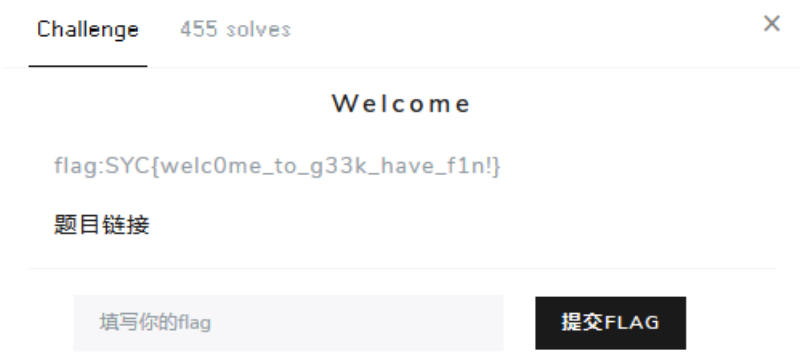
SYC极客大挑战部分题目writeup

转载

weixin_30709809 于 2018-10-27 12:42:00 发布 361 收藏
文章标签： php
原文链接：http://www.cnblogs.com/vhhi/p/9822352.html
版权

Welcome

复制黏贴flag即可



我相信你正在与我相遇的路上马不停蹄

关注微信工作号回复"我要flag"即可获得flag

代号为geek的行动第一幕：毒雾初现

发现flag为摩尔斯密码SYC{--. . . -.- .- -.-. - .. --- -. .... .- ... -... . --. ..- -. }

翻译网站百度找

翻译结果为:GEEKACTIONHASBEGUN

对应的flag:SYC{GEEKACTIONHASBEGUN}

2000字的检讨

看到是一个提交界面，打开万能检讨书准备复制黏贴提交。

发现内容复制不了，F12审查元素复制下来。

粘贴到提交框中，成功获取flag！

学工处-提交检讨　Sycl0ver版万能检讨书　会员充值

提交成功！

This is Your Flag

SYC{evoA_Y0ur_JusT_3Scap3_Th3_Jav4scr1pt_I1m1T}

幸运大挑战

看到题目先点击提交看看结果。根据题意得知应该是只有Get10.00才能拿到Macbook pro(也就是flag)

Get10

提交

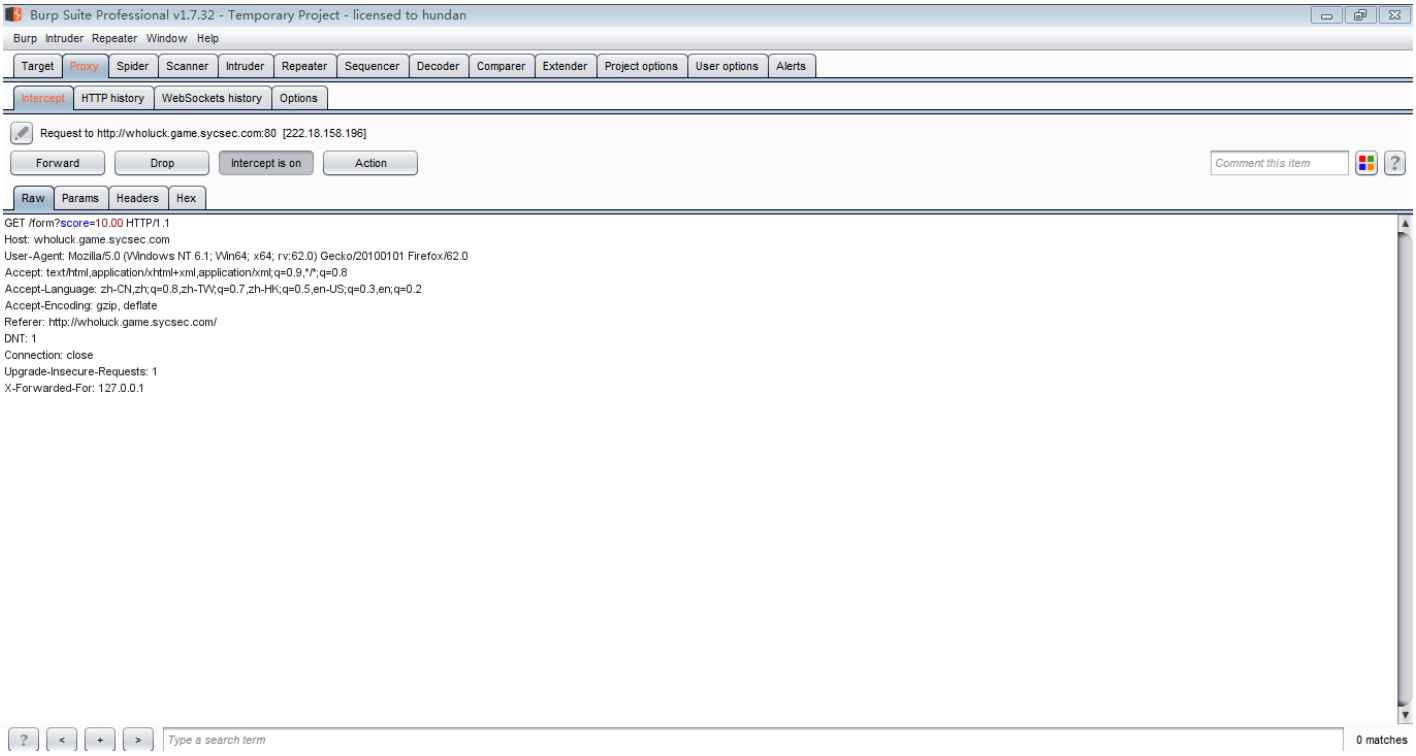
Get10

你的分数是

只有Get10.00才能赢得Macbook pro哦，先到先得！

不服

用burp修改值然后传入



成功获得安慰奖flag一枚hhh

Get10

WoW! You Get 10.00!!!

灰常抱歉，10台Mac已经全部送出！

中奖者信息

1. 江师傅
2. 江师傅
3. 江师傅
4. 江师傅
5. 江师傅
6. 江师傅
7. 江师傅
8. 江师傅
9. 江师傅
10. 江师傅

作为安慰送你一个Flag吧

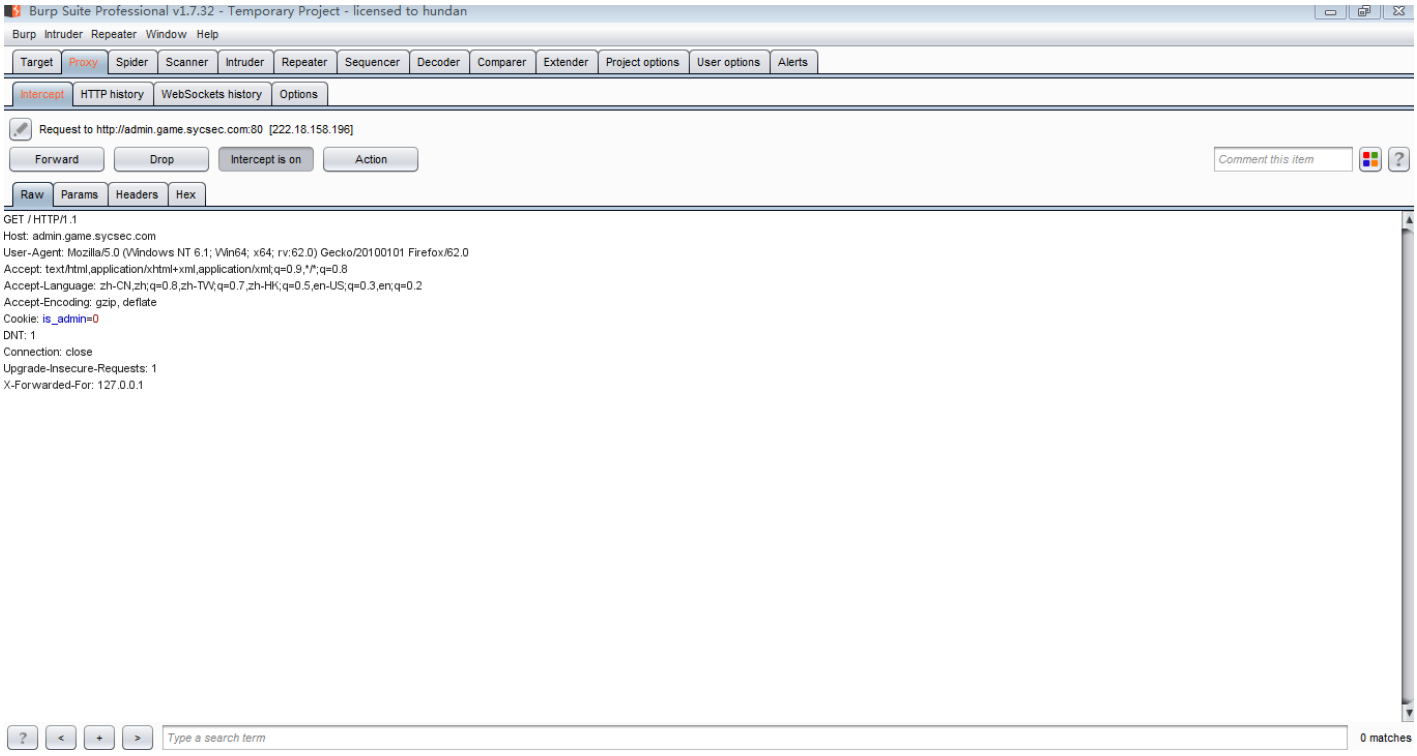
Here is Your Flag: SYC{evoA_U_are_V3ry_FanTaStic_2_G3t_l0!}

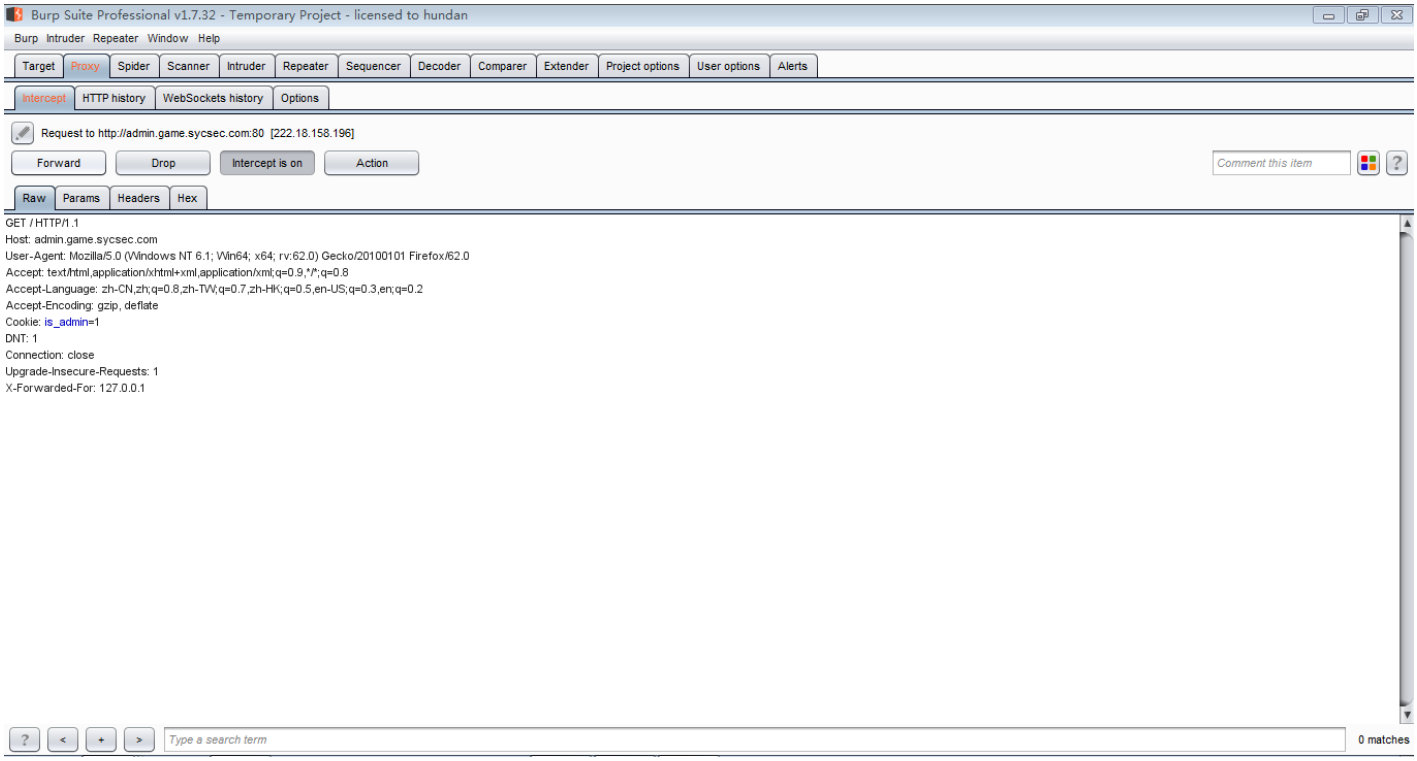
再玩一次

代号为geek的行动第三幕：暗网追击

看到图片显示不是管理员，可能存在某种判断，burp抓包看一下信息

发现cookie中is_admin的属性值为0，改成1看看





Cool Get Flag!

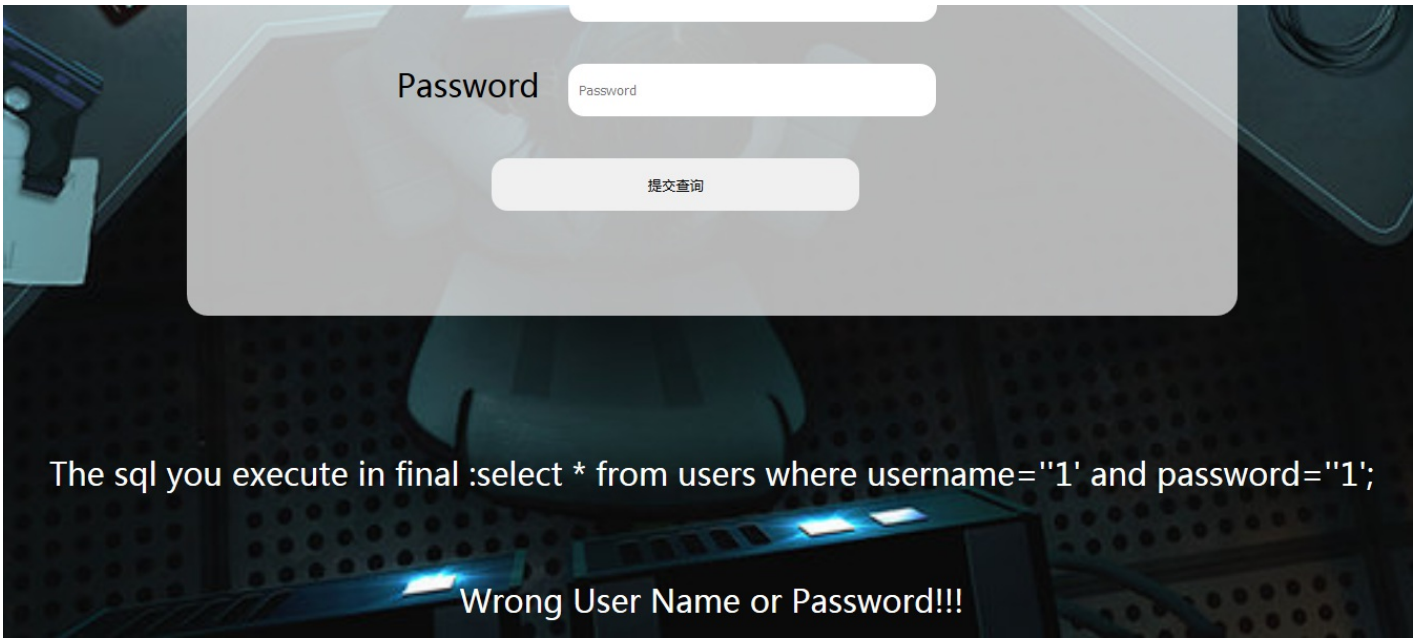
初来乍到

根据题意来找源码，打开页面源代码，ctrl+f搜索到flag


```
ass="nav-list-link" href="/atom.xml" target="_self">RSS</a></li></ul><!-- flag: SYC{View_Page_Source_to_Get_Flag} --></header><main class="container"><div clas
```

代号为geek的行动第二幕：废弃的地下黑客论坛

来到一个后台，先随便乱输一通看看返回的结果



返回了一个sql的语句，是后台登录的逻辑判断，得知这题应该是逻辑绕过

通过对语句的分析构造出判断结果恒为真的语句

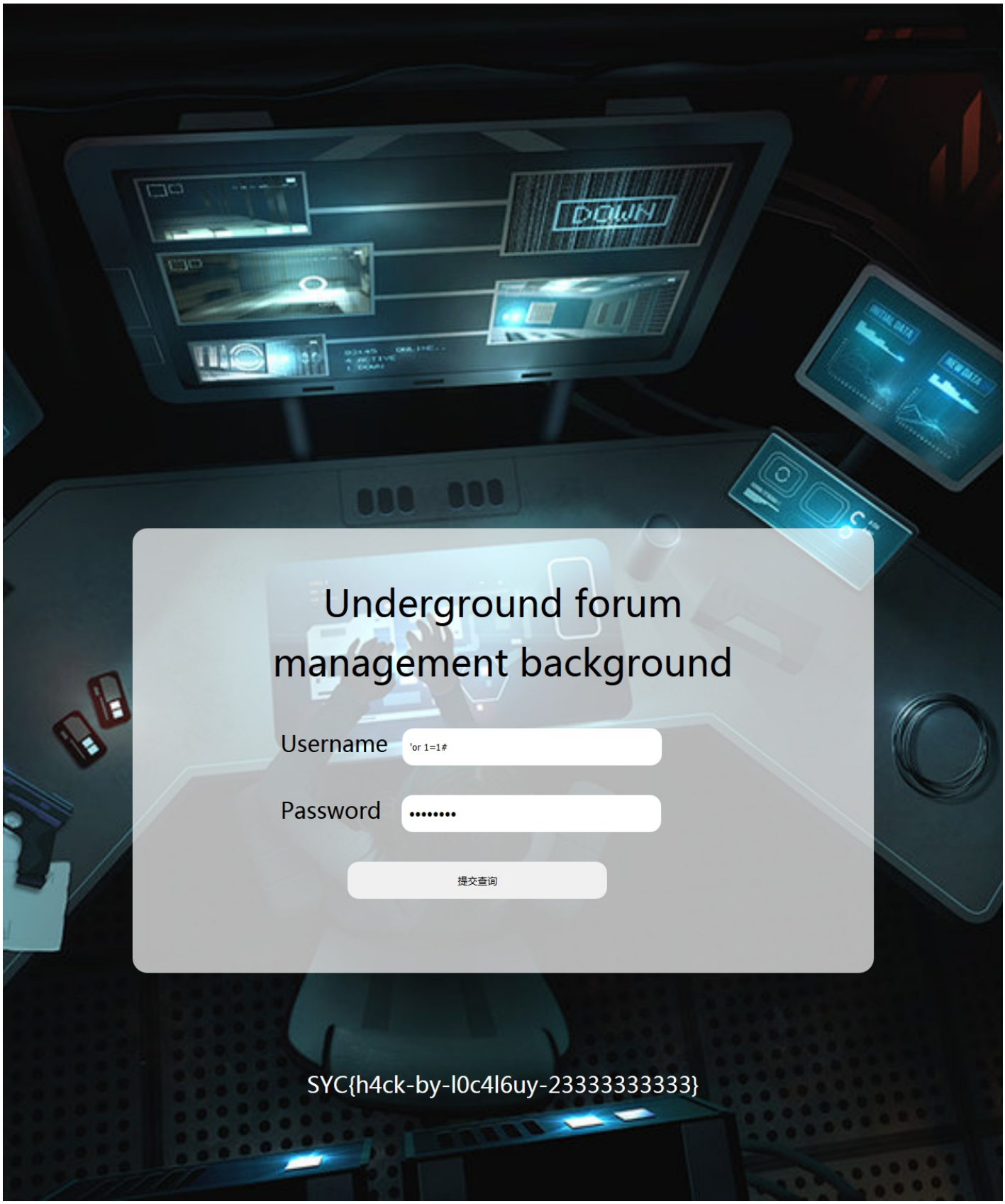
先要想办法将 '' 内的语句逃逸出来，需要在payload前加 ' 单引号闭合引号，中间加入or的判断为真的语句，然后在最后添加#号或--注释掉后面的多余内容

构造出的payload如下:

username: 'or 1=1# 或 'or 1=1--

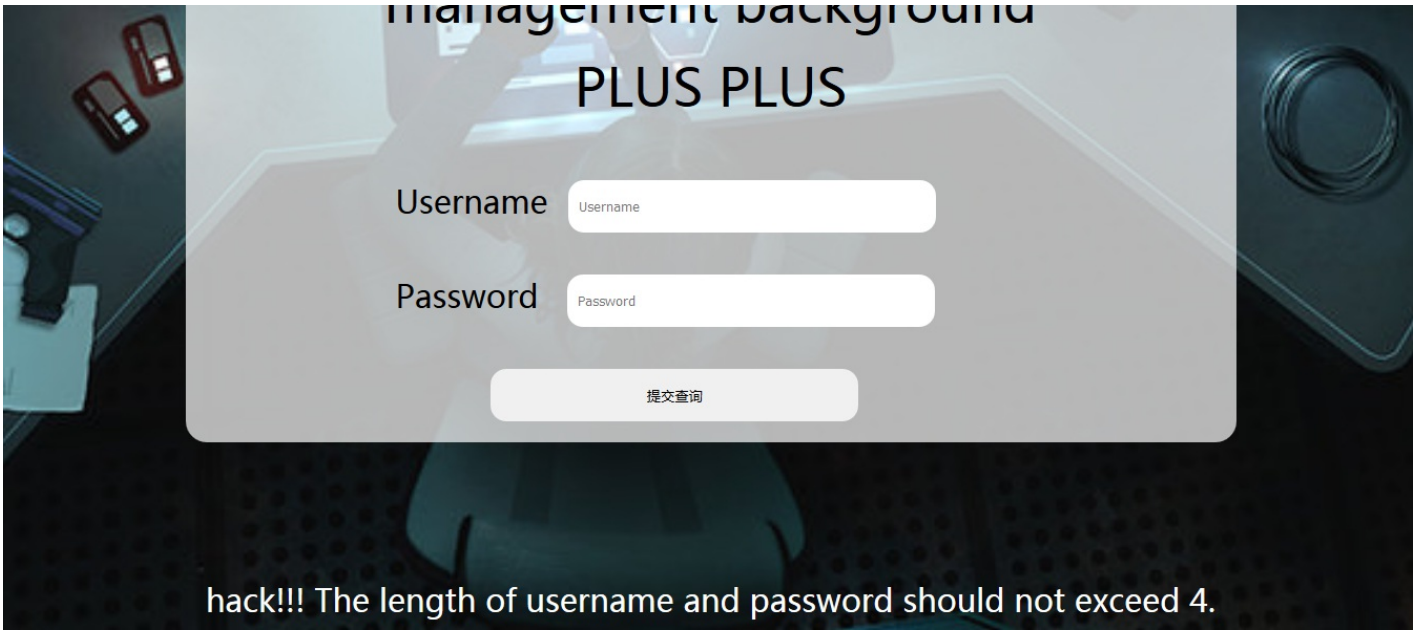
用了上述语句后password随便填

成功绕过，拿到flag~



geek番外篇之废弃的地下黑客论坛

刚才那题的升级版，简单测试一下，发现限制了字符的长度:



于是我们构造出更短的payload:

username输入 \

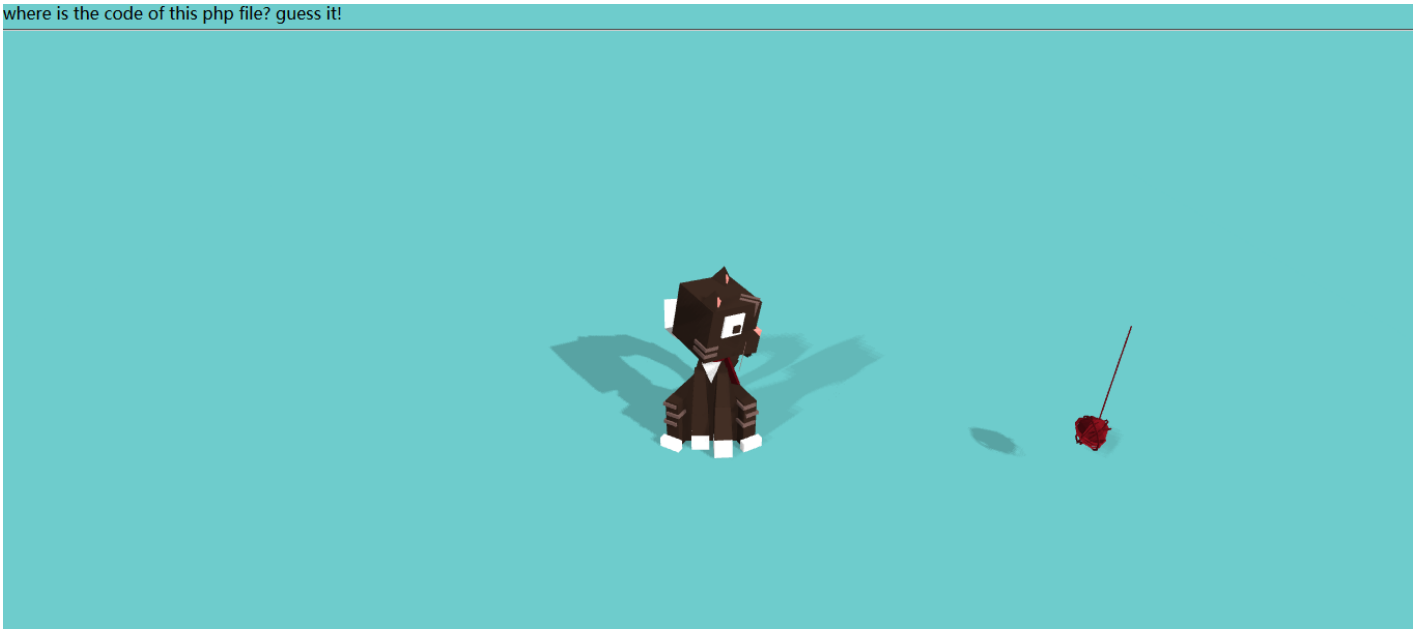
password输入 ||1#

Get flag

一起来和php撸猫啊(该题wp由 羁浪提供)

首先先来分析源码中的php代码

where is the code of this php file? guess it!



```
</body>
<!--
if (isset($_GET['p1'])){

    if ($_GET['p1'] > 99999999 && strlen($_GET['p1']) < 9){

        if (isset ( $_GET ['p2'] )) {
                $p2 = $_GET ['p2'];
                if (is_numeric($p2)){
                    die('Input cannot be a number!!!');
                }
                else{
                    switch ($p2) {
                        case 0 :
                            break;
                        case 1 :
                            break;
                        case 2 :
                            echo "flag{xxxxx}";
                            break;
                        default :
                            echo "2333333";
                            break;
                    }
                }

            }
    }

}
-->
```

通过审计得知整个判断获取flag的过程

先是判断p1变量存在，值大于99999999等等条件，如果成立则继续判断p2是否存在并且不为数字

上述传参皆用GET请求完成，构造出的payload如下图:

babycat.game.sycsec.com/index.php?p1=9e100000&p2=2"2"

传入，然后get flag

where is the code of this php file? guess it!

SYC{pHP_1s_th3_most_p0werfu11}

代号为geek的行动第四幕：绝密情报(该题wp由 羁浪提供)

首先分析php源码:

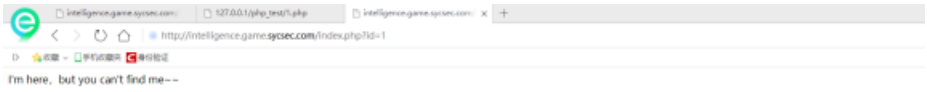
```
<?php
error_reporting(0);
if  (!empty($_GET)||!empty($_POST)){
        if(preg_match("syclover",$_GET['id']))  {
                    echo("<p>you're  a  gay,  not  allowed  !</p>");
                    exit();
        }

        $_GET['id']  =  urldecode($_GET['id']);

        if($_GET['id']  ==  "syclover")
        {
                    echo  "<p>Wow~  ,You're  smart,  Access  granted!</p>";

                    $f  =  $_POST[file];
                    $str  =  $f.".php";
                @require  $str;
        }
        else
        {
                    @require('showpass.php');
        }

}
else  {
        highlight_file("index.php");
}

?>
```

```php
<?php
error_reporting(0);  //关闭错误报告
if (!empty($_GET)||!empty($_POST)){    if(preg_match("syclover",$_GET['id'])) {
        echo("<p>you're a gay, not allowed !</p>");
        exit();
    }

    $_GET['id'] = urldecode($_GET['id']); //对获取的值进行url解码

    if($_GET['id'] == "syclover") //判断值是否等于 “syclover”等于就往下执行
    {
        echo "<p>Wow~ ,You're smart, Access granted!</";

        $f = $_POST[file]; //接收post数据接变量的参数是file
        $str = $f.".php"; //字符拼接这里是拼接个后缀名
       @require $str;  //文件包含
    }
    else
    {
        @require('showpass.php'); //文件包含
    }

}
else {
    highlight_file("index.php");
}

?>
```

看完代码就看看文件包含的是什么妖魔鬼怪访问链接:

http://intelligence.game.sycsec.com/showpass.php

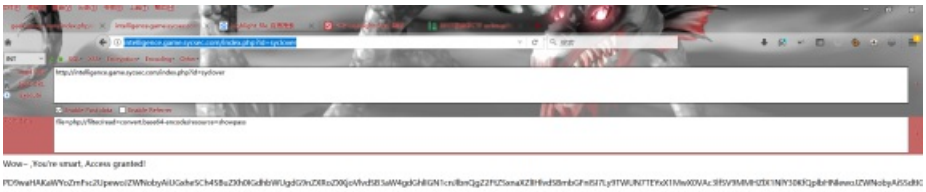
用火狐会有乱码推荐用360打开选择gbk编码



翻译说:它就在这里但是我看不到 我们就利用下面的代码来看看到底写了什么 利用如下代码

```php
        $f = $_POST[file]; //接收post数据接变量的参数是file
        $str = $f.".php"; //字符拼接这里是拼接个后缀名
       @require $str;  //文件包含
```

Payloads :file=php://filter/read=convert.base64-encode/resource=showpass



出来是一段base64，去转一下码即可拿到flag

江江师傅的秘密

首先先审题，题意是让我们找到这个c盘下的study.txt，可能就是flag

打开后并没发现有什么不对的地方

然后想到file协议读取本地文件看看

flag到手~

三叶草代理服务

请输入URL　例: http://www.baidu.com

file:///C:/study.txt

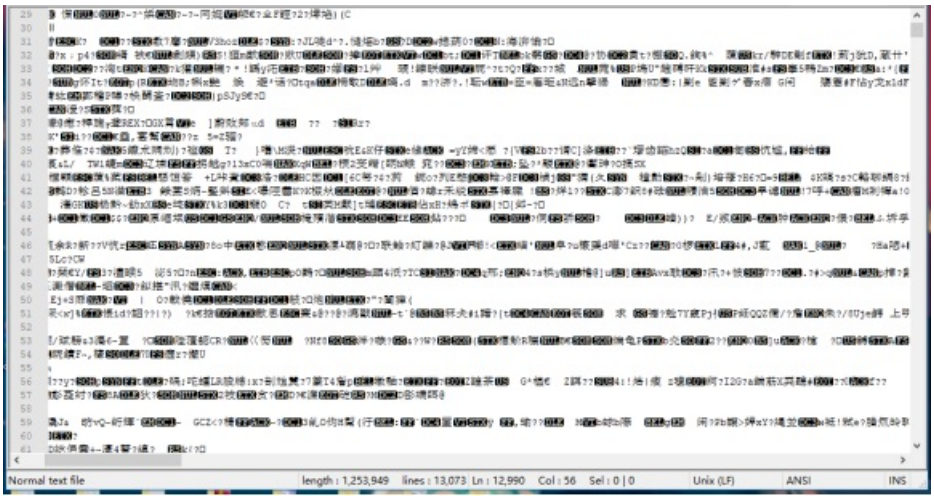
提交

SYC{evoA_W0W_Y0u_k0nW_th3_file_Pr0t0c0l}

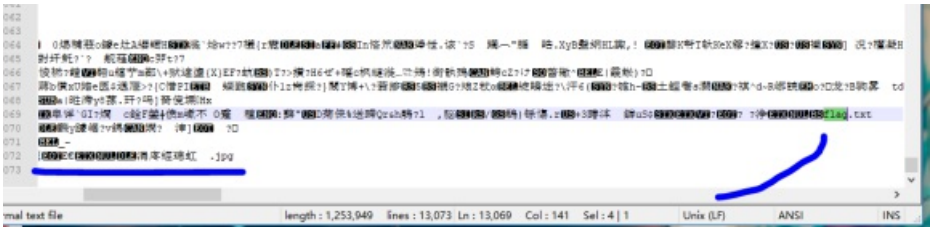
点~击~查~看~高~清~无~码~多~人~大~戏~刺激包爽~深夜一个人看的视频

萌萌的血小板(该题wp 由羁浪提供)

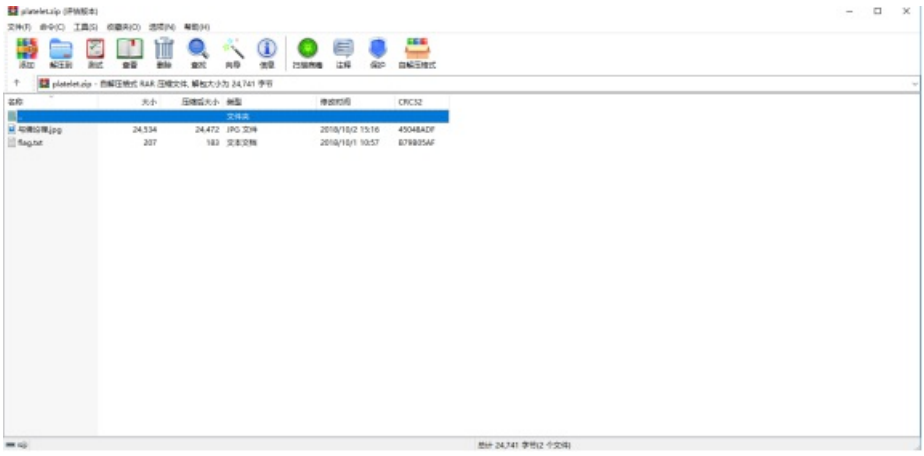
咋一看, 是一张图片,其实它可以是一个图片也可以是一个压缩包。怎么判断它是压缩包呢 我们用notepad++打开图片



咋一看没撒子问题 我们Ctrl+f 快捷搜索下有没有flag 这些关键字 因为里面存放这我们需要的东西



Flag.txt + xxx.jpg 觉得是压缩包 那么把后缀名改成.zip探究竟夭寿了！！！ 居然可行



看到flag.txt那就直接打开咯

我尼玛 这啥玩意....

稍加思索 看准图片 与佛论禅 百度一波

呦吼这个居然是个加密方法 在线解密地址：

http://www.keyfc.net/bbs/tools/tudoucode.aspx

这玩意拿来也不会用呀 于是我就乱点 终于普渡众生哪里有了使用教程

然后我们就把

佛曰：哆真阿怯菩諦勝缽室不俱悉孕怯豆皤爍缽槃缽舍竟奢迦竟姪俱伊藐俱多蘇罰苦侄帝諳寫缽寫夷若侄菩羯逝除薩伽豆提吶上罰謹俱尼缽地能冥無恐遠咒薩不姪所

这一段放到 佛家秒语那一栏 点击参悟佛所言的真谛就可以得到flag了

小帅圆圆的发际线，你也想要么？(该题wp由小金星提供)

发际线

binwalk一下，发现是个rar

更改后缀名，直接解压得到666.jpg，打开发现上面有一串brainfuck语句，

010打开，别用**记事本**会出现错误，010打开后在最后面将brainfuck语句copy出来

> ```
> +++++ ++++[ ->+++ +++++ +<]>+ +.+++ +++.< ++++[ ->--- -<]>- ----- .<+++
> ++++[ ->+++ ++++< ]>+++ ++++. <++++ [->-- --<]> ---.. ....- ----- ---.<
> +++++ [->-- ---<] >---- ..... .<+++ +++[- >++++ ++<]> +++++ +++++ ++.<+
> +++[- >---- <]>-. +++++ +++.+ ++++. ----- ---.< +++[- >+++< ]>+++ +++..
> ..<++ ++[-> ----< ]>--. +++++ +++.< +++[- >---< ]>--- .<+++ ++[-> +++++
> <]>+. <++++ ++++[ ->--- ----- <]>-- ----- --.<+ +++++ ++[-> +++++ +++<]
> >++++ +.<++ ++[-> ----< ]>--- ---.. +++++ +++.+ +++++ ++.++ +++.< ++++[
> ->--- -<]>- ----. <+++[ ->+++ <]>+. <+++[ ->+++ <]>++ .<+++ +++++ +[->-
> ----- ---<] >--.< +++++ ++++[ ->+++ +++++ +<]>+ +++++ +++++ .<
> ```

用在线工具解码得到*SYC{hhhhhh_BBBBBBrainfuuuuck_y0u__got_it!}*

代号为geek的行动第五幕：损坏的镜像(该题wp 由小金星提供)

同样binwalk跑一下，发现有很多东西
然后
```
foremost 文件名　　//还原镜像中的文件
```
得到的文件中有个flag.txt，flag就在其中

-*- ----------Stop---------- -*-

Writeup by Rose Ctf Team(RCT):一个由众多ctf小白组成的菜鸟战队,各种天外异型皆在其中

微信公众号:地心报社

Please pay attention to us.

转载于:https://www.cnblogs.com/vhhi/p/9822352.html