xctf web i-got-id-200

原创

doudoudedi 于 2019-06-20 13:00:22 发布 3579 收藏 2

分类专栏： xctf 文章标签： xctf web

本文链接：https://blog.csdn.net/qq_37433000/article/details/93016297

今天就一个毛概课但是很热啊

中午来写一个wp

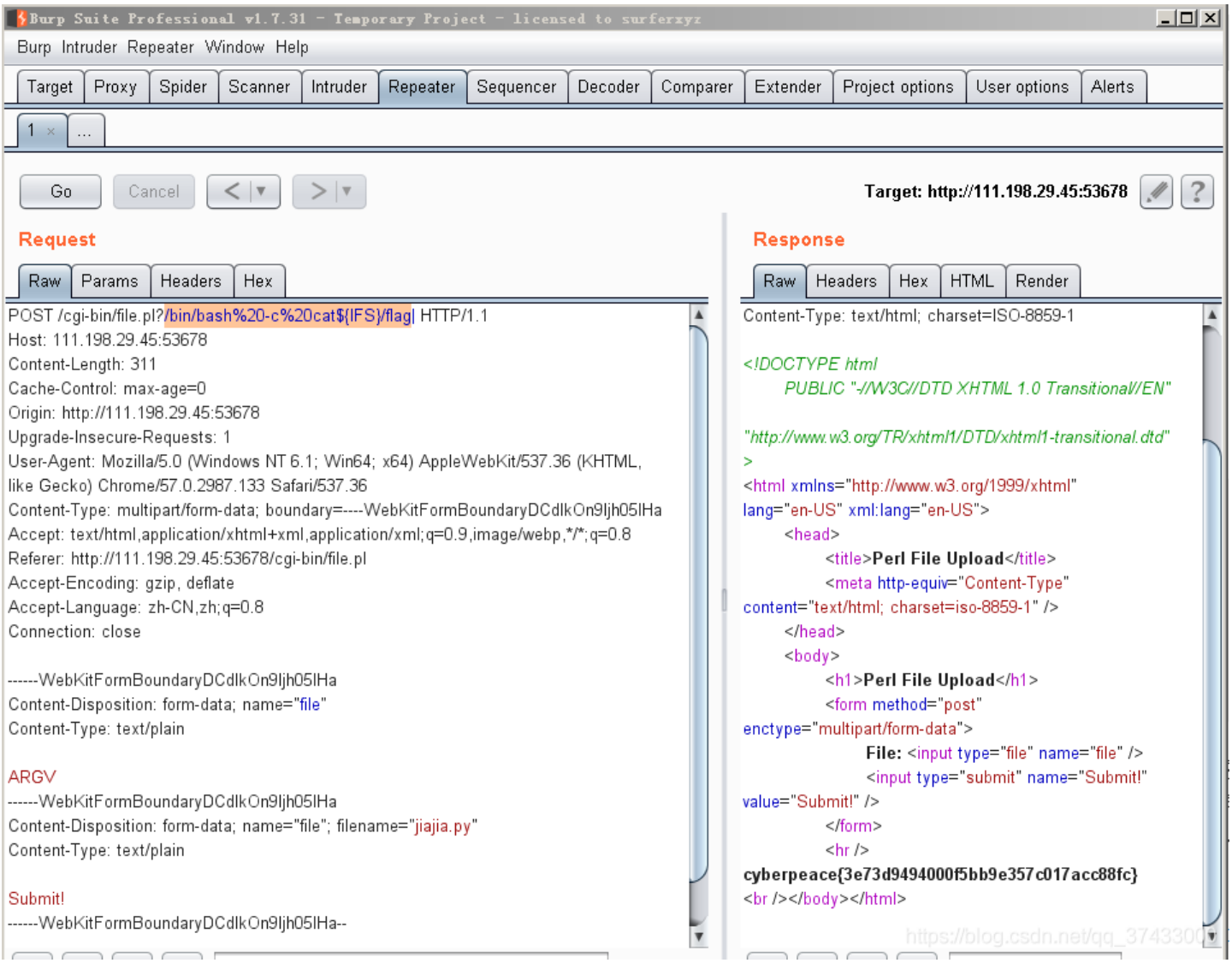
打开题目会有

直接跳到文件会有一个上传，但它会将上传的内容显示出来

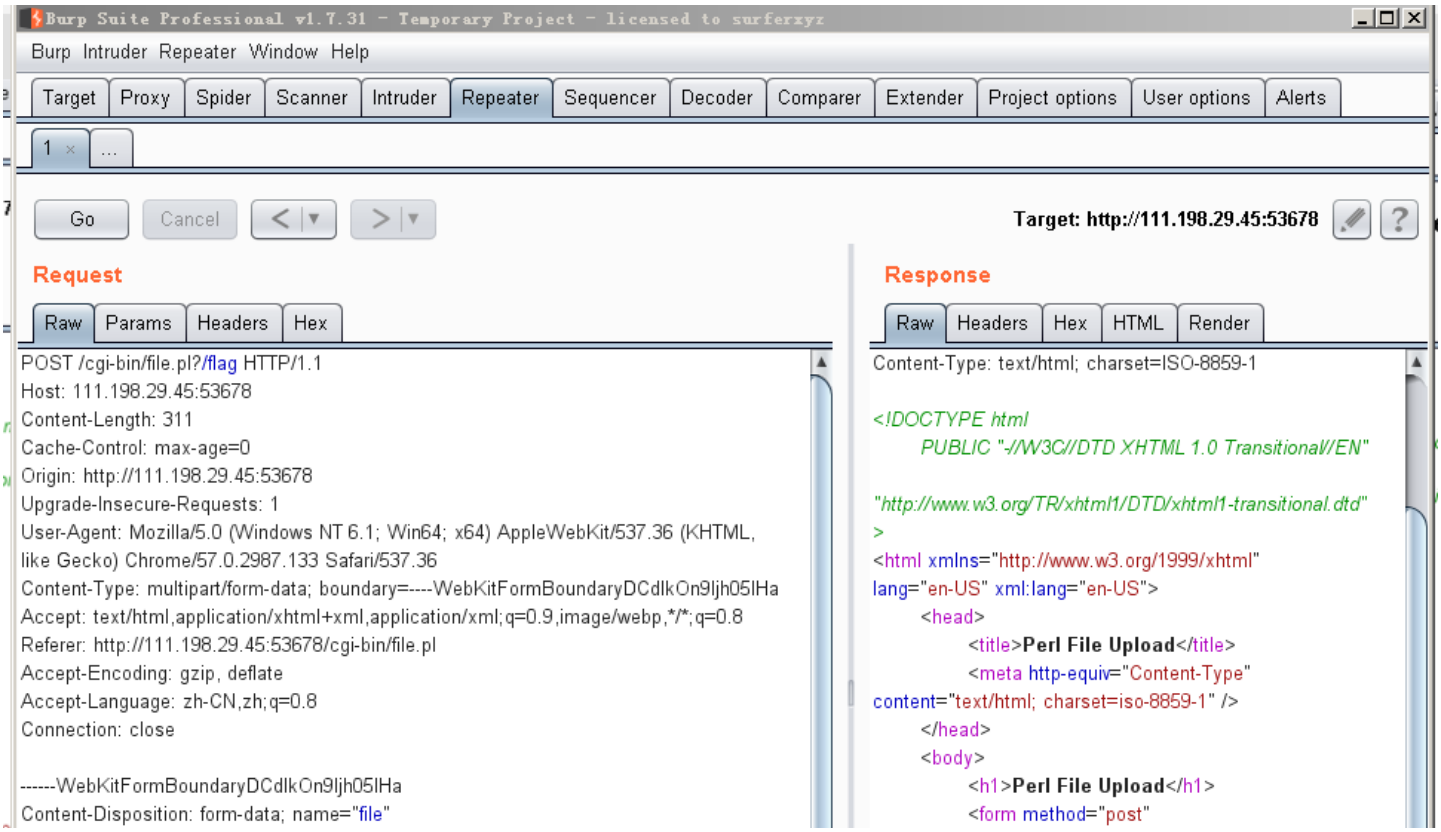
哦们可以猜测他的php代码（前面还有提示哦）

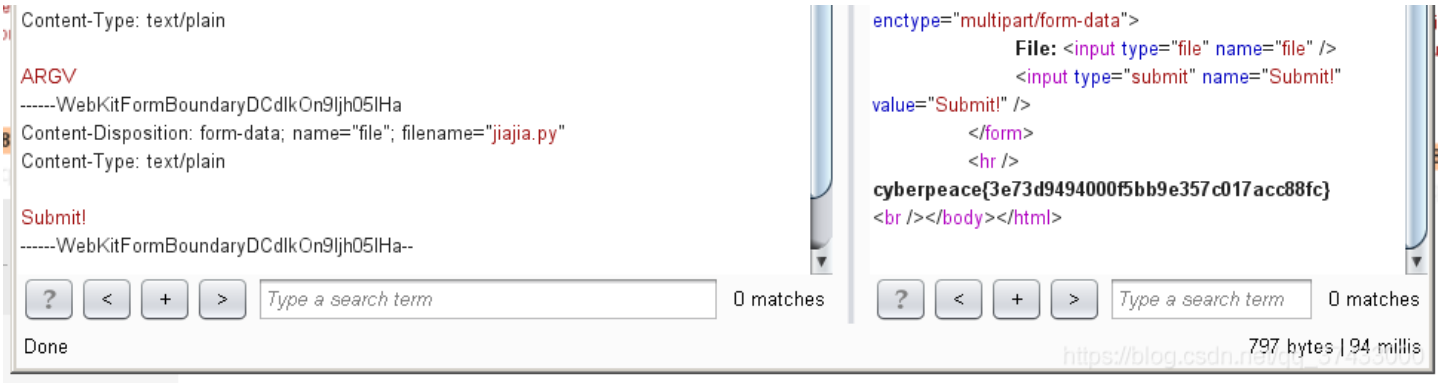
```perl use strict; use warnings; use CGI;
my $cgi= CGI->new;
if ( $cgi->upload( 'file' ) )
{ my $file= $cgi->param( 'file' );
while ( <$file> )
{ print "$_";
} }
```

那么，这里就存在一个可以利用的地方，param()函数会返回一个列表的文件但是只有第一个文件会被放入到下面的file变量中。而对于下面的读文件逻辑来说，如果我们传入一个ARGV的文件，那么Perl会将传入的参数作为文件名读出来。这样，我们的利用方法就出现了：在正常的上传文件前面加上一个文件上传项ARGV，然后在URL中传入文件路径参数，这样就可以读取任意文件了。



这里还可以猜flag的比如





水完了哈哈

/bin/bash%20-c%20ls$IFS/|/bin/bash${IFS}/flag|