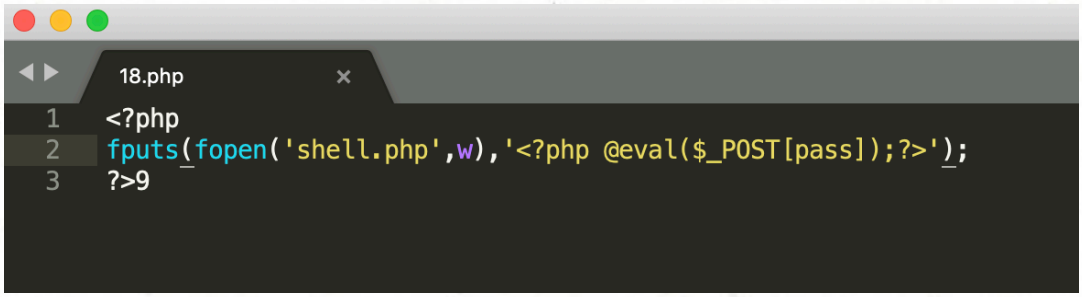
这个题目的逻辑为任何文件都可以上传，上传之后判断是不是图片类型，不是的话就删除（unlink函数）

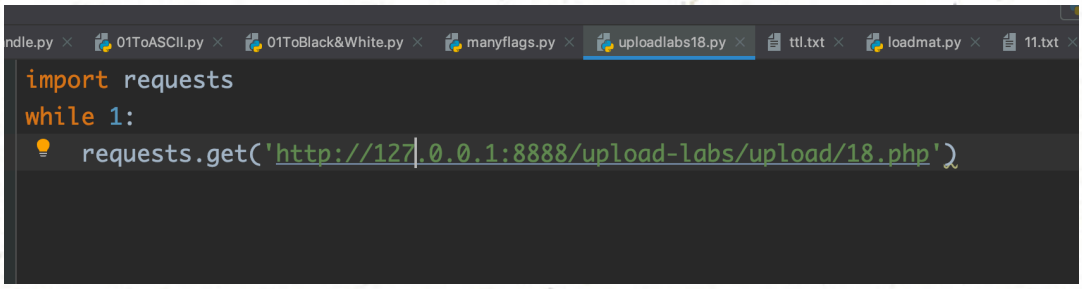
这个题没法像前面几题一样利用图片马，因为没有文件包含漏洞

所以我们就要在文件被删除之前利用它

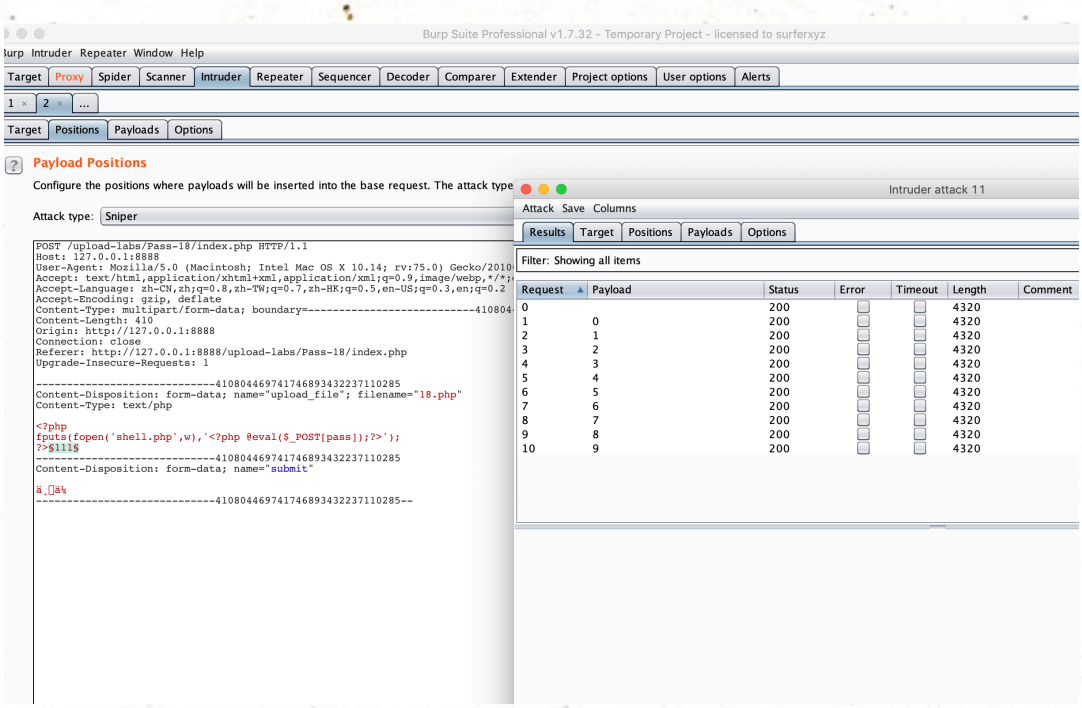
方法为利用竞争条件上传，写18.php，内容为植入另一个木马



然后写一个脚本，不断访问upload下的18.php



然后用burp的intruder不断上传



这里为了将对脚本的影响减少到最低，我自定义了变换的位置，放在了?>后面，不影响php的访问，这也是为什么上面18.php截图最后面有一个9

爆破，同时运行py脚本（但是仍然无法及时访问，为了测试我把第18关的index.php删除那一行注销了才测试成功，看来还是删除的速度快呀）