The main purpose of Faraday is to re-use the available tools in the community to take advantage of them in a multiuser way.

> You break it. We keep track of the pieces!

To maximize flexibility Faraday Plugins run only on the client, which means you can have custom, private plugins all for yourself!

There are three kinds of plugins available for Faraday; **console**, **report** and **API** also called **online**. However, these are not mutually exclusive, meaning that some tools have more than one Plugin to process their output. For example, **Nmap** has a Console plugin which allows you to run it directly from ZSH, but it also has a Report one, in order to import scans that were run outside of Faraday.

Console

Plugins that intercept commands, fired directly when a command is detected in the console. These are transparent to you and no additional action on your part is needed.

Report

Plugins that import file reports. You have to copy the report to `~/.faraday/report/{workspacename}` (replacing **{workspacename}** with the actual name of your Workspace) and Faraday GTK client will automatically detect, process and add it to the HostTree.

If Faraday is not capable to detect the plugin needed to process the report, you can manually choose which plugin will be used by adding `_faraday_pluginName` to the file name before the extension.

For example, if the **Burp** report named `burp_1456983368.xml` is not being recognized, try renaming it to `Burp_1456983368_faraday_Burp.xml`. Now copy it to the Workspace directory and Faraday should now run the plugin and import all vulnerabilities.

Keep in mind that this functionality is **case sensitive**. The names of the available plugins are:

- Acunetix
- Arachni
- Burp
- Core Impact
- Maltego
- Metasploit
- Nessus
- Netsparker
- Nexpose
- NexposeFull
- Nikto

- Nmap
- Openvas
- Qualysguard
- Retina
- W3af
- X1
- Zap

API

Plugin connectors or online ([[BeEF]], [[Metasploit]], Burp), these connect to external APIs or databases, or talk directly to Faraday's RPC API.

List

If you think your favourite tool is missing code your own plugin or ask us to do it!

- Acunetix (REPORT) (XML)
- Amap (CONSOLE)
- Arachni (REPORT, CONSOLE) (XML)
- arp-scan (CONSOLE)
- BeEF (API)
- Burp, BurpPro (REPORT, API) (XML)
- Core Impact, Core Impact (REPORT) (XML)
- Dig (CONSOLE)
- Dirb (CONSOLE)
- Dnsenum (CONSOLE)
- Dnsmap (CONSOLE)
- Dnsrecon (CONSOLE)
- Dnswalk (CONSOLE)
- evilgrade (API)
- Fierce (CONSOLE)
- Fruitywifi (API)
- ftp (CONSOLE)
- Goohost (CONSOLE)
- hping3 (CONSOLE)
- Hydra (CONSOLE) (XML)
- Immunity Canvas (API)
- Linys (REPORT)
- Listurls (CONSOLE)
- Maltego (REPORT)
- masscan (REPORT, CONSOLE) (XML)
- Medusa (CONSOLE)
- Metagoofil (CONSOLE)
- Metasploit, (REPORT, API) (XML) XML report

- Ndiff (REPORT, CONSOLE)
- Nessus, (REPORT) (XML .nessus)
- Netcat (CONSOLE)
- Netdiscover (CONSOLE)
- Netsparker (REPORT) (XML)
- Netsparker Cloud (REPORT)
- Nexpose, Nexpose Enterprise, (REPORT) (simple XML, XML Export plugin (2.0))
- Nikto (REPORT, CONSOLE) (XML)
- Nmap (REPORT, CONSOLE) (XML)
- Openvas (REPORT) (XML)
- PasteAnalyzer (CONSOLE)
- Peeping Tom (CONSOLE)
- ping (CONSOLE)
- propecia (CONSOLE)
- Qualysguard (REPORT) (XML)
- Retina (REPORT) (XML)
- Reverseraider (CONSOLE)
- Sentinel (API)
- Shodan (API)
- Skipfish (CONSOLE)
- Sqlmap (CONSOLE)
- SSHdefaultscan (CONSOLE)
- SSLcheck (CONSOLE)
- Telnet (CONSOLE)
- Theharvester (CONSOLE)
- Traceroute (CONSOLE)
- W3af (REPORT) (XML)
- Wapiti (CONSOLE)
- Wcscan (CONSOLE)
- Webfuzzer (CONSOLE)
- whois (CONSOLE)
- WPScan (CONSOLE)
- X1, Onapsis (REPORT) (XML)
- Zap (REPORT) (XML)