mitmproxy

Intercepting HTTP(S) proxy

CONCEPTS

Only intercept traffic from devices and apps you own or are explicitly authorised to inspect.

Three front ends share one engine: mitmproxy (TUI), mitmweb (browser UI) and mitmdump (no UI, scripts and files).

HTTPS only works once the client trusts the mitmproxy CA; browse to mitm.it through the proxy to install it.

FLOW LIST

`j` / `k`
Move down / up

`Enter`
Open the focused flow

`q`
Back / leave current view

`f`
Set the view filter

`d`
Delete flow from view

`z`
Clear the whole flow list

FLOW VIEW

`Tab`
Switch request / response / detail

`e`
Edit URL, header, body or method

`m`
Choose content view (JSON, hex...)

INTERCEPT AND REPLAY

`i`
Set intercept filter, e.g. ~u api & ~q

`a`
Resume the intercepted flow

`A`
Resume all intercepted flows

INTERCEPT AND REPLAY (cont.)

`r`
Replay request to the server

`x`
Export flow (curl, httpie, raw...)

SAVE, LOAD, GLOBAL

`w`
Save listed flows to file

`L`
Load flows from file

`?`
Context-sensitive help

FILTER EXPRESSIONS

`~u` *`<regex>`*
Match URL

`~d` *`<regex>`*
Match domain

`~m` *`<regex>`*
Match method

`~c` *`<code>`*
Match response status code

`~h` *`<regex>`*
Match any header

`~b` *`<regex>`*
Match any body

`! / & / | / ( )`
Not, and, or, grouping

COMMAND LINE

`mitmproxy -p` *`<port>`*
Listen on another port

`mitmweb`
Web interface

`mitmdump -w` *`<file>`*
Record flows to file

`mitmproxy -r` *`<file>`*
Open a saved flow file

CERTIFICATES

`http://mitm.it`
Download CA via the proxy

`~/.mitmproxy/mitmproxy-ca-cert.pem`
CA certificate (non-Windows)