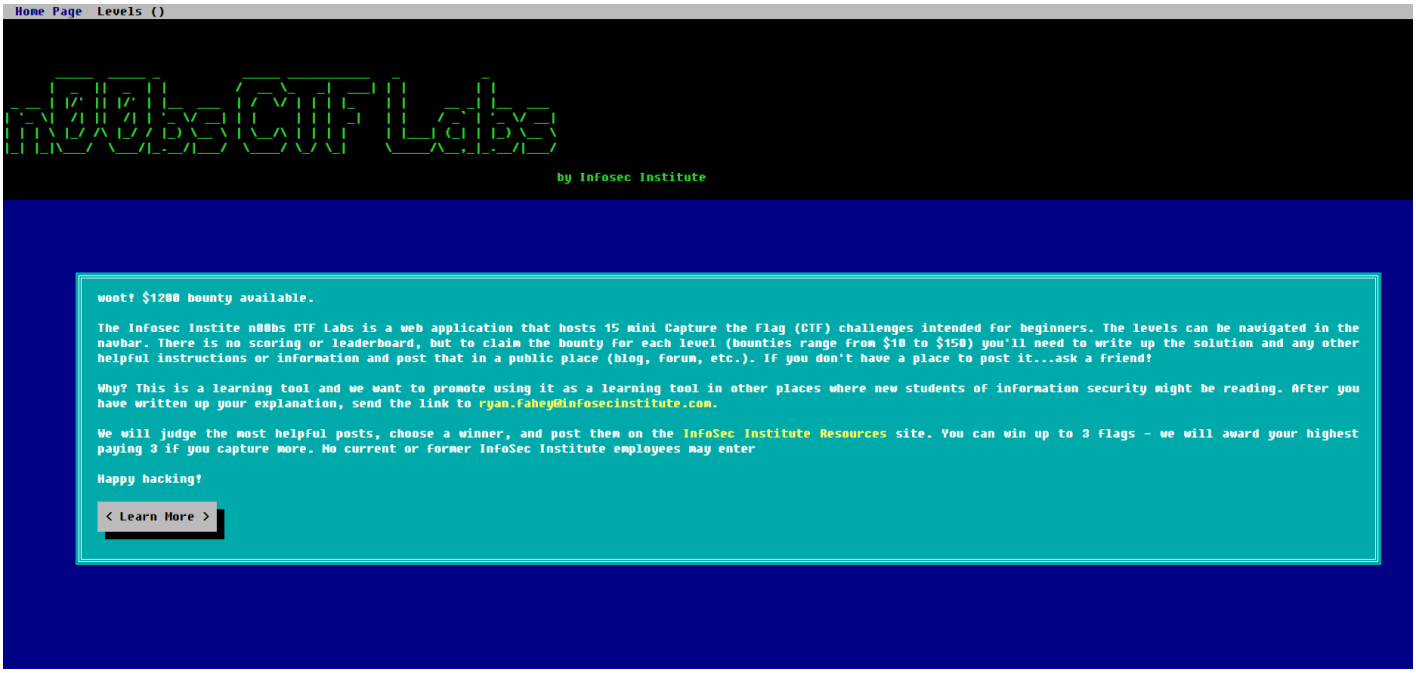
n00bs CTF writeup

转载

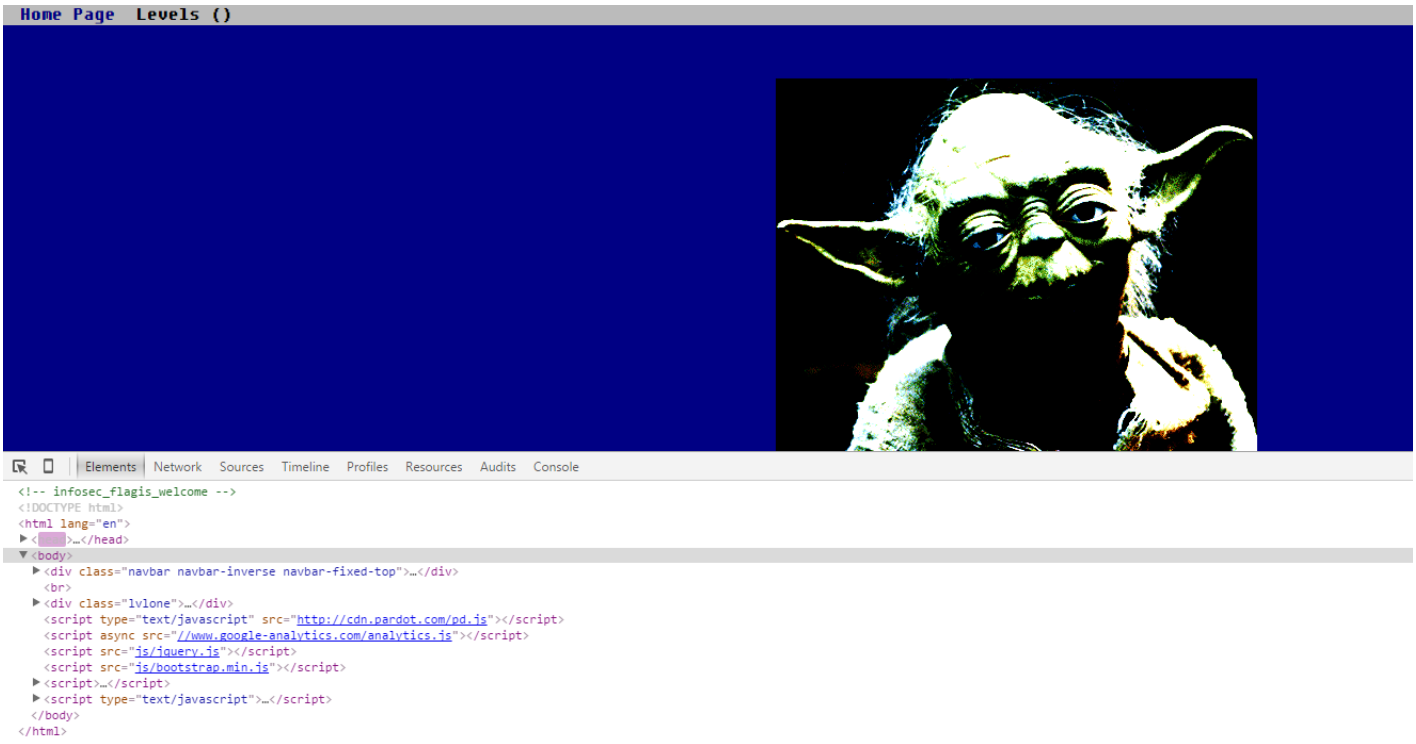
weixin_30887919 于 2015-12-14 00:50:00 发布 23 收藏
原文链接：http://www.cnblogs.com/soroki/p/5043989.html
版权
这个CTF挑战有点意思，我们来看一下，

首页看上去挺不错的。



Level1

直接F12就可以看到flag了。



flag:infosec_flagis_welcome

Level2

"这个图片看上去坏了,你能检查下吗?"

要是搁我假如玩过Linux的话,就很简单了一个curl命令就能可以查看内容（果然linux大法好）。但是我是windows，有点麻烦？下载下来用UE打开看看咯？不要那样！

直接右键是不能查看源代码的，那就加上view-source:吧。好样的。

```
aW5mb3NlY19mbGFnaXNfd2VhcmVqdXN0c3RhcnRpbmc=
```

看样子是base64加密。。。（我只要看到字符串以=结尾，就以为是base64。。。。）

的确是base64，用firefox的hackbar插件解出来

flag:infosec_flagis_wearejuststarting

Level3

有一个二维码？扫一扫也许有惊喜。。。

由于没有手机，我选择了在线的二维码解析器。解析出来的结果为：

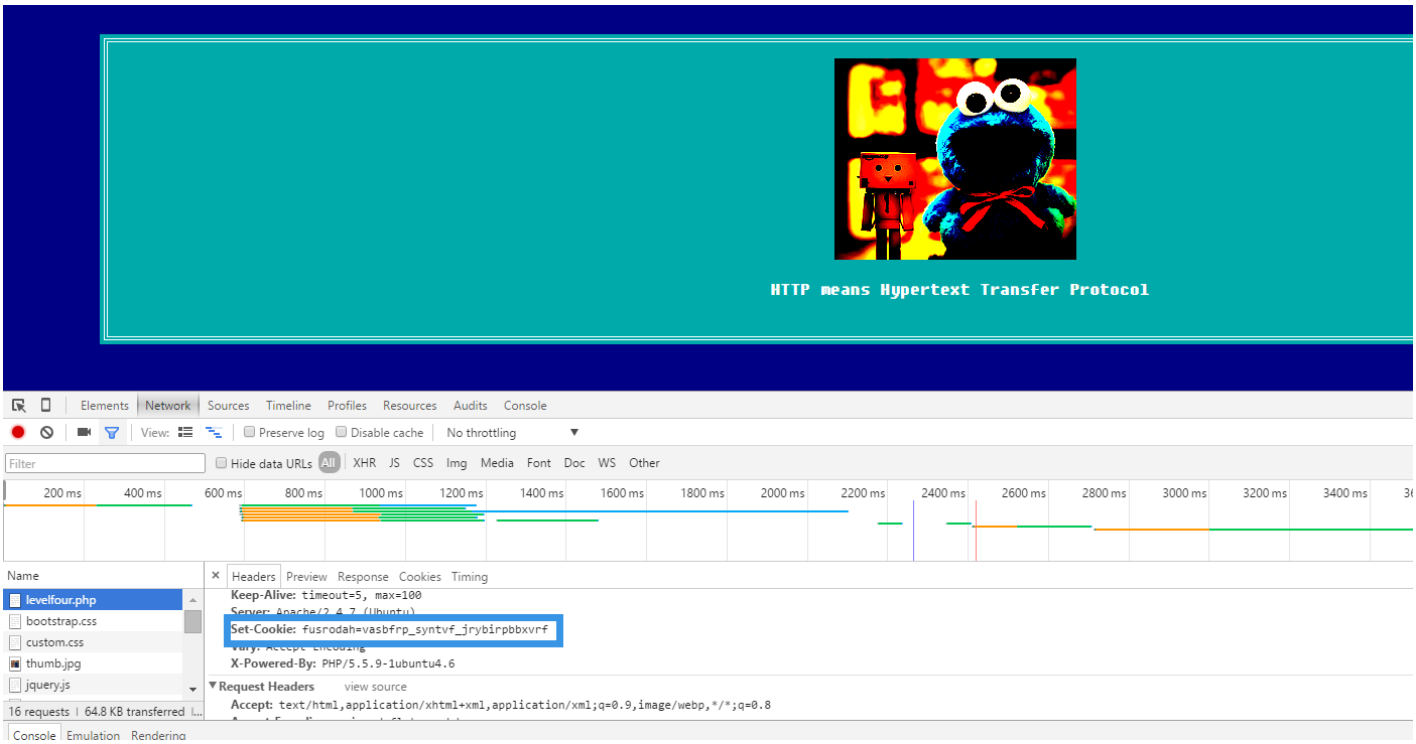
经常看侦探电影里面看到这种电报密码（摩斯码），用自己写的一个小工具就搞定了。（斜眼笑）

flag:INFOSECFLAGISMORSING

Level4

这一关说的HTTP是超文本协议，然后不停的弹窗（然而我点了禁止弹出，所以然并软。。。）

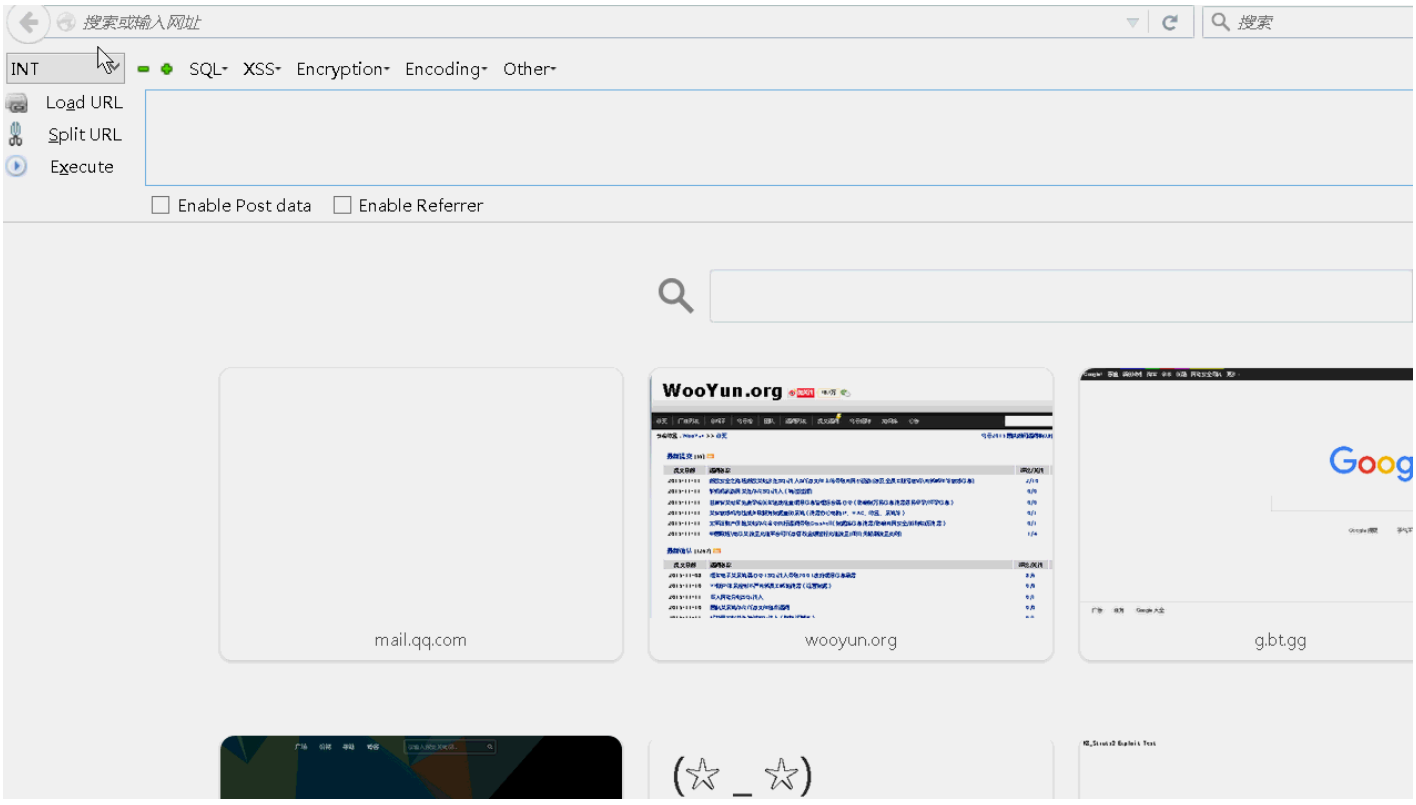
其实这是一个TIP，可以分析下响应头，发现里面有一个参数很可疑。



这里会不会是flag呢。。。。我也不知道。。猜下。。前面几关的flag都有某种规律（正确的说是遵循了格式），都是以infosec（大小写不敏感）开头。

所以里面的vasbfrp是密文，infosec是明文。这样推导就是ROT13，这种加密是以前国外论坛很常见的加密方式。

行动吧，用firefox的hackbar插件验证一下就知道了。



果然，接下来就是逆推出明文了。所谓的ROT13其实感觉就是凯撒密码的一种（移位13）。我的python已经饥渴难耐了~~~

```
from string import maketrans,translate
b= "abcdefghijklmnopqrstuvwxyz"
a= "nopqrstuvwxyzabcdefghijklm"
trantab = maketrans(b, a)

str = "fusrodah=vasbfrp_syntvf_jrybirpbbxvrf";
print str.translate(trantab);
```

```
Python 2.7.10 (default, May 23 2015, 09:44:00) [MSC v.1500 64 bit (AMD64)] on wi
n32
Type "copyright", "credits" or "license()" for more information.
>>> ================================ RESTART ================================
>>>
shfebqnu=infosec_flagis_welovecookies
>>>
```

得到shfebqnu=infosec_flagis_welovecookies，shfebqnu估计没什么用。所以flag:infosec_flagis_welovecookies

未完待续。。。。

转载于:https://www.cnblogs.com/soroki/p/5043989.html