 提交

好吧，在做完刚才的编程题后，您已经成功地来到第九关了，恭喜恭喜！什么？你用笔算出来的？I 服了 YOU！

累了这么长时间，Monyer不会忘记给你送个MM消遣一下，当然第十关密码也在图片里，你得往美女肉里面看，看仔细哦！

嗯，那个图片就不截图了。。。
把图片下载下来发现也没有 binwalk 什么事
用 winhex 打开能看到最后有有意义的字符，直接粘进去就过了

```
00149856  89 D9 5E C3 76 AA ED BE  2A 7B 49 DE 7A 1E E8 D6  ‰Ù^Ãvªí¾*{IÞz èÖ
00149872  5E A8 69 D8 BE 53 52 57  D0 56 9A 36 9B 5A 94 87  ^¨iØ¾SRWÐVš6›Z”‡
00149888  14 28 96 B2 90 A2 48 9A  B0 84 C0 FF D9 B9 FE B9   (–² ¢Hš°„ÀÿÙ¹þ¹
00149904  FE A3 A1 0D 0A C4 C7 BE  E4 B9 E3 B8 E6 B4 CA BD  þ£¡  ÄÇ¾ä¹ã¸æ´Ê½
00149920  D0 CA B2 C3 B4 C0 B4 D7  C5 A3 BF 0D 0A B6 D4 A3  ÐÊ²Ã´À´×Å£¿  ¶Ô£
00149936  AC A1 B0 D4 DA D5 E2 C0  EF A3 AC D4 DA D5 E2 C0  ¬¡°ÔÚÕâÀï£¬ÔÚÕâÀ
00149952  EF A3 AC D4 DA D5 E2 C0  EF 2E 2E 2E 2E 2E 2E A1  ï£¬ÔÚÕâÀï.....¡
00149968  B1 0D 0A B9 A7 CF B2 C4  E3 A3 A1 0D 0A B5 DA CA  ±  ¹§Ï²Ää£¡  µÚÊ
00149984  AE B9 D8 C3 DC C2 EB CE  AA A3 BA 4D 6F 6E 79 65  ®¹ØÃÜÂëÎª£ºMonye
00150000  72 4C 69 6B 65 59 6F 75  5F 74 68 65 31 30 6C 65  rLikeYou_the10le
00150016  76 65 6C 0D 0A B4 D3 CF  D6 D4 DA BF AA CA BC C9  vel  ´ÓÏÖÔÚ¿ªÊ¼É
00150032  E6 BC B0 B5 BD C9 D9 D0  ED B5 C4 B6 AF CC AC B6  æ¼°µ½ÉÙÐíµÄ¶¯Ì¬¶
00150048  AB CE F7 A3 AC B5 AB C4  E3 B6 BC BF C9 D2 D4 B0  «Î÷£¬µ«Ää¶¼¿ÉÒÔ°
00150064  B4 CC E1 CA BE CF DF CB  F7 CD EA B3 C9 B5 C4 A3  ´ÌáÊ¾ÏßË÷Íê³ÉµÄ£
00150080  A1 0D 0A CF E0 D0 C5 D7  D4 BC BA A3 AC C3 BB B4  ¡  ÏàÐÅ×Ô¼º£¬Ã»´
00150096  ED B5 C4 A3 A1                                    íµÄ£¡
```


Level 10

http://monyer.com/game/game1/MonyerLikeYou_the10level.php

欢迎您来到第10关

请输入密码进入第11关： 提交

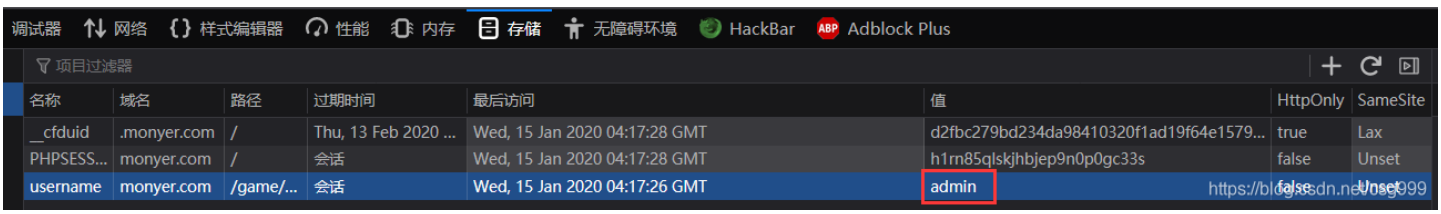
当前用户身份为simpleuser 不是admin，无法显示下一关密码

直接在 Cookie 里把simpleuser改成admin刷新一下密码就出来了

欢迎您来到第10关

请输入密码进入第11关： 提交

好聪明哦！下一关密码为：doyouknow



Level 11

http://monyer.com/game/game1/doyouknow.php?action=show_login_false

欢迎您来到第11关

请输入密码进入第12关： 提交

你的session不是passer，不能查看下一关密码

session 不是 passer 没找到什么有关的 cookie 之类的
看这个地址有点问题，结果把 false 改成 true 就过了

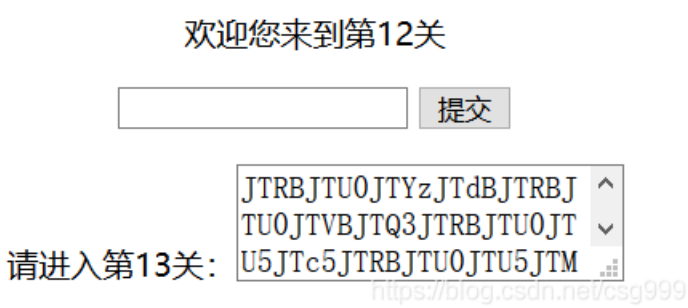
欢迎您来到第11关

请输入密码进入第12关： 提交

您的session为passer，所以您可以查看下一关密码：smartboy

Level 12

http://monyer.com/game/game1/smartboy.php



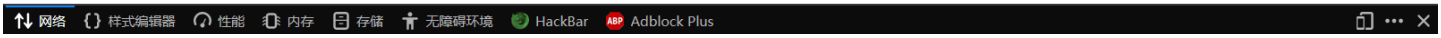
看着像 base64，试一下果然是base64，而且还是两次
有的网站解密之后会出 urlEncode 还得再解一次
这个网站只需要2次base64 base64 解密网站

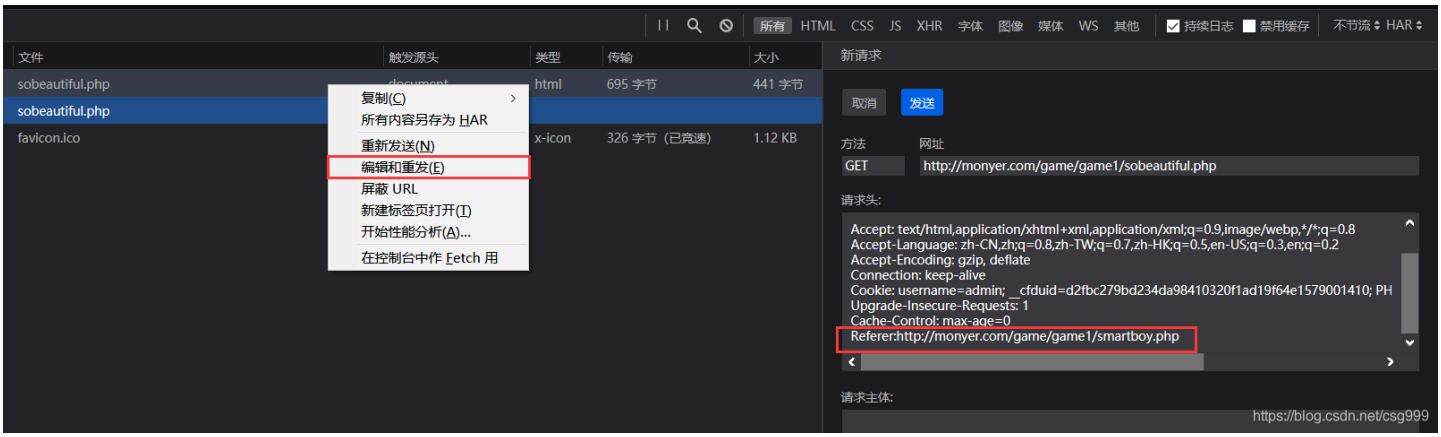
Level 13

http://monyer.com/game/game1/sobeautiful.php

本页禁止盗链!

在消息头里加上上一关的 Referer 即可





得到本关

欢迎您来到第13关

请输入密码进入第14关:

提交

没有输入密码 或 密码错误 或 系统错误!

查看源码发现是sql注入

```
<!DOCTYPE HTML>
<html>
<head>
<meta http-equiv="content-type" content="text/html; charset=UTF-8">
<meta name="robots" content="noindex,nofollow">
<title>梦之光芒/Monyer——Monyer's Game(第13关)</title>
<script type="text/javascript">
    function check(){
        window.location.href = document.getElementById("txt").value + ".php";
    }
</script>
</head>
<body>
<div align="center">
    <!--
dim connect
Response.Expires=0 '系统数据库连接
Set connect=Server.CreateObject("ADODB.Connection")
connect.Open "Provider=Microsoft.Jet.OLEDB.4.0;Data Source=" & server.MapPath("/Database.mdb") & ";Mode=ReadWrite|Share Deny None;Persist Security Info=False"

set rss=server.createobject("adodb.recordset")
sqlstr="select password,pwd from [user] where pwd='"&request("pwd")&"'"
rss.open sqlstr,connect,1,1
if rss.bof and rss.eof then
  response.write("密码错误")
else
  response.write(rss("password"))
end if
rss.close
set rss=nothing
connect.close
set connect=nothing
--><p>欢迎您来到第13关</p><p>请输入密码进入第14关:</p><input type="text" id="txt" value="">
            <input type="button" onClick="check()" value="提交"><br>
            下一关密码:whatyouneverknow</div>
</body>
</html>
```

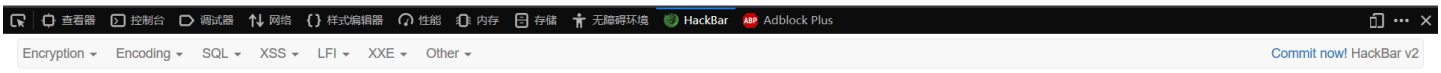
实验发现还是 HackBar 好用，并且pwd要post过去

欢迎您来到第13关

请输入密码进入第14关:

提交

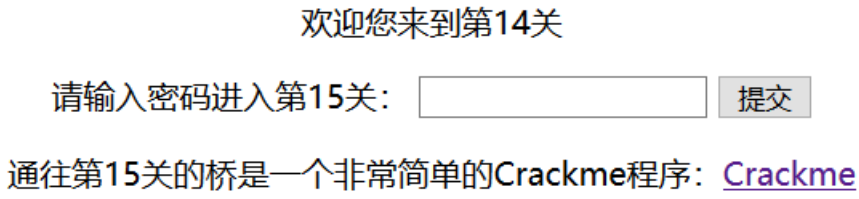
下一关密码:whatyouneverknow



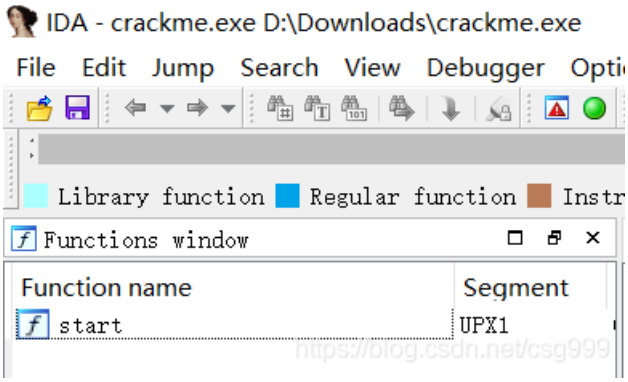
Level 14

---

http://monyer.com/game/game1/whatyouneverknow.php

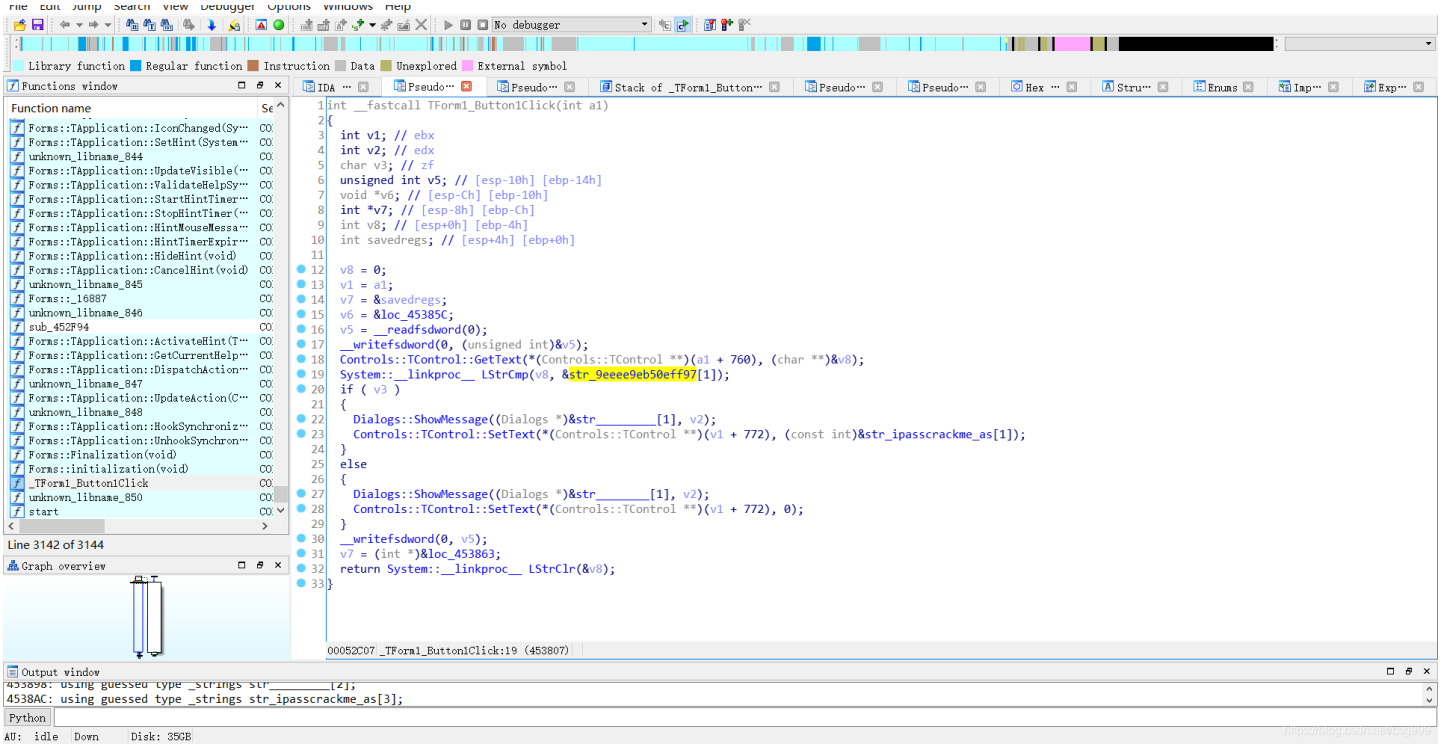


一个 Crackme，直接扔到 IDA 里



发现 UPX，需要先进行脱壳

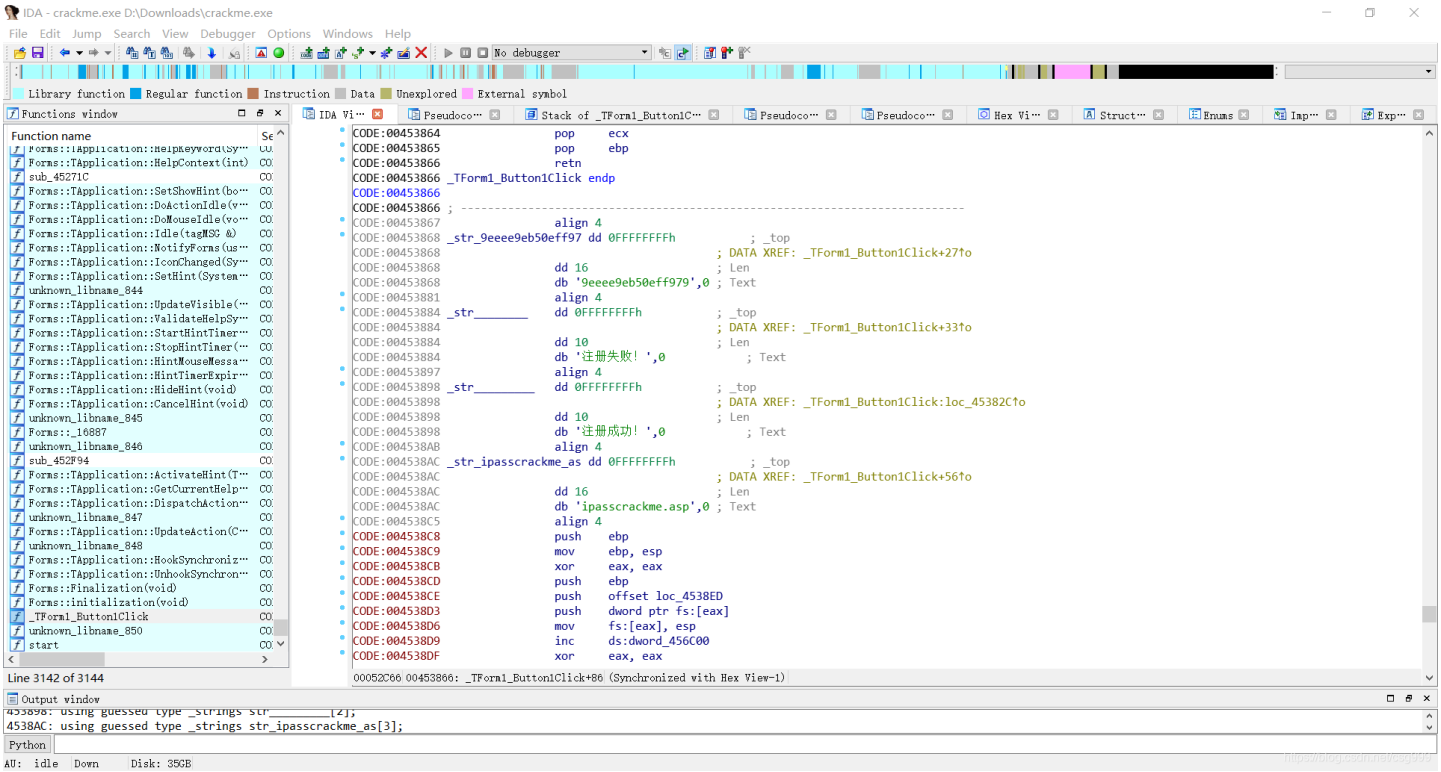
脱壳之后再扔进 IDA 看到按下按钮的方法里有字符串比较



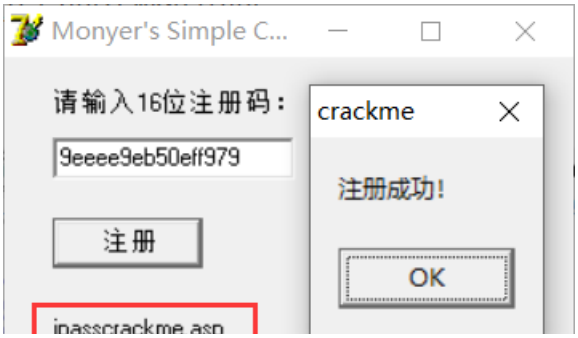
```
int __fastcall TForm1_Button1Click(int a1)
{
  int v1; // ebx
  int v2; // edx
  char v3; // zf
  unsigned int v5; // [esp-10h] [ebp-14h]
  void *v6; // [esp-Ch] [ebp-10h]
  int *v7; // [esp-8h] [ebp-Ch]
  int v8; // [esp+0h] [ebp-4h]
  int savedregs; // [esp+4h] [ebp+0h]

  v8 = 0;
  v1 = a1;
  v7 = &savedregs;
  v6 = &loc_45385C;
  v5 = __readfsdword(0);
  __writefsdword(0, (unsigned int)&v5);
  Controls::TControl::GetText(*(Controls::TControl **)(a1 + 760), (char **)&v8);
  System::__linkproc__ LStrCmp(v8, &str_9eeee9eb50eff97[1]);
  if ( v3 )
  {
    Dialogs::ShowMessage((Dialogs *)&str________[1], v2);
    Controls::TControl::SetText(*(Controls::TControl **)(v1 + 772), (const int)&str_ipasscrackme_as[1]);
  }
  else
  {
    Dialogs::ShowMessage((Dialogs *)&str________[1], v2);
    Controls::TControl::SetText(*(Controls::TControl **)(v1 + 772), 0);
  }
  __writefsdword(0, v5);
  v7 = (int *)&loc_453863;
  return System::__linkproc__ LStrClr(&v8);
}
```

查看字符串得到密码 9eeee9eb50eff979，直接粘进去发现 404 了

打开注册机注册一下发现真正页面在软件里面



```
CODE:00453864                 pop     ecx
CODE:00453865                 pop     ebp
CODE:00453866                 retn
CODE:00453866 _TForm1_Button1Click endp
CODE:00453866
CODE:00453866 ; ---------------------------------------------------------------------------
CODE:00453867                 align 4
CODE:00453868 _str_9eeee9eb50eff97 dd 0FFFFFFFFh          ; _top
CODE:00453868                                             ; DATA XREF: _TForm1_Button1Click+27↑o
CODE:00453868                 dd 16                       ; Len
CODE:00453868                 db '9eeee9eb50eff979',0     ; Text
CODE:00453881                 align 4
CODE:00453884 _str________    dd 0FFFFFFFFh               ; _top
CODE:00453884                                             ; DATA XREF: _TForm1_Button1Click+33↑o
CODE:00453884                 dd 10                       ; Len
CODE:00453884                 db '注册失败！',0              ; Text
CODE:00453897                 align 4
CODE:00453898 _str________    dd 0FFFFFFFFh               ; _top
CODE:00453898                                             ; DATA XREF: _TForm1_Button1Click:loc_45382C↑o
CODE:00453898                 dd 10                       ; Len
CODE:00453898                 db '注册成功！',0              ; Text
CODE:004538AB                 align 4
CODE:004538AC _str_ipasscrackme_as dd 0FFFFFFFFh          ; _top
CODE:004538AC                                             ; DATA XREF: _TForm1_Button1Click+56↑o
CODE:004538AC                 dd 16                       ; Len
CODE:004538AC                 db 'ipasscrackme.asp',0     ; Text
CODE:004538C5                 align 4
CODE:004538C8                 push    ebp
CODE:004538C9                 mov     ebp, esp
CODE:004538CB                 xor     eax, eax
CODE:004538CD                 push    ebp
CODE:004538CE                 push    offset loc_4538ED
CODE:004538D3                 push    dword ptr fs:[eax]
CODE:004538D6                 mov     fs:[eax], esp
CODE:004538D9                 inc     ds:dword_456C00
CODE:004538DF                 xor     eax, eax
```



这个 asp 也是假的，真正的页面还是 php 的

Level 15

---

http://monyer.com/game/game1/ipasscrackme.php
过关了！ ヾ(•ω•`)o