Hackthis!! Writeup——Basic+ Level

原创

Roverdoge 于 2019-03-04 14:19:04 发布 223 收藏

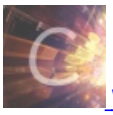
分类专栏： hackthis WP

本文链接：https://blog.csdn.net/qq_43148462/article/details/86697350

hackthis 同时被 2 个专栏收录

5 篇文章 0 订阅

订阅专栏



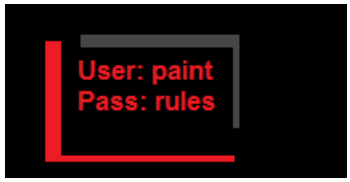
WP

5 篇文章 0 订阅

订阅专栏

Level 1:

首先在网站上可以下载到一个b1.txt,下载下来直接打开是乱码。于是用010editor打开进行分析，发现该文件格式是一个jpg文

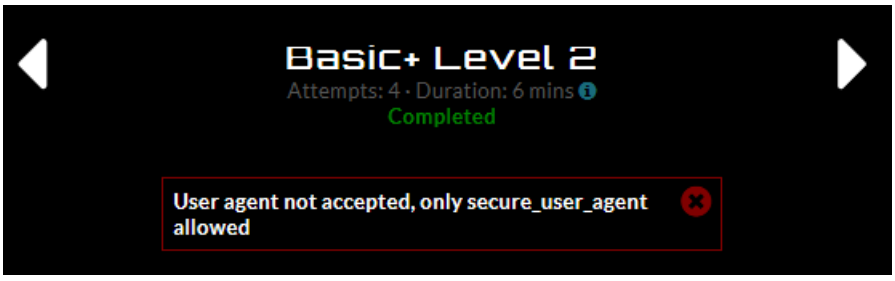


件，于是改后缀名为.jpg获得username和password

关于jpg格式的分析，可以看这篇文章

https://blog.csdn.net/su1041168096/article/details/80938977

Level 2:



题目中给了提示–UA(user agent)，于是随便找个插件（或者抓包修改数据）将自己的UA改为secure_user_agent，便能通过。

Level 3:

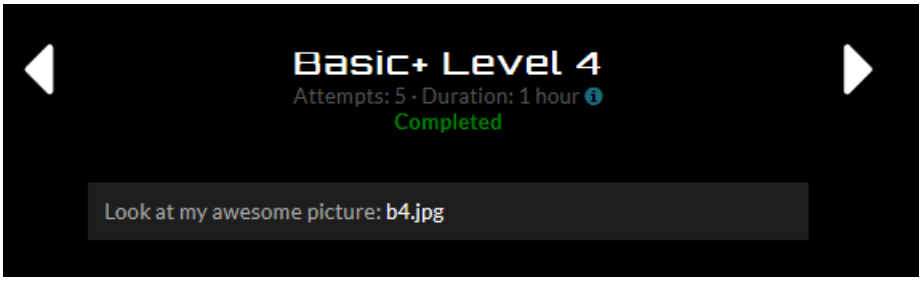
这个题我也不太会，也懒得去搞swf逆向了，现转载一个论坛里的分析

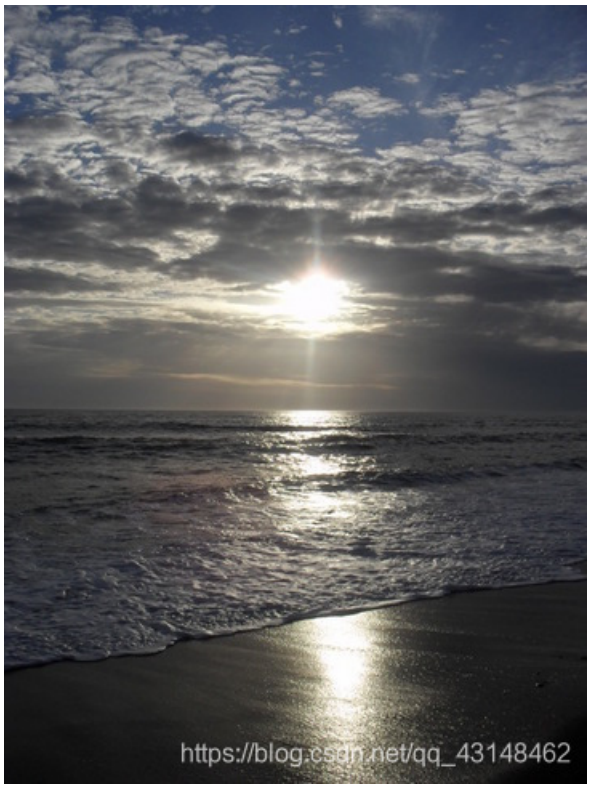
uuff Finally got the solution!!!
o, apparently, I have only scored 109384 in an online game, where I needed to score exactly 194175 to get top of the high-scores table.
Maybe I should still congratulate myself, huh? At least I scored that
much without playing that game even for one second!
Below the text, we see a Flash object, showing our total score. It is a good idea to inspect this object.
I looked at the source code of the webpage to locate where the Flash object resides. This part of the code shows the location:
Navigating to the highlighted link, I downloaded the Flash object
b3.swf. To understand how it interacts with the webpage about the
total score, I decided to reverse engineer it by decompiling the
object to get the source code.
Luckily, decompiling Flash is fairly straightforward in most cases.
Using an online tool , I performed the decompilation:
So, the object has a fairly simple code. There is a variable named
score, which holds the default score, and this variable is sent to the
website by a HTTP POST request, to the URL above. Apparently, we
learnt the mechanism going on behind the scenes. Now, what should we
do?
There came 2 ideas to my mind: 1 - Editing the decompiled source code,
so that score variable holds the score we want; then, compiling the
edited source code, and creating an HTML, embedding the compiled new
Flash object, clicking Submit on the Flash object.
2 - Creating an HTML form with a HTTP Post method which submits the
score we want with the name score.
I chose the latter idea, since it is simpler than the former. I
created the following simple HTML file*:
---

*To create an HTML file, you can simply open a text editor of your choice, type in some HTML code, and save the file with the file name extension .html.
Then, I opened this HTML file in my browser, and clicked the button.
That's it!
Idea no 3 :: You can inspect the source code of the challenge page and
simply add the above html code to footer part and rest you know what
to do ?
Enjoyyyyyyyyyyyyy!!!

做一个简单的总结，就是这位老哥下载下来了这个swf并做了一次逆向代码分析，然后发现这个swf是向这个网站post数据来更新分数，于是自己写了一个网页作为接口向这个网页post数据就OK啦！

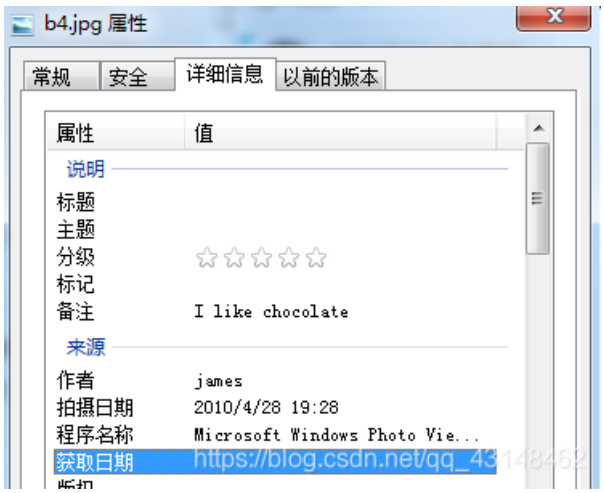
Level 4:





于是我们下载这个图片　　嗯，是这么一张图片。。

这道题一看上去还以为是通过对图片的二进制修改来进行的隐写，于是搞了好久也没找到答案，于是不得不向度娘寻求帮助。没



想到，居然是在详细信息里！　　这里可以看到作者是james，然后有一个“I LIKE CHOCOLATE”

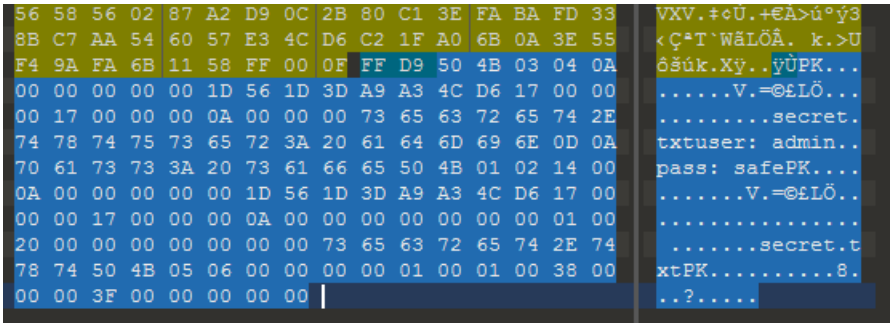
于是猜账号是james，密码是chocolate

你赢了。。。

Level 5:

嗯嗯。。这次又是一张图片　　这次总应该是图片隐写了吧。。。

拖进010editor分析文件，在图片的末尾发现了如!这个（蓝色框）



很明显，这道题利用的是图片在读到FF D9的结束字符后，便会自动忽略后面的内容的特性。后面的文件结构正好是一个zip文件的格式，拖出来新建成一个zip后便可以拿到flag

Level 6:

这道题我觉得算一道社工题吧？第一问查ip，用站长之家一查就能得到。第二问问服务器所处的公司，发现其dns中显示出linode。

第三问是百度出来的，用了gmail中的查看原始邮件功能。（说实话社这道题到现在都很懵，社工搞不来。。）

Level 7:

> We are running a suspicious looking service. Maybe it will give you the answer.

他提示运行着一个可疑的服务，那我门首先用nmap扫描一下他都有什么端口开着（没开linux虚拟机，就先不上图了）

发现6460和6776不知道是用来干什么的，于是我们用telnet连接一下，发现有一个返回了答案：mapthat。