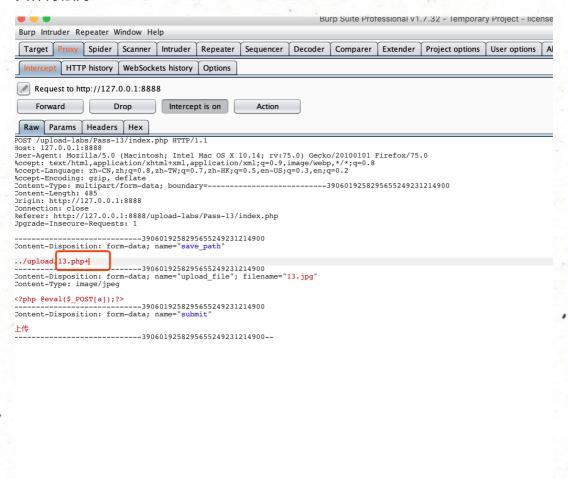
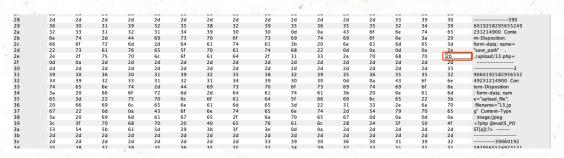
此题和上一题的区别为路径通过POST类型提交,但是%00并不能直接添加这是因为 %00 截断在 GET 中被 url 解码之后是空字符。但是在 POST 中%00 不会被 url 解码,所以只能通过 burpsuite 修改 hex 值为 00 (URL decode)进行截断。

具体方法为



后面跟一个+当占位符,其实任意一个就可以



找到这个+位置,"php"以6870结尾,然后后面是0d0a,中间那个2b就是+,改为00后即可完成截断,发包即可