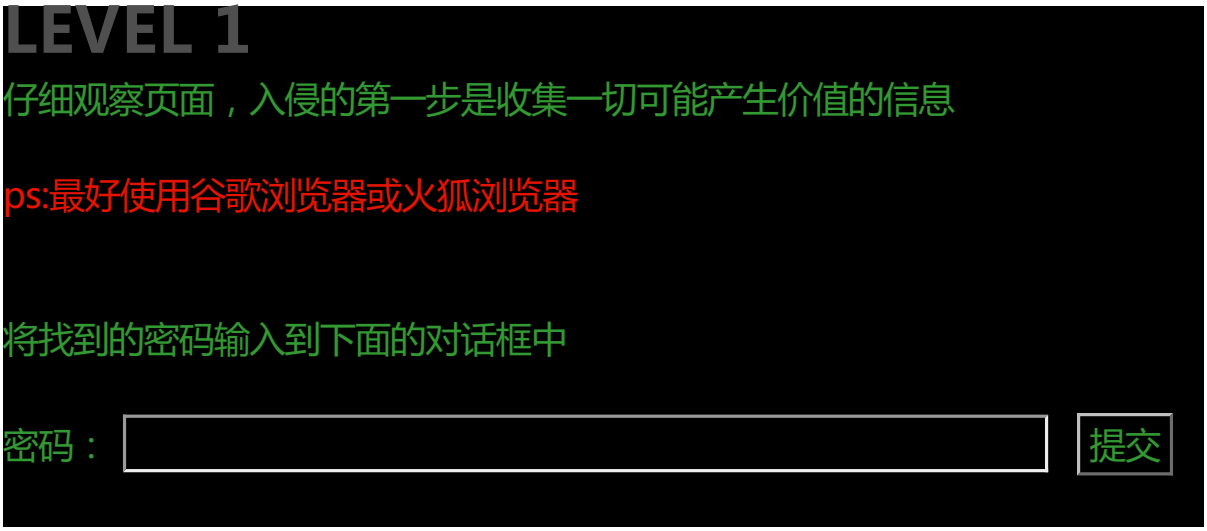
ISA TEST Writeup

原创

Justesss 于 2014-10-05 10:53:19 发布 2695 收藏
分类专栏： Hackgame 文章标签： Hack

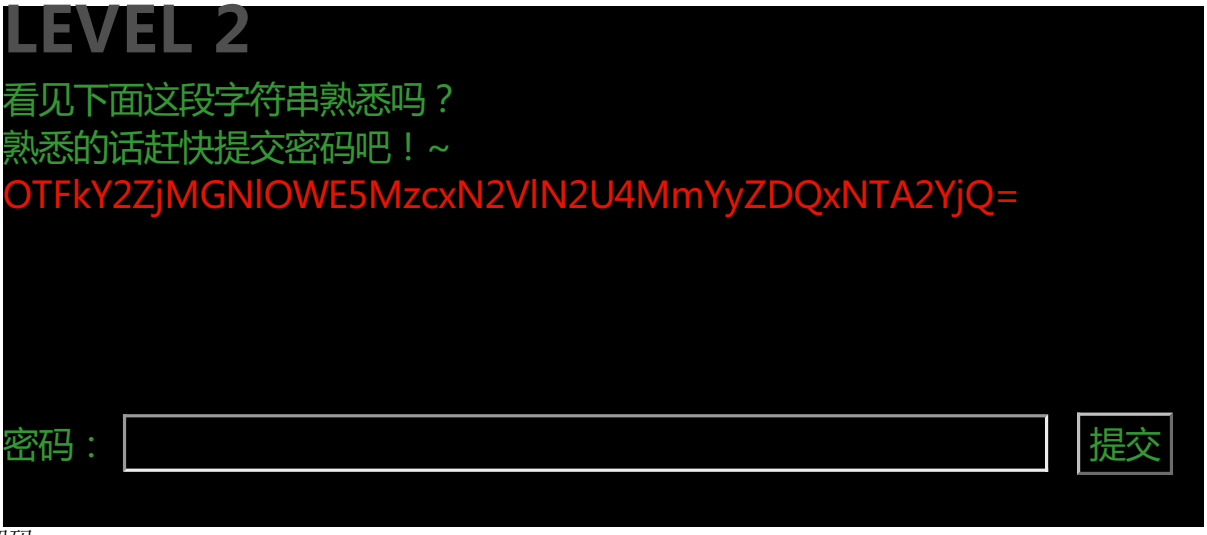
刚出来的hack小游戏，很简单，现在才7关，算是入门级的，没事可以玩一下。http://helloisa.com/



右键查看源码

LEVEL 1	
	<!--
	！！！提示！！！
	分析网页源码是黑客必备的基础技能
	既然你已经看到这句话
	就说明你已经符合 加入我们 的基本要求了
	进入第二关的密码是：186ba6199019568b69315a0f15ae7547
	！！！提示！！！

	-->



base64解码

key：91dcfc0ce9a93717ee7e82f2d41506b4

右键查看源码

LEVEL 3	
	本关的通关密码已经给出并填好，但貌似不能提交啊
	<!-- 绕过网页的本地验证，是黑客的必备技能 仔细看看表单提交的代码吧，你会有意想不到的收获 -->
	<form id="form" action="index.php"method="GET"autocomplete="off"onsubmit="return check();">
	密码：<input name='pwd' type="text"size="50"value="e555c3455a0415abbdbb2467fe3edf82"/>
	<input name='l' type="hidden"value="3"/>
	<input name='a' type="hidden"value="c"/>
	<input type="submit" value="提交">

```
</form>
</div>
<script>
function check(){
if(!form.pwd.value){
alert("密码不能为空");
}else if(form.pwd.value.length>30){
alert("密码不能长于30位");
}else{
alert("密码是 e555c3455a0415abbdbb2467fe3edf82 ");
form.pwd.value='e555c3455a0415abbdbb2467fe3edf82';
}
return false;
}
</script>
```

可以看出当你点击提交时，就会进入check函数，所以不点击提交，直接通过url的get参数提交

并且把url的a=s改为a=c

构造url：http://helloisa.com/test/index.php?l=3&a=c&pwd=e555c3455a0415abbdbb2467fe3edf82

LEVEL 4

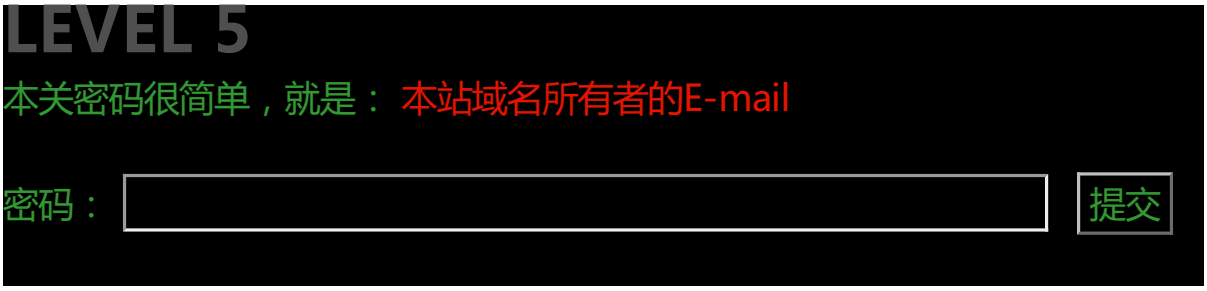
下面这张图片是社团的LOGO，下一关的密码就在里面哦~

密码： 提交

下载图片，hex（十六进制编辑器打开）

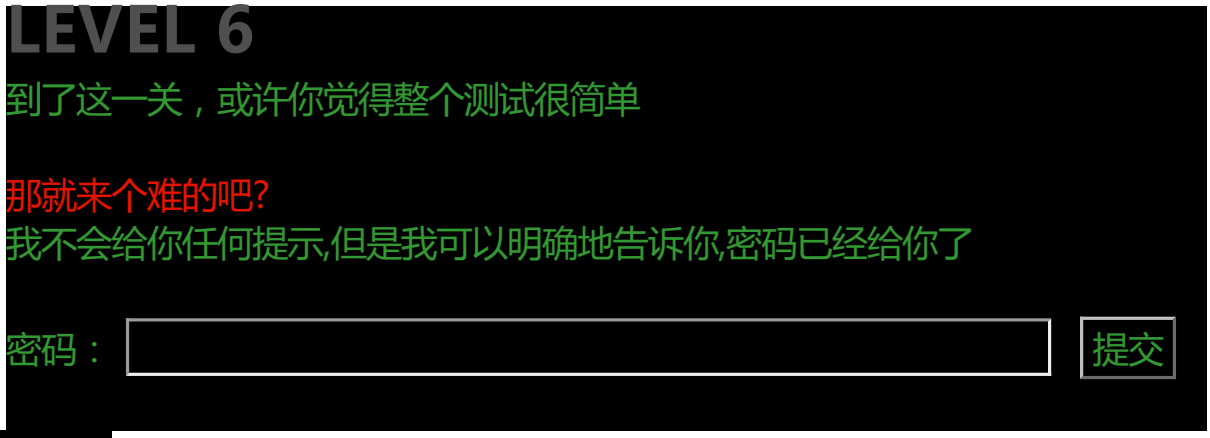
拉到最下面有一段不是乱码的就是key

key：2b4401c871613d0f80224f9c4317bab4



whois查询

key：xing3389@126.com



F12,查看头部

Set-Cookie:

ISA_Level_6_password=1ec8635c58b30741acf1311cb0178edb

LEVEL 7

我们的惯性思维会给我们造成一些阻碍

但是就算我很明确的告诉你密码是什么

你真的能通关吗？

密码：

提交

略坑.....

根据提示惯性思维和明确告诉得出

密码就是：什么