Nebu1ea 韩磊 [1504895347@qq.com](mailto:1504895347@qq.com)

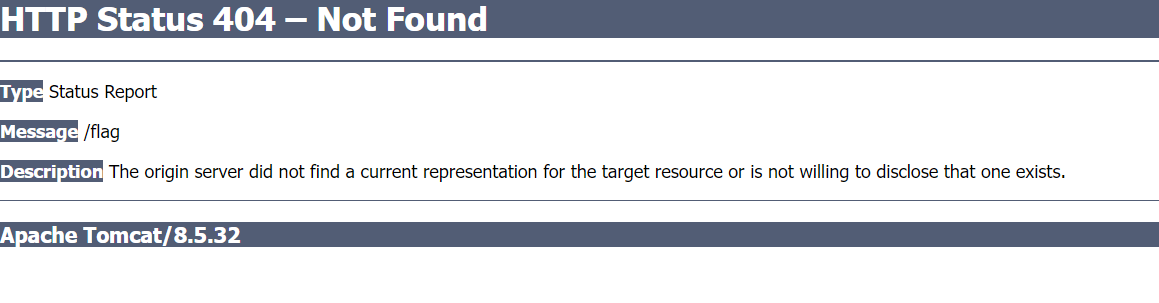
Web: 原神启动

解题思路：

初始目录填属性相克，发现success.html，输入flag，提示flag在flag.txt里



直接访问是假的flag，试试普通flag路由，发现抱错，



这个版本的tomcat有文件读取漏洞CVE-2020-1938，直接找网络上的exp:

<https://github.com/nibiwodong/CNVD-2020-10487-Tomcat-ajp-POC>

然后用python2跑一遍：

