WEB

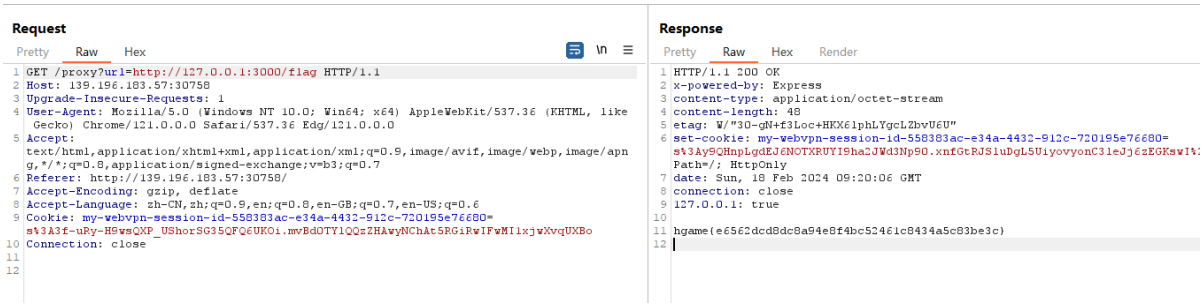
WebVPN

网页版代理，获取flag的路径是先完成登录，可在源码中找到user信息，包含username和password

然后通过`POST /user/info`利用update函数基于js原型链污染来使strategy带上目标

因为proxy的判定是基于`.hostname`，所以只需带上`127.0.0.1`即可 **如果是`127.0.0.1:3000`会导致服务器端返回的header出现错误，返回500而非flag**

完成污染后利用proxy访问flag



MISC

与ai聊天

反向复读，~~这样子肯定不是ai~~，检索到 [hackergame2020-自复读的复读机]

```
# 正向自复读：_='_=%r;print (_%%_)';print (_%_)

#payload
_=')]1-::[_%%_(tnirp;%r=_';print(_%_[::-1])
```

Blind SQL Injection

分析流量可知是sql盲注的记录，分析request可找出字符串各个位置上的值，目标应该是password字段

先将host导出，比对`geek`得出查询规律，~~大脑~~分析得出password的字符串，逆序输出转化后结果

```
AStr = "125 102 50 102 97 56 50 57 53 99 56 51 100 45 54 99 97 98 45 56 57 101 52
45 53 50 55 49 45 55 101 102 97 98 97 98 99 123 103 97 108 102 44"

Alist = AStr.split()
flag = ''.join([chr(int(char)) for char in reversed(Alist)])
print(flag)

# ,flag{cbabafe7-1725-4e98-bac6-d38c5928af2f}
```