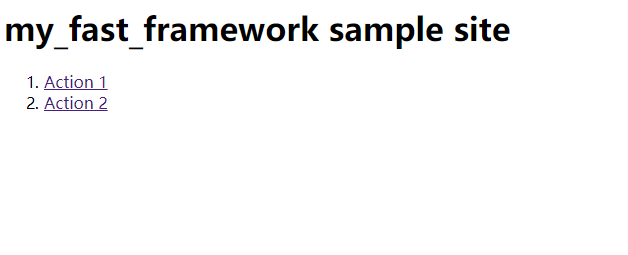
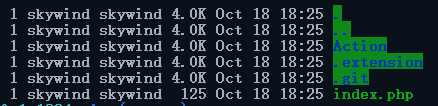
# ZSCTF-Not-Only-Web

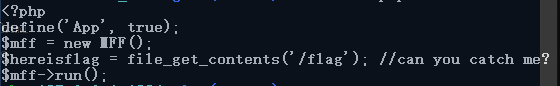
1.



首先页面上就俩链接 第一步是.git源码泄露 出来项目源码



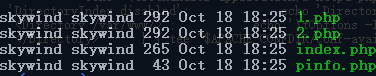
而index.php是这样的



实例化了个类 读取了flag 然后run了一下

而这个类在php默认的环境中是不存在的 是个第三方扩展里的类

然后Action 目录



其中1.php 2.php index.php里的内容分别是首页 action 1, action2的内容，

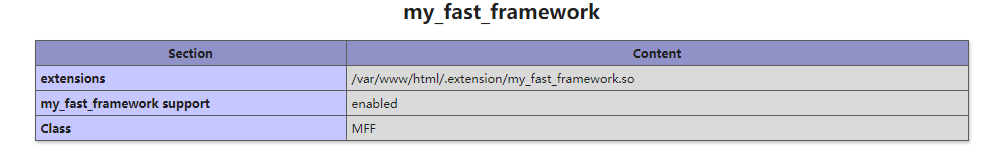
而pinfo.php



是个phpinfo()

根据action1/2的规则构造url: xxxxxxx/?action=pinfo看见phpinfo页面

在phpinfo信息中有个第三方扩展 并且扩展文件在web目录中

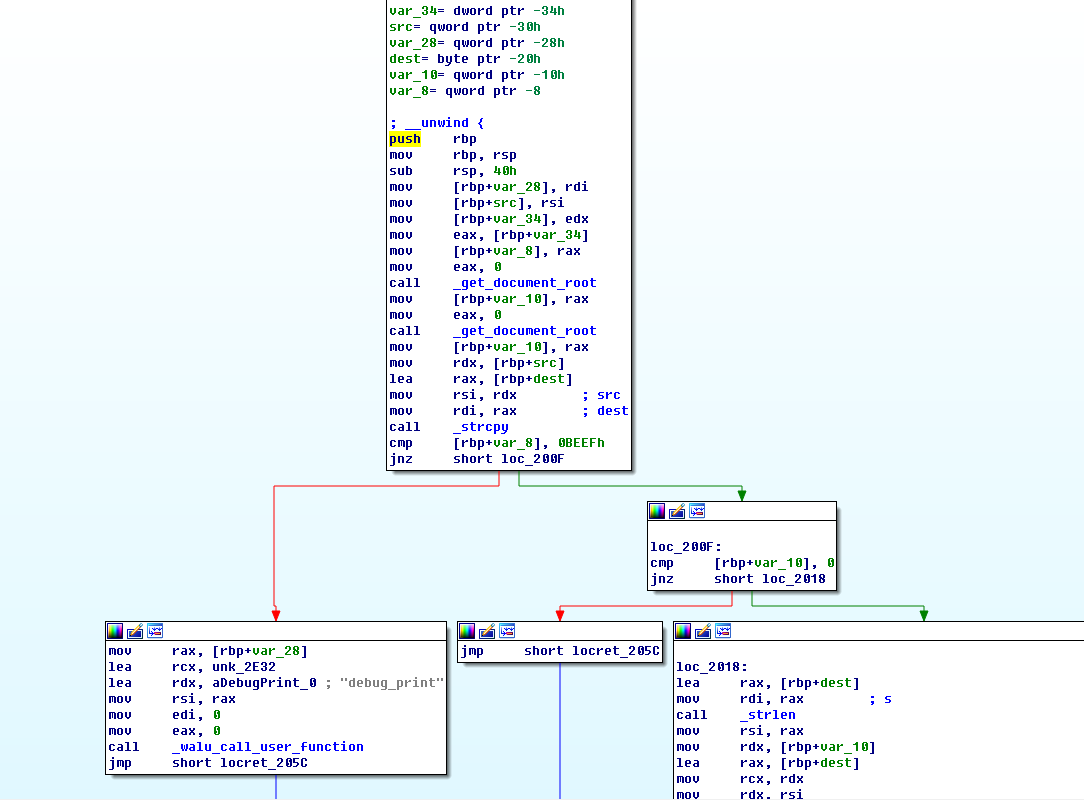


构造连接将my\_fast\_framework.so下载到本地

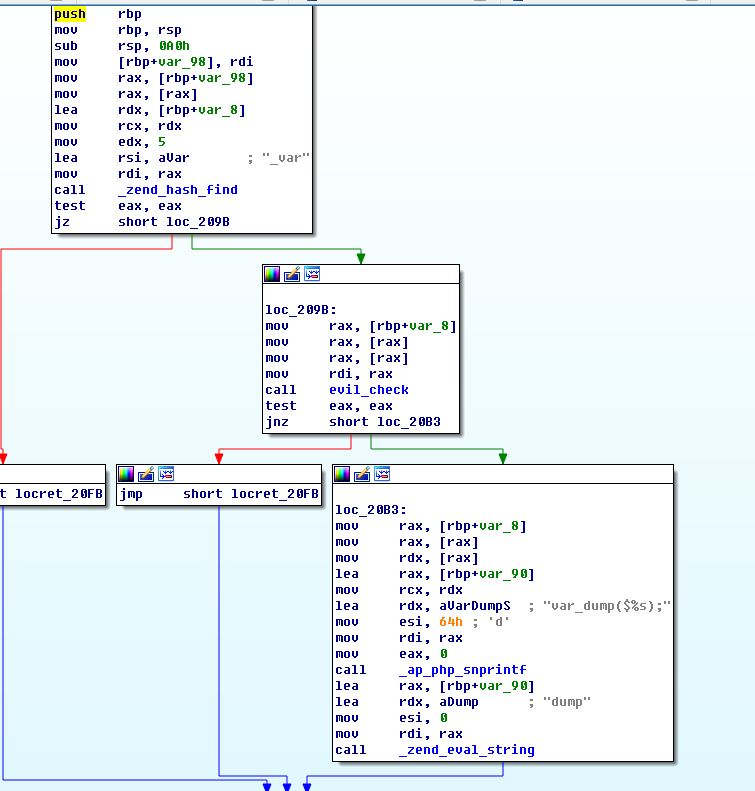
ida打开分析运行流程发现这个扩展注册了刚才看见的MFF类

并且完成了各action的加载

而加载途中有个函数perform\_action



如果var\_8的值为0xbeef的话 会进到debug\_print方法 而这个方法最终会进到debug\_print\_handler



debug\_print\_handler能打印任意变量

而在perform\_action中能看见储存action字符串的地方距离var\_8是24个字节

同时使用的是strcpy获取副本 可能发生溢出覆盖变量var\_8

于是构造出payload /?action=AAAAAAAAAAAAAA%EF%BE&\_var=hereisflag

完