链滴

# mitmdump 抓包

作者：AlwaysBeFriday

原文链接：https://ld246.com/article/1575604663544

来源网站：链滴

# mitmproxy、mitmdump、mitmweb 比较

- 启动 mitmdump,用 mitmproxy、mitmdump、mitmweb这三个命令中的任意一个即可，这三个令功能一致，且都可以加载自定义脚本，唯一的区别是交互界面的不同
- mitmproxy 会提供一个在终端下的图形界面，具有修改请求和响应，流量重放等功能，具体操作式有点 vim 的风格,mitmproxy 命令不支持在 windows 系统中运行
- mitmdump 可设定规则保存或重放请求和响应，mitmdump 的特点是支持 inline脚本，由于拥有以修改 request 和 response中每一个细节的能力，批量测试，劫持等都可以轻松实现
- mitmweb 提供的一个简单 web界面，简单实用，初学者或者对终端命令行不熟悉的可以用 mitmwb 界面
- 此外还有一款anyproxy，也具有类似功能

# mitmdump

- mitmdump 是 mitmproxy 的命令行版本。将tcpdump用于HTT
- 近似于charles的命令行版本
- python：mitmproxy
- 功能和charles、fiddler相似，强大之处在于它的工具 mitmdump可以直接对接python 对请求做理
- mitmdump是mitmproxy的命令行窗口，同时还可对接python对请求进行处理，因此就不用手动获和分析http请求和响应，只需要写好请求和响应的处理逻辑即可
- 可用参数

```
-p PORT --port PORT # 设置 mitmproxy 的代理端口

-T --transparent # 设置透明代理

--socks # 设置 SOCKS5 代理

-s "script.py --bar" # 执行脚本，通过双引号来添加参数

-t FILTER # 过滤参数
```

## 实例

- 启动脚本 index.py, 监控端口8888,

```
mitmdump -s index.py -p 8888
```

# mitmweb

## 会启动一个web界面，127.0.0.1:8081

- 启动后，可以直接修改脚本函数内容，不需要重新启动

```
mitmweb -s index.py -p 8888
```

# mitmproxy模块使用

- 官网　https://mitmproxy.org/
- 文档　https://docs.mitmproxy.org/stable/
- mitmproxy是具有控制台界面的HTTP和HTTPS的交互式中间人代理

## 安装

```
pip install mitmproxy
```

## 脚本使用

- addons，是个数组，每个元素是一个类实例，这些类有若干方法，这些方法实现了某些mitmproxy提供的事件，mitmproxy 会在某个事件发生时调用对应的方法。这些类，称为一个addon
- 容易管理和拓展

```
addons = [
    Counter()  # Countrer是类实例，实现了mitmproxy的事件
  ]
```

- 获取响应请求，传入参数为(flow)

```
def request(flow):

def response(flow):
```

- 获得请求的url，header，text

```
flow.request.url
flow.request.headers
flow.response.text
```

- 添加二级代理

```
proxy = ("114.240.101.242", 5672)
flow.live.change_upstream_proxy_server(proxy)
```

- 脚本实例

```
def request(flow):

    if flow.request.url.startswith("https://www.baidu.com"):
        requesturl = flow.request.url
        requestheaders = str(flow.request.headers)
        data = dict()

        url = "http://xxxx/url"
        data["url"] = requesturl
        data["debug"] = False
        data["headers"] = requestheaders
```

```
# 通过redis传递请求
sa(data)
```

## 证书

- 安装证书
  - 文档　https://docs.mitmproxy.org/stable/concepts-certificates
  - 对于使用证书固定（ssl Pinning）的app无效
  - 运行 mitmweb 或 mitmproxy 后，会在用户目录下生成证书
  - C:\Users\XXXXX\.mitmproxy，XXXXX 为用户目录

mitmproxy-ca.pem, PEM格式的证书私钥
mitmproxy-ca-cert.pem PEM格式证书，适用于大多数非Windows平台
mitmproxy-ca-cert.p12 PKCS12格式的证书，适用于大多数Windows平台
mitmproxy-ca-cert.cer 与 mitmproxy-ca-cert.pem, 相同（只是后缀名不同），适用于大部分Android平台

- mitmproxy-dhparam.pem PEM格式的秘钥文件，用于增强SSL安全性,证书安装到受信任的根目中

## 使用步骤

1. 安装 mitmdump 或 mitmproxy
2. 启动，然后安装证书
3. 监听 mitmdump -s index.py -p 8888
4. 监听 8888 端口
5. 设置代理或VPN(drony)，指向 mitmproxy，如果是本机，则指向127.0.0.1:8888（Drony中的hos和port）
6. 浏览器代理
7. 手机模拟器代理
8. 手机wifi代理
9. 修改脚本