个人CTF入门训练过程WriteUp

原创

LastButNotLeast 于 2019-11-18 18:17:55 发布 1100 收藏 4

文章标签： ctf 入门兴趣小游戏 WriteUp

本文链接：https://blog.csdn.net/LastButNotLeast/article/details/103125820

1.梦之光芒入门体会

游戏入口 http://www.monyer.com/game/game1/

Game 0:

```
(view-source:http://www.monyer.com/game/game1/)
查看网页源代码      → <a href="first.php"></a> ←        php
```

Game 1:

```
1.[http://www.monyer.com/game/game1/first.php]
php关联
<script type="text/javascript">
    function check(){
        if(document.getElementById('txt').value==""  "){
            window.location.href="hello.php";
        }else{
            alert("密码错误");
        }
    }
</script>
//答案在value==""  "     下一关是"hello.php"
```

Game 2:

```
Chrome  F12 检查（因为右键禁用） [JS作怪]
Sources  hello.php

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;
        }
    }
意思是要算出a的值，在console里面打个a就好了
Console  a    424178
```

Game 3:

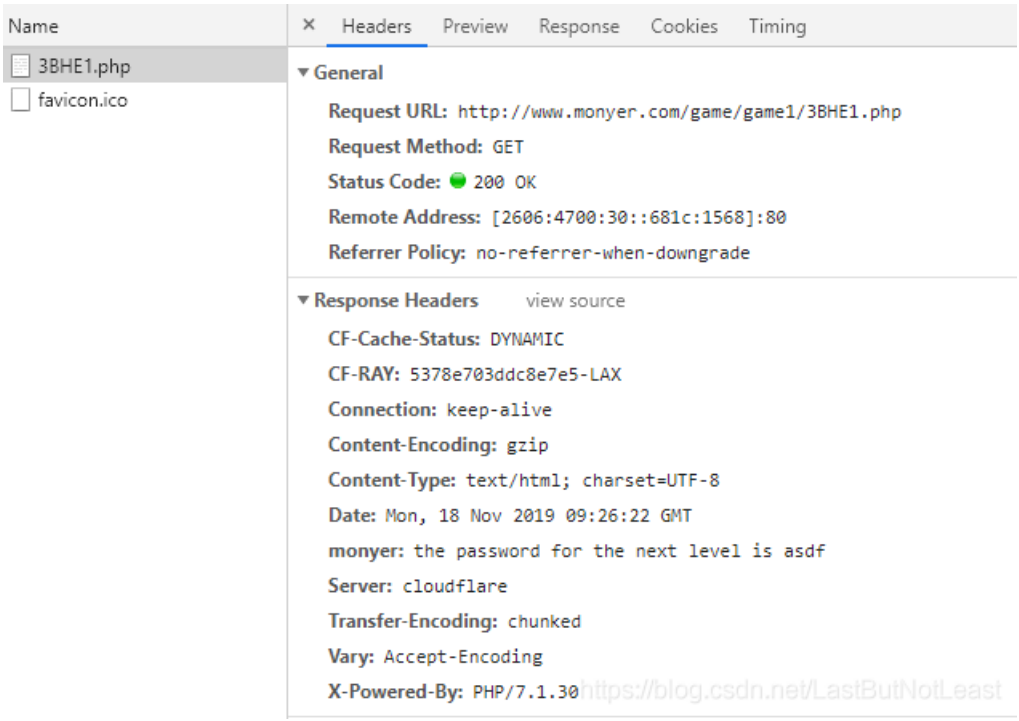
```
加密函数   eval
eval(String.fromCharCode(102,117,110,99,116,105,111,110,32,99,104,101,99,107,40,41,123,13,10,09,118,97,114,32,97
,32,61,32,39,100,52,103,39,59,13,10,09,105,102,40,100,111,99,117,109,101,110,116,46,103,101,116,69,108,101,109,1
01,110,116,66,121,73,100,40,39,116,120,116,39,41,46,118,97,108,117,101,61,61,97,41,123,13,10,09,09,119,105,110,1
00,111,119,46,108,111,99,97,116,105,111,110,46,104,114,101,102,61,97,43,34,46,112,104,112,34,59,13,10,09,125,101
,108,115,101,123,13,10,09,09,97,108,101,114,116,40,34,23494,30721,38169,35823,34,41,59,13,10,09,125,13,10,125))
直接在console里面把eval(),括号里面的内容(包括括号)复制进去console就得到结果了
或者是alert() ,把那括号里面内容(包括括号)加进alert的括号内

"function check(){
 var a = 'd4g';
 if(document.getElementById('txt').value==a){
  window.location.href=a+".php";
 }else{
  alert("密码错误");
 }
}"
```

Game 4:

```
网页进行了重定向、利用Esc按钮强制停止跳转(或者使用BurpSuite)
Sources  解密两个eval函数
类Game3  在console里面敲a
a=atoUpperCase()+1
atoUpperCase()是转换大写的。+是字符串连接符号
3BHE1
```

Game 5:

```
Chrome  F12   Network   3BHE1.php   重新刷新请求一遍
Headers   Response Headers
monyer: the password for the next level is asdf
```



Game 6:

```
<img alt="请通过以下图片中线索寻找密码" src="img/tupian1.jpg"/>
[http://www.monyer.com/game/game1/img/tupian1.jpg]
对打码字反搜索  用谷歌引擎
有点社工的感觉

或者图片另存为用notepad++查看、发现PS关键词
PS调色发现  色差对比
```

Game 7:

```
联想上一关蒙一个 eighteen
或者网上破解MD5    MD5：5e023995fb3f5e840ee684784f8f0799
https://cmd5.com/     查询结果：  eighteen8
```

Game 8:

```
不要被骗了，直接查F12
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。
    因为只要你肯努力，不畏惧挫折，这个世界上没有难倒你的事。
    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
把答案的5736396  换上网址url上的.php
http://www.monyer.com/game/game1/5736396.php

c++代码
#include "pch.h"
#include <iostream>
using namespace std;
int main()
{
 int a, b, sum=0;
 for (a = 1; a <= 10000; a++)
 {
  for (b = 2; b < a; b++)
  {
   if (a%b == 0)
    break;
  }  //此时遍历完a是为了下面a=b 得出这是质数
  if (a == b)
  {
   sum = sum + a;
  }
 }
 cout << sum << endl;
 system("pause");
}
5736396   改它对应的url ，同前面
http://www.monyer.com/game/game1/5736396.php
```

Game 9:

```
http://www.monyer.com/game/game1/img/4681851790659554.jpg
图片另存为后，用Notepad++打开拖到最下面
简单的图片隐写术
它使用linux的文件组合命令然后保存为jpg
MonyerLikeYou_the10level
```

Game 10:

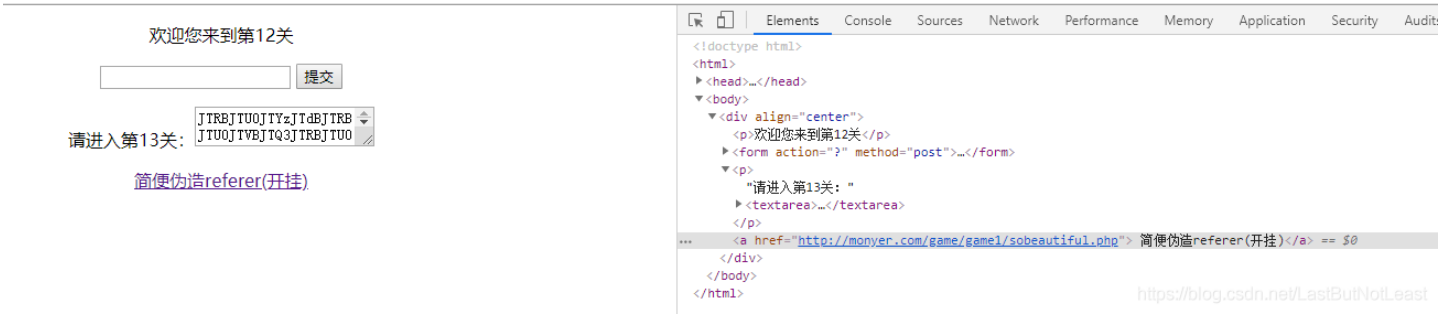
```
http://www.monyer.com/game/game1/MonyerLikeYou_the10level.php
F12   Application   Storage   Cookies    把username的Value中的simpleuser改成admin  然后刷新一下就好了
直接删掉username 会另外的界面   会被嘲讽了一下
Cookie是客户端的数据、而Session是服务端的数据、所以没办法直接修改

<!--此处对最后一关有点影响-->  不然最后会验证是跳关的
以前改了的cookies没改回来不行
在console输入
document.cookie="username=admin"
```

Game 11

```
域名url出有一个action的认证数据  把false改成true就行了
session    https://blog.csdn.net/hjc1984117/article/details/53995816
web端的session  一个重要的东西(这里参考了一篇博文,还没完全掌握)

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

http://www.monyer.com/game/game1/smartboy.php?
```

Game 12:

```
URL安全的base64解码
原始(JTRBJTU0JTYzJTdBJTRBJTU0JTVBJTQ3JTRBJTU0JTU5JTc5JTRBJTU0JTU5JTMxJTRBJTU0JTU5JTc4JTRBJTU0JTYzJTMxJTRBJTU0JTYzJTMwJTRBJTU0JTU5JTM1JTRBJTU0JTU5JTMyJTRBJTU0JTYzJTMxJTRBJTU0JTVBJTQ0JTRBJTU0JTRBJTQ2JTRBJTU0JTYzJTc3JTRBJTU0JTU5JTM0JTRBJTU0JTYzJTc3)

base64(JTczJTZGJTYyJTY1JTYxJTc1JTc0JTY5JTY2JTc1JTZDJTJFJTcwJTY4JTcw)     一次

base64(sobeautiful.php)        两次

但是不能直接跳转、提交内容也不行 (会显示本页禁止盗链)
发现url上有?
审查元素、发现from表单的action对象缺失、把对象修改为sobeautiful.php即可
需要伪造http referer
什么时候会被认为是盗链呢？无非是从外站访问嘛！估计很多人下载软件时都遇到过这个问题（特别是天空），而解决办法就是到它的网站找链接下载。所以本关即使如此，你需要在本站上构造一个链接进入第13关（当然你也可以通过改数据包

但实际最终是edit HTML  在上面加上
<a href="http://monyer.com/game/game1/sobeautiful.php"> 简便伪造referer</a>
```



Game 13:

```
用sql的万能密码' or 1=1搞定
或者
<!--sqlstr="select password,pwd from [user] where pwd='"&request("pwd")&"'"
从数据库中检索匹配的数据]-->
key=whatyouneverknow
```

Game 14:

```
http://monyer.com/game/game1/whatyouneverknow.php
exe的逆向破解

PEID查看crackme.exe程序，发现程序已经upx加壳
使用upx脱壳
PEID查看，是个Delphi 6.0程序
Ollydbg载入程序，直接查找引用的字符串，找到注册成功的语句
得到"ipasscrackme"


以前改了的cookies没改回来不行
[会有这样一句话](你最终没能把cookies设为admin)
在console输入
document.cookie="username=admin"
```

但是cookie这个东西还是不太懂，还待好好研究啊