**涉及知识点：**

**·upload 的pclzip漏洞**

**·目录穿越**

**·源码审计**

**·apache解析漏洞**

**·利用010构造zip下的非法文件名**

**所需工具：**

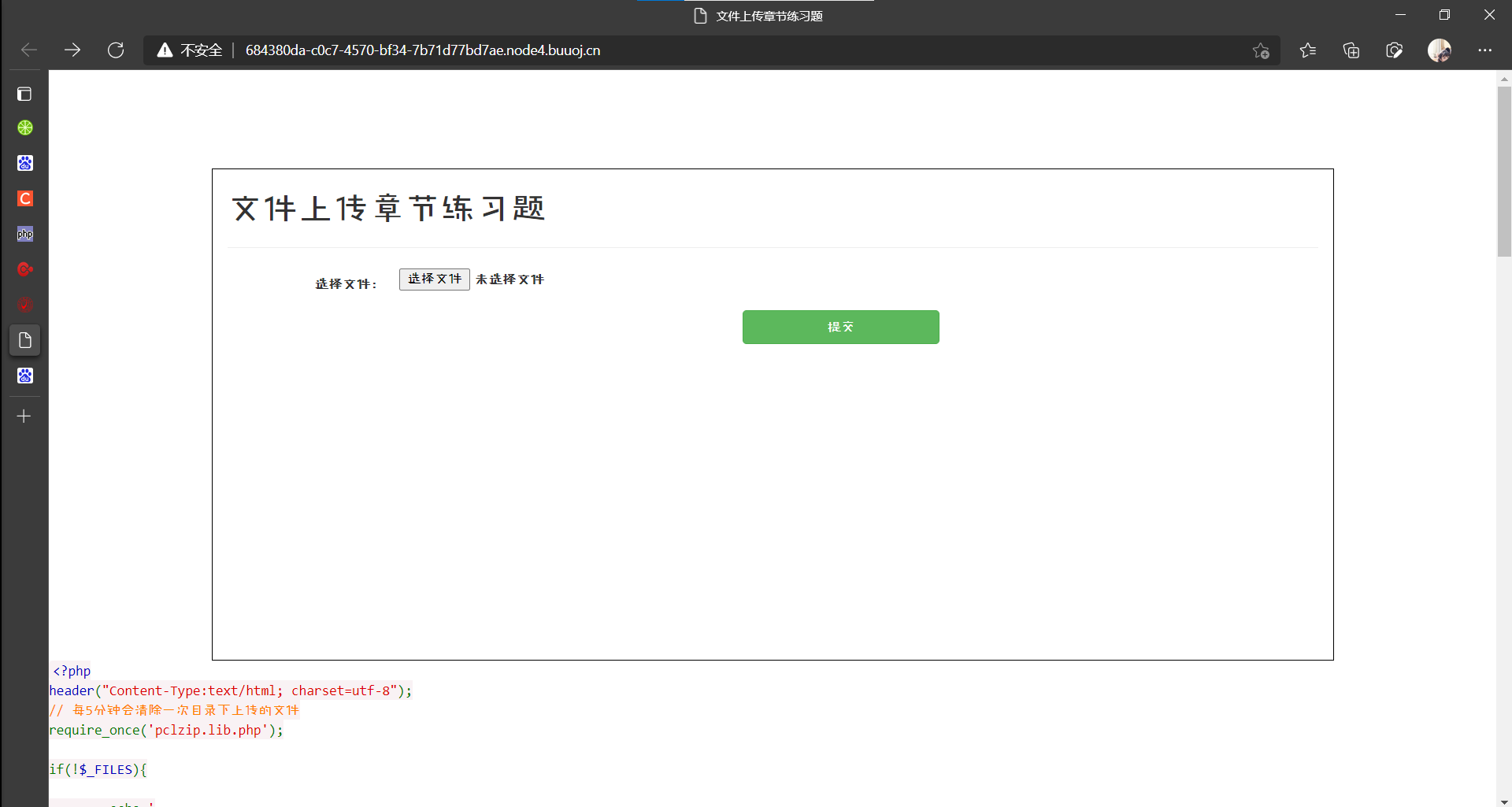
**·010editor**

**·010的template模块**

**·压缩软件**

**ZIP压缩例题WP**

进入题目：



发现题目下面就有源码：

<?php

header("Content-Type:text/html; charset=utf-8");

*// 每5分钟会清除一次目录下上传的文件*

*//会包含文件pclzip.lib.php，这个php里面是有一些针对zip包进行解压等的操作的*

require\_once('pclzip.lib.php');

*//要是没上传文件，就输出上传页面*

if(!$\_FILES){

echo ' '

show\_source(\_\_FILE\_\_);

}else{

$file = $\_FILES['file'];

*//限制上传的文件名不为空*

if(!$file){

exit("请勿上传空文件");

}

$name = $file['name'];

$dir = 'upload/';

*//strrchr($name, '.')*

*//strrchr() 函数查找字符串在另一个字符串中最后一次出现的位置，并返回从该位置到字符串结尾的所有字符。*

*//比如上传的文件名为$name=1.php.txt，这里strrchr($name, '.') 执行结果为.txt*

*//substr(strrchr($name, '.'), 1)*

*//substr字符串截取，从下标为1开始截取，那就是把点略过，截取后为txt*

*//通过strtolower函数将所有字符转换为小写，赋值给ext变量*

$ext = strtolower(substr(strrchr($name, '.'), 1));

*//如果我们上传的文件名为1.txt，那么path变量就为upload/1.txt*

$path = $dir.$name;

*//检查是否为目录*

function check\_dir($dir){

$handle = opendir($dir);

while(($f = readdir($handle)) !== false){

if(!in\_array($f, array('.', '..'))){

if(is\_dir($dir.$f)){

check\_dir($dir.$f.'/');

}else{

$ext = strtolower(substr(strrchr($f, '.'), 1));

if(!in\_array($ext, array('jpg', 'gif', 'png'))){

unlink($dir.$f);

}

}

}

}

}

*//创建目录*

if(!is\_dir($dir)){

mkdir($dir);

}

*//将目录名拼接一个随机数，读到这里，基本上就知道需要路径穿越了，因为我们不知道随机数值，所以就算绕过上传，解析也是一大关*

$temp\_dir = $dir.md5(time(). rand(1000,9999));

if(!is\_dir($temp\_dir)){

mkdir($temp\_dir);

}

*//首先进行后缀的校验，把刚刚拿到的，最后一个.后面的字符串和这里的zip、jpg、gif、png进行对比校验*

if(in\_array($ext, array('zip', 'jpg', 'gif', 'png'))){

if($ext == 'zip'){

*//使用PclZip进行解压缩*

$archive = new PclZip($file['tmp\_name']);

*//遍历解压缩后的每个目录*

foreach($archive->listContent() as $value){

$filename = $value["filename"];

*//一段较为简单的正则，就是匹配每个文件结尾的位置，是否是.php*

if(preg\_match('/\.php$/', $filename)){

exit("压缩包内不允许含有php文件!");

}

}

if ($archive->extract(PCLZIP\_OPT\_PATH, $temp\_dir, PCLZIP\_OPT\_REPLACE\_NEWER) == 0) {

check\_dir($dir);

exit("解压失败");

}

check\_dir($dir);

exit('上传成功!');

}else{

move\_uploaded\_file($file['tmp\_name'], $temp\_dir.'/'.$file['name']);

check\_dir($dir);

exit('上传成功!');

}

}else{

exit('仅允许上传zip、jpg、gif、png文件!');

}

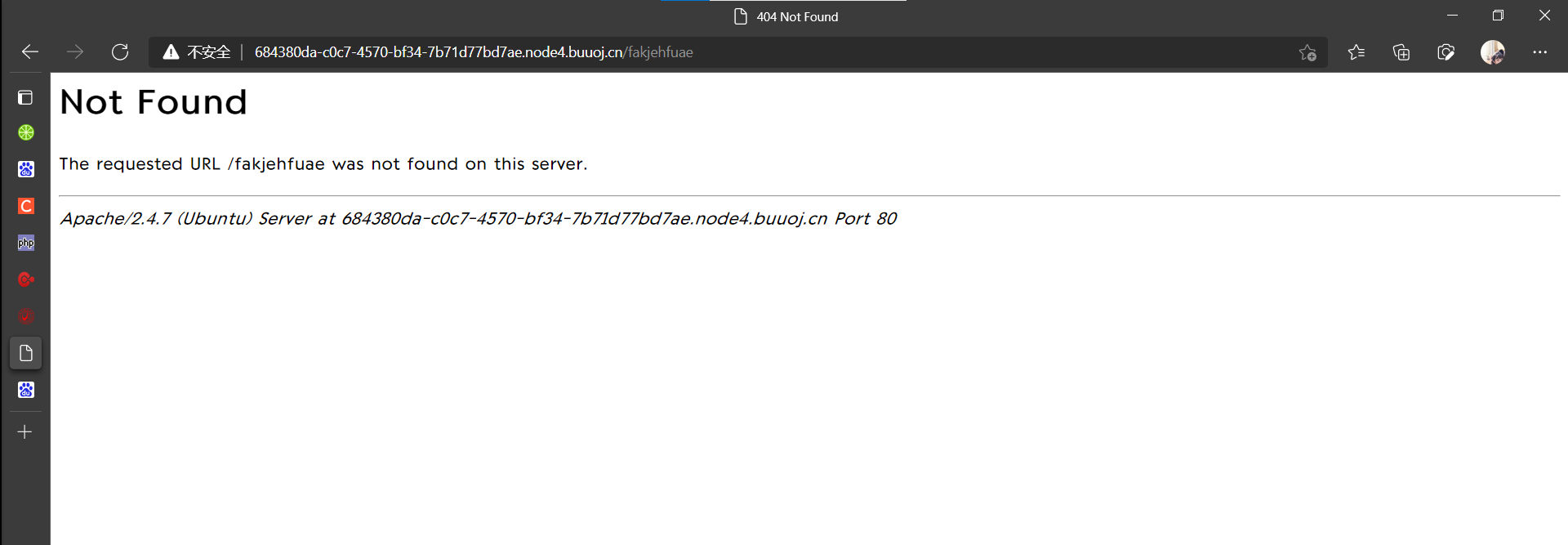
}

代码审计后了解到本题无法得知文件保存的路径（很不容易，MD5爆破一下也许可以......吧，我的猜测）

所以我们只能利用zip的解压缩来构造目录穿越来确定我们的上传路径

首先审计源码知道我们的文件保存在 /upload/随机MD5值/上传文件 路径，为了绕过这个随机的MD5值，我们需要目录穿越到两级前，也就是在zip的文件中加入 ../../ ，再去上传

首先在URL处乱敲一些目录看报错：



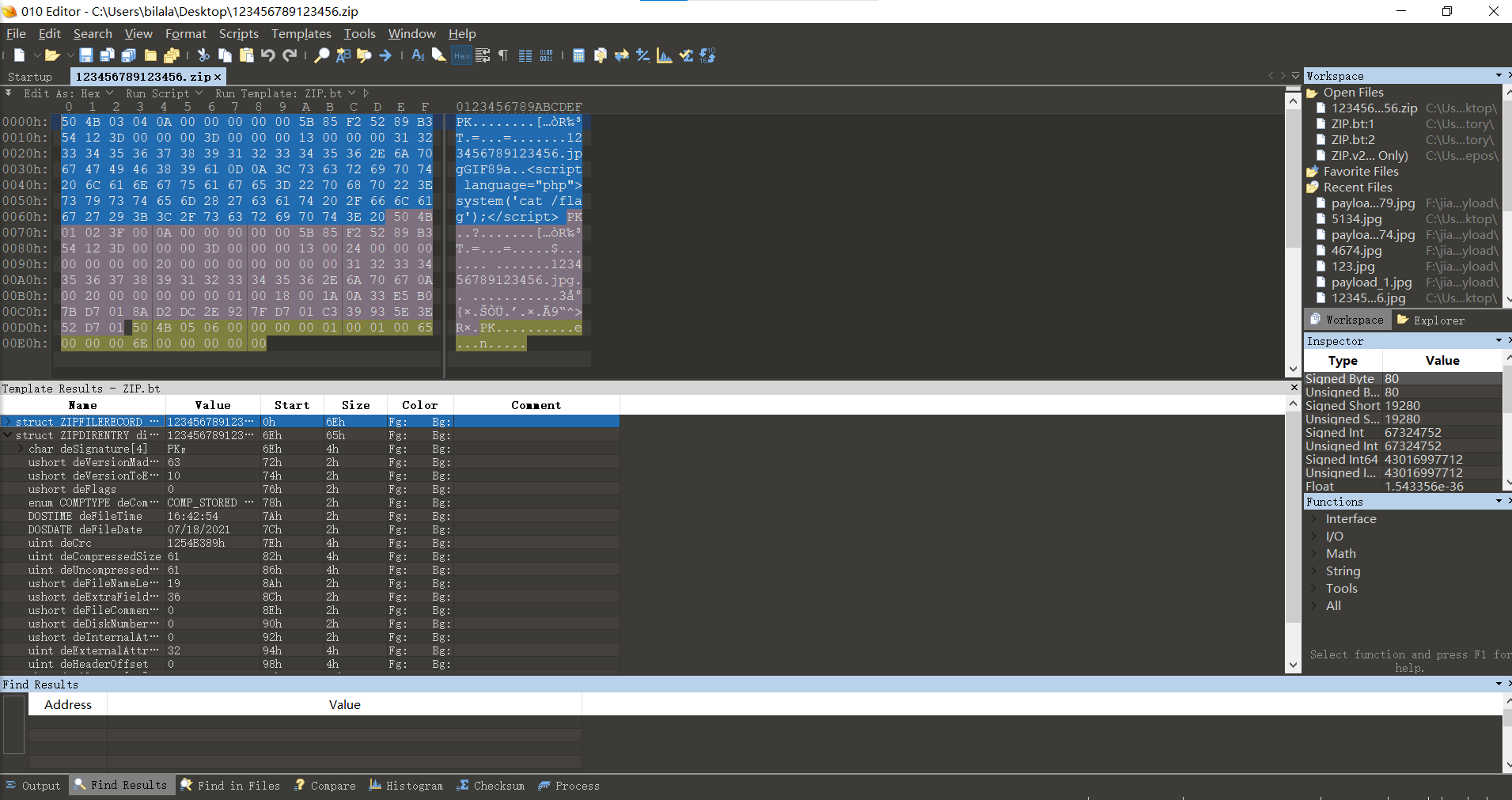
得到信息，apache服务器，想到apache的解析漏洞

审计源码可知zip中不允许php后缀文件，再加上apache解析漏洞，很快可以得出我们需要构造的文件名应该为shell.php.xxx ，再加上目录穿越，最终的文件名应为 ../../shell.php.xxx

操作：先写个一句话木马保存为1.php ，首先数一数我们最终文件名的字符数：19个。然后将这个1.php重命名为19个字符的文件，比如123456789123456.php ，然后添加进压缩包（右键文件或其他压缩操作）

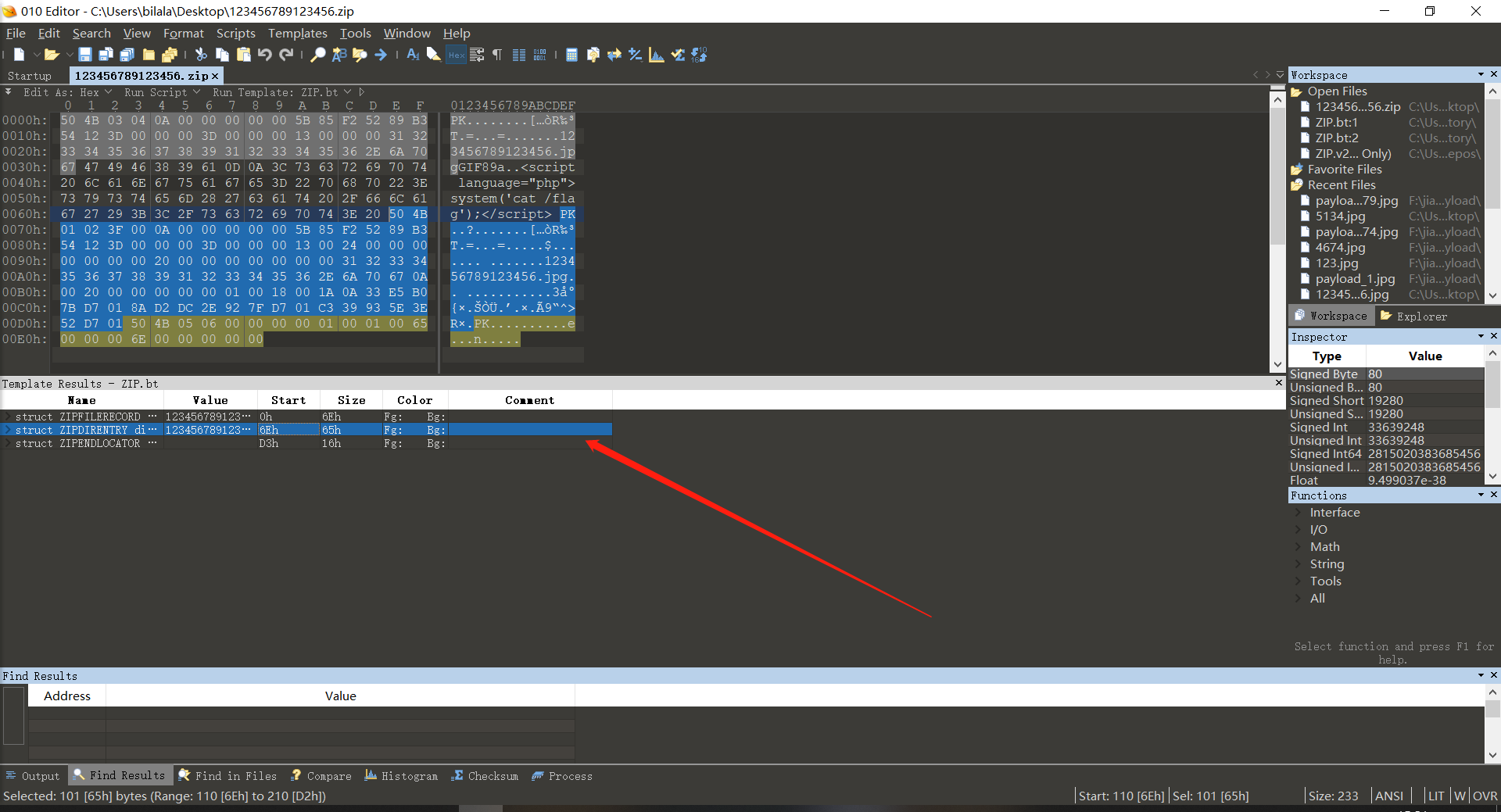


再将生成的压缩包放进010editor下：

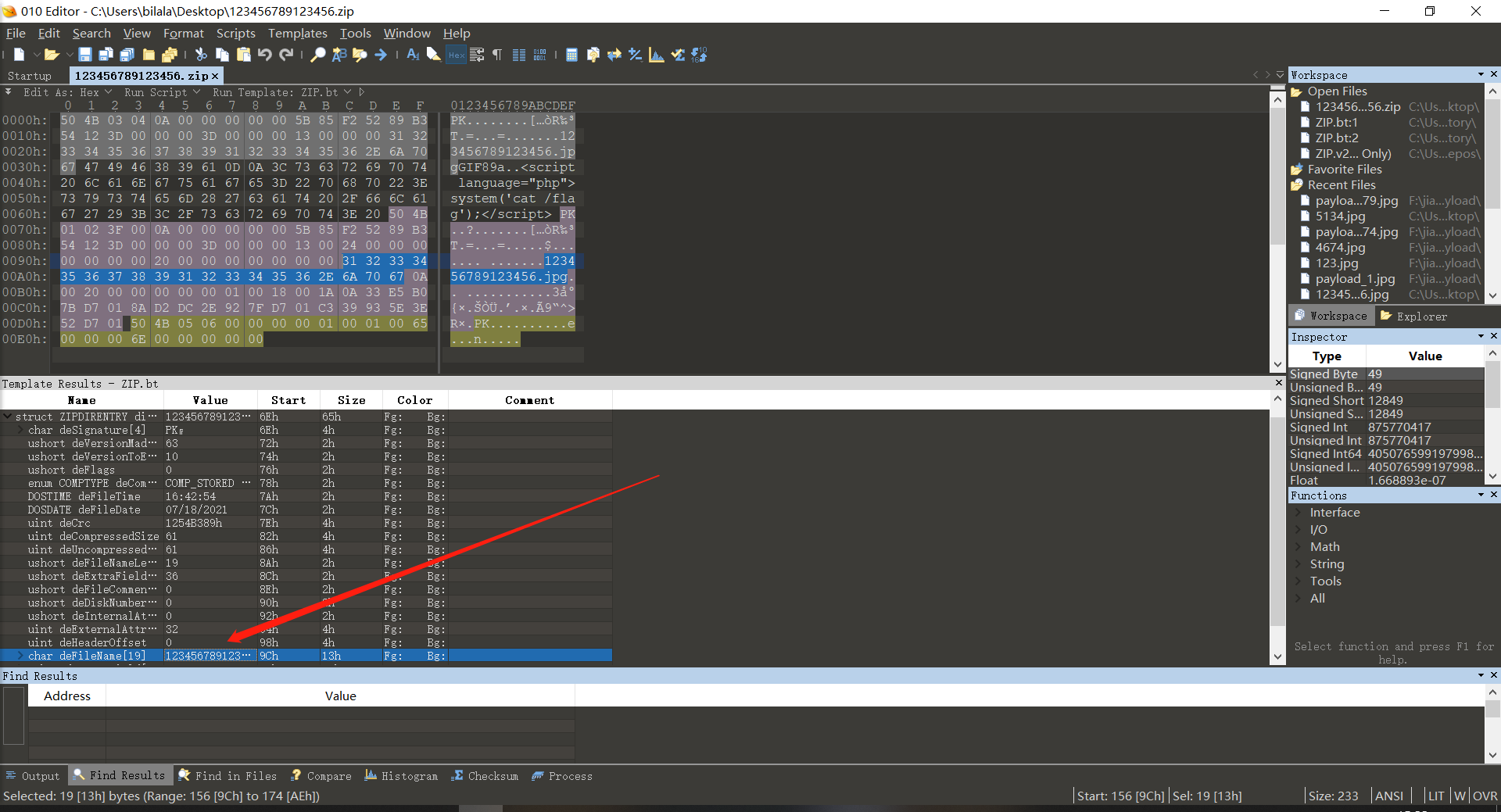


*## 如果你没有这样的界面，跳转到最后去看一下教程*

点开

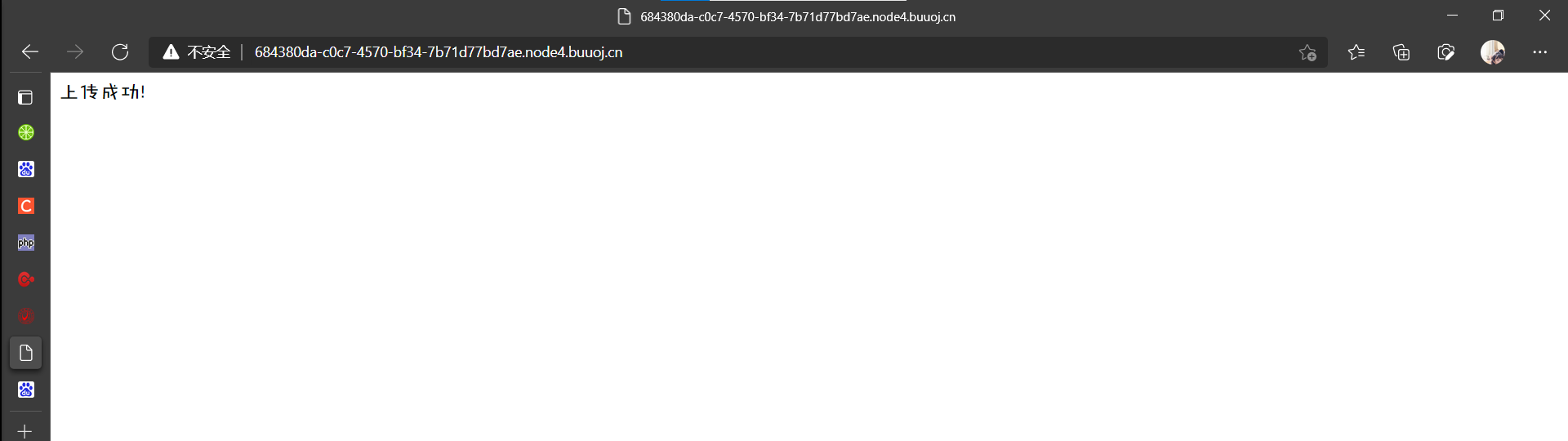


将此处改为../../shell.php.xxx

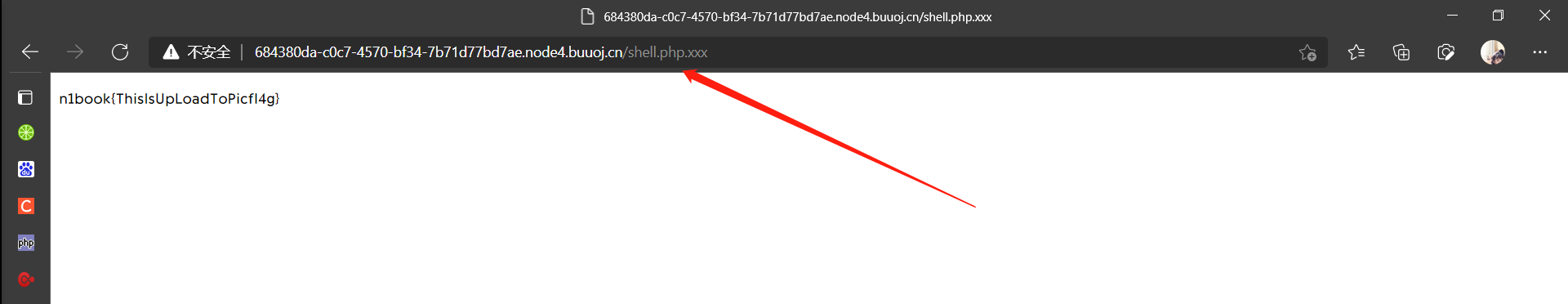


然后保存

再将这个zip上传

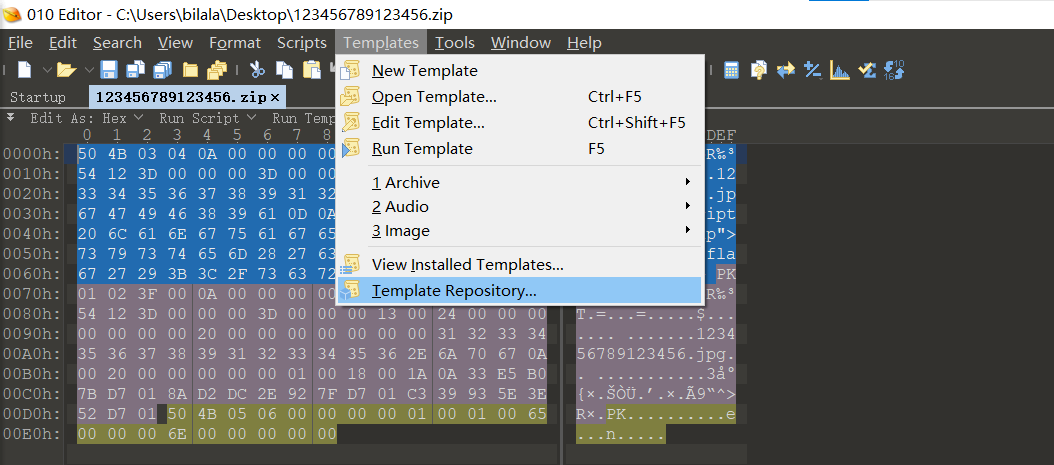


访问我们保存的路径得到flag

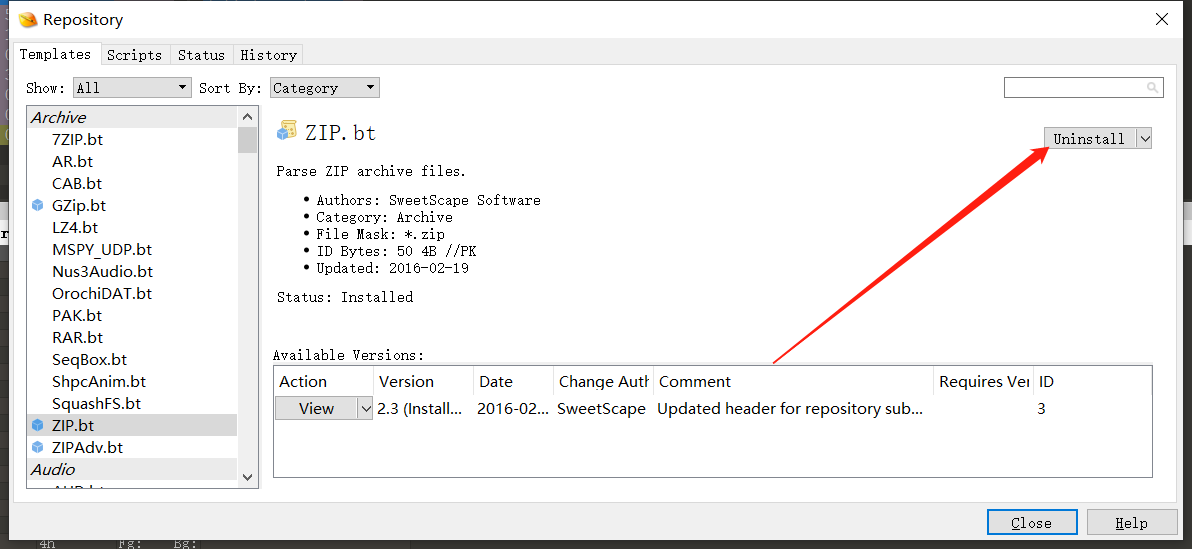


**010 template界面打开教程**

先点这个



然后找到zip.bt ， 点击install（如果和我一样是uninstall说明你已经安装了）



然后点这个就可以出来界面

