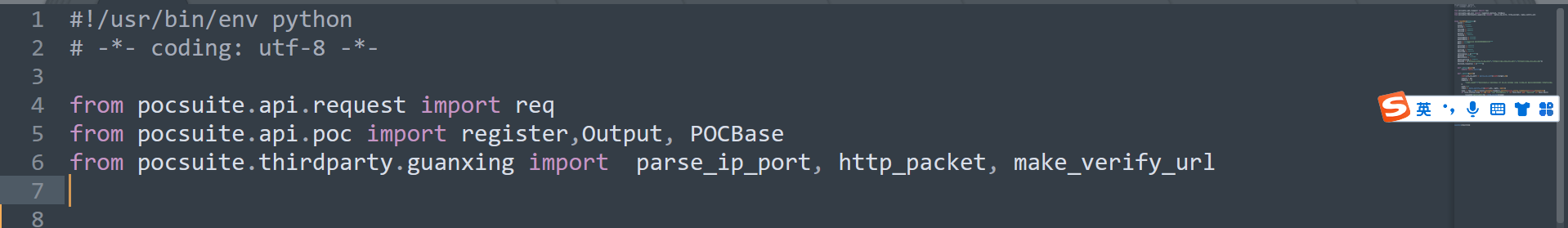
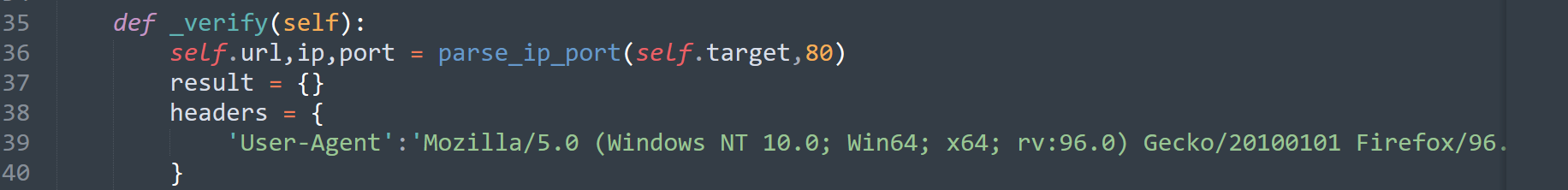
POC编写及提交注意事项

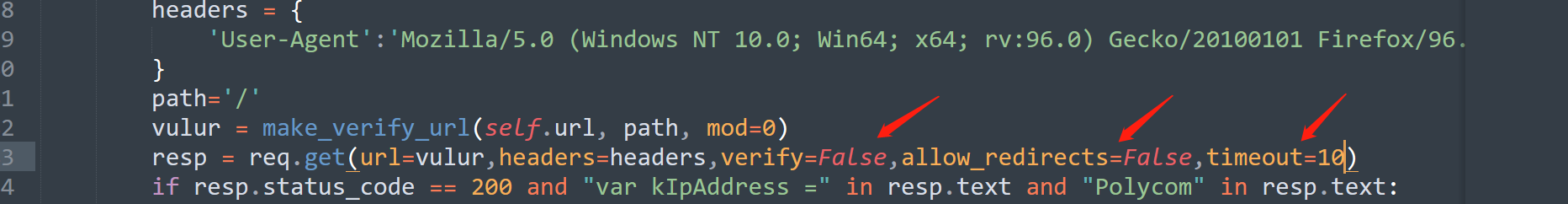
1. 当前POC用不到的模块不加



1. 验证模块 “self.url,ip,port = parse\_ip\_port(self.target,80)” 必须放在第一句.

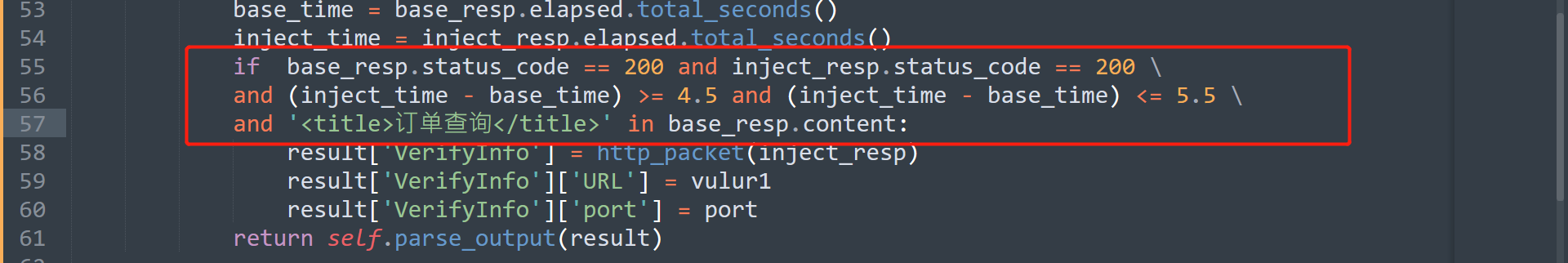


1. 以下三个字段必须添加,如无特殊请求都禁止重定向,超时时间默认10秒(视站而定)

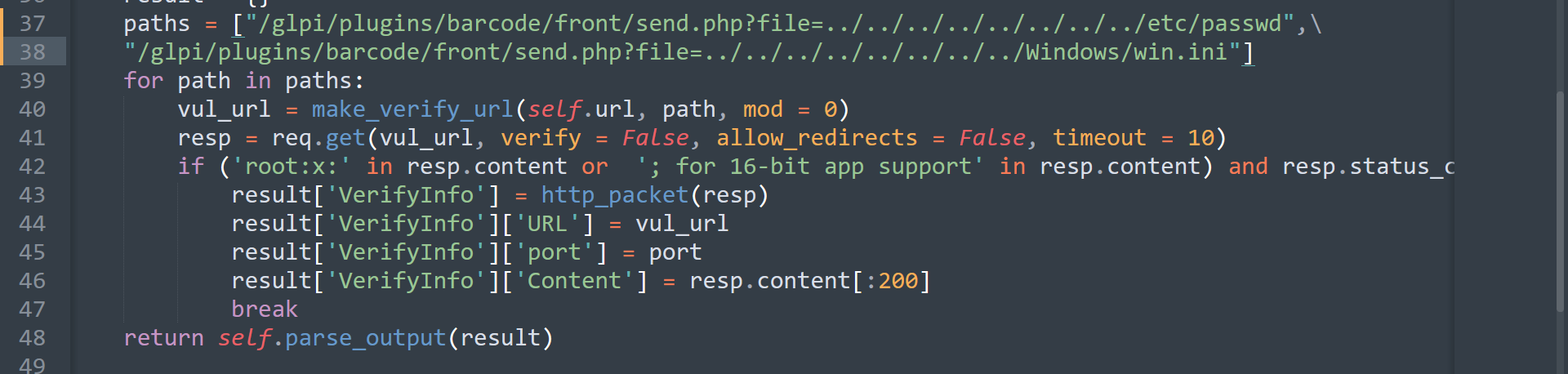


1. POC的判断条件应严谨.如以下案例.

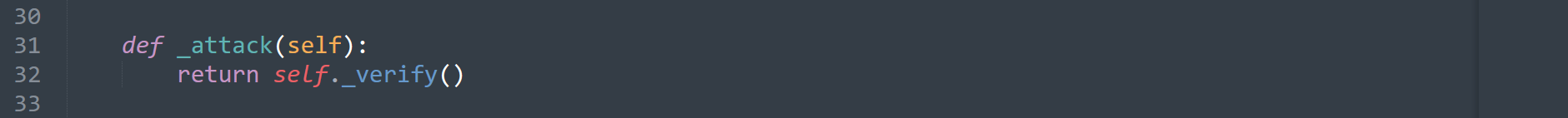
例如:延时注入POC,判断状态码,延时时间(控制在一个区间内),页面特征等.



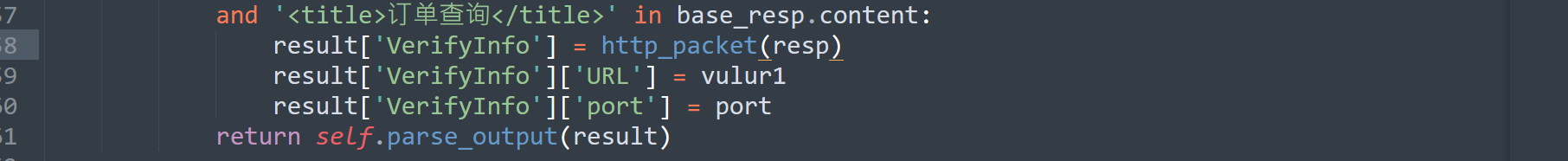
例如:任意文件读取漏洞,应把windows和linux系统环境的路径都写POC中.



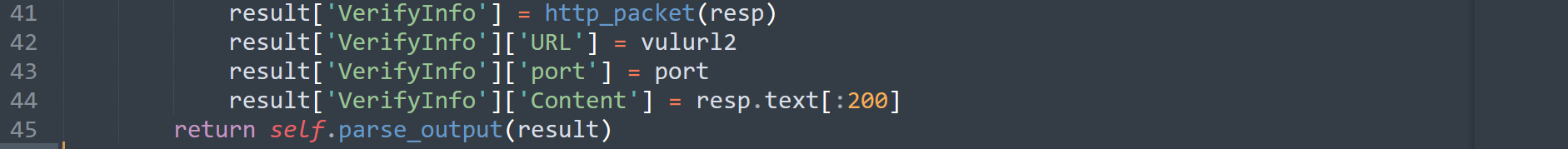
1. 如无攻击模块,写成如下格式.



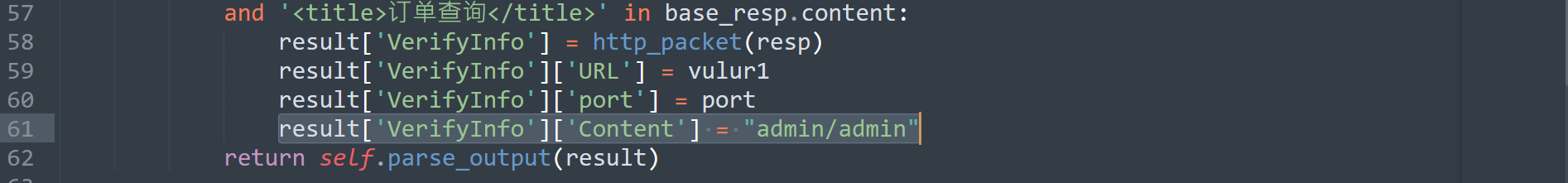
1. 当漏洞验证/攻击成功后，应按照规范返回漏洞相关信息，示例如下：



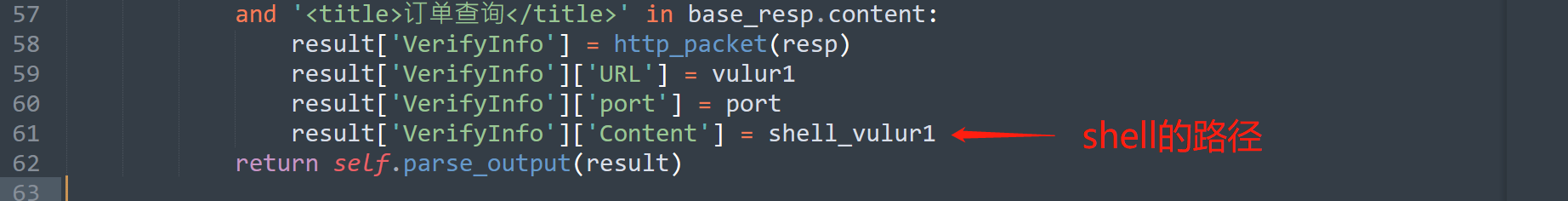
如果是任意文件下载/读取漏洞,信息泄露漏洞,需要添加result['VerifyInfo']['Content'] = resp.text[:200]



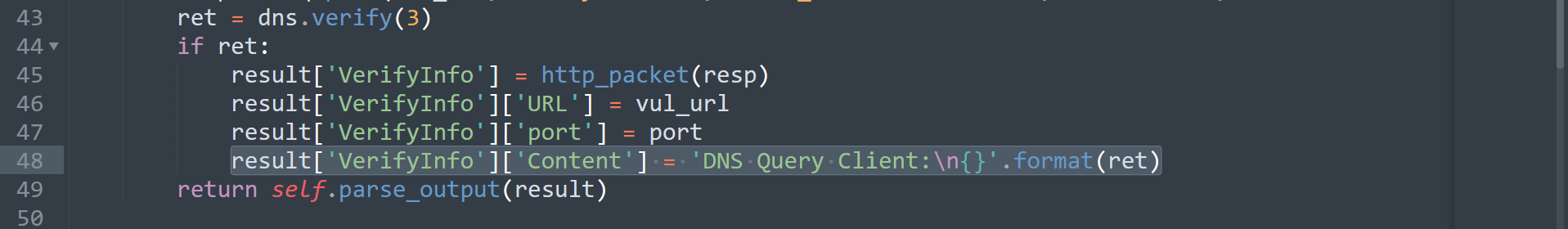
如果是默认账号密码漏洞,任意用户添加漏洞,需要添加 result['VerifyInfo']['Content'] = "用户名/密码"



如果是任意文件上传漏洞,命令执行写入文件的,需要添加result['VerifyInfo']['Content'] = shell\_vulur1



如果PING DNS 的POC,需要添加result['VerifyInfo']['Content'] = 'DNS Query Client:\n{}'.format(ret)



如果当前POC有多个请求, result['VerifyInfo'] = http\_packet(resp)写最重要的请求的返回包



1. 提交POC的基本信息填写



漏洞简介填写:可以参考CNVD,CNNVD,或者其他安全平台的漏洞简介.

例如:某网安的漏洞简介



修复方案填写

有修复补丁写:

目前厂商已发布了漏洞修复补丁,请及时关注更新.

补丁链接: https://www.xxx.com

无修复补丁写:

请关注厂商并更新至安全版本

厂商链接: <https://www.xxx.com>

Ps:新出的漏洞,厂商没有更新补丁的,有缓解措施的话,就把缓解措施写在修复方案中.