mitmproxy

- Man In The Middle Proxy.
- Can intercept, analyse, modify and replay packet flows.
- Supports a number of proxy modes.
- TLS cert generation.
- And more.....

mitmproxy

2 Main operation modes:

1. Explicit – user connects directly to the proxy.
2. Transparent – data is redirected to the proxy.

mitmproxy

Transparent Mode

1. Become the man in the middle (arp spoofing, fake ap ...etc).
2. Redirect data from port 80 to mitmproxy.
3. Run mitmproxy in transparent mode.

mitmproxy

How To Build An Attack

1. Analyse normal behaviour.
2. Use a basic setup to test the simplest form of the attack.
3. Start with a simple case that can be extended to run your final attack.
4. Test the simple case against the target the actual target setup.
5. Test the more complex case against the target setup

mitmproxy

How To Build An Attack

1. Analyse normal behaviour.
2. Use a basic setup to test the simplest form of the attack.
3. Start with a simple case that can be extended to run your final attack.
4. Test the simple case against the target the actual target setup.
5. Test the more complex case against the target setup

mitmproxy

How To Build An Attack

1. Analyse normal behaviour.
2. Use a basic setup to test the simplest form of the attack.
3. Start with a simple case that can be extended to run your final attack.
4. Test the simple case against the target the actual target setup.
5. Test the more complex case against the target setup

mitmproxy

How To Build An Attack

1. Analyse normal behaviour.
2. Use a basic setup to test the simplest form of the attack.
3. Start with a simple case that can be extended to run your final attack.
4. Test the simple case against the target the actual target setup.
5. Test the more complex case against the target setup

mitmproxy

How To Build An Attack

1. Analyse normal behaviour.
2. Use a basic setup to test the simplest form of the attack.
3. Start with a simple case that can be extended to run your final attack.
4. Test the simple case against the target the actual target setup.
5. Test the more complex case against the target setup

mitmproxy

How To Build An Attack

1. Analyse normal behaviour.
2. Use a basic setup to test the simplest form of the attack.
3. Start with a simple case that can be extended to run your final attack.
4. Test the simple case against the target the actual target setup.
5. Test the more complex case against the target setup