Data Flow in O-Saft

O-Saft

Host[:Port] demo

Start +check +cipher +info +quick +protocols +vulns Load

☐ --header ☐ --enabled ☐ --no-dns ☐ --no-http ☐ --no-sni ☐ --no-sslv2 ☐ --no-tlsv13

Commands Options Filter (1) Load

```
o-saft.pl '--cfg_cmd=vulns=beast breach crime drown freak heartbleed logjam lucky13 poodle r
c4 sloth sweet32 time hassslv2 hassslv3 pfs_cipher session_random' --ignore-output=https_bod
y +info demo

=== reading: ./o-saft.pl (RC-FILE done) ===
=== reading: /usr/share/perl5/IO/Socket/SSL.pm (IO SSL module done) ===
=== reading: Net/SSLinfo.pm (O-Saft module done) ===
Given hostname:                 demo
IP for given hostname:          127.0.1.2
Reverse resolved hostname:      demo
DNS entries for given hostname: 127.0.1.2 demo;
Certificate Version:            3 (0x2)
Certificate Common Name:        demo
Certificate Subject:            /C=xy/ST=some, L=Lummerland/L=<img src="//o.saft/city-f
rom-SSL"/>/O=sic[!]sec GmbH/OU=ou, OU=b\xC3\x83\xC2\xBCro/CN=demo
Certificate Subject Name Hash:  f6e9b9c5
Certificate Issuer:             /C=xy/ST=some, L=Lummerland/L=<img src="//o.saft/city-f
rom-SSL"/>/O=sic[!]sec GmbH/OU=ou, OU=b\xC3\x83\xC2\xBCro/CN=demo
Certificate Issuer Name Hash:   f6e9b9c5
Certificate Serial Number:      ba:72:80:02:89:b5:2b:82
Certificate Fingerprint:        SHA1 Fingerprint=55D7A8009A0FB2B2467716A8F209FF7F6AA8C9
5B
Certificate Fingerprint Algorithm: SHA1
```

Save STDOUT Filter   Close TAB

Quit

o-saft.tcl

legend:

▭ **O-Saft modules**

▭ **Perl modules**

▭ **openssl executable and OS libraries**

▶ procedure call

▶ data flow

bunt.pl
HTML-table.awk
XML-value.awk
...

„postprocess"

build GUI
called once at startup

+help

+help=cmd   **+help=options**

execute commands
called for each command

+*   **--***

o-saft.pl

+cipher
--openssl=*

+check   **+cipherall**

+info   **+cipher**

checkAllCiphers.pl

Net::SSLinfo   **Net::SSLhello**

IO::Socket
::SSL   ::INET

openssl   **Net::SSLeay**

libcrypto. dll so   **libssl.** dll so   **Net::DNS**

some.tld:443

starttls.tld:25
(smtp, imap,...)

17.05.17