WEB1

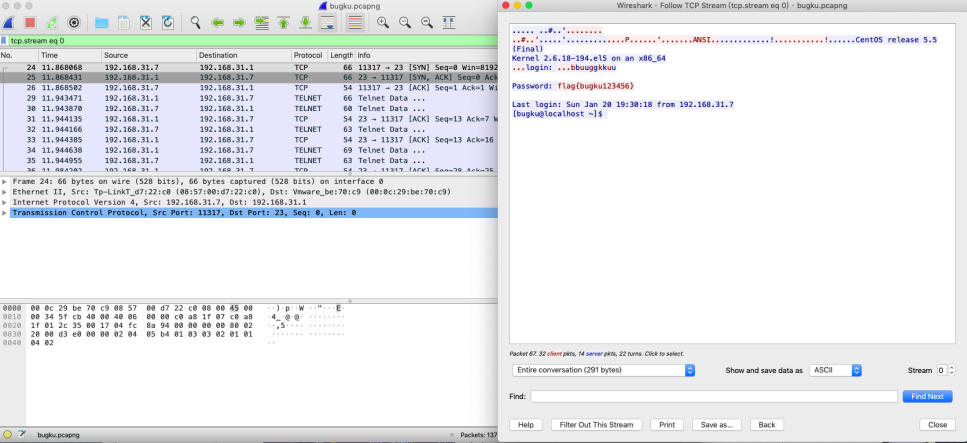


根据代码可以知道想要得到flag，是通过判断a是否与c的值是否相等，而c的值取决于b，但是有extract方法，所以知道是变量覆盖，c经过trim后c的值变成空了，所以此时验证a==c，只需要a的值也是空就行了，构造一下得到flag

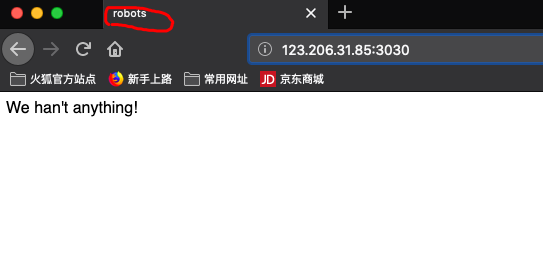


流量分析

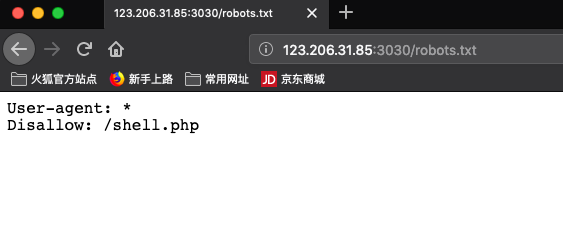
简单的流量分析题，直接查看TCP，再追踪一下TCP流即可



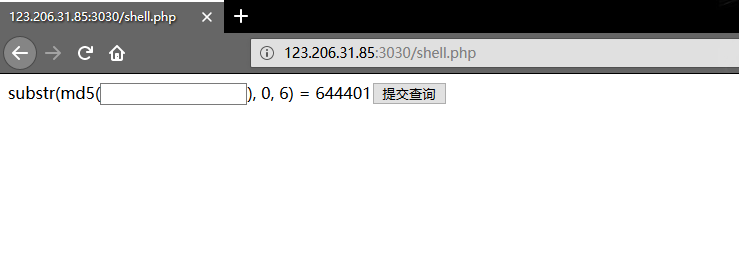
Web11



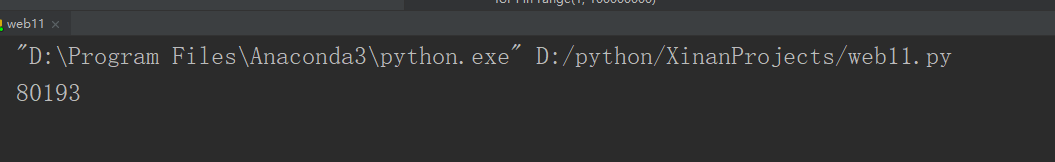
通过标题可以看出包含robots文件，所以URL构造一下看看，发现有个shell.php

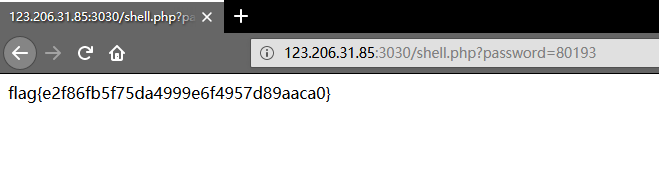


再次构造URL查看

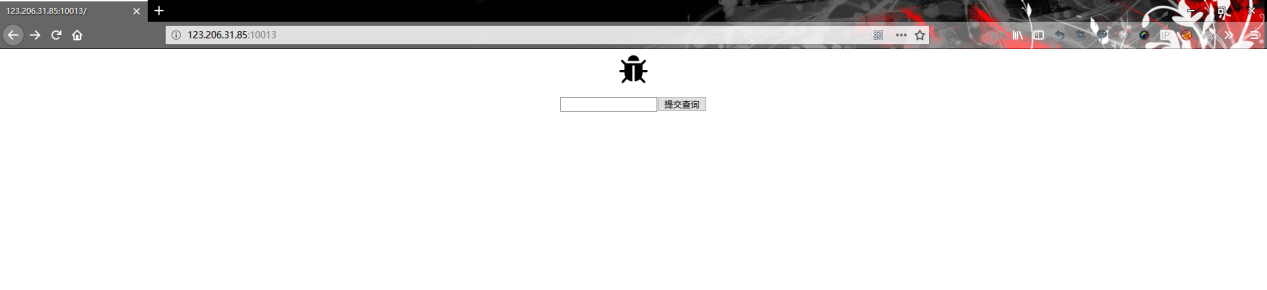


## 发现是mad5匹配，这里直接运行脚本既可以得到flag





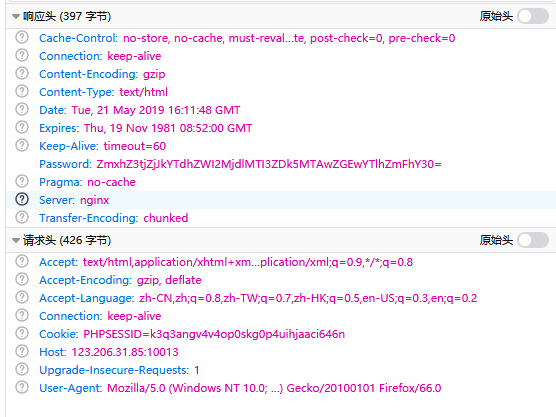
WEB13



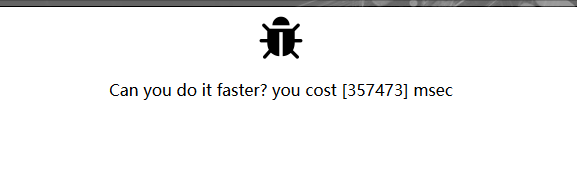
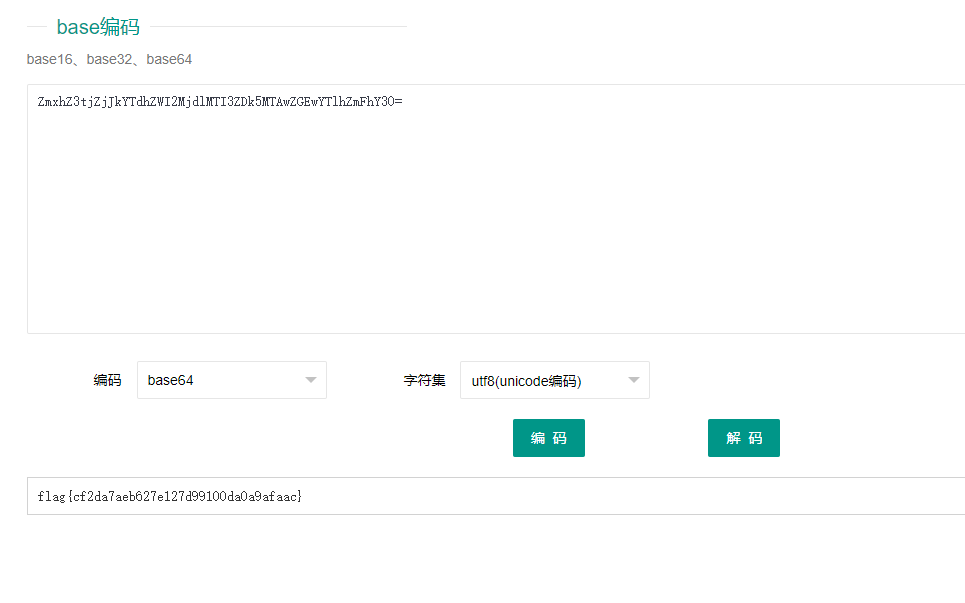
随便提交一个查看返回值



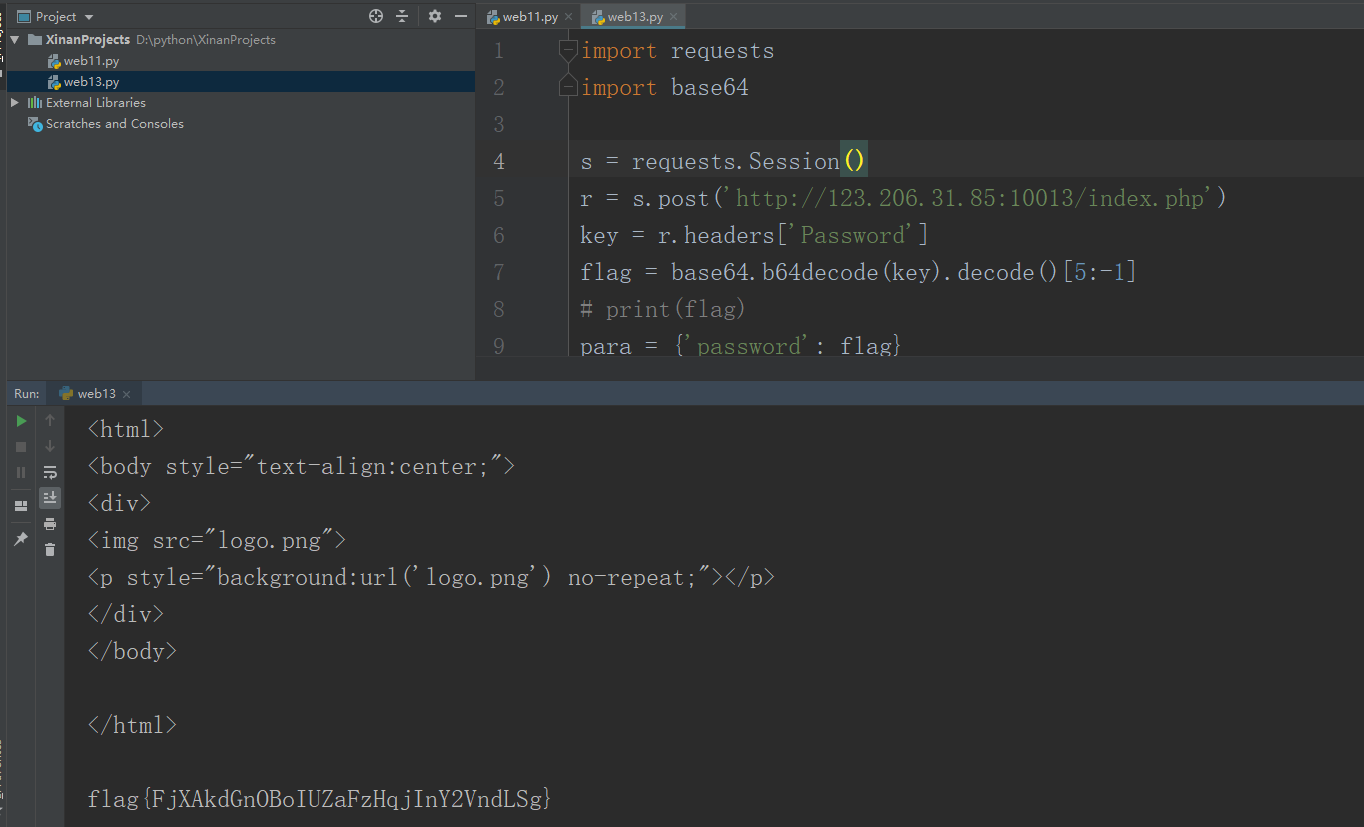
查看源码和请求，发现响应头里面有一个password，但是经过了base64加密



解密得到flag，提交看看



发现考查的是脚本，和bugku的秋名山车神题差不多，直接上脚本，得到真正的flag

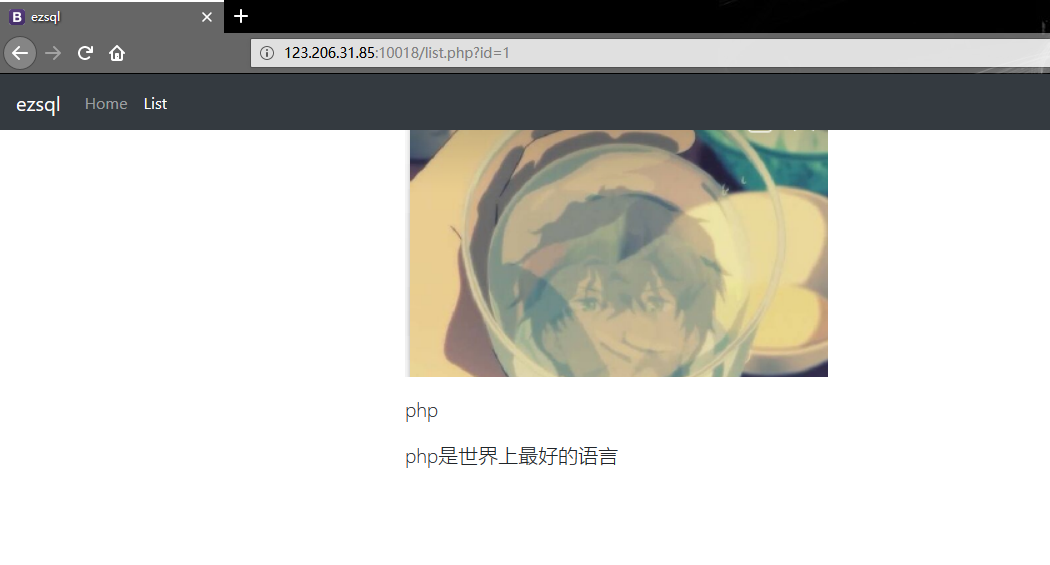


WEB18

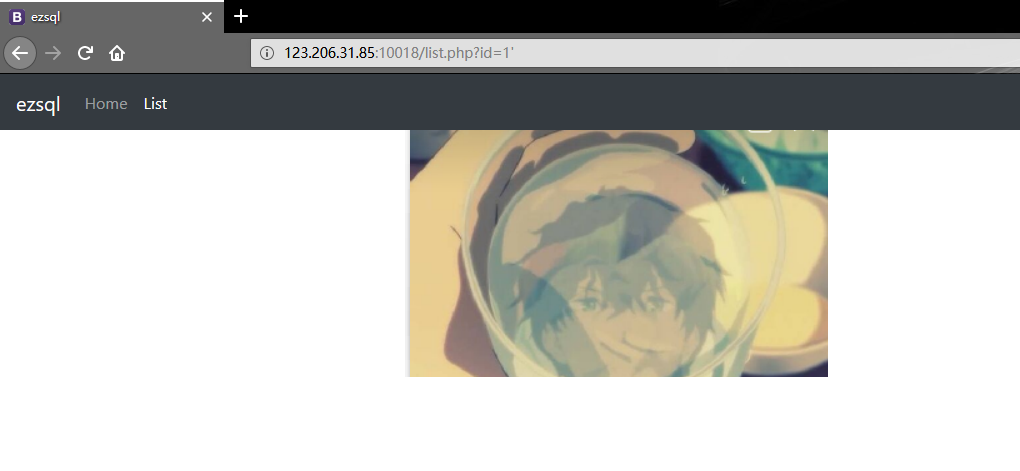
根据标题提示考察SQL注入



进入list界面

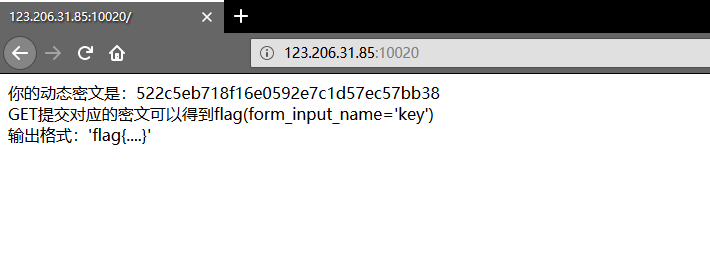


修改URL发现出现异常，可能存在注入点，尝试进行注入，不过没成功，没做出来。。。



WEB20

打开网址发现又是一个类似考验速度的



根据提示，需要通过GET方式提交所给的密文，才会出现flag，不过由于这个密文是动态的，在不断刷新，手动提交的话根本不会成功，这时候就需要脚本了，直接跑脚本，不断运行就会出现flag

