一些好用的bp插件、bp小技巧

bp小技巧

代理小技巧

在渗透测试的时候难免会搜索一些东西，然后这些搜索的网站会影响我们对渗透目标的判断

这里我们可以在代理的时候过滤掉这些网址

展示收集了这些地址

```
127.0.0.1
::1
localhost
*.chrome.*
*.mozilla.*
*.google-analytics.*
*.google.*
*.googleadservices.*
*.googleadsserving.*
*.googleapis.*
*.googlesyndication.*
*.googletagmanager.*
*.googleusercontent.*
*.gstatic.*
*.baidu.*
*.baidustatic.*
*.bdstatic.*
*.sogou.*
*.sogoucdn.*
*.microsoftonline.*
```

```
*.microsoft.*
*.bing.*
*.csdnimg.*
*.csdn.*
*.51cto.*
*.cnblogs.*
*.zhihu.*
*.freebuf.*
*.huoxian.*
*.alicdn.*
*.aliyun.*
*.butian.*
*.anquanke.*
*.threatbook.*
*.geetest.*
*.github.*
fofa.so
*.like996.*
buuoj.cn
```

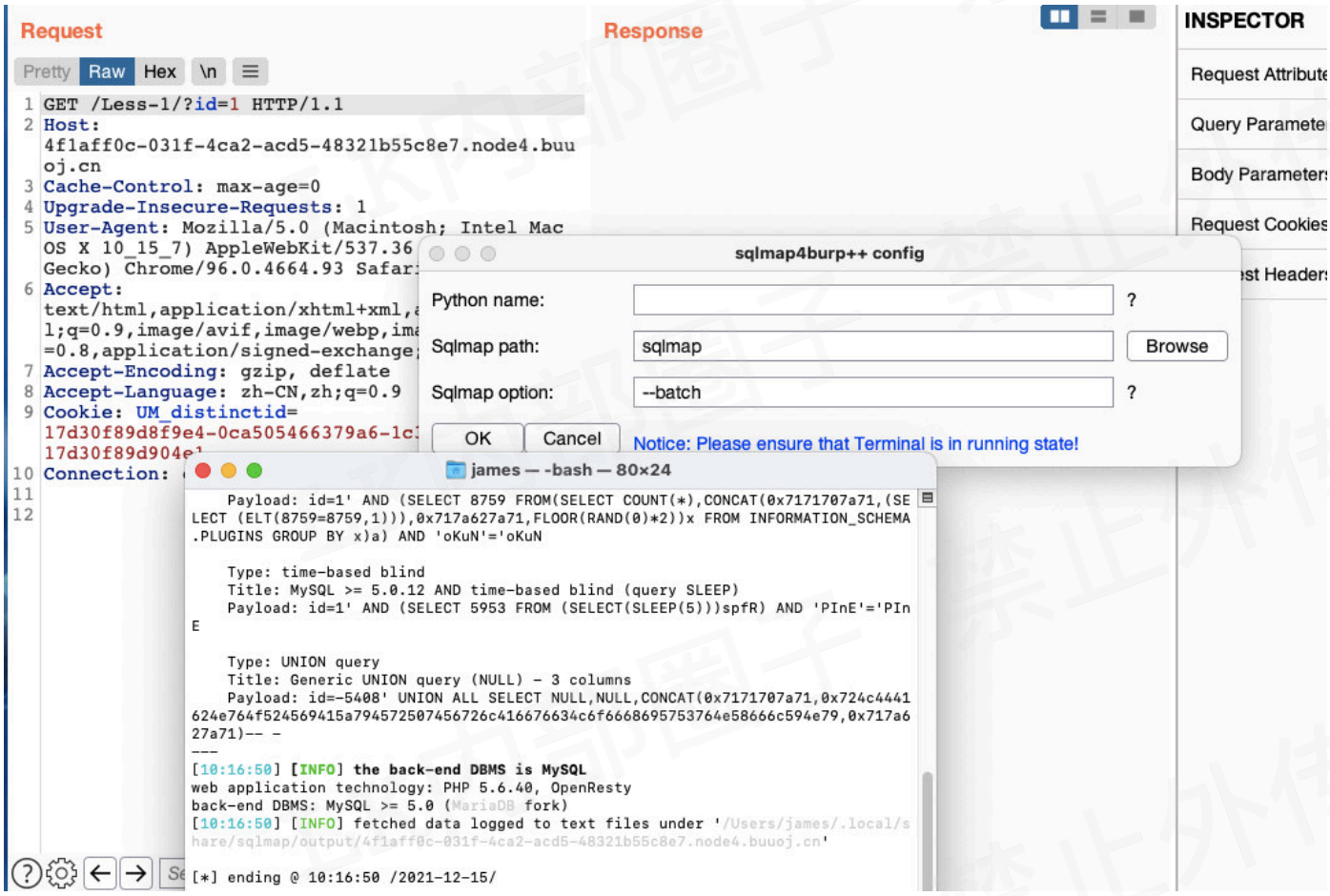
丰富了一下自己的bp插件，方便自己在渗透测试中更加丝滑

插件

sqlmap4burp++

下载地址：https://github.com/c0ny1/sqlmap4burp-plus-plus

这个插件可以说是非常丝滑的联动sqlmap，测试效果不错



Hack Bar

下载地址:https://github.com/d3vilbug/HackBar

SSRF-King

https://github.com/ethicalhackingplayground/ssrf-king

支持扫描和自动发现SSRF漏洞。

burp-sensive-param-extractor

下载地址：https://github.com/theLSA/burp-sensitive-param-extractor

检测敏感参数

Burp-unauth-checker

下载地址:https://github.com/theLSA/burp-unauth-checker
检测未授权

FastjsonScan

下载地址:https://github.com/zilong3033/fastjsonScan

BurpShiroPassiveScan

下载地址:https://github.com/pmiaowu/BurpShiroPassiveScan

自动检测Shiro+发现密钥，不依赖dnslog来检查。

403Bypasser

下载地址：https://github.com/sting8k/BurpSuite_403Bypasser
用各种姿势来绕过403访问

Shelling

https://github.com/ewilded/shelling

Reflector

下载地址:https://github.com/elkokc/reflector

通过设置Content-Type, 我们可以快速找到请求中的参数哪个被返回到回显的Body。

BurpJSLinkFinder

下载地址：https://github.com/InitRoot/BurpJSLinkFinder

Unexpected information

下载地址：https://github.com/ScriptKid-Beta/Unexpected_information

用于高亮特征和定位敏感信息

JSON decoder

商店有，美化json