**风荷青年**

风荷青年write-up

1、Sign

Good Luck！flag{X-nuca@GoodLuck!}

这个题是送分题

2、BaseCoding

提示：这是编码不是加密哦!一般什么编码里常见等号？

这一串字符好奇怪的样子，里面会不会隐藏什么信息？[http://question1.erangelab.com/](http://question1.erangelab.com)

这个就是base64加密了一下

3、BaseInjection

账号: admin' or 1=1#

密码随便输

即可登录成功

4、BaseReconstruction

提示过滤了单引号…

原来是提交的时候调用了js，直接审查元素把submit那里的onclick=function那个去掉，然后同样：

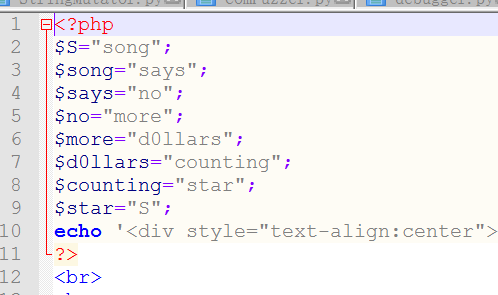
账号： admin' or 1=1#

密码随便输

即可登录成功

5、CountingStars

提示mac侧漏，所以试一下.DS\_Store，发现可以下载，文本编辑器打开后发现有个文件名epLF1rEihQp5AjCUcgGry330jkFSC1C7.zip，URL访问下载下来，即可看到源代码：



总共有109个$，所以结果是d0llars，输入之后提交发现并没看到什么，用burpsuite抓包可以看到返回包，发现flag，原来用了302跳转…

6、Invisible

隐藏IP来保护自己。[http://121.195.186.234](http://121.195.186.234" \t "_blank)

修改头 把X-Forwarded-For加上 改成127.0.0.1就可以了

10、AdminLogin

On the way in。[http://121.195.186.238/index.php](http://121.195.186.238/index.php" \t "_blank)

这个题目首先进行注入 把Referer改成index.php，就可以进行注入了 有union select 然后查看数据库，获得admin 还有pass是Administrat0r，然后目录里面发现有.svn/文件夹，还有robots.txt，在里面看到了一个xnucactfwebadmin目录，进去这个目录的.svn可以看到登录的地址，用刚才的用户名密码登录，登陆之后就可以看到有一张图片 显示出来就好了，下面是图。



index