

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](#)

版权声明: 本文为博主原创文章, 遵循[CC 4.0 BY-SA](#)版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/csg999/article/details/103985501>

版权



[CTF 专栏收录该内容](#)

23 篇文章 0 订阅

订阅专栏

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

Level 0

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

<https://blog.csdn.net/csg999>

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

```
<br>
如果您参加本游戏，则视为您已经同意
<strong>“这仅仅是个小游戏”</strong>
这个原则，所以请不要在技术上过于较真，谢谢！
<br>
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！
<br>
<br>
请点击链接进入第1关：
<span>连接在左边→</span>
[空白]
<a href="first.php"></a>
<span>←连接在右边</span>
<br>
</div>
▼ <div class="desc">
    <a target="_blank" href="https://www.zhihu.com/people/monyer/activities">Monyer的知乎</a>
    <br>
    ▼ <ol class="list">
        ▼ <li>
            ::marker
            <span class="name">1. NetPatch</span>

```

html > body > div.info > a https://blog.csdn.net/csg999

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 X

1 <!DOCTYPE HTML>
2 <html>
3 <head>
4 <meta http-equiv="content-type" content="text/html; charset=UTF-8">
5 <meta name="robots" content="noindex,nofollow">
6 <title>梦之光芒/Monyer—Monyer's Game(第1关)</title>
7 </head>
8 <body>
9 <script type="text/javascript">
10     function check(){
11         if(document.getElementById('txt').value=="  "){
12             window.location.href="hello.php";
13         }else{
14             alert("密码错误");
15         }
16     }
17 </script>
18 <div align="center">
19     <p>欢迎您来到第1关</p>
20     <p>请输入密码进入第2关：
21         <input type="text" id="txt" value="">
22         <input type="button" onClick="check()" value="提交">
23     </p>
24 </div>
25 </body>
26 </html>
```

<https://blog.csdn.net/csg999>

Level 2

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

```
7 <script type="text/javascript">
8     document.oncontextmenu=function(){return false};
9
10    var a,b,c,d,e,f,g;
11    a = 3.14;
12    b = a * 2;
13    c = a + b;
14    d = c / b + a;
15    e = c - d * b + a;
16    f = e + d /c -b * a;
17    g = f * e - d + c * b + a;
18    a = g * g;
19    a = Math.floor(a);
20
21    function check(){
22        if(document.getElementById("txt").value==a){
23            window.location.href=a + ".php";
24        }else{
25            alert("密码错误");
26            return false;
27        }
28    }
29 </script>
30 </body>
```

<https://blog.csdn.net/csg999>



The screenshot shows a browser's developer tools with the '控制台' (Console) tab selected. The console output displays the execution of a JavaScript script. The final result, '424178', is highlighted with a red oval.

```
>> 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);

<-- 424178
```

<https://blog.csdn.net/csg999>

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

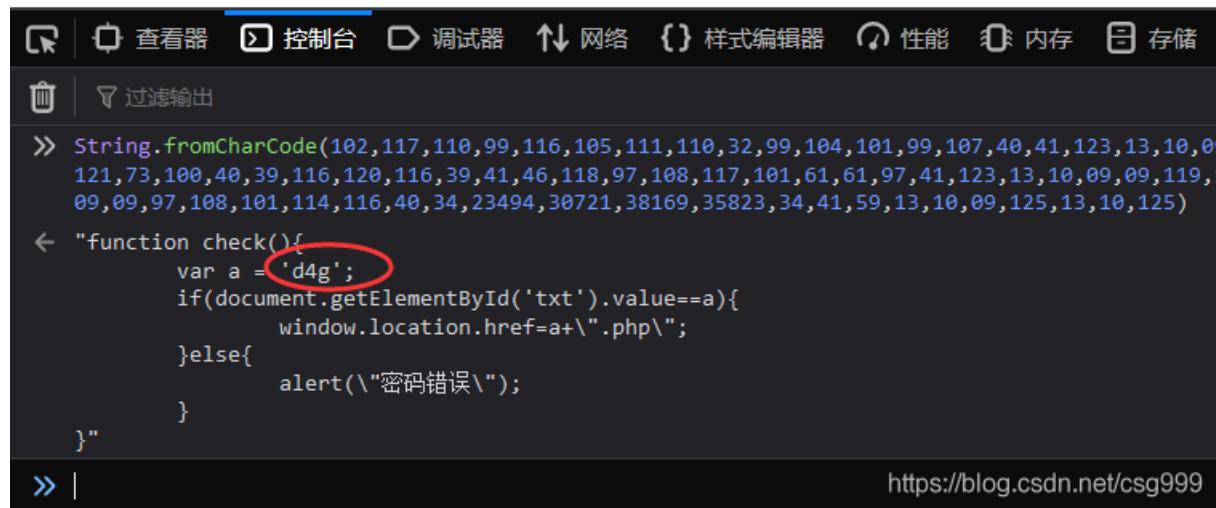
恭喜恭喜！顺便问一下：第2关有多少人是用计算器算出来的？嘿嘿

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 ×
1 <!DOCTYPE HTML>
2 <html>
3 <head>
4 <meta http-equiv="content-type" content="text/html; charset=UTF-8">
5 <meta name="robots" content="noindex,nofollow">
6 <title>梦之光芒/Monyer—Monyer's Game(第3关)</title>
7 <script type="text/javascript">
8   eval(String.fromCharCode(102,117,110,99,116,105,111,110,32,99,104,101,99,107,40,41,123,13,10,09,118,97,114,32,97,32,61,32,39,100,52,16
9 </script>
10 </head>
11 <body>
12 <div align="center">
13   <p>欢迎您来到第3关</p>
14   <p>请输入密码进入第4关:</p>
15   <input type="text" id="txt" value="">
16   <input type="button" onClick="check()" value="提交">
17 </p>
18   <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>
19 </div>
20 </body>
21 </html>
```

<https://blog.csdn.net/csg999>



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(102,117,110,99,116,105,111,110,32,99,104,101,99,107,40,41,123,13,10,09,118,97,114,32,97,32,61,32,39,100,52,16
121,73,100,40,39,116,120,116,39,41,46,118,97,108,117,101,61,61,97,41,123,13,10,09,09,119,109,09,97,108,101,114,116,40,34,23494,30721,38169,35823,34,41,59,13,10,09,125,13,10,125)
← "function check(){
  var a ='d4g';
  if(document.getElementById('txt').value==a){
    window.location.href=a+".php";
  }else{
    alert(\"密码错误\");
  }
}"
```

<https://blog.csdn.net/csg999>

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

```
1 <!DOCTYPE HTML>
2 <html>
3 <head>
4 <meta http-equiv="content-type" content="text/html; charset=UTF-8">
5 <meta name="robots" content="noindex, nofollow">
6 <meta http-equiv="refresh" content="0;url=424178.php">
7 <title>梦之光芒/Monyer——Monyer's Game(第4关)</title>
8 <script type="text/javascript">
9   eval(function(p,a,c,k,e,d){e=function(c){return c.toString(36)};if(!''.replace(/\/,String)){while(c--)d[ctoString(a)]||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]);return p}('a="'+a";d c(){b(9.8('7')).6==a){5.4.3=a".2"}1{("密码错误")}}},15,15,'alert')else{p.href=location.window.value;txt.getElementById(document).innerHTML=checkFunction|3bhe .split(' ')},{}))
10 </script>
11 </head>
12 <body>
13 <div align="center">
14   <p>欢迎您来到第4关</p>
15   <p>请输入密码进入第5关:</p>
16   <input type="text" id="txt" value="">
17   <input type="button" onClick="check()" value="提交">
18 </p>
19 </div>
20 </body>
21 <script type="text/javascript">
22   eval("\141\75\141\56\164\157\125\160\160\145\162\103\141\163\145\50\51\53\61\73");
23 </script>
24 </html>
```

<https://blog.csdn.net/csg999>

直接把两段代码扔进控制台试试

一个是 `3bhe` 另一个 `a=a.toUpperCase()+1;`

```
>> eval(function(p,a,c,k,e,d){e=function(c){return c.toString(36)};if(!''.replace(/\/,String)){while(c--)d[ctoString(a)]||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]);return p}('a="'+a";d c(){b(9.8('7')).6==a){5.4.3=a".2"}1{("密码错误")}}),15,15,'alert')else{p.href=location.window.value;txt.getElementById(document).innerHTML=checkFunction|3bhe .split(' ')},{}))
<- "3bhe"
>> "
<- "\141\75\141\56\164\157\125\160\160\145\162\103\141\163\145\50\51\53\61\73"
<- "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(\')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>

欢迎您来到第5关

请输入密码进入第6关: 提交

密码在哪儿？额，我藏在页面里了哦！

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

消息头 Cookie 参数 响应 耗时

请求网址: <http://monyer.com/game/game1/3BHE1.php>
请求方法: GET
远程地址: 104.28.20.104:80
状态码: 200 OK ②
版本: HTTP/1.1 编辑和重发

过滤消息头

▼ 响应头 (373 字节) 原始头

Alt-Svc: h2=":443"; ma=60
CF-Cache-Status: DYNAMIC
CF-RAY: 5554dcfb2e17eb25-LAX
② Connection: keep-alive
② Content-Encoding: gzip
② Content-Type: text/html; charset=UTF-8
② Date: Wed, 15 Jan 2020 03:46:32 GMT
monyer: the password for the next level is asdf
② Server: cloudflare
② Transfer-Encoding: chunked
② Vary: Accept-Encoding
X-Powered-By: PHP/7.1.30

<https://blog.csdn.net/csg999>

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

Web Images Video News Maps Gmail more ▾

Google [REDACTED]

Web Results 1 - 10 of about 22,100,000 for [REDACTED] [definition]. (0.06 s)

[REDACTED].com
Get the latest fashion, beauty, dating, and health tips. Plus, win freebies, take quizzes, and check your daily horoscope!
[www.\[REDACTED\].com/](#) - 63k - Cached - Similar pages

Freebies Horoscopes
Quizzes Health, Sex and Fitness
Fashion Hairstyle Ideas for Teens
Hair, Skin and Makeup - Beauty Tips Fun Stuff

[More results from \[REDACTED\].com »](#)

[REDACTED].co.za/ - 2k - Cached - Similar pages

[REDACTED] (magazine) - Wikipedia, the free encyclopedia
[REDACTED] was first published in 1944 and is

<https://blog.csdn.net/csg999>

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

Google Get the latest fashion, beauty, dating, and health tips. Microphone Search

All Images News Videos Maps More Settings Tools

About 87,700,000 results (0.65 seconds)

[docooler/monyer - GitHub](#)
https://github.com/monyer/blob/master/6_gate6 ▾ Translate this page
Get the latest fashion, beauty, dating, and health tips. Plus, win freebies, take quizzes, and check your daily horoscope! Girl Games - 9000+ Free Games for Girls ...

[Seventeen Magazine: Cute Hairstyles, Celeb News, Fun ...](#)
<https://www.seventeen.com> ▾
Get the latest fashion, beauty, dating, and health tips. Plus, win freebies, and take quizzes.
Beauty · Fashion · Health · Mental Health

[Get the latest fashion, beauty, dating, and health tips. Plus, win ...](#)
https://www.pinterest.ca/pin ▾
Get the latest fashion, beauty, dating, and health tips. Plus, win freebies, take quizzes, and check your daily horoscope!

<https://blog.csdn.net/csg999>

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](#)

The screenshot shows an MD5 search interface. At the top, there is a text input field containing the MD5 hash: "密文: 5e023995fb3f5e840ee684784f8f0799". Below it is a dropdown menu labeled "类型: 自动". To the right of the dropdown are two buttons: a red "查询" (Search) button and a blue "加密" (Encrypt) button. In the bottom left corner of the main search area, the text "查询结果:" is followed by "eighteen8". In the bottom right corner of the entire interface, the URL "https://blog.csdn.net/csg999" is visible.

Level 8

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.

<https://blog.csdn.net/csg999>

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。因为只要你不倒你的事。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

The screenshot shows the browser's developer tools with the 'Elements' tab selected. The left pane displays the HTML structure of the 404 page, which includes an

Not Found

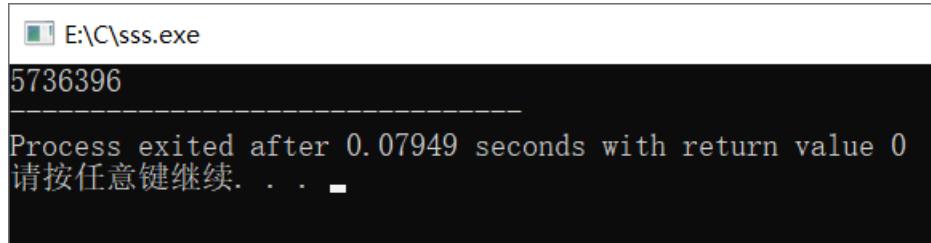
 heading and a paragraph of explanatory text. The right pane shows the associated CSS styles. A red arrow points to a specific rule: '元素 & { display:none; }'. This rule is applied to all elements with the class '&' (the ampersand selector), effectively hiding the page content.

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



```
E:\C\sss.exe
5736396
-----
Process exited after 0.07949 seconds with return value 0
请按任意键继续. . .
```

Level 9

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？！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 ¾Ù^Ãv*i%*{IBz èÖ
00149872 5E A8 69 D8 BE 53 52 57 D0 56 9A 36 9B 5A 94 87 ^~iØ%SRWÈVš6>Z"‡
00149888 14 28 96 B2 90 A2 48 9A B0 84 C0 FF D9 B9 FE B9 (‐‐ cHš° „ÄyÜíþ¹
00149904 FE A3 A1 0D 0A C4 C7 BE E4 B9 E3 B8 E6 B4 CA BD þé; Äç¾ä³ä,æ'È¾
00149920 D0 CA B2 C3 B4 C0 B4 D7 C5 A3 BF 0D 0A B6 D4 A3 ðÈ·Ã'À'×Ã£ç qÔ£
00149936 AC A1 B0 D4 DA D5 E2 C0 EF A3 AC D4 DA D5 E2 C0 -i°ÔÚðåÀif-ÔÚðåÀ
00149952 EF A3 AC D4 DA D5 E2 C0 EF 2E 2E 2E 2E 2E Al iè-ÔÚðåÀiü.....i
00149968 B1 0D 0A B9 A7 CF B2 C4 E3 A3 A1 0D 0A B5 DA CA ± 'SÍ*Ãäf; µÙÈ
00149984 AE B9 D8 C3 DC C2 EB CE AA A3 BA 4D 6F 6E 79 65 g·øÄÜåéí·£ºMonye
00150000 72 4C 69 6B 65 59 6F 75 5F 74 68 65 31 30 6C 65 rLikeYou_thelole
00150016 76 65 6C 0D 0A B4 D3 CF D6 D4 DA BF AA CA BC C9 vel 'Óiçòúç*È·É
00150032 E6 BC B0 B5 BD C9 D9 D0 ED B5 C4 B6 AF CC AC B6 æ·ºµ·ÉÜðíµÄq-ì-¶
00150048 AB CE F7 A3 AC B5 AB C4 E3 B6 BC BF C9 D2 D4 B0 «Í-£-µ«Ää¶¶çÉÓº
00150064 B4 CC E1 CA BE CF DF CB F7 CD EA B3 C9 B5 C4 A3 'ÍáÈ·íðÈ·íè·ÉµÃ£
00150080 A1 0D 0A CF E0 D0 C5 D7 D4 BC BA A3 AC C3 BB B4 ; ÍàBÃ·Óç·£-Ã»'
00150096 ED B5 C4 A3 A1 https://bl...n.net/csg999
https://bl...n.net/csg999
```

Level 10

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

调试器							↑ 网络	{ } 样式编辑器	Ø 性能	内存	存储	无无障碍环境	HackBar	ABP Adblock Plus
名称	域名	路径	过期时间	最后访问	值	HttpOnly	SameSite							
_cfduid	.monyer.com	/	Thu, 13 Feb 2020 ...	Wed, 15 Jan 2020 04:17:28 GMT	d2fb279bd234da98410320f1ad19f64e1579...	true	Lax							
PHPSESS...	monyer.com	/	会话	Wed, 15 Jan 2020 04:17:28 GMT	h1m85qlskjhbjep9n0p0gc33s	false	Unset							
username	monyer.com	/game/...	会话	Wed, 15 Jan 2020 04:17:26 GMT	admin	https://bl...n.net/csg999	false	Unset						

Level 11

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

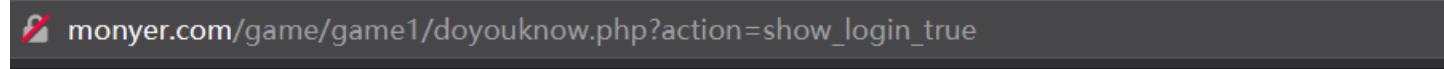
欢迎您来到第11关

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

 monyer.com/game/game1/doyouknow.php?action=show_login_true

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

<https://blog.csdn.net/csg999>

Level 12

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

欢迎您来到第12关

提交

JTRBJTU0JTYzJTdBTRBJ
TU0JTVBQTQ3JTRBJTU0JT

请进入第13关: U5JTc5JTRBJTU0JTU5JTM

<https://blog.csdn.net/csg999>

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](#)

BASE64加密解密

请将要加密或解密的内容复制到以下区域

sobeautiful.php

BASE64加密 BASE64解密

<https://blog.csdn.net/csg999>

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

```

1 <!DOCTYPE HTML>
2 <html>
3 <head>
4 <meta http-equiv="content-type" content="text/html; charset=UTF-8">
5 <meta name="robots" content="noindex, nofollow">
6 <title>梦之光芒/Monyer——Monyer's Game(第13关)</title>
7 <script type="text/javascript">
8     function check() {
9         window.location.href = document.getElementById("txt").value + ".php";
10    }
11 </script>
12 </head>
13 <body>
14 <div align="center">
15     <!--
16 dim connect
17 Response.Expires=0 '系统数据库连接
18 Set connect=Server.CreateObject("ADODB.Connection")
19 connect.Open "Provider=Microsoft.Jet.OLEDB.4.0;Data Source=" & server.MapPath("/Database.mdb") & ";Mode=ReadWrite/Share Deny None;Persist Security Info=False"
20
21 set rss=server.createobject("adodb.recordset")
22 sqlstr="select password, pwd from [user] where pwd='&request('pwd')&'"
23 rss.open sqlstr,connect,1,1
24 if rss.bof and rss.eof then
25     response.write("密码错误")
26 else
27     response.write(rss("password"))
28 end if
29 rss.close
30 set rss=nothing
31 connect.close
32 set connect=nothing
33 --><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="">
34     <input type="button" onClick="check()" value="提交"><br>
35     下一关密码：whatyouneverknow</div>
36 </body>
37 </html>

```

https://blog.csdn.net/csg999

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

Load URL
Split URL
Execute
Post data Referer User Agent Cookies Clear All
pwd=%27%20or%201=1
R http://monyer.com/game/game1/smartyboy.php
https://blog.csdn.net/csg999

Level 14

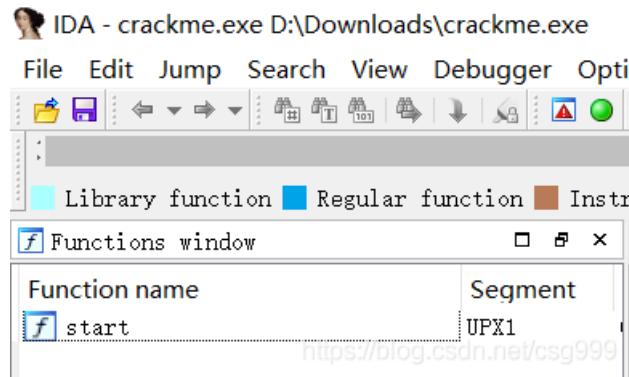
<http://monyer.com/game/game1/whatyouneverknow.php>

欢迎您来到第14关

请输入密码进入第15关: 提交

通往第15关的桥是一个非常简单的Crackme程序: [Crackme](#)

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

IDA Pro - 00052C07 _TForm1_Button1Click+19 (453807)

```

Function name: _TForm1_Button1Click
Se
1 int __fastcall TForm1_Button1Click(int a1)
2 {
3     int v1; // ebx
4     int v2; // edx
5     char v3; // zf
6     unsigned int v5; // [esp-10h] [ebp-14h]
7     void *v6; // [esp-Ch] [ebp-10h]
8     int *v7; // [esp-8h] [ebp-Ch]
9     int v8; // [esp+0h] [ebp-4h]
10    int savedregs; // [esp+4h] [ebp+0h]
11
12    v8 = 0;
13    v1 = a1;
14    v7 = &savedregs;
15    v6 = &loc_45385C;
16    v5 = __readfsdword(0);
17    __writefsdword(0, (unsigned int)&v5);
18    Controls::TControl::GetText(*Controls::TControl **)(a1 + 760), (char *&)v8);
19    Controls::TControl::SetText(*Controls::TControl **)(v1 + 772), (const int)&str_ipasscrackme_as[1];
20    if ( v3 )
21    {
22        Dialogs::ShowMessage((Dialogs *)&str_____[1], v2);
23        Controls::TControl::SetText(*Controls::TControl **)(v1 + 772), (const int)&str_ipasscrackme_as[1]);
24    }
25    else
26    {
27        Dialogs::ShowMessage((Dialogs *)&str_____[1], v2);
28        Controls::TControl::SetText(*Controls::TControl **)(v1 + 772), 0);
29    }
30    __writefsdword(0, v5);
31    v7 = (int *)&loc_453863;
32    return System::__linkproc__ LStrClr(&v8);
33}

```

Output window:

```

453807: using guessed type _strings str_____[2];
4538AC: using guessed type _strings str_ipasscrackme_as[3];
Python
AU: idle Down Disk: 35GB

```

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

IDA - crackme.exe D:\Downloads\crackme.exe

```

File Edit Jump Search View Debugger Options Windows Help
File Edit Jump Search View Debugger Options Windows Help
Library function Regular function Instruction Data Unexplored External symbol
Functions window IDA Vi... Pseudoco... Stack of _TForm1_Button1C... Pseudoco... Pseudoco... Hex Vi... A Struct... Enums Iap... Exp...
Function name: _TForm1_Button1Click
Se
CODE:00453864 pop    ecx
CODE:00453865 pop    ebp
CODE:00453866 _TForm1_Button1Click endp
CODE:00453866 ;
CODE:00453867 align 4
CODE:00453868 _str_9eeee9eb50eff97 dd 0FFFFFFFh ; DATA XREF: _TForm1_Button1Click+27t0
CODE:00453868 dd 16 ; Len
CODE:00453868 db '9eeee9eb50eff979',0 ; Text
CODE:00453881 align 4
CODE:00453881 dd 0FFFFFFFh ; _top
CODE:00453881 ; DATA XREF: _TForm1_Button1Click+33t0
CODE:00453881 dd 10 ; Len
CODE:00453881 db '注册失败!',0 ; Text
CODE:00453897 align 4
CODE:00453897 dd 0FFFFFFFh ; _top
CODE:00453897 ; DATA XREF: _TForm1_Button1Click:loc_45382Ct0
CODE:00453897 dd 10 ; Len
CODE:00453897 db '注册成功!',0 ; Text
CODE:00453898 align 4
CODE:00453898 dd 0FFFFFFFh ; _top
CODE:00453898 ; DATA XREF: _TForm1_Button1Click+56t0
CODE:00453898 dd 16 ; Len
CODE:00453898 db 'ipasscrackme.asp',0 ; Text
CODE:004538C5 align 4
CODE:004538C8 push   ebp
CODE:004538C8 mov    ebp, esp
CODE:004538C9 xor    eax, eax
CODE:004538CB push   ebp
CODE:004538CD push   offset loc_453BED
CODE:004538CE push   dword ptr fs:[eax]
CODE:004538D3 push   fs:[eax], esp
CODE:004538D6 mov    fs:[eax], esp
CODE:004538D9 inc    ds:[word_456C00]
CODE:004538DF xor    eax, eax

```

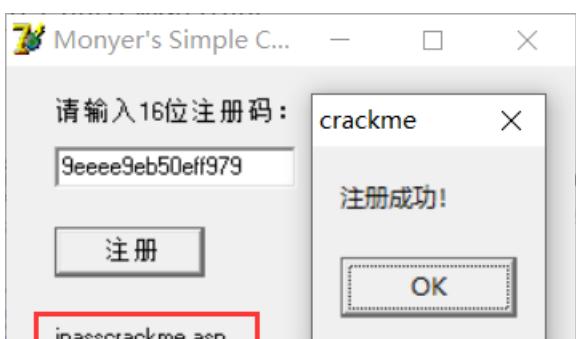
Line 3142 of 3144

Output window:

```

453807: using guessed type _strings str_____[2];
4538AC: using guessed type _strings str_ipasscrackme_as[3];
Python
AU: idle Down Disk: 35GB

```



<https://blog.csdn.net/csg999>

这个 asp 也是假的，真正的页面还是 php 的

Level 15

<http://monyer.com/game/game1/i pass crackme.php>

过关了！ヽ(•ω•)o

欢迎来到关底

请输入你的大名

请输入你的网站&博客&Email

提交

<https://blog.csdn.net/csg999>