ETHICAL HACKING TOOLS

INTRODUCTION:

we are going to perform penetration test on the given target site.

Target site: www.apple.com

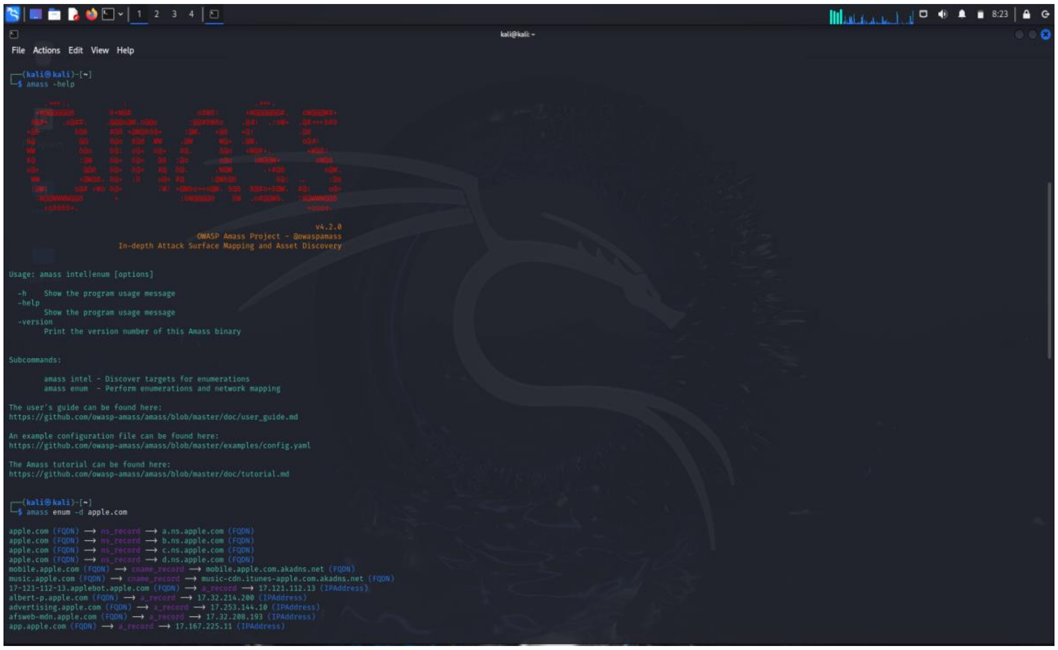
Tools performed:

- ✓ Sublist3r
- ✓ Amass
- ✓ Findomain
- ✓ Assetfinder
- ✓ Securitytrails.com
- ✓ Dirsearch
- ✓ LinkFinder
- ✓ Waybackurls
- ✓ ParamSpider
- ✓ FFUF
- ✓ SSRFmap
- ✓ Sqlmap
- ✓ Dalfox
- ✓ retire.js

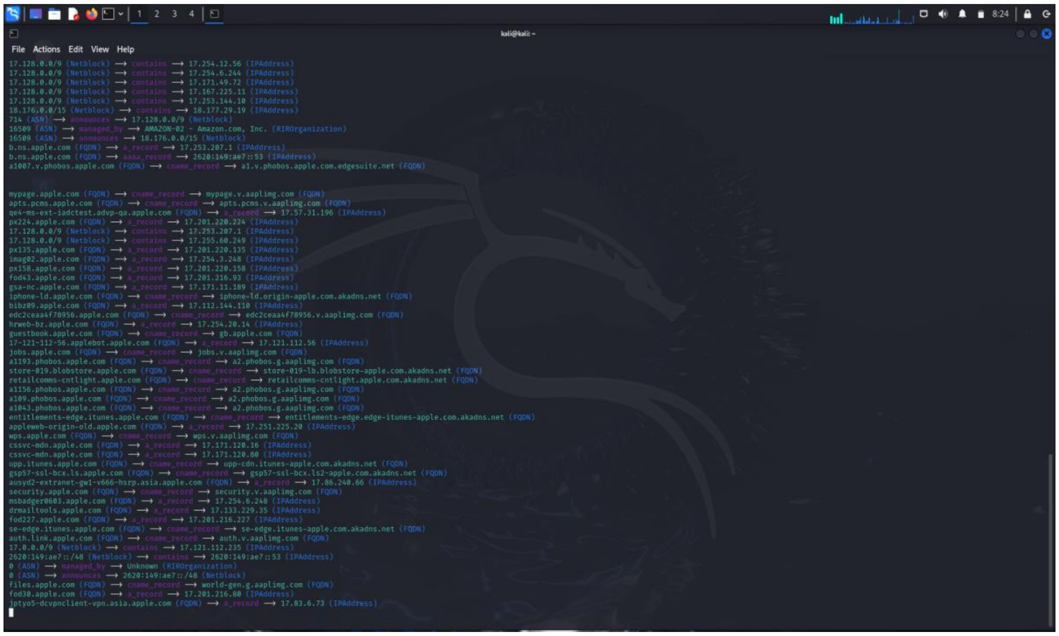
1.Reconnaissance & Subdomain Enumeration

➢ AMASS

Purpose: Amass used for Identifying sub domains



```
┌──(kali㉿kali)-[~]
└─$ amass -help

                                                                    v4.2.0
                                        OWASP Amass Project - @owaspamass
                          In-depth Attack Surface Mapping and Asset Discovery

Usage: amass intel|enum [options]

  -h    Show the program usage message
  -help
        Show the program usage message
  -version
        Print the version number of this Amass binary


Subcommands:

        amass intel - Discover targets for enumerations
        amass enum  - Perform enumerations and network mapping

The user's guide can be found here:
https://github.com/owasp-amass/amass/blob/master/doc/user_guide.md

An example configuration file can be found here:
https://github.com/owasp-amass/amass/blob/master/examples/config.yaml

The Amass tutorial can be found here:
https://github.com/owasp-amass/amass/blob/master/doc/tutorial.md


┌──(kali㉿kali)-[~]
└─$ amass enum -d apple.com

apple.com (FQDN) ⟶ ns_record ⟶ a.ns.apple.com (FQDN)
apple.com (FQDN) ⟶ ns_record ⟶ b.ns.apple.com (FQDN)
apple.com (FQDN) ⟶ ns_record ⟶ c.ns.apple.com (FQDN)
apple.com (FQDN) ⟶ ns_record ⟶ d.ns.apple.com (FQDN)
mobile.apple.com (FQDN) ⟶ cname_record ⟶ mobile.apple.com.akadns.net (FQDN)
music.apple.com (FQDN) ⟶ cname_record ⟶ music-cdn.itunes-apple.com.akadns.net (FQDN)
17-121-112-13.applebot.apple.com (FQDN) ⟶ a_record ⟶ 17.121.112.13 (IPAddress)
albert-p.apple.com (FQDN) ⟶ a_record ⟶ 17.32.214.200 (IPAddress)
advertising.apple.com (FQDN) ⟶ a_record ⟶ 17.253.144.10 (IPAddress)
afsweb-mdn.apple.com (FQDN) ⟶ a_record ⟶ 17.32.208.193 (IPAddress)
app.apple.com (FQDN) ⟶ a_record ⟶ 17.167.225.11 (IPAddress)
```

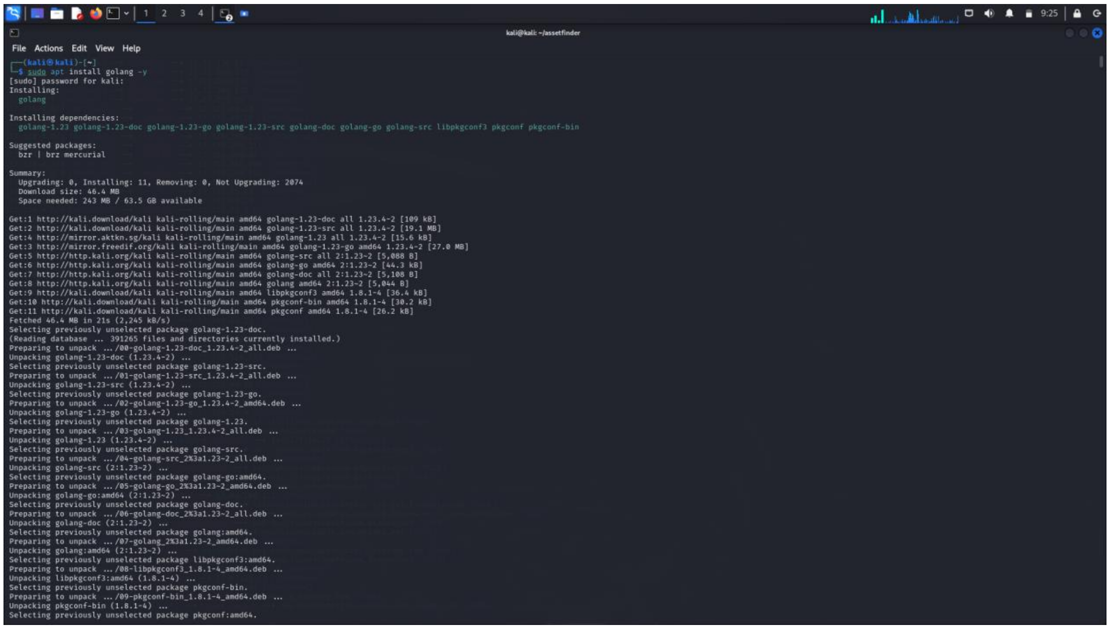


```
17.128.0.0/9 (Netblock) ⟶ contains ⟶ 17.254.12.56 (IPAddress)
17.128.0.0/9 (Netblock) ⟶ contains ⟶ 17.254.6.244 (IPAddress)
17.128.0.0/9 (Netblock) ⟶ contains ⟶ 17.171.49.72 (IPAddress)
17.128.0.0/9 (Netblock) ⟶ contains ⟶ 17.167.225.11 (IPAddress)
17.128.0.0/9 (Netblock) ⟶ contains ⟶ 17.253.144.10 (IPAddress)
18.176.0.0/15 (Netblock) ⟶ contains ⟶ 18.177.29.19 (IPAddress)
714 (ASN) ⟶ announces ⟶ 17.128.0.0/9 (Netblock)
16509 (ASN) ⟶ managed_by ⟶ AMAZON-02 - Amazon.com, Inc. (RIROrganization)
16509 (ASN) ⟶ announces ⟶ 18.176.0.0/15 (Netblock)
b.ns.apple.com (FQDN) ⟶ a_record ⟶ 17.253.207.1 (IPAddress)
b.ns.apple.com (FQDN) ⟶ aaaa_record ⟶ 2620:149:ae7::53 (IPAddress)
a1007.v.phobos.apple.com (FQDN) ⟶ cname_record ⟶ a1.v.phobos.apple.com.edgesuite.net (FQDN)


mypage.apple.com (FQDN) ⟶ cname_record ⟶ mypage.v.aaplimg.com (FQDN)
apts.pcms.apple.com (FQDN) ⟶ cname_record ⟶ apts.pcms.v.aaplimg.com (FQDN)
qe4-ms-ext-iadctest.advp-qa.apple.com (FQDN) ⟶ a_record ⟶ 17.57.31.196 (IPAddress)
px224.apple.com (FQDN) ⟶ a_record ⟶ 17.201.220.224 (IPAddress)
17.128.0.0/9 (Netblock) ⟶ contains ⟶ 17.253.207.1 (IPAddress)
17.128.0.0/9 (Netblock) ⟶ contains ⟶ 17.255.60.249 (IPAddress)
px135.apple.com (FQDN) ⟶ a_record ⟶ 17.201.220.135 (IPAddress)
imag02.apple.com (FQDN) ⟶ a_record ⟶ 17.254.3.248 (IPAddress)
px158.apple.com (FQDN) ⟶ a_record ⟶ 17.201.220.158 (IPAddress)
fod43.apple.com (FQDN) ⟶ a_record ⟶ 17.201.216.93 (IPAddress)
gsa-nc.apple.com (FQDN) ⟶ a_record ⟶ 17.171.11.189 (IPAddress)
iphone-ld.apple.com (FQDN) ⟶ cname_record ⟶ iphone-ld.origin-apple.com.akadns.net (FQDN)
bibz09.apple.com (FQDN) ⟶ a_record ⟶ 17.112.144.110 (IPAddress)
edc2ceaa4f78956.apple.com (FQDN) ⟶ cname_record ⟶ edc2ceaa4f78956.v.aaplimg.com (FQDN)
hrweb-bz.apple.com (FQDN) ⟶ a_record ⟶ 17.254.20.14 (IPAddress)
guestbook.apple.com (FQDN) ⟶ cname_record ⟶ gb.apple.com (FQDN)
17-121-112-56.applebot.apple.com (FQDN) ⟶ a_record ⟶ 17.121.112.56 (IPAddress)
jobs.apple.com (FQDN) ⟶ cname_record ⟶ jobs.v.aaplimg.com (FQDN)
a1193.phobos.apple.com (FQDN) ⟶ cname_record ⟶ a2.phobos.g.aaplimg.com (FQDN)
store-019.blobstore.apple.com (FQDN) ⟶ cname_record ⟶ store-019-lb.blobstore-apple.com.akadns.net (FQDN)
retailcomms-cntlight.apple.com (FQDN) ⟶ cname_record ⟶ retailcomms-cntlight.apple.com.akadns.net (FQDN)
a1156.phobos.apple.com (FQDN) ⟶ cname_record ⟶ a2.phobos.g.aaplimg.com (FQDN)
a109.phobos.apple.com (FQDN) ⟶ cname_record ⟶ a2.phobos.g.aaplimg.com (FQDN)
a1043.phobos.apple.com (FQDN) ⟶ cname_record ⟶ a2.phobos.g.aaplimg.com (FQDN)
entitlements-edge.itunes.apple.com (FQDN) ⟶ cname_record ⟶ entitlements-edge.edge-itunes-apple.com.akadns.net (FQDN)
appleweb-origin-old.apple.com (FQDN) ⟶ a_record ⟶ 17.251.225.20 (IPAddress)
wps.apple.com (FQDN) ⟶ cname_record ⟶ wps.v.aaplimg.com (FQDN)
cssvc-mdn.apple.com (FQDN) ⟶ a_record ⟶ 17.171.120.16 (IPAddress)
cssvc-mdn.apple.com (FQDN) ⟶ a_record ⟶ 17.171.120.80 (IPAddress)
upp.itunes.apple.com (FQDN) ⟶ cname_record ⟶ upp-cdn.itunes-apple.com.akadns.net (FQDN)
gsp57-ssl-bcx.ls.apple.com (FQDN) ⟶ cname_record ⟶ gsp57-ssl-bcx.ls2-apple.com.akadns.net (FQDN)
ausyd2-extranet-gw1-v666-hsrp.asia.apple.com (FQDN) ⟶ a_record ⟶ 17.86.240.66 (IPAddress)
security.apple.com (FQDN) ⟶ cname_record ⟶ security.v.aaplimg.com (FQDN)
msbadger0603.apple.com (FQDN) ⟶ a_record ⟶ 17.254.6.248 (IPAddress)
drmailtools.apple.com (FQDN) ⟶ a_record ⟶ 17.133.229.35 (IPAddress)
fod227.apple.com (FQDN) ⟶ a_record ⟶ 17.201.216.227 (IPAddress)
se-edge.itunes.apple.com (FQDN) ⟶ cname_record ⟶ se-edge.itunes-apple.com.akadns.net (FQDN)
auth.link.apple.com (FQDN) ⟶ cname_record ⟶ auth.v.aaplimg.com (FQDN)
17.0.0.0/9 (Netblock) ⟶ contains ⟶ 17.121.112.235 (IPAddress)
2620:149:ae7::/48 (Netblock) ⟶ contains ⟶ 2620:149:ae7::53 (IPAddress)
0 (ASN) ⟶ managed_by ⟶ Unknown (RIROrganization)
0 (ASN) ⟶ announces ⟶ 2620:149:ae7::/48 (Netblock)
files.apple.com (FQDN) ⟶ cname_record ⟶ world-gen.g.aaplimg.com (FQDN)
fod30.apple.com (FQDN) ⟶ a_record ⟶ 17.201.216.80 (IPAddress)
jptyo5-dcvpnclient-vpn.asia.apple.com (FQDN) ⟶ a_record ⟶ 17.83.6.73 (IPAddress)
```

➢ ASSETFINDER

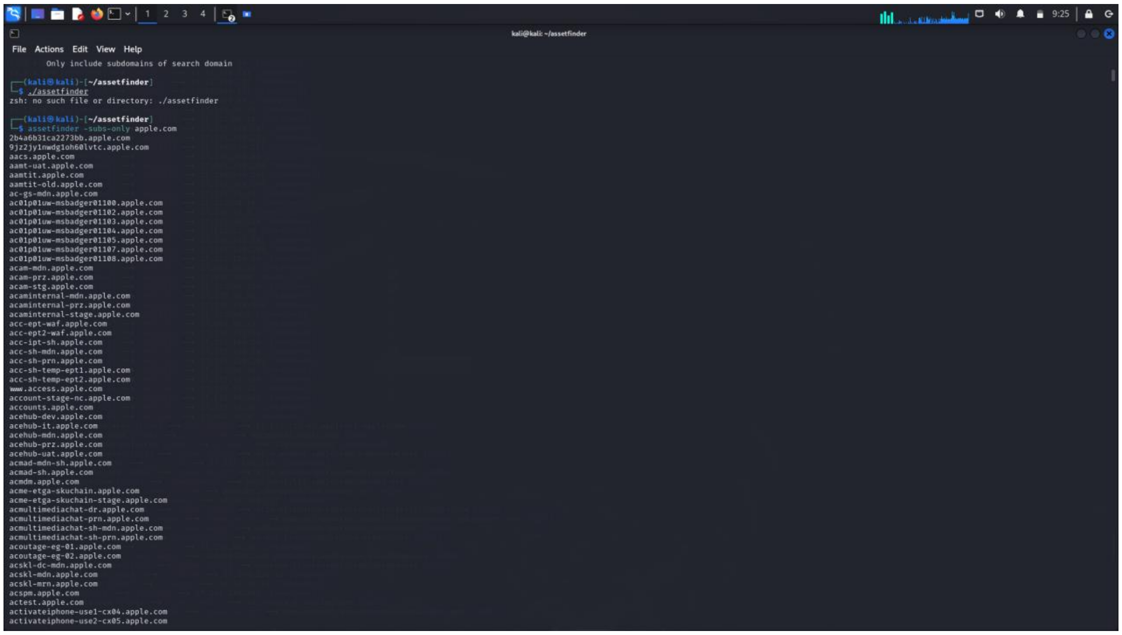
Purpose:This tool also helps to find the hidden sub domains

Prerequirement⇨ Go language

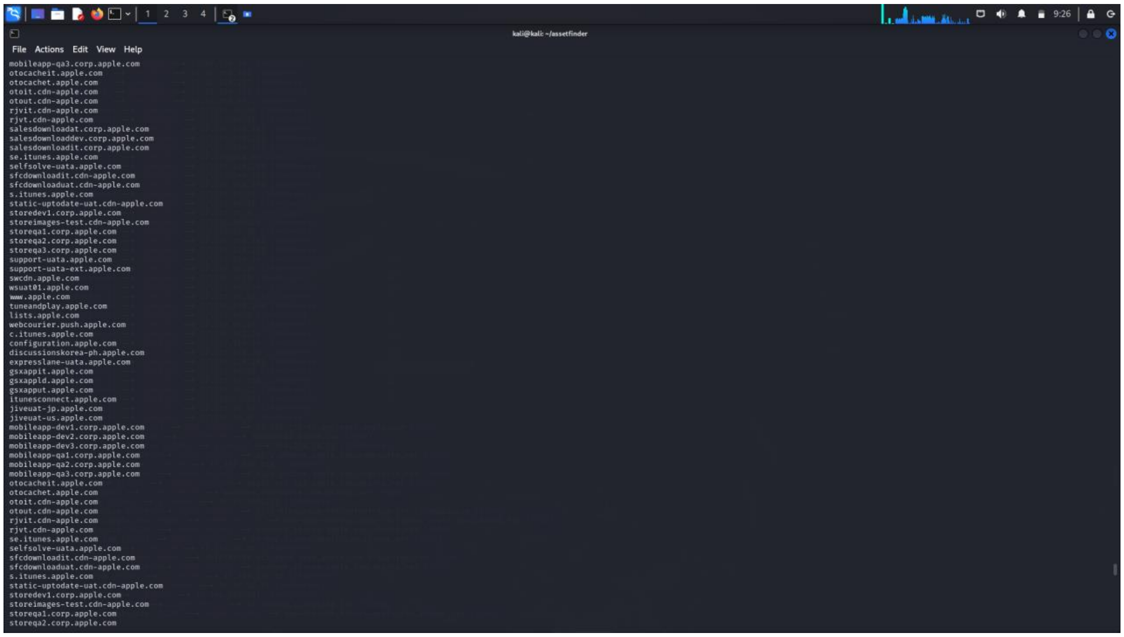


```
┌──(kali㉿kali)-[~]
└─$ sudo apt install golang -y
[sudo] password for kali:
Installing:
  golang

Installing dependencies:
  golang-1.23 golang-1.23-doc golang-1.23-go golang-1.23-src golang-doc golang-go golang-src libpkgconf3 pkgconf pkgconf-bin

Suggested packages:
  bzr | brz mercurial

Summary:
  Upgrading: 0, Installing: 11, Removing: 0, Not Upgrading: 2074
  Download size: 46.4 MB
  Space needed: 243 MB / 63.5 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 golang-1.23-doc all 1.23.4-2 [109 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 golang-1.23-src all 1.23.4-2 [19.1 MB]
Get:4 http://mirror.aktkn.sg/kali kali-rolling/main amd64 golang-1.23 all 1.23.4-2 [15.6 kB]
Get:3 http://mirror.freedif.org/kali kali-rolling/main amd64 golang-1.23-go amd64 1.23.4-2 [27.0 MB]
Get:5 http://http.kali.org/kali kali-rolling/main amd64 golang-src all 2:1.23~2 [5,088 B]
Get:6 http://http.kali.org/kali kali-rolling/main amd64 golang-go amd64 2:1.23~2 [44.3 kB]
Get:7 http://http.kali.org/kali kali-rolling/main amd64 golang-doc all 2:1.23~2 [5,108 B]
Get:8 http://http.kali.org/kali kali-rolling/main amd64 golang amd64 2:1.23~2 [5,044 B]
Get:9 http://kali.download/kali kali-rolling/main amd64 libpkgconf3 amd64 1.8.1-4 [36.4 kB]
Get:10 http://kali.download/kali kali-rolling/main amd64 pkgconf-bin amd64 1.8.1-4 [30.2 kB]
Get:11 http://kali.download/kali kali-rolling/main amd64 pkgconf amd64 1.8.1-4 [26.2 kB]
Fetched 46.4 MB in 21s (2,245 kB/s)
Selecting previously unselected package golang-1.23-doc.
(Reading database ... 391265 files and directories currently installed.)
Preparing to unpack .../00-golang-1.23-doc_1.23.4-2_all.deb ...
Unpacking golang-1.23-doc (1.23.4-2) ...
Selecting previously unselected package golang-1.23-src.
Preparing to unpack .../01-golang-1.23-src_1.23.4-2_all.deb ...
Unpacking golang-1.23-src (1.23.4-2) ...
Selecting previously unselected package golang-1.23-go.
Preparing to unpack .../02-golang-1.23-go_1.23.4-2_amd64.deb ...
Unpacking golang-1.23-go (1.23.4-2) ...
Selecting previously unselected package golang-1.23.
Preparing to unpack .../03-golang-1.23_1.23.4-2_all.deb ...
Unpacking golang-1.23 (1.23.4-2) ...
Selecting previously unselected package golang-src.
Preparing to unpack .../04-golang-src_2%3a1.23~2_all.deb ...
Unpacking golang-src (2:1.23~2) ...
Selecting previously unselected package golang-go:amd64.
Preparing to unpack .../05-golang-go_2%3a1.23~2_amd64.deb ...
Unpacking golang-go:amd64 (2:1.23~2) ...
Selecting previously unselected package golang-doc.
Preparing to unpack .../06-golang-doc_2%3a1.23~2_all.deb ...
Unpacking golang-doc (2:1.23~2) ...
Selecting previously unselected package golang:amd64.
Preparing to unpack .../07-golang_2%3a1.23~2_amd64.deb ...
Unpacking golang:amd64 (2:1.23~2) ...
Selecting previously unselected package libpkgconf3:amd64.
Preparing to unpack .../08-libpkgconf3_1.8.1-4_amd64.deb ...
Unpacking libpkgconf3:amd64 (1.8.1-4) ...
Selecting previously unselected package pkgconf-bin.
Preparing to unpack .../09-pkgconf-bin_1.8.1-4_amd64.deb ...
Unpacking pkgconf-bin (1.8.1-4) ...
Selecting previously unselected package pkgconf:amd64.
```

<u>IDENTIFIED SUB-SUBDOMAINS</u>



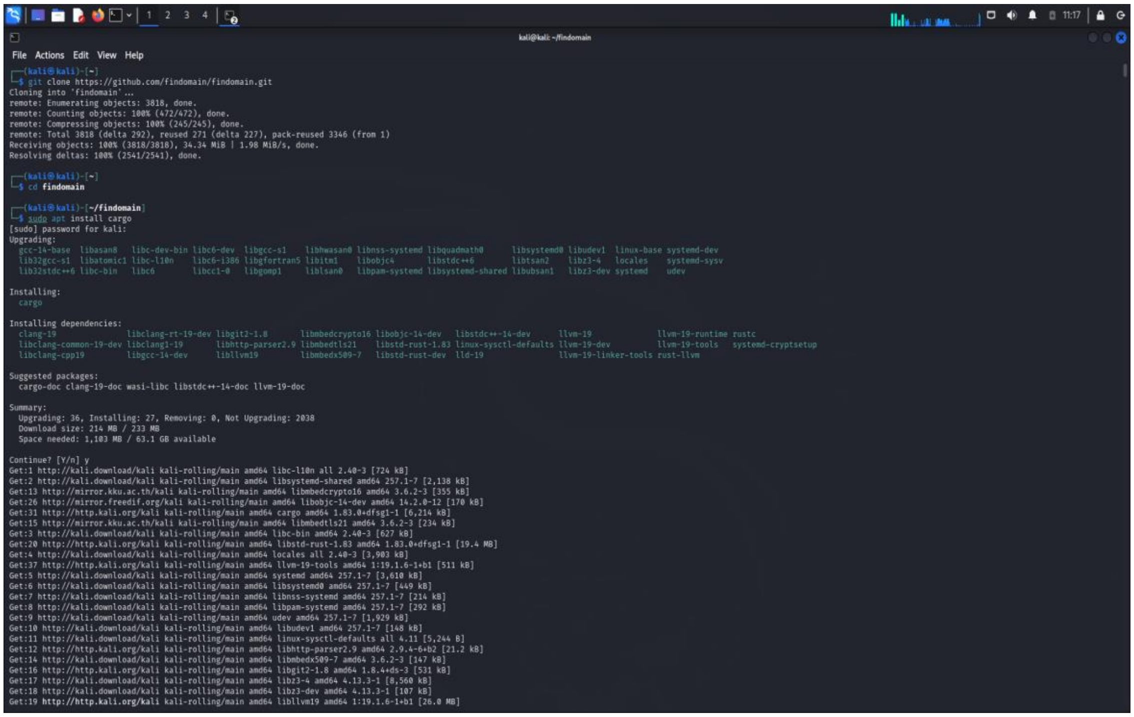
```
        Only include subdomains of search domain

┌──(kali㉿kali)-[~/assetfinder]
└─$ ./assetfinder
zsh: no such file or directory: ./assetfinder

┌──(kali㉿kali)-[~/assetfinder]
└─$ assetfinder -subs-only apple.com
2b4a6b31ca2273bb.apple.com
9jz2jy1nwdg1oh60lvtc.apple.com
aacs.apple.com
aamt-uat.apple.com
aamtit.apple.com
aamtit-old.apple.com
ac-gs-mdn.apple.com
ac01p01uw-msbadger01100.apple.com
ac01p01uw-msbadger01102.apple.com
ac01p01uw-msbadger01103.apple.com
ac01p01uw-msbadger01104.apple.com
ac01p01uw-msbadger01105.apple.com
ac01p01uw-msbadger01107.apple.com
ac01p01uw-msbadger01108.apple.com
acam-mdn.apple.com
acam-prz.apple.com
acam-stg.apple.com
acaminternal-mdn.apple.com
acaminternal-prz.apple.com
acaminternal-stage.apple.com
acc-ept-waf.apple.com
acc-ept2-waf.apple.com
acc-ipt-sh.apple.com
acc-sh-mdn.apple.com
acc-sh-prn.apple.com
acc-sh-temp-ept1.apple.com
acc-sh-temp-ept2.apple.com
www.access.apple.com
account-stage-nc.apple.com
accounts.apple.com
acehub-dev.apple.com
acehub-it.apple.com
acehub-mdn.apple.com
acehub-prz.apple.com
acehub-uat.apple.com
acmad-mdn-sh.apple.com
acmad-sh.apple.com
acmdm.apple.com
acme-etga-skuchain.apple.com
acme-etga-skuchain-stage.apple.com
acmultimediachat-dr.apple.com
acmultimediachat-prn.apple.com
acmultimediachat-sh-mdn.apple.com
acmultimediachat-sh-prn.apple.com
acoutage-eg-01.apple.com
acoutage-eg-02.apple.com
acskl-dc-mdn.apple.com
acskl-mdn.apple.com
acskl-mrn.apple.com
acspm.apple.com
actest.apple.com
activateiphone-use1-cx04.apple.com
activateiphone-use2-cx05.apple.com
```



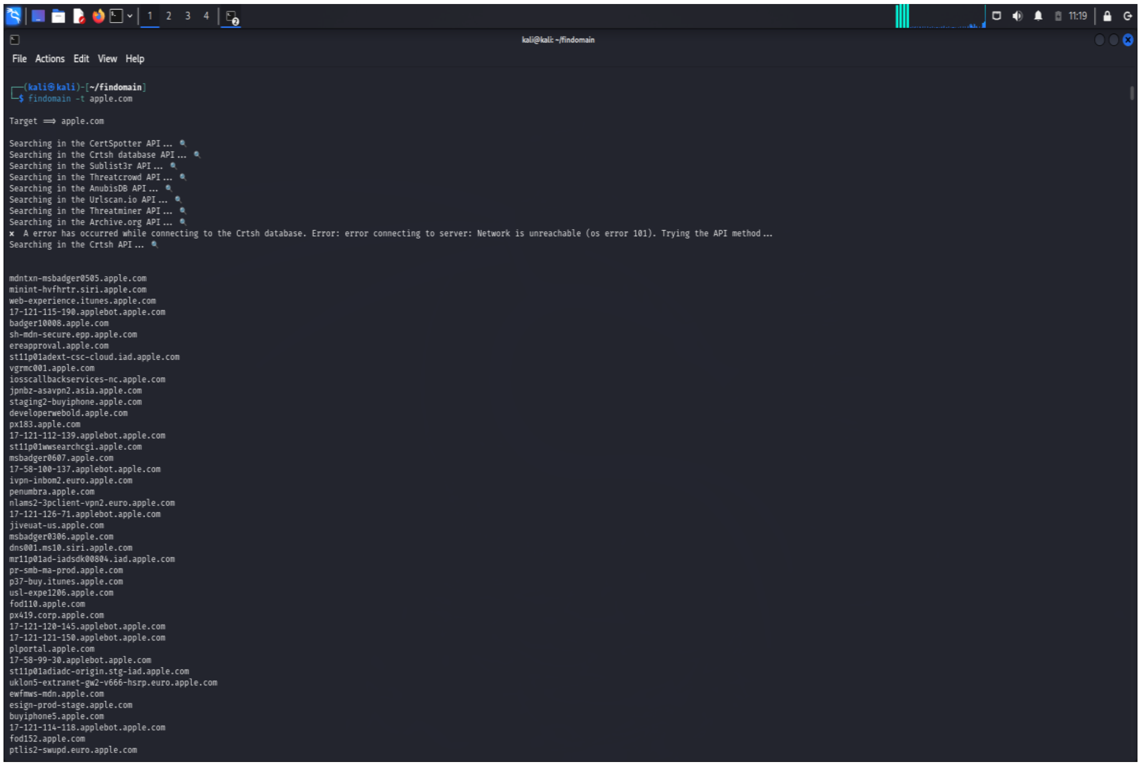
```
mobileapp-qa3.corp.apple.com
otocacheit.apple.com
otocachet.apple.com
otoit.cdn-apple.com
otout.cdn-apple.com
rjvit.cdn-apple.com
rjvt.cdn-apple.com
salesdownloadat.corp.apple.com
salesdownloaddev.corp.apple.com
salesdownloadit.corp.apple.com
se.itunes.apple.com
selfsolve-uata.apple.com
sfcdownloadit.cdn-apple.com
sfcdownloaduat.cdn-apple.com
s.itunes.apple.com
static-uptodate-uat.cdn-apple.com
storedev1.corp.apple.com
storeimages-test.cdn-apple.com
storeqa1.corp.apple.com
storeqa2.corp.apple.com
storeqa3.corp.apple.com
support-uata.apple.com
support-uata-ext.apple.com
swcdn.apple.com
wsuat01.apple.com
www.apple.com
tuneandplay.apple.com
lists.apple.com
webcourier.push.apple.com
c.itunes.apple.com
configuration.apple.com
discussionskorea-ph.apple.com
expresslane-uata.apple.com
gsxappit.apple.com
gsxappld.apple.com
gsxapput.apple.com
itunesconnect.apple.com
jiveuat-jp.apple.com
jiveuat-us.apple.com
mobileapp-dev1.corp.apple.com
mobileapp-dev2.corp.apple.com
mobileapp-dev3.corp.apple.com
mobileapp-qa1.corp.apple.com
mobileapp-qa2.corp.apple.com
mobileapp-qa3.corp.apple.com
otocacheit.apple.com
otocachet.apple.com
otoit.cdn-apple.com
otout.cdn-apple.com
rjvit.cdn-apple.com
rjvt.cdn-apple.com
se.itunes.apple.com
selfsolve-uata.apple.com
sfcdownloadit.cdn-apple.com
sfcdownloaduat.cdn-apple.com
s.itunes.apple.com
static-uptodate-uat.cdn-apple.com
storedev1.corp.apple.com
storeimages-test.cdn-apple.com
storeqa1.corp.apple.com
storeqa2.corp.apple.com
```

➢ FINDOMAIN

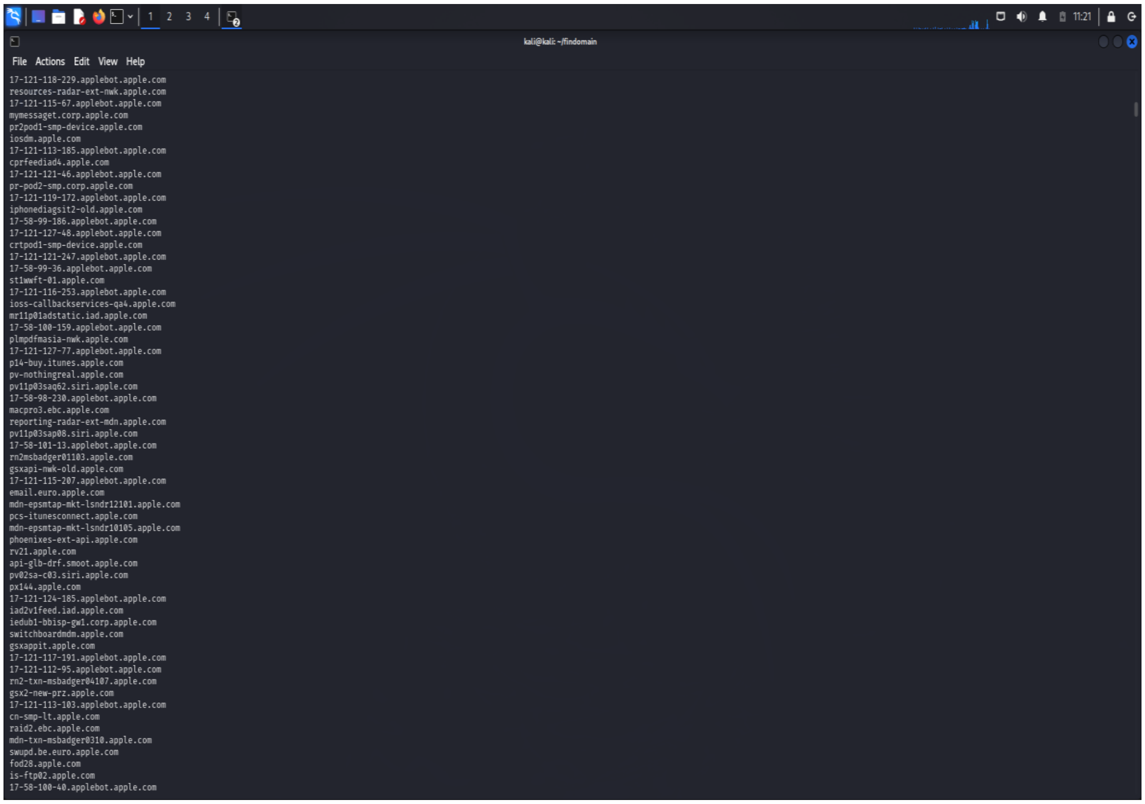
Purpose:Findomain helps to identifying the subdomains of website



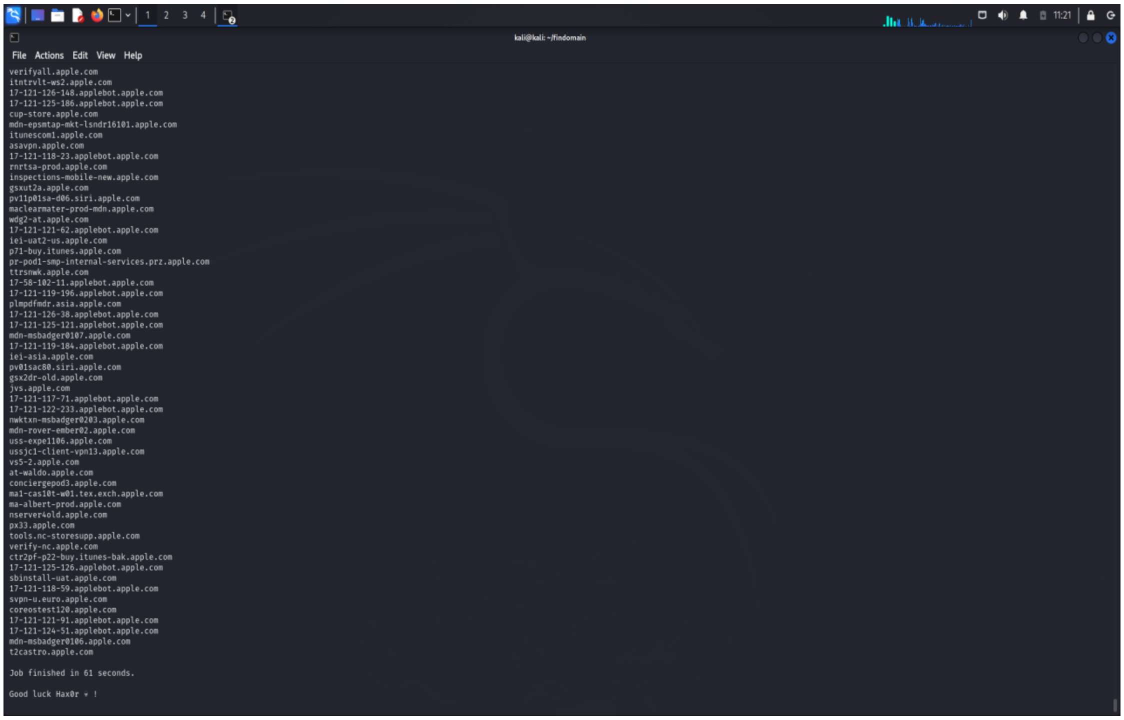
```
┌──(kali㉿kali)-[~]
└─$ git clone https://github.com/findomain/findomain.git
Cloning into 'findomain'...
remote: Enumerating objects: 3818, done.
remote: Counting objects: 100% (472/472), done.
remote: Compressing objects: 100% (245/245), done.
remote: Total 3818 (delta 292), reused 271 (delta 227), pack-reused 3346 (from 1)
Receiving objects: 100% (3818/3818), 34.34 MiB | 1.98 MiB/s, done.
Resolving deltas: 100% (2541/2541), done.

┌──(kali㉿kali)-[~]
└─$ cd findomain

┌──(kali㉿kali)-[~/findomain]
└─$ sudo apt install cargo
[sudo] password for kali:
Upgrading:
  gcc-14-base  libasan8   libc-dev-bin libc6-dev  libgcc-s1    libhwasan0 libnss-systemd libquadmath0      libsystemd0 libudev1  linux-base systemd-dev
  lib32gcc-s1  libatomic1 libc-l10n    libc6-i386 libgfortran5 libitm1    libobjc4       libstdc++6        libtsan2    libz3-4   locales    systemd-sysv
  lib32stdc++6 libc-bin   libc6        libcc1-0   libgomp1     liblsan0   libpam-systemd libsystemd-shared libubsan1   libz3-dev systemd    udev

Installing:
  cargo

Installing dependencies:
  clang-19               libclang-rt-19-dev libgit2-1.8        libmbedcrypto16 libobjc-14-dev    libstdc++-14-dev       llvm-19               llvm-19-runtime rustc
  libclang-common-19-dev libclang1-19       libhttp-parser2.9 libmbedtls21    libstd-rust-1.83 linux-sysctl-defaults llvm-19-dev           llvm-19-tools   systemd-cryptsetup
  libclang-cpp19         libgcc-14-dev      libllvm19          libmbedx509-7   libstd-rust-dev  lld-19                 llvm-19-linker-tools rust-llvm

Suggested packages:
  cargo-doc clang-19-doc wasi-libc libstdc++-14-doc llvm-19-doc

Summary:
  Upgrading: 36, Installing: 27, Removing: 0, Not Upgrading: 2038
  Download size: 214 MB / 233 MB
  Space needed: 1,103 MB / 63.1 GB available

Continue? [Y/n] y
Get:1 http://kali.download/kali kali-rolling/main amd64 libc-l10n all 2.40-3 [724 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 libsystemd-shared amd64 257.1-7 [2,138 kB]
Get:13 http://mirror.kku.ac.th/kali kali-rolling/main amd64 libmbedcrypto16 amd64 3.6.2-3 [355 kB]
Get:26 http://mirror.freedif.org/kali kali-rolling/main amd64 libobjc-14-dev amd64 14.2.0-12 [170 kB]
Get:31 http://http.kali.org/kali kali-rolling/main amd64 cargo amd64 1.83.0+dfsg1-1 [6,214 kB]
Get:15 http://mirror.kku.ac.th/kali kali-rolling/main amd64 libmbedtls21 amd64 3.6.2-3 [234 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 libc-bin amd64 2.40-3 [627 kB]
Get:20 http://http.kali.org/kali kali-rolling/main amd64 libstd-rust-1.83 amd64 1.83.0+dfsg1-1 [19.4 MB]
Get:4 http://kali.download/kali kali-rolling/main amd64 locales all 2.40-3 [3,903 kB]
Get:37 http://http.kali.org/kali kali-rolling/main amd64 llvm-19-tools amd64 1:19.1.6-1+b1 [511 kB]
Get:5 http://kali.download/kali kali-rolling/main amd64 systemd amd64 257.1-7 [3,610 kB]
Get:6 http://kali.download/kali kali-rolling/main amd64 libsystemd0 amd64 257.1-7 [449 kB]
Get:7 http://kali.download/kali kali-rolling/main amd64 libnss-systemd amd64 257.1-7 [214 kB]
Get:8 http://kali.download/kali kali-rolling/main amd64 libpam-systemd amd64 257.1-7 [292 kB]
Get:9 http://kali.download/kali kali-rolling/main amd64 udev amd64 257.1-7 [1,929 kB]
Get:10 http://kali.download/kali kali-rolling/main amd64 libudev1 amd64 257.1-7 [148 kB]
Get:11 http://kali.download/kali kali-rolling/main amd64 linux-sysctl-defaults all 4.11 [5,244 B]
Get:12 http://http.kali.org/kali kali-rolling/main amd64 libhttp-parser2.9 amd64 2.9.4-6+b2 [21.2 kB]
Get:14 http://kali.download/kali kali-rolling/main amd64 libmbedx509-7 amd64 3.6.2-3 [147 kB]
Get:16 http://http.kali.org/kali kali-rolling/main amd64 libgit2-1.8 amd64 1.8.4+ds-3 [531 kB]
Get:17 http://kali.download/kali kali-rolling/main amd64 libz3-4 amd64 4.13.3-1 [8,560 kB]
Get:18 http://kali.download/kali kali-rolling/main amd64 libz3-dev amd64 4.13.3-1 [107 kB]
Get:19 http://http.kali.org/kali kali-rolling/main amd64 libllvm19 amd64 1:19.1.6-1+b1 [26.0 MB]
```



```
┌──(kali㉿kali)-[~/findomain]
└─$ findomain -t apple.com

Target ⟹ apple.com

Searching in the CertSpotter API ... 🔍
Searching in the Crtsh database API ... 🔍
Searching in the Sublist3r API ... 🔍
Searching in the Threatcrowd API ... 🔍
Searching in the AnubisDB API ... 🔍
Searching in the Urlscan.io API ... 🔍
Searching in the Threatminer API ... 🔍
Searching in the Archive.org API ... 🔍
✗  A error has occurred while connecting to the Crtsh database. Error: error connecting to server: Network is unreachable (os error 101). Trying the API method ...
Searching in the Crtsh API ... 🔍


mdntxn-msbadger0505.apple.com
minint-hvfhrtr.siri.apple.com
web-experience.itunes.apple.com
17-121-115-190.applebot.apple.com
badger10008.apple.com
sh-mdn-secure.epp.apple.com
ereapproval.apple.com
st11p01adext-csc-cloud.iad.apple.com
vgrmc001.apple.com
iosscallbackservices-nc.apple.com
jpnbz-asavpn2.asia.apple.com
staging2-buyiphone.apple.com
developerwebold.apple.com
px183.apple.com
17-121-112-139.applebot.apple.com
st11p01wwsearchcgi.apple.com
msbadger0607.apple.com
17-58-100-137.applebot.apple.com
ivpn-inbom2.euro.apple.com
penumbra.apple.com
nlams2-3pclient-vpn2.euro.apple.com
17-121-126-71.applebot.apple.com
jiveuat-us.apple.com
msbadger0306.apple.com
dns001.ms10.siri.apple.com
mr11p01ad-iadsdk00804.iad.apple.com
pr-smb-ma-prod.apple.com
p37-buy.itunes.apple.com
usl-expe1206.apple.com
fod110.apple.com
px419.corp.apple.com
17-121-120-145.applebot.apple.com
17-121-121-150.applebot.apple.com
plportal.apple.com
17-58-99-30.applebot.apple.com
st11p01adiadc-origin.stg-iad.apple.com
uklon5-extranet-gw2-v666-hsrp.euro.apple.com
ewfmws-mdn.apple.com
esign-prod-stage.apple.com
buyiphone5.apple.com
17-121-114-118.applebot.apple.com
fod152.apple.com
ptlis2-swupd.euro.apple.com
```



```
17-121-118-229.applebot.apple.com
resources-radar-ext-nwk.apple.com
17-121-115-67.applebot.apple.com
mymessaget.corp.apple.com
pr2pod1-smp-device.apple.com
iosdm.apple.com
17-121-113-185.applebot.apple.com
cprfeediad4.apple.com
17-121-121-46.applebot.apple.com
pr-pod2-smp.corp.apple.com
17-121-119-172.applebot.apple.com
iphonediagsit2-old.apple.com
17-58-99-186.applebot.apple.com
17-121-127-48.applebot.apple.com
crtpod1-smp-device.apple.com
17-121-121-247.applebot.apple.com
17-58-99-36.applebot.apple.com
st1wwft-01.apple.com
17-121-116-253.applebot.apple.com
ioss-callbackservices-qa4.apple.com
mr11p01adstatic.iad.apple.com
17-58-100-159.applebot.apple.com
plmpdfmasia-nwk.apple.com
17-121-127-77.applebot.apple.com
p14-buy.itunes.apple.com
pv-nothingreal.apple.com
pv11p03saq62.siri.apple.com
17-58-98-230.applebot.apple.com
macpro3.ebc.apple.com
reporting-radar-ext-mdn.apple.com
pv11p03sap08.siri.apple.com
17-58-101-13.applebot.apple.com
rn2msbadger01103.apple.com
gsxapi-nwk-old.apple.com
17-121-115-207.applebot.apple.com
email.euro.apple.com
mdn-epsmtap-mkt-lsndr12101.apple.com
pcs-itunesconnect.apple.com
mdn-epsmtap-mkt-lsndr10105.apple.com
phoenixes-ext-api.apple.com
rv21.apple.com
api-glb-drf.smoot.apple.com
pv02sa-c03.siri.apple.com
px144.apple.com
17-121-124-185.applebot.apple.com
iad2v1feed.iad.apple.com
iedub1-bbisp-gw1.corp.apple.com
switchboardmdm.apple.com
gsxappit.apple.com
17-121-117-191.applebot.apple.com
17-121-112-95.applebot.apple.com
rn2-txn-msbadger04107.apple.com
gsx2-new-prz.apple.com
17-121-113-103.applebot.apple.com
cn-smp-lt.apple.com
raid2.ebc.apple.com
mdn-txn-msbadger0310.apple.com
swupd.be.euro.apple.com
fod28.apple.com
is-ftp02.apple.com
17-58-100-40.applebot.apple.com
```

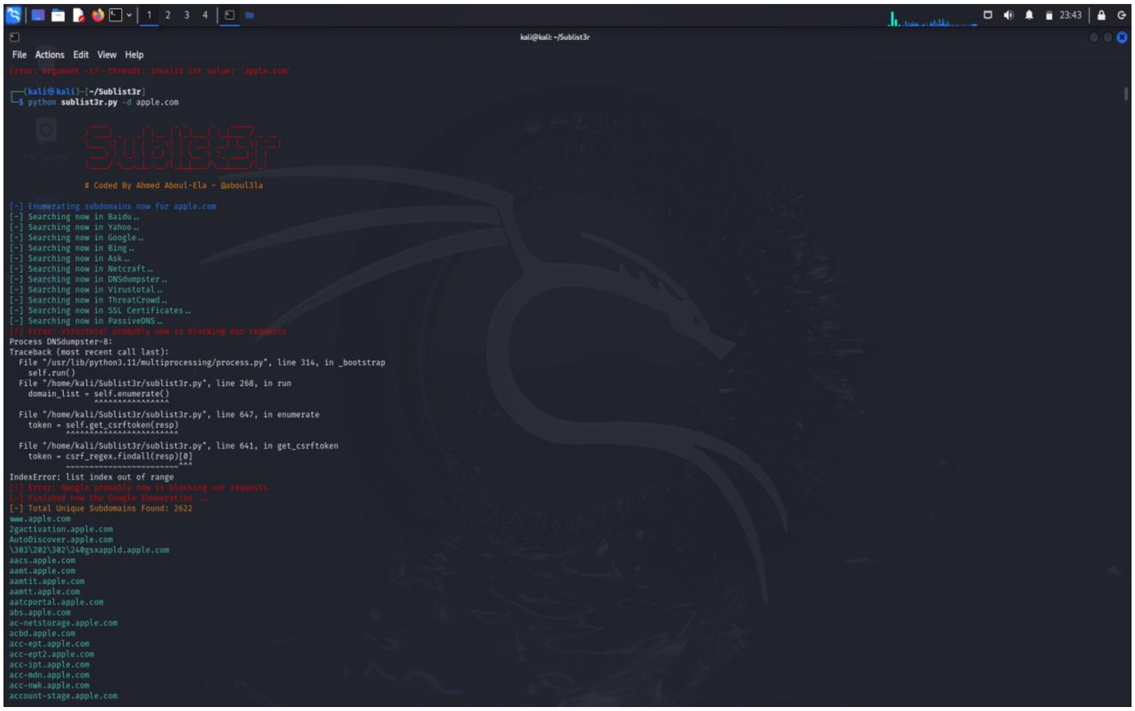


```
verifyall.apple.com
itntrvlt-ws2.apple.com
17-121-126-148.applebot.apple.com
17-121-125-186.applebot.apple.com
cup-store.apple.com
mdn-epsmtap-mkt-lsndr16101.apple.com
itunescom1.apple.com
asavpn.apple.com
17-121-118-23.applebot.apple.com
rnrtsa-prod.apple.com
inspections-mobile-new.apple.com
gsxut2a.apple.com
pv11p01sa-d06.siri.apple.com
maclearmater-prod-mdn.apple.com
wdg2-at.apple.com
17-121-121-62.applebot.apple.com
iei-uat2-us.apple.com
p71-buy.itunes.apple.com
pr-pod1-smp-internal-services.prz.apple.com
ttrsnwk.apple.com
17-58-102-11.applebot.apple.com
17-121-119-196.applebot.apple.com
plmpdfmdr.asia.apple.com
17-121-126-38.applebot.apple.com
17-121-125-121.applebot.apple.com
mdn-msbadger0107.apple.com
17-121-119-184.applebot.apple.com
iei-asia.apple.com
pv01sac80.siri.apple.com
gsx2dr-old.apple.com
jvs.apple.com
17-121-117-71.applebot.apple.com
17-121-122-233.applebot.apple.com
nwktxn-msbadger0203.apple.com
mdn-rover-ember02.apple.com
uss-expe1106.apple.com
ussjc1-client-vpn13.apple.com
vs5-2.apple.com
at-waldo.apple.com
conciergepod3.apple.com
ma1-cas10t-w01.tex.exch.apple.com
ma-albert-prod.apple.com
nserver4old.apple.com
px33.apple.com
tools.nc-storesupp.apple.com
verify-nc.apple.com
ctr2pf-p22-buy.itunes-bak.apple.com
17-121-125-126.applebot.apple.com
sbinstall-uat.apple.com
17-121-118-59.applebot.apple.com
svpn-u.euro.apple.com
coreostest120.apple.com
17-121-121-91.applebot.apple.com
17-121-124-51.applebot.apple.com
mdn-msbadger0106.apple.com
t2castro.apple.com

Job finished in 61 seconds.

Good luck Hax0r 💀 !
```

➢ Sublist3r

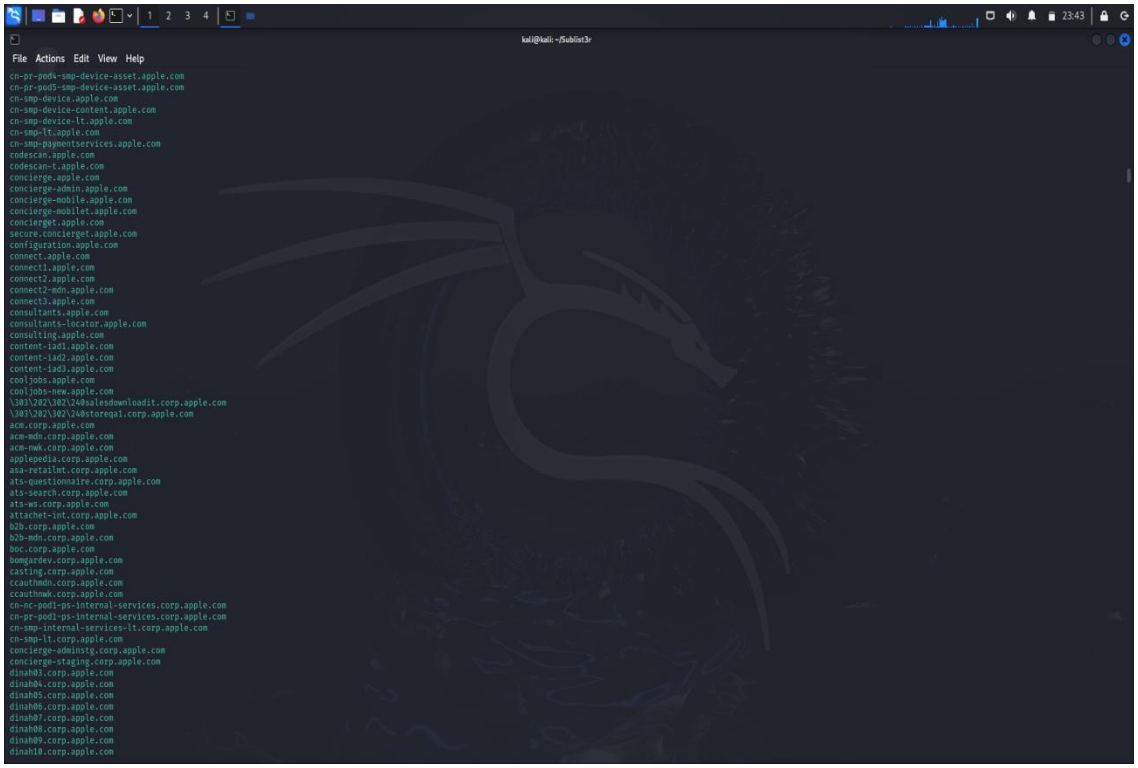
Purpose: Sublist3r tool helps to find the hidden sub domains

Pre-Requirement:Python

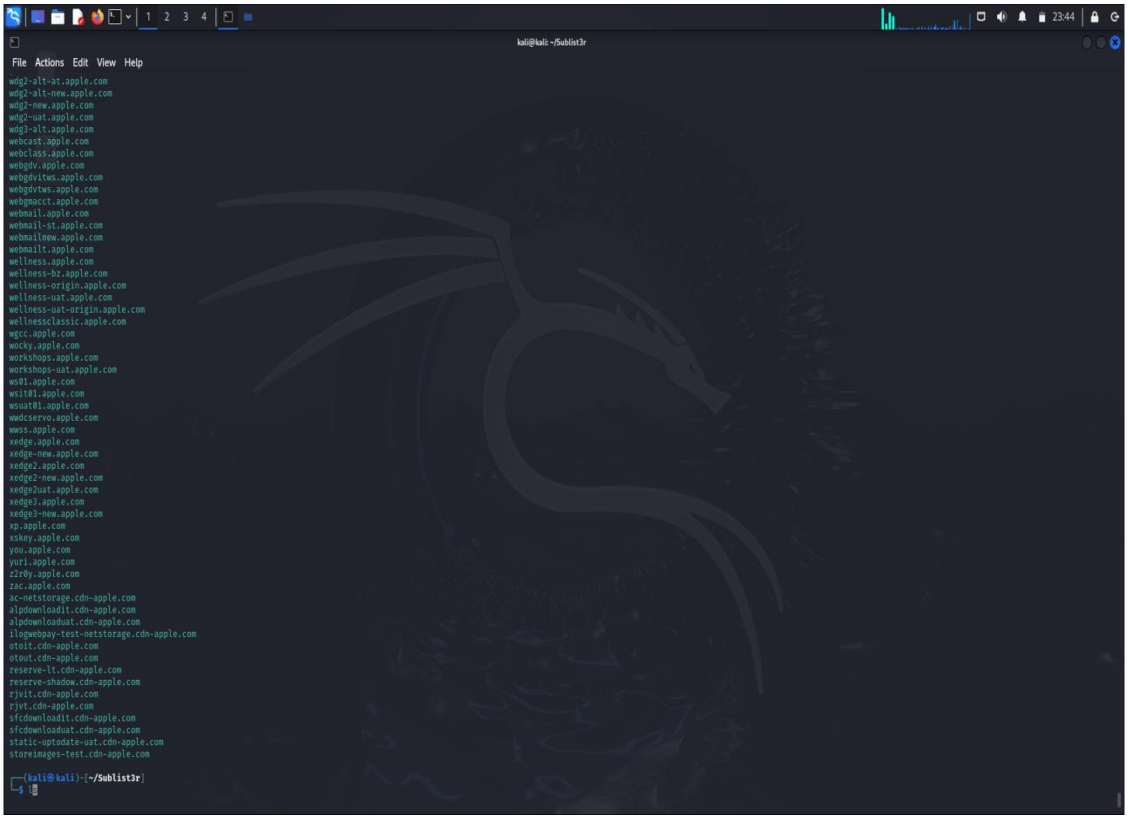


```
Error: argument -t/--threads: invalid int value: 'apple.com'

┌──(kali㉿kali)-[~/Sublist3r]
└─$ python sublist3r.py -d apple.com

                # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for apple.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
Process DNSdumpster-8:
Traceback (most recent call last):
  File "/usr/lib/python3.11/multiprocessing/process.py", line 314, in _bootstrap
    self.run()
  File "/home/kali/Sublist3r/sublist3r.py", line 268, in run
    domain_list = self.enumerate()
                  ^^^^^^^^^^^^^^^^

  File "/home/kali/Sublist3r/sublist3r.py", line 647, in enumerate
    token = self.get_csrftoken(resp)
            ^^^^^^^^^^^^^^^^^^^^^^^^

  File "/home/kali/Sublist3r/sublist3r.py", line 641, in get_csrftoken
    token = csrf_regex.findall(resp)[0]
            ~~~~~~~~~~~~~~~~~~~~~~~~^^^
IndexError: list index out of range
[!] Error: Google probably now is blocking our requests
[~] Finished now the Google Enumeration ...
[-] Total Unique Subdomains Found: 2622
www.apple.com
2gactivation.apple.com
AutoDiscover.apple.com
\303\202\302\240gsxappld.apple.com
aacs.apple.com
aamt.apple.com
aamtit.apple.com
aamtt.apple.com
aatcportal.apple.com
abs.apple.com
ac-netstorage.apple.com
acbd.apple.com
acc-ept.apple.com
acc-ept2.apple.com
acc-ipt.apple.com
acc-mdn.apple.com
acc-nwk.apple.com
account-stage.apple.com
```

<u>Command used</u>: Python sublist3r.py –d apple.com



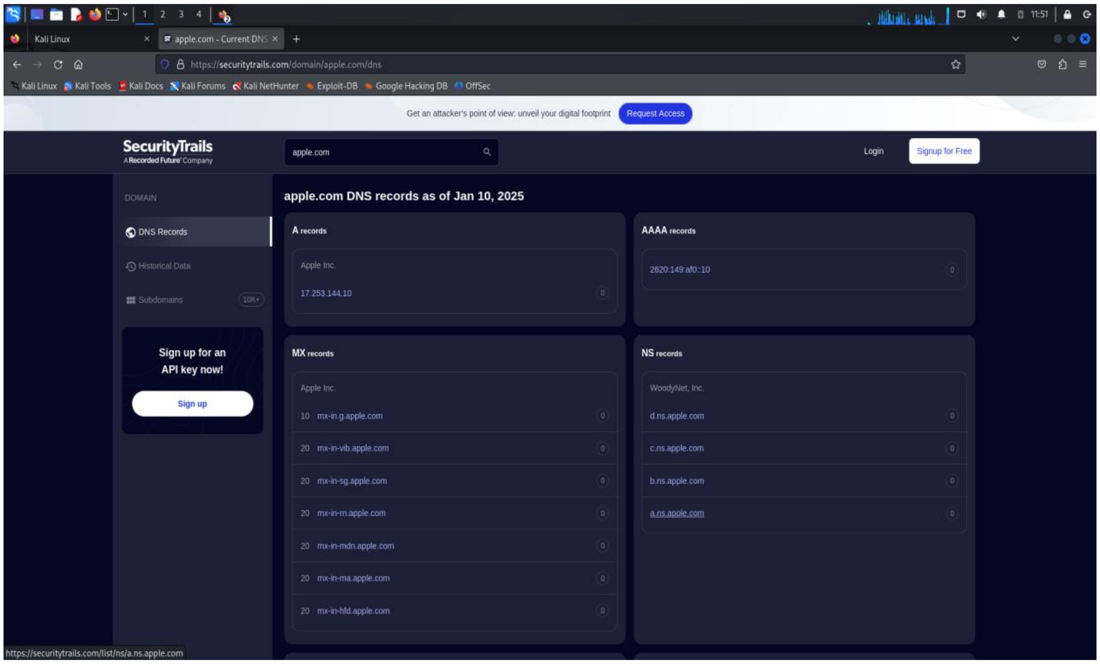
```
cn-pr-pod4-smp-device-asset.apple.com
cn-pr-pod5-smp-device-asset.apple.com
cn-smp-device.apple.com
cn-smp-device-content.apple.com
cn-smp-device-lt.apple.com
cn-smp-lt.apple.com
cn-smp-paymentservices.apple.com
codescan.apple.com
codescan-t.apple.com
concierge.apple.com
concierge-admin.apple.com
concierge-mobile.apple.com
concierge-mobilet.apple.com
concierget.apple.com
secure.concierget.apple.com
configuration.apple.com
connect.apple.com
connect1.apple.com
connect2.apple.com
connect2-mdn.apple.com
connect3.apple.com
consultants.apple.com
consultants-locator.apple.com
consulting.apple.com
content-iad1.apple.com
content-iad2.apple.com
content-iad3.apple.com
cooljobs.apple.com
cooljobs-new.apple.com
\303\202\302\240salesdownloadit.corp.apple.com
\303\202\302\240storeqa1.corp.apple.com
acm.corp.apple.com
acm-mdn.corp.apple.com
acm-nwk.corp.apple.com
applepedia.corp.apple.com
asa-retailmt.corp.apple.com
ats-questionnaire.corp.apple.com
ats-search.corp.apple.com
ats-ws.corp.apple.com
attachet-int.corp.apple.com
b2b.corp.apple.com
b2b-mdn.corp.apple.com
boc.corp.apple.com
bomgardev.corp.apple.com
casting.corp.apple.com
ccauthmdn.corp.apple.com
ccauthnwk.corp.apple.com
cn-nc-pod1-ps-internal-services.corp.apple.com
cn-pr-pod1-ps-internal-services.corp.apple.com
cn-smp-internal-services-lt.corp.apple.com
cn-smp-lt.corp.apple.com
concierge-adminstg.corp.apple.com
concierge-staging.corp.apple.com
dinah03.corp.apple.com
dinah04.corp.apple.com
dinah05.corp.apple.com
dinah06.corp.apple.com
dinah07.corp.apple.com
dinah08.corp.apple.com
dinah09.corp.apple.com
dinah10.corp.apple.com
```



```
wdg2-alt-at.apple.com
wdg2-alt-new.apple.com
wdg2-new.apple.com
wdg2-uat.apple.com
wdg3-alt.apple.com
webcast.apple.com
webclass.apple.com
webgdv.apple.com
webgdvitws.apple.com
webgdvtws.apple.com
webgmacct.apple.com
webmail.apple.com
webmail-st.apple.com
webmailnew.apple.com
webmailt.apple.com
wellness.apple.com
wellness-bz.apple.com
wellness-origin.apple.com
wellness-uat.apple.com
wellness-uat-origin.apple.com
wellnessclassic.apple.com
wgcc.apple.com
wocky.apple.com
workshops.apple.com
workshops-uat.apple.com
ws01.apple.com
wsit01.apple.com
wsuat01.apple.com
wwdcservo.apple.com
wwss.apple.com
xedge.apple.com
xedge-new.apple.com
xedge2.apple.com
xedge2-new.apple.com
xedge2uat.apple.com
xedge3.apple.com
xedge3-new.apple.com
xp.apple.com
xskey.apple.com
you.apple.com
yuri.apple.com
z2r0y.apple.com
zac.apple.com
ac-netstorage.cdn-apple.com
alpdownloadit.cdn-apple.com
alpdownloaduat.cdn-apple.com
ilogwebpay-test-netstorage.cdn-apple.com
otoit.cdn-apple.com
otout.cdn-apple.com
reserve-lt.cdn-apple.com
reserve-shadow.cdn-apple.com
rjvit.cdn-apple.com
rjvt.cdn-apple.com
sfcdownloadit.cdn-apple.com
sfcdownloaduat.cdn-apple.com
static-uptodate-uat.cdn-apple.com
storeimages-test.cdn-apple.com

┌──(kali㉿kali)-[~/Sublist3r]
└─$ ls
```

➢ Securitytrails.com

Purpose:Securitytrails.com is a online website will used for finding the subdomains


Kali Linux
apple.com - Current DNS
https://securitytrails.com/domain/apple.com/dns
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Get an attacker's point of view: unveil your digital footprint
Request Access
SecurityTrails
A Recorded Future Company
apple.com
Login
Signup for Free
DOMAIN
DNS Records
Historical Data
Subdomains 10K+
Sign up for an API key now!
Sign up
https://securitytrails.com/list/ns/a.ns.apple.com

apple.com DNS records as of Jan 10, 2025

A records

Apple Inc.
17.253.144.10 0

AAAA records

2620:149:af0::10 0

MX records

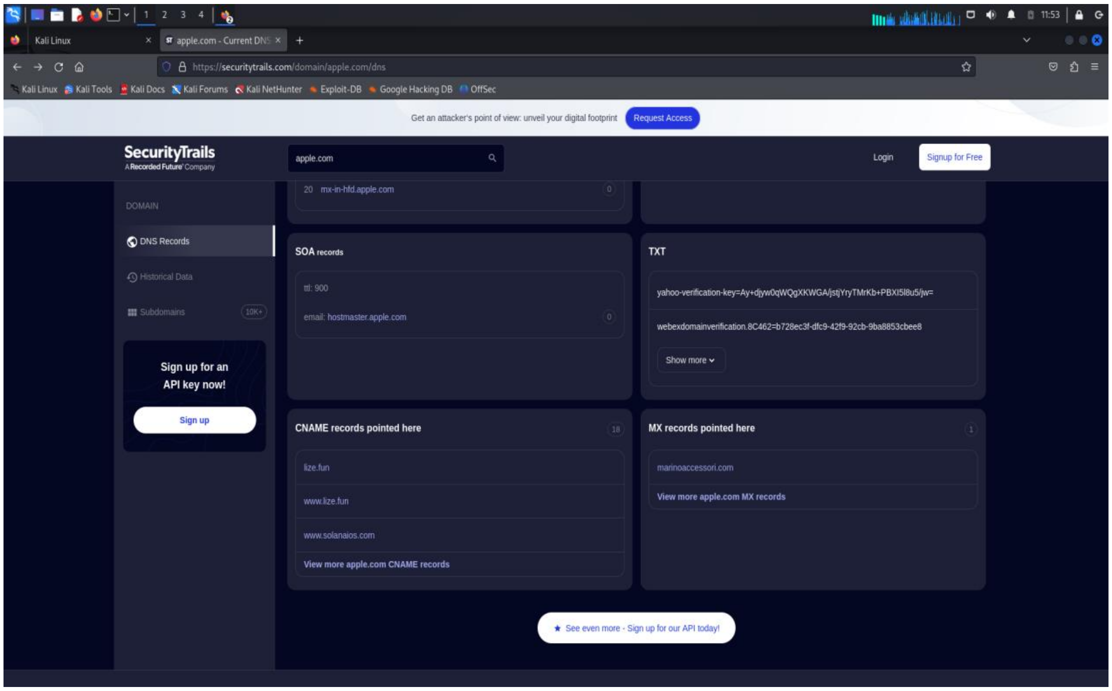
Apple Inc.

```
10  mx-in.g.apple.com      0
20  mx-in-vib.apple.com    0
20  mx-in-sg.apple.com     0
20  mx-in-rn.apple.com     0
20  mx-in-mdn.apple.com    0
20  mx-in-ma.apple.com     0
20  mx-in-hfd.apple.com    0
```

NS records

WoodyNet, Inc.

```
d.ns.apple.com  0
c.ns.apple.com  0
b.ns.apple.com  0
a.ns.apple.com  0
```


Kali Linux
apple.com - Current DNS
https://securitytrails.com/domain/apple.com/dns
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Get an attacker's point of view: unveil your digital footprint
Request Access
SecurityTrails
A Recorded Future Company
apple.com
Login
Signup for Free
DOMAIN
DNS Records
Historical Data
Subdomains 10K+
Sign up for an API key now!
Sign up

20 mx-in-hfd.apple.com 0

SOA records

ttl: 900
email: hostmaster.apple.com 0

TXT

```
yahoo-verification-key=Ay+djyw0qWQgXKWGA/jstjYryTMrKb+PBXI5l8u5/jw=
webexdomainverification.8C462=b728ec3f-dfc9-42f9-92cb-9ba8853cbee8
```

Show more

CNAME records pointed here 18

lize.fun
www.lize.fun
www.solanaios.com
View more apple.com CNAME records

MX records pointed here 1

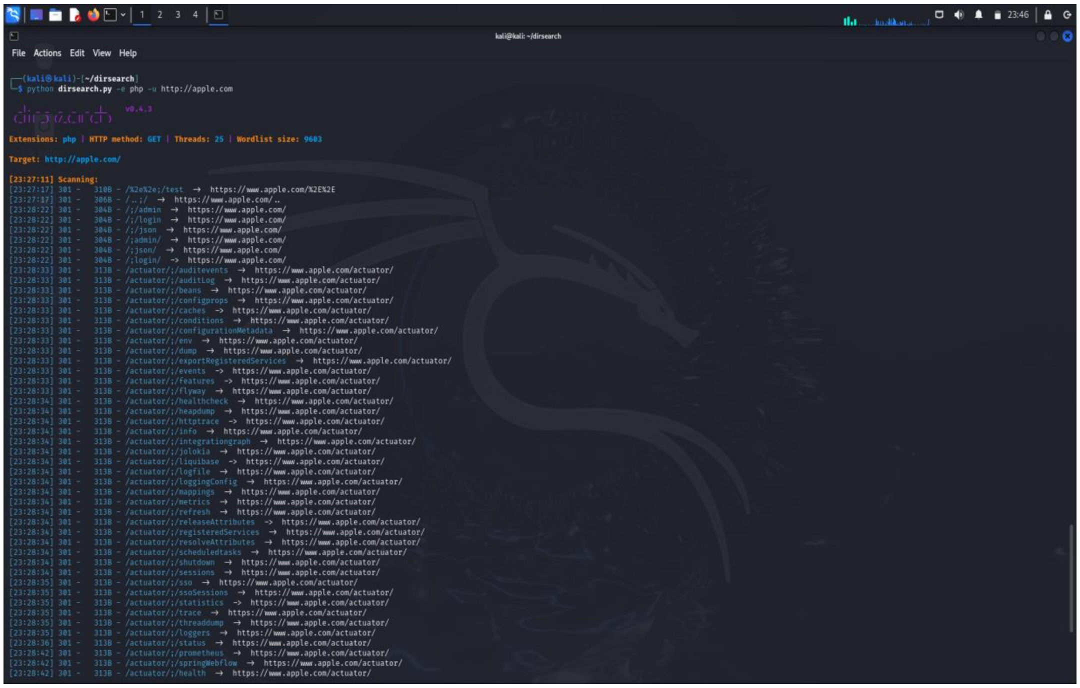
marinoaccessori.com
View more apple.com MX records

★ See even more - Sign up for our API today!

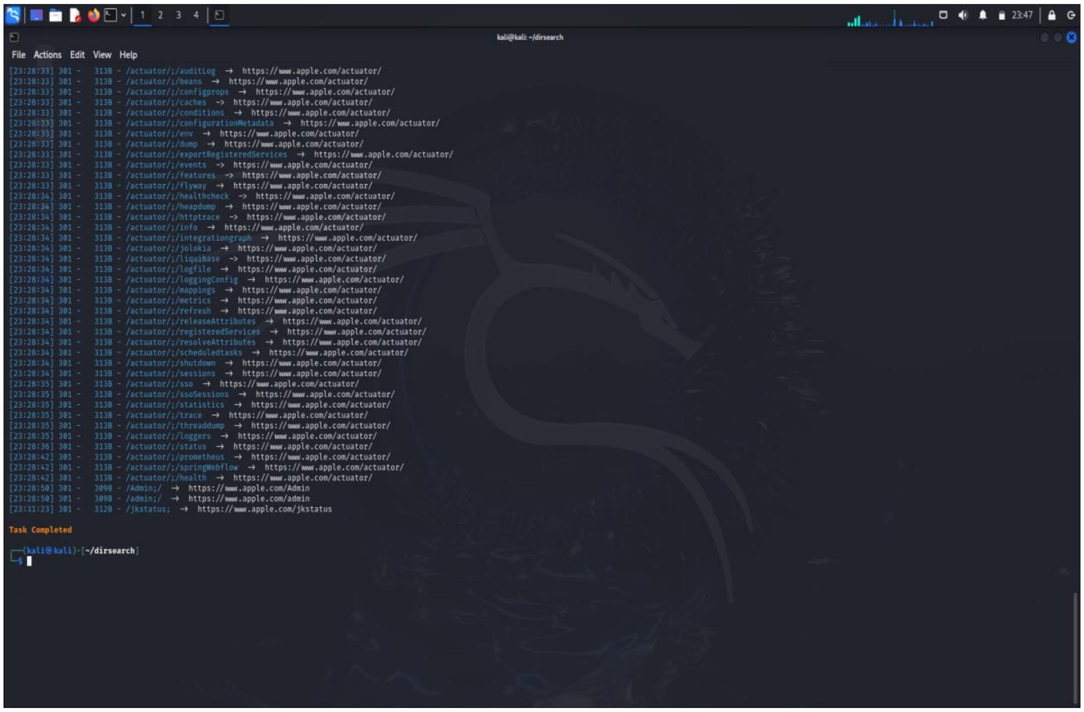
2.Directory & File Enumeration

➢ Dirsearch

Purpose:Dirsearch helps to find the hidden directories



```
┌──(kali㉿kali)-[~/dirsearch]
└─$ python dirsearch.py -e php -u http://apple.com

                        v0.4.3

Extensions: php | HTTP method: GET | Threads: 25 | Wordlist size: 9603

Target: http://apple.com/

[23:27:11] Scanning:
[23:27:17] 301 -   310B - /%2e%2e;/test  →  https://www.apple.com/%2E%2E
[23:27:17] 301 -   306B - /..;/  →  https://www.apple.com/..
[23:28:22] 301 -   304B - /;/admin  →  https://www.apple.com/
[23:28:22] 301 -   304B - /;/login  →  https://www.apple.com/
[23:28:22] 301 -   304B - /;/json  →  https://www.apple.com/
[23:28:22] 301 -   304B - /;admin/  →  https://www.apple.com/
[23:28:22] 301 -   304B - /;json/  →  https://www.apple.com/
[23:28:22] 301 -   304B - /;login/  ->  https://www.apple.com/
[23:28:33] 301 -   313B - /actuator/;/auditevents  →  https://www.apple.com/actuator/
[23:28:33] 301 -   313B - /actuator/;/auditLog  →  https://www.apple.com/actuator/
[23:28:33] 301 -   313B - /actuator/;/beans  →  https://www.apple.com/actuator/
[23:28:33] 301 -   313B - /actuator/;/configprops  →  https://www.apple.com/actuator/
[23:28:33] 301 -   313B - /actuator/;/caches  ->  https://www.apple.com/actuator/
[23:28:33] 301 -   313B - /actuator/;/conditions  →  https://www.apple.com/actuator/
[23:28:33] 301 -   313B - /actuator/;/configurationMetadata  →  https://www.apple.com/actuator/
[23:28:33] 301 -   313B - /actuator/;/env  →  https://www.apple.com/actuator/
[23:28:33] 301 -   313B - /actuator/;/dump  →  https://www.apple.com/actuator/
[23:28:33] 301 -   313B - /actuator/;/exportRegisteredServices  →  https://www.apple.com/actuator/
[23:28:33] 301 -   313B - /actuator/;/events  ->  https://www.apple.com/actuator/
[23:28:33] 301 -   313B - /actuator/;/features  ->  https://www.apple.com/actuator/
[23:28:33] 301 -   313B - /actuator/;/flyway  →  https://www.apple.com/actuator/
[23:28:34] 301 -   313B - /actuator/;/healthcheck  →  https://www.apple.com/actuator/
[23:28:34] 301 -   313B - /actuator/;/heapdump  →  https://www.apple.com/actuator/
[23:28:34] 301 -   313B - /actuator/;/httptrace  ->  https://www.apple.com/actuator/
[23:28:34] 301 -   313B - /actuator/;/info  →  https://www.apple.com/actuator/
[23:28:34] 301 -   313B - /actuator/;/integrationgraph  →  https://www.apple.com/actuator/
[23:28:34] 301 -   313B - /actuator/;/jolokia  →  https://www.apple.com/actuator/
[23:28:34] 301 -   313B - /actuator/;/liquibase  ->  https://www.apple.com/actuator/
[23:28:34] 301 -   313B - /actuator/;/logfile  →  https://www.apple.com/actuator/
[23:28:34] 301 -   313B - /actuator/;/loggingConfig  →  https://www.apple.com/actuator/
[23:28:34] 301 -   313B - /actuator/;/mappings  →  https://www.apple.com/actuator/
[23:28:34] 301 -   313B - /actuator/;/metrics  →  https://www.apple.com/actuator/
[23:28:34] 301 -   313B - /actuator/;/refresh  →  https://www.apple.com/actuator/
[23:28:34] 301 -   313B - /actuator/;/releaseAttributes  ->  https://www.apple.com/actuator/
[23:28:34] 301 -   313B - /actuator/;/registeredServices  →  https://www.apple.com/actuator/
[23:28:34] 301 -   313B - /actuator/;/resolveAttributes  →  https://www.apple.com/actuator/
[23:28:34] 301 -   313B - /actuator/;/scheduledtasks  →  https://www.apple.com/actuator/
[23:28:34] 301 -   313B - /actuator/;/shutdown  →  https://www.apple.com/actuator/
[23:28:34] 301 -   313B - /actuator/;/sessions  →  https://www.apple.com/actuator/
[23:28:35] 301 -   313B - /actuator/;/sso  →  https://www.apple.com/actuator/
[23:28:35] 301 -   313B - /actuator/;/ssoSessions  →  https://www.apple.com/actuator/
[23:28:35] 301 -   313B - /actuator/;/statistics  ->  https://www.apple.com/actuator/
[23:28:35] 301 -   313B - /actuator/;/trace  →  https://www.apple.com/actuator/
[23:28:35] 301 -   313B - /actuator/;/threaddump  →  https://www.apple.com/actuator/
[23:28:35] 301 -   313B - /actuator/;/loggers  →  https://www.apple.com/actuator/
[23:28:36] 301 -   313B - /actuator/;/status  →  https://www.apple.com/actuator/
[23:28:42] 301 -   313B - /actuator/;/prometheus  →  https://www.apple.com/actuator/
[23:28:42] 301 -   313B - /actuator/;/springWebflow  →  https://www.apple.com/actuator/
[23:28:42] 301 -   313B - /actuator/;/health  →  https://www.apple.com/actuator/
```

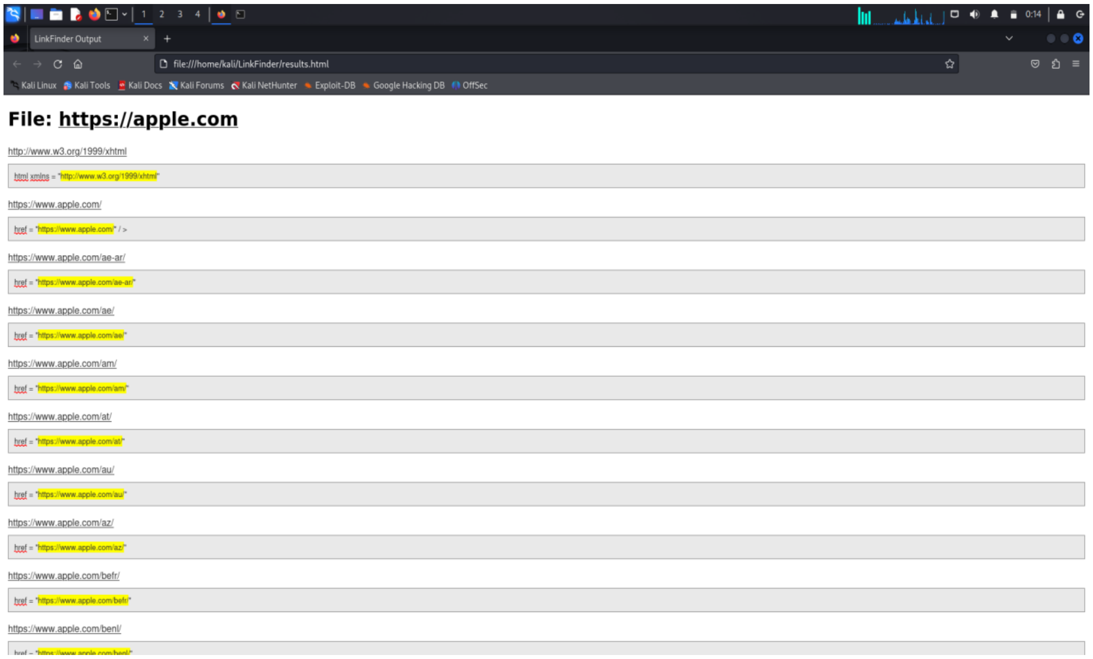


```
[23:28:33] 301 -   313B - /actuator/;/auditLog  →  https://www.apple.com/actuator/
[23:28:33] 301 -   313B - /actuator/;/beans  →  https://www.apple.com/actuator/
[23:28:33] 301 -   313B - /actuator/;/configprops  →  https://www.apple.com/actuator/
[23:28:33] 301 -   313B - /actuator/;/caches  ->  https://www.apple.com/actuator/
[23:28:33] 301 -   313B - /actuator/;/conditions  →  https://www.apple.com/actuator/
[23:28:33] 301 -   313B - /actuator/;/configurationMetadata  →  https://www.apple.com/actuator/
[23:28:33] 301 -   313B - /actuator/;/env  →  https://www.apple.com/actuator/
[23:28:33] 301 -   313B - /actuator/;/dump  →  https://www.apple.com/actuator/
[23:28:33] 301 -   313B - /actuator/;/exportRegisteredServices  →  https://www.apple.com/actuator/
[23:28:33] 301 -   313B - /actuator/;/events  ->  https://www.apple.com/actuator/
[23:28:33] 301 -   313B - /actuator/;/features  ->  https://www.apple.com/actuator/
[23:28:33] 301 -   313B - /actuator/;/flyway  →  https://www.apple.com/actuator/
[23:28:34] 301 -   313B - /actuator/;/healthcheck  ->  https://www.apple.com/actuator/
[23:28:34] 301 -   313B - /actuator/;/heapdump  →  https://www.apple.com/actuator/
[23:28:34] 301 -   313B - /actuator/;/httptrace  ->  https://www.apple.com/actuator/
[23:28:34] 301 -   313B - /actuator/;/info  →  https://www.apple.com/actuator/
[23:28:34] 301 -   313B - /actuator/;/integrationgraph  →  https://www.apple.com/actuator/
[23:28:34] 301 -   313B - /actuator/;/jolokia  →  https://www.apple.com/actuator/
[23:28:34] 301 -   313B - /actuator/;/liquibase  ->  https://www.apple.com/actuator/
[23:28:34] 301 -   313B - /actuator/;/logfile  →  https://www.apple.com/actuator/
[23:28:34] 301 -   313B - /actuator/;/loggingConfig  →  https://www.apple.com/actuator/
[23:28:34] 301 -   313B - /actuator/;/mappings  →  https://www.apple.com/actuator/
[23:28:34] 301 -   313B - /actuator/;/metrics  →  https://www.apple.com/actuator/
[23:28:34] 301 -   313B - /actuator/;/refresh  →  https://www.apple.com/actuator/
[23:28:34] 301 -   313B - /actuator/;/releaseAttributes  →  https://www.apple.com/actuator/
[23:28:34] 301 -   313B - /actuator/;/registeredServices  →  https://www.apple.com/actuator/
[23:28:34] 301 -   313B - /actuator/;/resolveAttributes  →  https://www.apple.com/actuator/
[23:28:34] 301 -   313B - /actuator/;/scheduledtasks  →  https://www.apple.com/actuator/
[23:28:34] 301 -   313B - /actuator/;/shutdown  →  https://www.apple.com/actuator/
[23:28:34] 301 -   313B - /actuator/;/sessions  →  https://www.apple.com/actuator/
[23:28:35] 301 -   313B - /actuator/;/sso  →  https://www.apple.com/actuator/
[23:28:35] 301 -   313B - /actuator/;/ssoSessions  →  https://www.apple.com/actuator/
[23:28:35] 301 -   313B - /actuator/;/statistics  →  https://www.apple.com/actuator/
[23:28:35] 301 -   313B - /actuator/;/trace  →  https://www.apple.com/actuator/
[23:28:35] 301 -   313B - /actuator/;/threaddump  →  https://www.apple.com/actuator/
[23:28:35] 301 -   313B - /actuator/;/loggers  →  https://www.apple.com/actuator/
[23:28:36] 301 -   313B - /actuator/;/status  →  https://www.apple.com/actuator/
[23:28:42] 301 -   313B - /actuator/;/prometheus  →  https://www.apple.com/actuator/
[23:28:42] 301 -   313B - /actuator/;/springWebflow  →  https://www.apple.com/actuator/
[23:28:42] 301 -   313B - /actuator/;/health  →  https://www.apple.com/actuator/
[23:28:50] 301 -   309B - /Admin;/  →  https://www.apple.com/Admin
[23:28:50] 301 -   309B - /admin;/  →  https://www.apple.com/admin
[23:31:23] 301 -   312B - /jkstatus;  →  https://www.apple.com/jkstatus

Task Completed

┌──(kali㉿kali)-[~/dirsearch]
└─$ █
```

3.Analyzing JavaScript Files

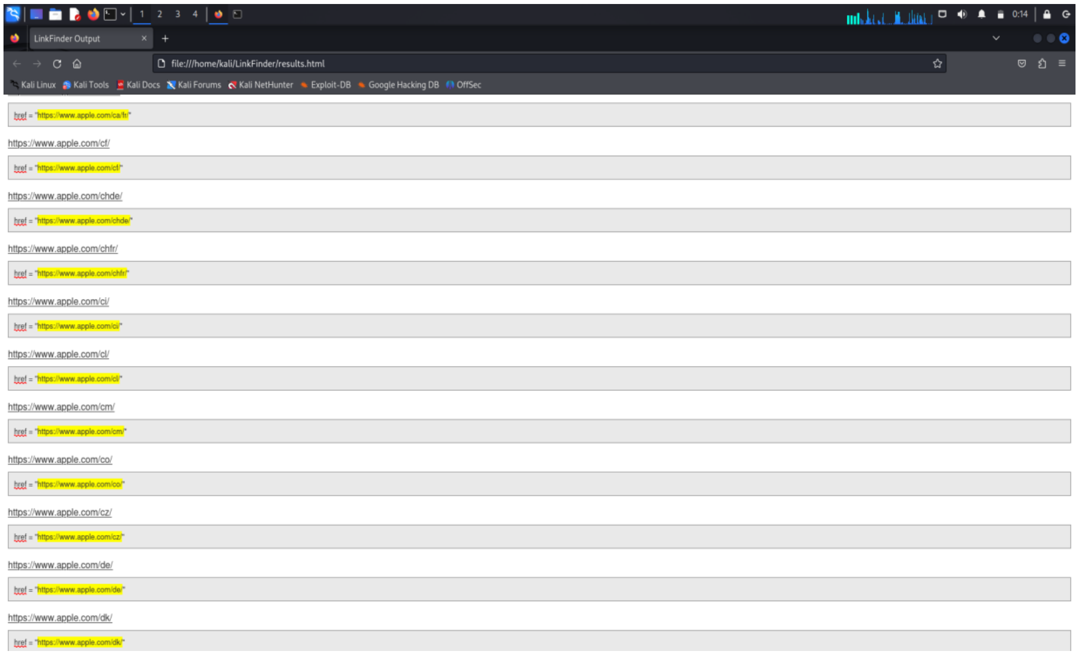
➢ LinkFinder

Purpose:LinkFinder is helps to extracts endpoints from the Javascript file

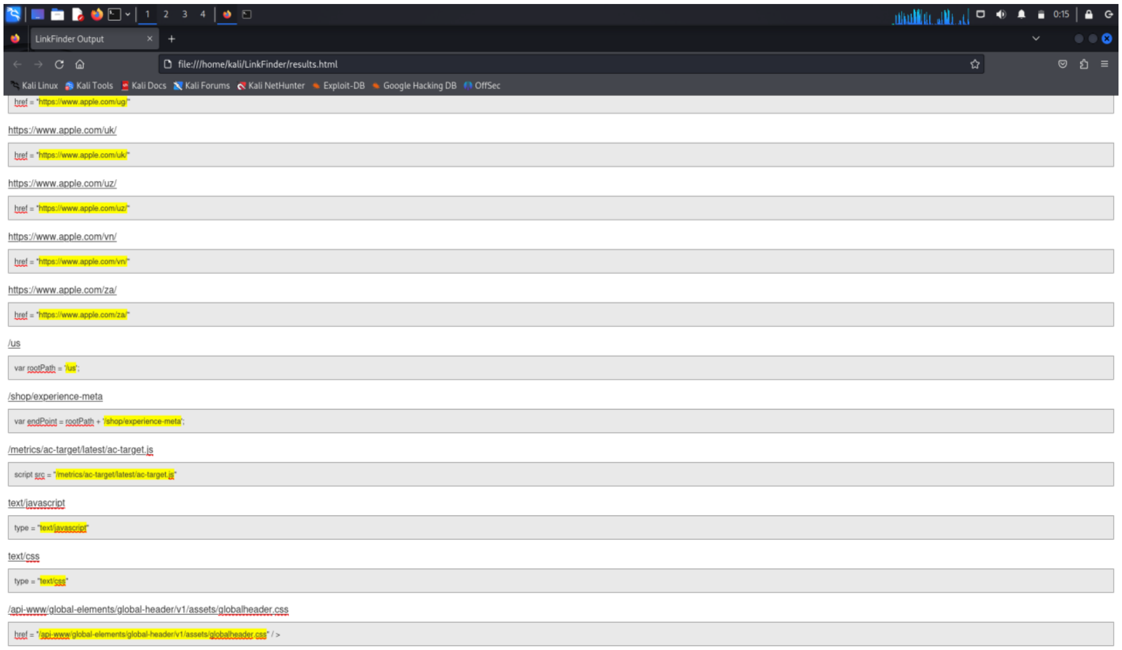


File: https://apple.com

```
http://www.w3.org/1999/xhtml
html xmlns = "http://www.w3.org/1999/xhtml"
https://www.apple.com/
href = "https://www.apple.com/" / >
https://www.apple.com/ae-ar/
href = "https://www.apple.com/ae-ar/"
https://www.apple.com/ae/
href = "https://www.apple.com/ae/"
https://www.apple.com/am/
href = "https://www.apple.com/am/"
https://www.apple.com/at/
href = "https://www.apple.com/at/"
https://www.apple.com/au/
href = "https://www.apple.com/au/"
https://www.apple.com/az/
href = "https://www.apple.com/az/"
https://www.apple.com/befr/
href = "https://www.apple.com/befr/"
https://www.apple.com/benl/
href = "https://www.apple.com/benl/"
```



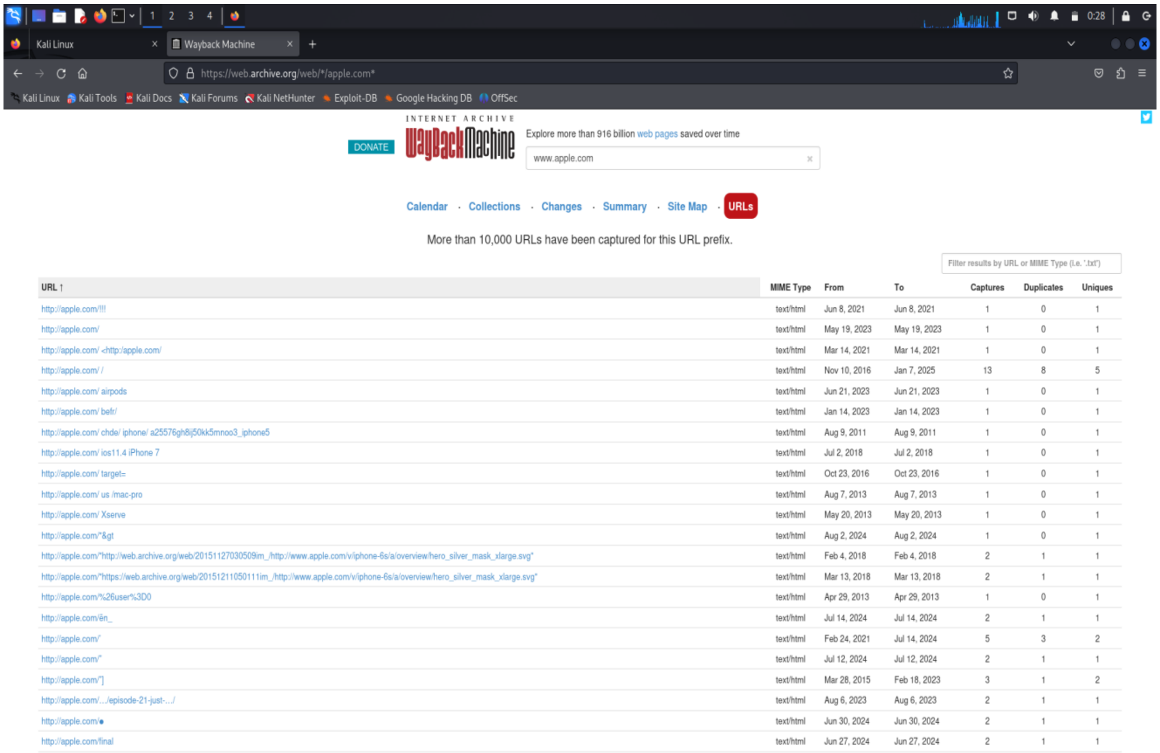
```
href = "https://www.apple.com/ca/fr/"
https://www.apple.com/cf/
href = "https://www.apple.com/cf/"
https://www.apple.com/chde/
href = "https://www.apple.com/chde/"
https://www.apple.com/chfr/
href = "https://www.apple.com/chfr/"
https://www.apple.com/ci/
href = "https://www.apple.com/ci/"
https://www.apple.com/cl/
href = "https://www.apple.com/cl/"
https://www.apple.com/cm/
href = "https://www.apple.com/cm/"
https://www.apple.com/co/
href = "https://www.apple.com/co/"
https://www.apple.com/cz/
href = "https://www.apple.com/cz/"
https://www.apple.com/de/
href = "https://www.apple.com/de/"
https://www.apple.com/dk/
href = "https://www.apple.com/dk/"
```



```
href = "https://www.apple.com/ug/"

https://www.apple.com/uk/
href = "https://www.apple.com/uk/"

https://www.apple.com/uz/
href = "https://www.apple.com/uz/"

https://www.apple.com/vn/
href = "https://www.apple.com/vn/"

https://www.apple.com/za/
href = "https://www.apple.com/za/"

/us
var rootPath = '/us';

/shop/experience-meta
var endPoint = rootPath + '/shop/experience-meta';

/metrics/ac-target/latest/ac-target.js
script src = "/metrics/ac-target/latest/ac-target.js"

text/javascript
type = "text/javascript"

text/css
type = "text/css"

/api-www/global-elements/global-header/v1/assets/globalheader.css
href = "/api-www/global-elements/global-header/v1/assets/globalheader.css" / >
```

➢ Waybackurls

Purpose: This helps to Fetches historical URLs from archive services



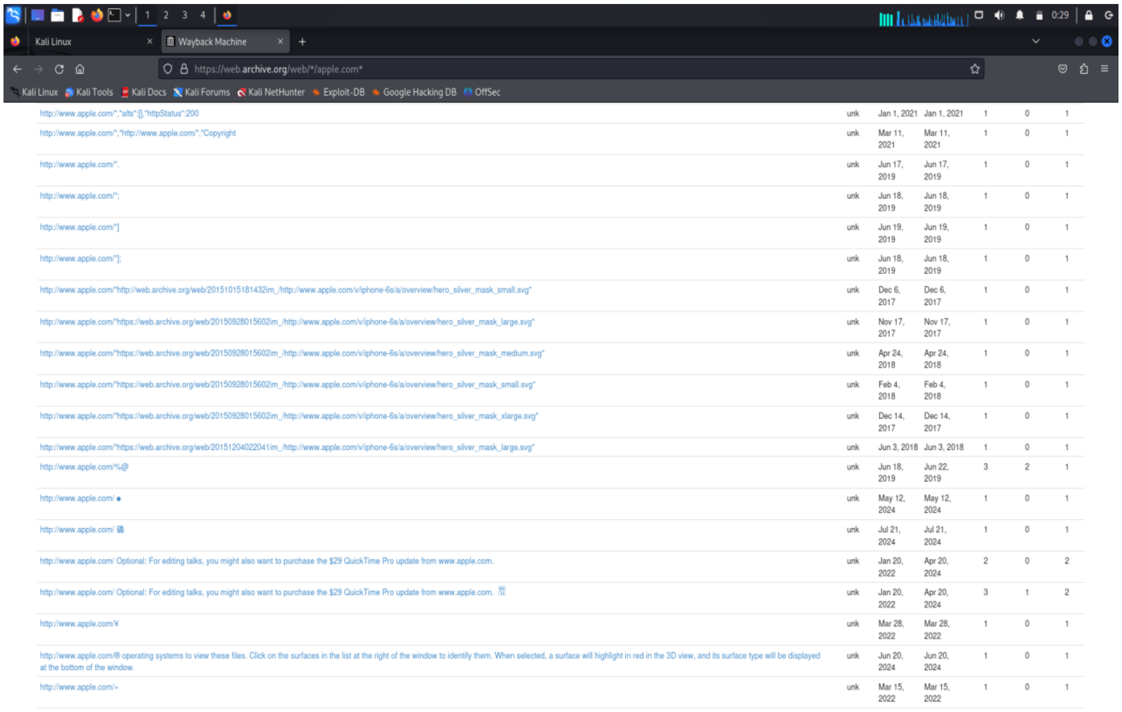
Explore more than 916 billion web pages saved over time

www.apple.com

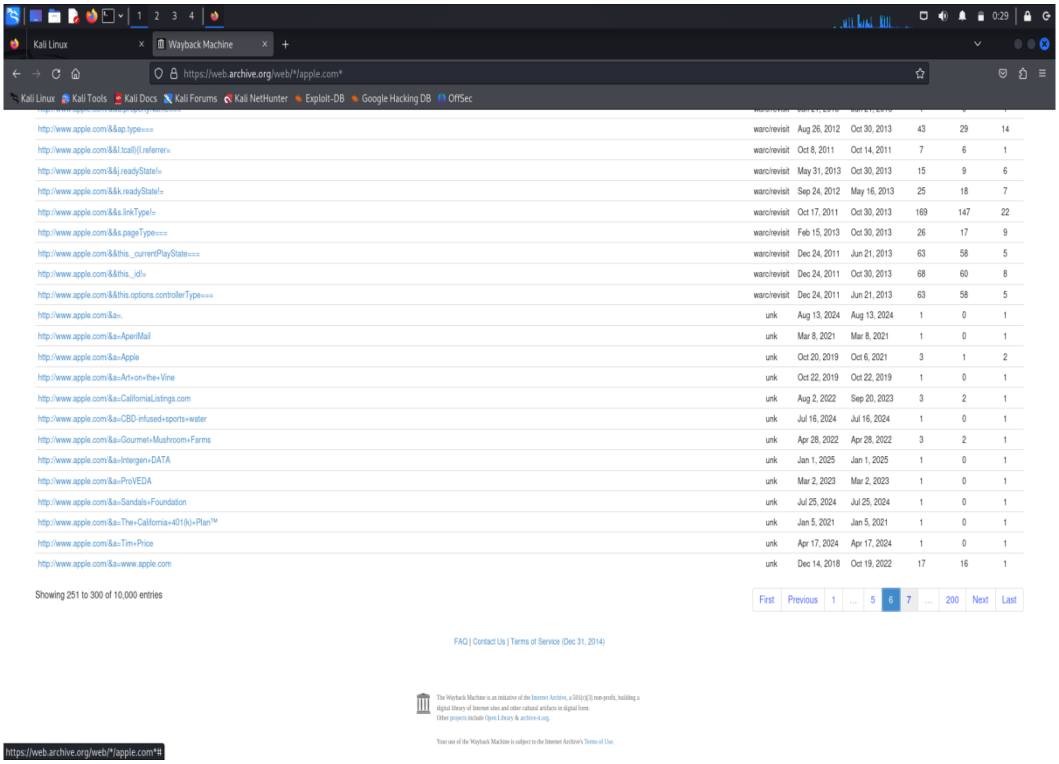
More than 10,000 URLs have been captured for this URL prefix.

Filter results by URL or MIME Type (i.e. '.txt')

URL ↑	MIME Type	From	To	Captures	Duplicates	Uniques
http://apple.com/!!!	text/html	Jun 8, 2021	Jun 8, 2021	1	0	1
http://apple.com/	text/html	May 19, 2023	May 19, 2023	1	0	1
http://apple.com/ <http:/apple.com/	text/html	Mar 14, 2021	Mar 14, 2021	1	0	1
http://apple.com/ /	text/html	Nov 10, 2016	Jan 7, 2025	13	8	5
http://apple.com/ airpods	text/html	Jun 21, 2023	Jun 21, 2023	1	0	1
http://apple.com/ befr/	text/html	Jan 14, 2023	Jan 14, 2023	1	0	1
http://apple.com/ chde/ iphone/ a25576gh8ij50kk5mnoo3_iphone5	text/html	Aug 9, 2011	Aug 9, 2011	1	0	1
http://apple.com/ ios11.4 iPhone 7	text/html	Jul 2, 2018	Jul 2, 2018	1	0	1
http://apple.com/ target=	text/html	Oct 23, 2016	Oct 23, 2016	1	0	1
http://apple.com/ us /mac-pro	text/html	Aug 7, 2013	Aug 7, 2013	1	0	1
http://apple.com/ Xserve	text/html	May 20, 2013	May 20, 2013	1	0	1
http://apple.com/"&gt	text/html	Aug 2, 2024	Aug 2, 2024	1	0	1
http://apple.com/"http://web.archive.org/web/20151127030509im_/http://www.apple.com/v/iphone-6s/a/overview/hero_silver_mask_xlarge.svg"	text/html	Feb 4, 2018	Feb 4, 2018	2	1	1
http://apple.com/"https://web.archive.org/web/20151211050111im_/http://www.apple.com/v/iphone-6s/a/overview/hero_silver_mask_xlarge.svg"	text/html	Mar 13, 2018	Mar 13, 2018	2	1	1
http://apple.com/%26user%3D0	text/html	Apr 29, 2013	Apr 29, 2013	1	0	1
http://apple.com/ĕn_	text/html	Jul 14, 2024	Jul 14, 2024	2	1	1
http://apple.com/'	text/html	Feb 24, 2021	Jul 14, 2024	5	3	2
http://apple.com/"	text/html	Jul 12, 2024	Jul 12, 2024	2	1	1
http://apple.com/"]	text/html	Mar 28, 2015	Feb 18, 2023	3	1	2
http://apple.com/…/episode-21-just-…/	text/html	Aug 6, 2023	Aug 6, 2023	2	1	1
http://apple.com/●	text/html	Jun 30, 2024	Jun 30, 2024	2	1	1
http://apple.com/final	text/html	Jun 27, 2024	Jun 27, 2024	2	1	1



http://www.apple.com/","alts":[],"httpStatus":200	unk	Jan 1, 2021	Jan 1, 2021	1	0	1
http://www.apple.com/","http://www.apple.com/","Copyright	unk	Mar 11, 2021	Mar 11, 2021	1	0	1
http://www.apple.com/".	unk	Jun 17, 2019	Jun 17, 2019	1	0	1
http://www.apple.com/";	unk	Jun 18, 2019	Jun 18, 2019	1	0	1
http://www.apple.com/"]	unk	Jun 19, 2019	Jun 19, 2019	1	0	1
http://www.apple.com/"];	unk	Jun 18, 2019	Jun 18, 2019	1	0	1
http://www.apple.com/"http://web.archive.org/web/20151015181432im_/http://www.apple.com/v/iphone-6s/a/overview/hero_silver_mask_small.svg"	unk	Dec 6, 2017	Dec 6, 2017	1	0	1
http://www.apple.com/"https://web.archive.org/web/20150928015602im_/http://www.apple.com/v/iphone-6s/a/overview/hero_silver_mask_large.svg"	unk	Nov 17, 2017	Nov 17, 2017	1	0	1
http://www.apple.com/"https://web.archive.org/web/20150928015602im_/http://www.apple.com/v/iphone-6s/a/overview/hero_silver_mask_medium.svg"	unk	Apr 24, 2018	Apr 24, 2018	1	0	1
http://www.apple.com/"https://web.archive.org/web/20150928015602im_/http://www.apple.com/v/iphone-6s/a/overview/hero_silver_mask_small.svg"	unk	Feb 4, 2018	Feb 4, 2018	1	0	1
http://www.apple.com/"https://web.archive.org/web/20150928015602im_/http://www.apple.com/v/iphone-6s/a/overview/hero_silver_mask_xlarge.svg"	unk	Dec 14, 2017	Dec 14, 2017	1	0	1
http://www.apple.com/"https://web.archive.org/web/20151204022041im_/http://www.apple.com/v/iphone-6s/a/overview/hero_silver_mask_large.svg"	unk	Jun 3, 2018	Jun 3, 2018	1	0	1
http://www.apple.com/%@	unk	Jun 18, 2019	Jun 22, 2019	3	2	1
http://www.apple.com/ ●	unk	May 12, 2024	May 12, 2024	1	0	1
http://www.apple.com/ 确	unk	Jul 21, 2024	Jul 21, 2024	1	0	1
http://www.apple.com/ Optional: For editing talks, you might also want to purchase the $29 QuickTime Pro update from www.apple.com.	unk	Jan 20, 2022	Apr 20, 2024	2	0	2
http://www.apple.com/ Optional: For editing talks, you might also want to purchase the $29 QuickTime Pro update from www.apple.com. ⍰	unk	Jan 20, 2022	Apr 20, 2024	3	1	2
http://www.apple.com/¥	unk	Mar 28, 2022	Mar 28, 2022	1	0	1
http://www.apple.com/® operating systems to view these files. Click on the surfaces in the list at the right of the window to identify them. When selected, a surface will highlight in red in the 3D view, and its surface type will be displayed at the bottom of the window.	unk	Jun 20, 2024	Jun 20, 2024	1	0	1
http://www.apple.com/»	unk	Mar 15, 2022	Mar 15, 2022	1	0	1



http://www.apple.com/&&ap.type===	warc/revisit	Aug 26, 2012	Oct 30, 2013	43	29	14
http://www.apple.com/&&l.tcall)(l.referrer=	warc/revisit	Oct 8, 2011	Oct 14, 2011	7	6	1
http://www.apple.com/&&j.readyState!=	warc/revisit	May 31, 2013	Oct 30, 2013	15	9	6
http://www.apple.com/&&k.readyState!=	warc/revisit	Sep 24, 2012	May 16, 2013	25	18	7
http://www.apple.com/&&s.linkType!=	warc/revisit	Oct 17, 2011	Oct 30, 2013	169	147	22
http://www.apple.com/&&s.pageType===	warc/revisit	Feb 15, 2013	Oct 30, 2013	26	17	9
http://www.apple.com/&&this._currentPlayState===	warc/revisit	Dec 24, 2011	Jun 21, 2013	63	58	5
http://www.apple.com/&&this._id!=	warc/revisit	Dec 24, 2011	Oct 30, 2013	68	60	8
http://www.apple.com/&&this.options.controllerType===	warc/revisit	Dec 24, 2011	Jun 21, 2013	63	58	5
http://www.apple.com/&a=.	unk	Aug 13, 2024	Aug 13, 2024	1	0	1
http://www.apple.com/&a=AperiMail	unk	Mar 8, 2021	Mar 8, 2021	1	0	1
http://www.apple.com/&a=Apple	unk	Oct 20, 2019	Oct 6, 2021	3	1	2
http://www.apple.com/&a=Art+on+the+Vine	unk	Oct 22, 2019	Oct 22, 2019	1	0	1
http://www.apple.com/&a=CaliforniaListings.com	unk	Aug 2, 2022	Sep 20, 2023	3	2	1
http://www.apple.com/&a=CBD-infused+sports+water	unk	Jul 16, 2024	Jul 16, 2024	1	0	1
http://www.apple.com/&a=Gourmet+Mushroom+Farms	unk	Apr 28, 2022	Apr 28, 2022	3	2	1
http://www.apple.com/&a=Intergen+DATA	unk	Jan 1, 2025	Jan 1, 2025	1	0	1
http://www.apple.com/&a=ProVEDA	unk	Mar 2, 2023	Mar 2, 2023	1	0	1
http://www.apple.com/&a=Sandals+Foundation	unk	Jul 25, 2024	Jul 25, 2024	1	0	1
http://www.apple.com/&a=The+California+401(k)+Plan™	unk	Jan 5, 2021	Jan 5, 2021	1	0	1
http://www.apple.com/&a=Tim+Price	unk	Apr 17, 2024	Apr 17, 2024	1	0	1
http://www.apple.com/&a=www.apple.com	unk	Dec 14, 2018	Oct 19, 2022	17	16	1

Showing 251 to 300 of 10,000 entries

FAQ | Contact Us | Terms of Service (Dec 31, 2014)

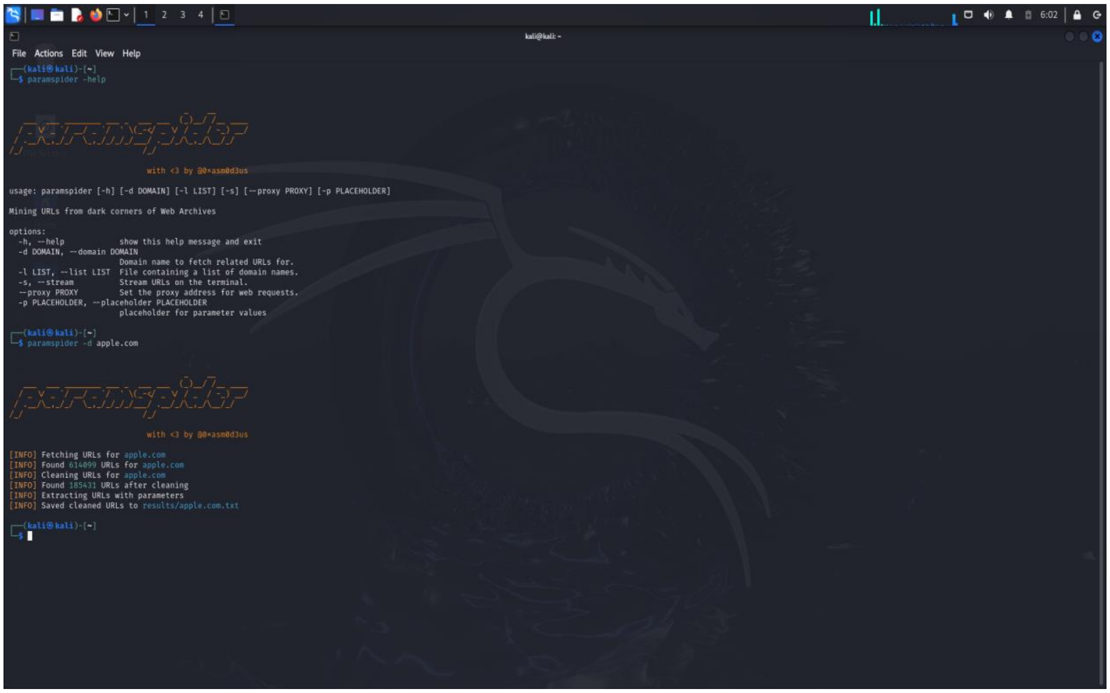
The Wayback Machine is an initiative of the Internet Archive, a 501(c)(3) non-profit, building a digital library of Internet sites and other cultural artifacts in digital form.
Other projects include Open Library & archive-it.org.

Your use of the Wayback Machine is subject to the Internet Archive's Terms of Use.

https://web.archive.org/web/*/apple.com*#

➢ ParamSpider

Purpose:This helps to find the URL parameters

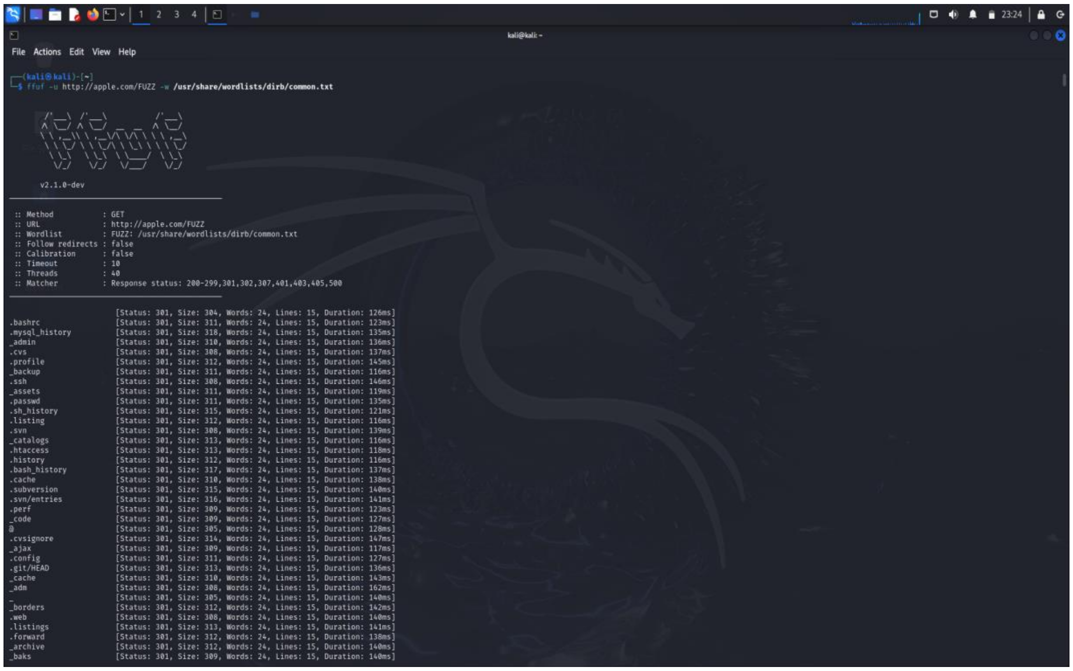


```
┌──(kali㉿kali)-[~]
└─$ paramspider -help

                     with <3 by @0×asm0d3us

usage: paramspider [-h] [-d DOMAIN] [-l LIST] [-s] [--proxy PROXY] [-p PLACEHOLDER]

Mining URLs from dark corners of Web Archives

options:
  -h, --help            show this help message and exit
  -d DOMAIN, --domain DOMAIN
                        Domain name to fetch related URLs for.
  -l LIST, --list LIST  File containing a list of domain names.
  -s, --stream          Stream URLs on the terminal.
  --proxy PROXY         Set the proxy address for web requests.
  -p PLACEHOLDER, --placeholder PLACEHOLDER
                        placeholder for parameter values

┌──(kali㉿kali)-[~]
└─$ paramspider -d apple.com

                     with <3 by @0×asm0d3us

[INFO] Fetching URLs for apple.com
[INFO] Found 614099 URLs for apple.com
[INFO] Cleaning URLs for apple.com
[INFO] Found 185431 URLs after cleaning
[INFO] Extracting URLs with parameters
[INFO] Saved cleaned URLs to results/apple.com.txt

┌──(kali㉿kali)-[~]
└─$ 
```

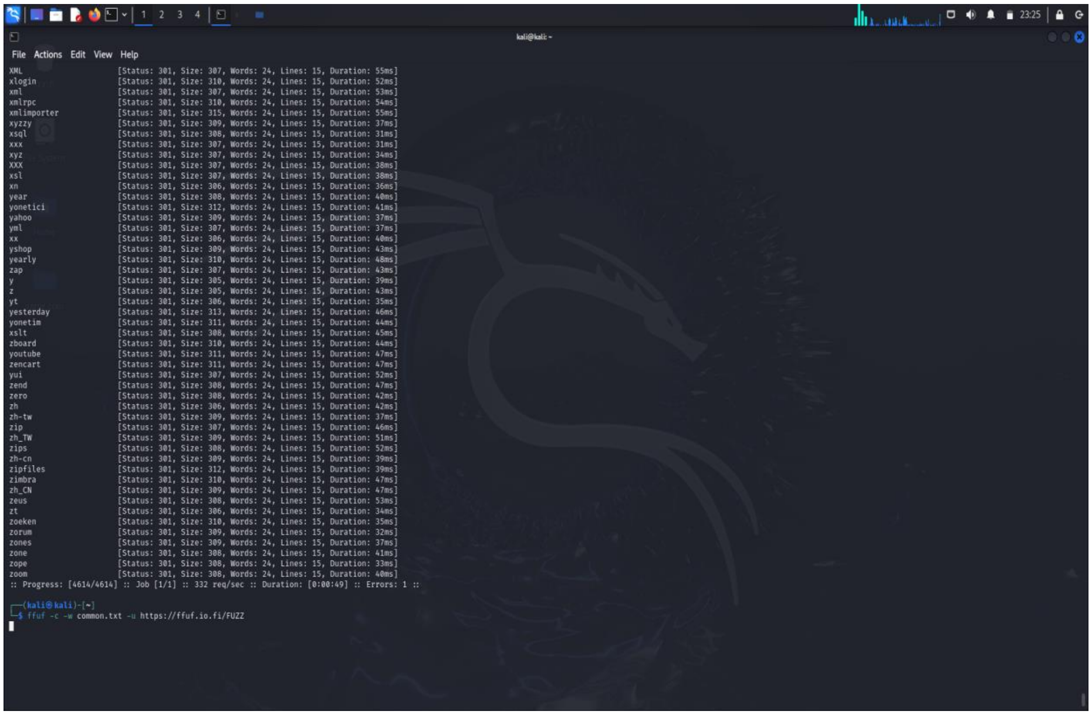
4.Fuzzing

➢ FFUF

Purpose: Use **FFUF** for fuzzing endpoints and parameters to identify hidden functionalities or resources.

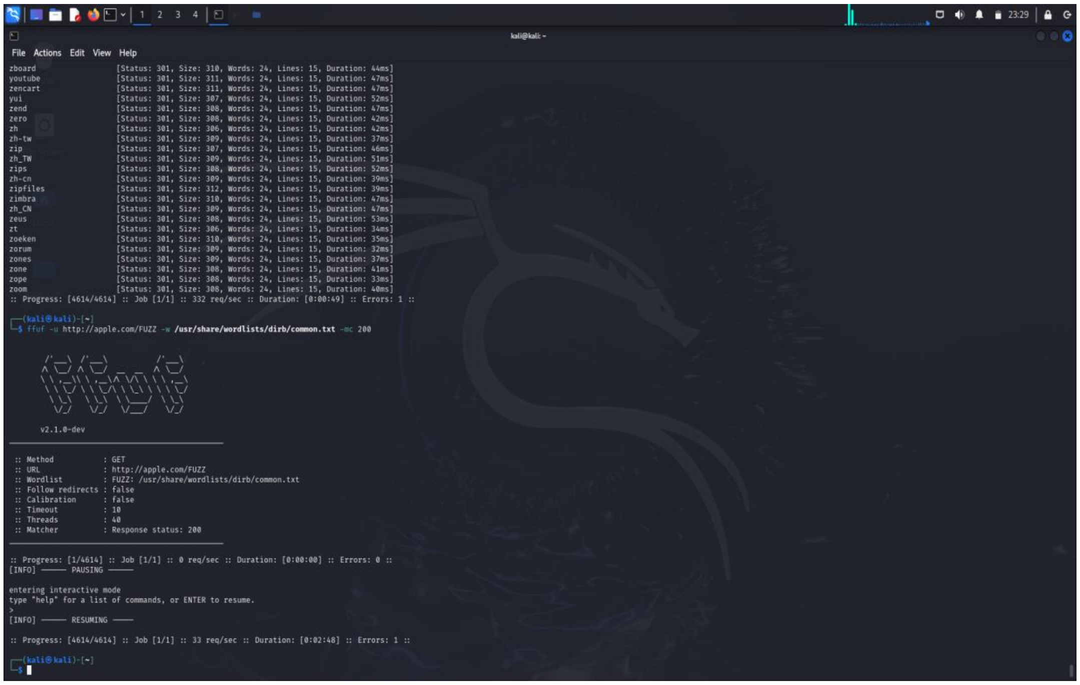


```
┌──(kali㉿kali)-[~]
└─$ ffuf -u http://apple.com/FUZZ -w /usr/share/wordlists/dirb/common.txt

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://apple.com/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirb/common.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

                        [Status: 301, Size: 304, Words: 24, Lines: 15, Duration: 126ms]
.bashrc                 [Status: 301, Size: 311, Words: 24, Lines: 15, Duration: 123ms]
.mysql_history          [Status: 301, Size: 318, Words: 24, Lines: 15, Duration: 135ms]
_admin                  [Status: 301, Size: 310, Words: 24, Lines: 15, Duration: 136ms]
.cvs                    [Status: 301, Size: 308, Words: 24, Lines: 15, Duration: 137ms]
.profile                [Status: 301, Size: 312, Words: 24, Lines: 15, Duration: 145ms]
_backup                 [Status: 301, Size: 311, Words: 24, Lines: 15, Duration: 116ms]
.ssh                    [Status: 301, Size: 308, Words: 24, Lines: 15, Duration: 146ms]
_assets                 [Status: 301, Size: 311, Words: 24, Lines: 15, Duration: 119ms]
.passwd                 [Status: 301, Size: 311, Words: 24, Lines: 15, Duration: 135ms]
.sh_history             [Status: 301, Size: 315, Words: 24, Lines: 15, Duration: 121ms]
.listing                [Status: 301, Size: 312, Words: 24, Lines: 15, Duration: 116ms]
.svn                    [Status: 301, Size: 308, Words: 24, Lines: 15, Duration: 139ms]
_catalogs               [Status: 301, Size: 313, Words: 24, Lines: 15, Duration: 116ms]
.htaccess               [Status: 301, Size: 313, Words: 24, Lines: 15, Duration: 118ms]
.history                [Status: 301, Size: 312, Words: 24, Lines: 15, Duration: 116ms]
.bash_history           [Status: 301, Size: 317, Words: 24, Lines: 15, Duration: 137ms]
.cache                  [Status: 301, Size: 310, Words: 24, Lines: 15, Duration: 138ms]
.subversion             [Status: 301, Size: 315, Words: 24, Lines: 15, Duration: 140ms]
.svn/entries            [Status: 301, Size: 316, Words: 24, Lines: 15, Duration: 141ms]
.perf                   [Status: 301, Size: 309, Words: 24, Lines: 15, Duration: 123ms]
_code                   [Status: 301, Size: 309, Words: 24, Lines: 15, Duration: 127ms]
@                       [Status: 301, Size: 305, Words: 24, Lines: 15, Duration: 128ms]
.cvsignore              [Status: 301, Size: 314, Words: 24, Lines: 15, Duration: 147ms]
_ajax                   [Status: 301, Size: 309, Words: 24, Lines: 15, Duration: 117ms]
.config                 [Status: 301, Size: 311, Words: 24, Lines: 15, Duration: 127ms]
.git/HEAD               [Status: 301, Size: 313, Words: 24, Lines: 15, Duration: 136ms]
_cache                  [Status: 301, Size: 310, Words: 24, Lines: 15, Duration: 143ms]
_adm                    [Status: 301, Size: 308, Words: 24, Lines: 15, Duration: 162ms]
_                       [Status: 301, Size: 305, Words: 24, Lines: 15, Duration: 140ms]
_borders                [Status: 301, Size: 312, Words: 24, Lines: 15, Duration: 142ms]
.web                    [Status: 301, Size: 308, Words: 24, Lines: 15, Duration: 140ms]
.listings               [Status: 301, Size: 313, Words: 24, Lines: 15, Duration: 141ms]
.forward                [Status: 301, Size: 312, Words: 24, Lines: 15, Duration: 138ms]
_archive                [Status: 301, Size: 312, Words: 24, Lines: 15, Duration: 140ms]
_baks                   [Status: 301, Size: 309, Words: 24, Lines: 15, Duration: 140ms]
```



```
XML                     [Status: 301, Size: 307, Words: 24, Lines: 15, Duration: 55ms]
xlogin                  [Status: 301, Size: 310, Words: 24, Lines: 15, Duration: 52ms]
xml                     [Status: 301, Size: 307, Words: 24, Lines: 15, Duration: 53ms]
xmlrpc                  [Status: 301, Size: 310, Words: 24, Lines: 15, Duration: 54ms]
xmlimporter             [Status: 301, Size: 315, Words: 24, Lines: 15, Duration: 55ms]
xyzzy                   [Status: 301, Size: 309, Words: 24, Lines: 15, Duration: 37ms]
xsql                    [Status: 301, Size: 308, Words: 24, Lines: 15, Duration: 31ms]
xxx                     [Status: 301, Size: 307, Words: 24, Lines: 15, Duration: 31ms]
xyz                     [Status: 301, Size: 307, Words: 24, Lines: 15, Duration: 34ms]
XXX                     [Status: 301, Size: 307, Words: 24, Lines: 15, Duration: 38ms]
xsl                     [Status: 301, Size: 307, Words: 24, Lines: 15, Duration: 38ms]
xn                      [Status: 301, Size: 306, Words: 24, Lines: 15, Duration: 36ms]
year                    [Status: 301, Size: 308, Words: 24, Lines: 15, Duration: 40ms]
yonetici                [Status: 301, Size: 312, Words: 24, Lines: 15, Duration: 41ms]
yahoo                   [Status: 301, Size: 309, Words: 24, Lines: 15, Duration: 37ms]
yml                     [Status: 301, Size: 307, Words: 24, Lines: 15, Duration: 37ms]
xx                      [Status: 301, Size: 306, Words: 24, Lines: 15, Duration: 40ms]
yshop                   [Status: 301, Size: 309, Words: 24, Lines: 15, Duration: 43ms]
yearly                  [Status: 301, Size: 310, Words: 24, Lines: 15, Duration: 48ms]
zap                     [Status: 301, Size: 307, Words: 24, Lines: 15, Duration: 43ms]
y                       [Status: 301, Size: 305, Words: 24, Lines: 15, Duration: 39ms]
z                       [Status: 301, Size: 305, Words: 24, Lines: 15, Duration: 43ms]
yt                      [Status: 301, Size: 306, Words: 24, Lines: 15, Duration: 35ms]
yesterday               [Status: 301, Size: 313, Words: 24, Lines: 15, Duration: 46ms]
yonetim                 [Status: 301, Size: 311, Words: 24, Lines: 15, Duration: 44ms]
xslt                    [Status: 301, Size: 308, Words: 24, Lines: 15, Duration: 45ms]
zboard                  [Status: 301, Size: 310, Words: 24, Lines: 15, Duration: 44ms]
youtube                 [Status: 301, Size: 311, Words: 24, Lines: 15, Duration: 47ms]
zencart                 [Status: 301, Size: 311, Words: 24, Lines: 15, Duration: 47ms]
yui                     [Status: 301, Size: 307, Words: 24, Lines: 15, Duration: 52ms]
zend                    [Status: 301, Size: 308, Words: 24, Lines: 15, Duration: 47ms]
zero                    [Status: 301, Size: 308, Words: 24, Lines: 15, Duration: 42ms]
zh                      [Status: 301, Size: 306, Words: 24, Lines: 15, Duration: 42ms]
zh-tw                   [Status: 301, Size: 309, Words: 24, Lines: 15, Duration: 37ms]
zip                     [Status: 301, Size: 307, Words: 24, Lines: 15, Duration: 46ms]
zh_TW                   [Status: 301, Size: 309, Words: 24, Lines: 15, Duration: 51ms]
zips                    [Status: 301, Size: 308, Words: 24, Lines: 15, Duration: 52ms]
zh-cn                   [Status: 301, Size: 309, Words: 24, Lines: 15, Duration: 39ms]
zipfiles                [Status: 301, Size: 312, Words: 24, Lines: 15, Duration: 39ms]
zimbra                  [Status: 301, Size: 310, Words: 24, Lines: 15, Duration: 47ms]
zh_CN                   [Status: 301, Size: 309, Words: 24, Lines: 15, Duration: 47ms]
zeus                    [Status: 301, Size: 308, Words: 24, Lines: 15, Duration: 53ms]
zt                      [Status: 301, Size: 306, Words: 24, Lines: 15, Duration: 34ms]
zoeken                  [Status: 301, Size: 310, Words: 24, Lines: 15, Duration: 35ms]
zorum                   [Status: 301, Size: 309, Words: 24, Lines: 15, Duration: 32ms]
zones                   [Status: 301, Size: 309, Words: 24, Lines: 15, Duration: 37ms]
zone                    [Status: 301, Size: 308, Words: 24, Lines: 15, Duration: 41ms]
zope                    [Status: 301, Size: 308, Words: 24, Lines: 15, Duration: 33ms]
zoom                    [Status: 301, Size: 308, Words: 24, Lines: 15, Duration: 40ms]
:: Progress: [4614/4614] :: Job [1/1] :: 332 req/sec :: Duration: [0:00:49] :: Errors: 1 ::

┌──(kali㉿kali)-[~]
└─$ ffuf -c -w common.txt -u https://ffuf.io.fi/FUZZ
▌
```

Scanning Only for Status Code 200

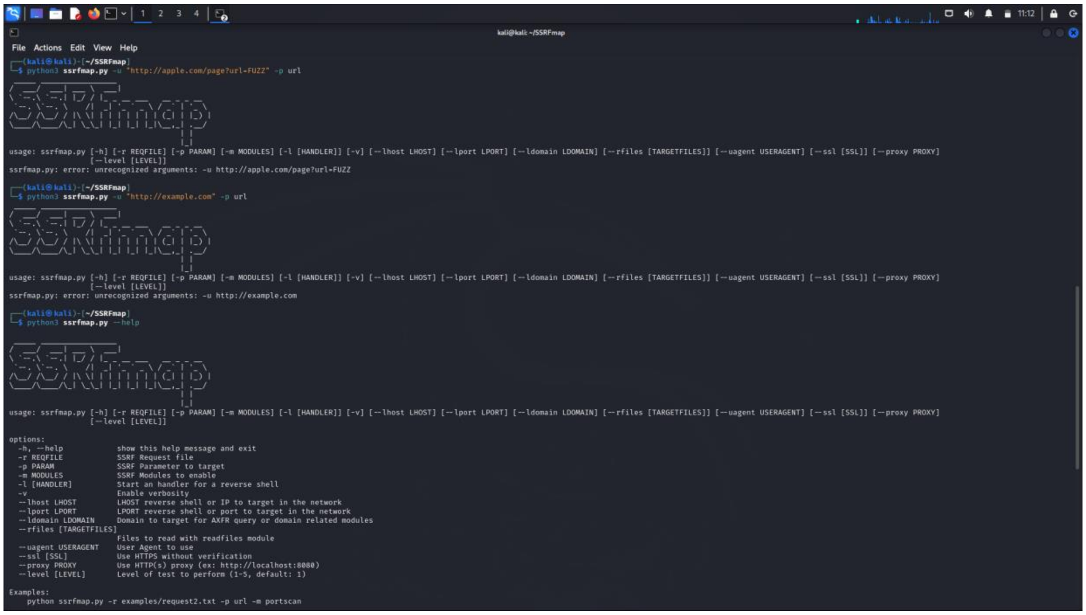


```
zboard                  [Status: 301, Size: 310, Words: 24, Lines: 15, Duration: 44ms]
youtube                 [Status: 301, Size: 311, Words: 24, Lines: 15, Duration: 47ms]
zencart                 [Status: 301, Size: 311, Words: 24, Lines: 15, Duration: 47ms]
yui                     [Status: 301, Size: 307, Words: 24, Lines: 15, Duration: 52ms]
zend                    [Status: 301, Size: 308, Words: 24, Lines: 15, Duration: 47ms]
zero                    [Status: 301, Size: 308, Words: 24, Lines: 15, Duration: 42ms]
zh                      [Status: 301, Size: 306, Words: 24, Lines: 15, Duration: 42ms]
zh-tw                   [Status: 301, Size: 309, Words: 24, Lines: 15, Duration: 37ms]
zip                     [Status: 301, Size: 307, Words: 24, Lines: 15, Duration: 46ms]
zh_TW                   [Status: 301, Size: 309, Words: 24, Lines: 15, Duration: 51ms]
zips                    [Status: 301, Size: 308, Words: 24, Lines: 15, Duration: 52ms]
zh-cn                   [Status: 301, Size: 309, Words: 24, Lines: 15, Duration: 39ms]
zipfiles                [Status: 301, Size: 312, Words: 24, Lines: 15, Duration: 39ms]
zimbra                  [Status: 301, Size: 310, Words: 24, Lines: 15, Duration: 47ms]
zh_CN                   [Status: 301, Size: 309, Words: 24, Lines: 15, Duration: 47ms]
zeus                    [Status: 301, Size: 308, Words: 24, Lines: 15, Duration: 53ms]
zt                      [Status: 301, Size: 306, Words: 24, Lines: 15, Duration: 34ms]
zoeken                  [Status: 301, Size: 310, Words: 24, Lines: 15, Duration: 35ms]
zorum                   [Status: 301, Size: 309, Words: 24, Lines: 15, Duration: 32ms]
zones                   [Status: 301, Size: 309, Words: 24, Lines: 15, Duration: 37ms]
zone                    [Status: 301, Size: 308, Words: 24, Lines: 15, Duration: 41ms]
zope                    [Status: 301, Size: 308, Words: 24, Lines: 15, Duration: 33ms]
zoom                    [Status: 301, Size: 308, Words: 24, Lines: 15, Duration: 40ms]
:: Progress: [4614/4614] :: Job [1/1] :: 332 req/sec :: Duration: [0:00:49] :: Errors: 1 ::

┌──(kali㉿kali)-[~]
└─$ ffuf -u http://apple.com/FUZZ -w /usr/share/wordlists/dirb/common.txt -mc 200

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://apple.com/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirb/common.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200
________________________________________________

:: Progress: [1/4614] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00] :: Errors: 0 ::
[INFO] ────── PAUSING ──────

entering interactive mode
type "help" for a list of commands, or ENTER to resume.
>
[INFO] ────── RESUMING ─────

:: Progress: [4614/4614] :: Job [1/1] :: 33 req/sec :: Duration: [0:02:48] :: Errors: 1 ::

┌──(kali㉿kali)-[~]
└─$
```

5.Server-Side Request Forgery (SSRF)

- SSRFmap

  Purpose:This tool is used to test for SSRF vulnerabilities

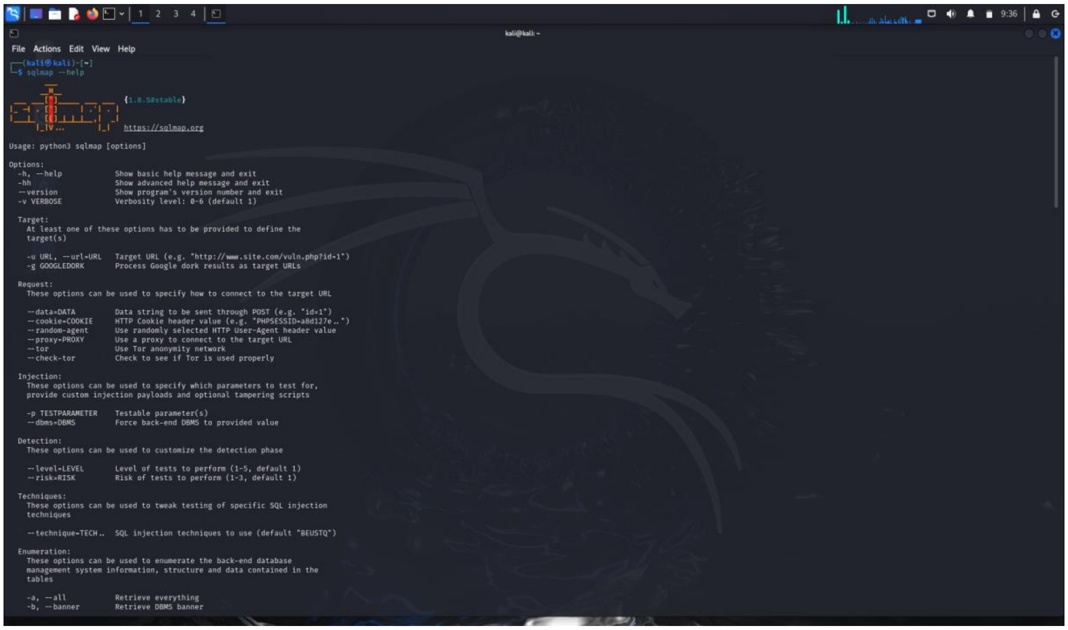


```
┌──(kali㉿kali)-[~/SSRFmap]
└─$ python3 ssrfmap.py -u "http://apple.com/page?url=FUZZ" -p url

usage: ssrfmap.py [-h] [-r REQFILE] [-p PARAM] [-m MODULES] [-l [HANDLER]] [-v] [--lhost LHOST] [--lport LPORT] [--ldomain LDOMAIN] [--rfiles [TARGETFILES]] [--uagent USERAGENT] [--ssl [SSL]] [--proxy PROXY]
                  [--level [LEVEL]]
ssrfmap.py: error: unrecognized arguments: -u http://apple.com/page?url=FUZZ

┌──(kali㉿kali)-[~/SSRFmap]
└─$ python3 ssrfmap.py -u "http://example.com" -p url

usage: ssrfmap.py [-h] [-r REQFILE] [-p PARAM] [-m MODULES] [-l [HANDLER]] [-v] [--lhost LHOST] [--lport LPORT] [--ldomain LDOMAIN] [--rfiles [TARGETFILES]] [--uagent USERAGENT] [--ssl [SSL]] [--proxy PROXY]
                  [--level [LEVEL]]
ssrfmap.py: error: unrecognized arguments: -u http://example.com

┌──(kali㉿kali)-[~/SSRFmap]
└─$ python3 ssrfmap.py --help

usage: ssrfmap.py [-h] [-r REQFILE] [-p PARAM] [-m MODULES] [-l [HANDLER]] [-v] [--lhost LHOST] [--lport LPORT] [--ldomain LDOMAIN] [--rfiles [TARGETFILES]] [--uagent USERAGENT] [--ssl [SSL]] [--proxy PROXY]
                  [--level [LEVEL]]

options:
  -h, --help            show this help message and exit
  -r REQFILE            SSRF Request file
  -p PARAM              SSRF Parameter to target
  -m MODULES            SSRF Modules to enable
  -l [HANDLER]          Start an handler for a reverse shell
  -v                    Enable verbosity
  --lhost LHOST         LHOST reverse shell or IP to target in the network
  --lport LPORT         LPORT reverse shell or port to target in the network
  --ldomain LDOMAIN     Domain to target for AXFR query or domain related modules
  --rfiles [TARGETFILES]
                        Files to read with readfiles module
  --uagent USERAGENT    User Agent to use
  --ssl [SSL]           Use HTTPS without verification
  --proxy PROXY         Use HTTP(s) proxy (ex: http://localhost:8080)
  --level [LEVEL]       Level of test to perform (1-5, default: 1)

Examples:
    python ssrfmap.py -r examples/request2.txt -p url -m portscan
```

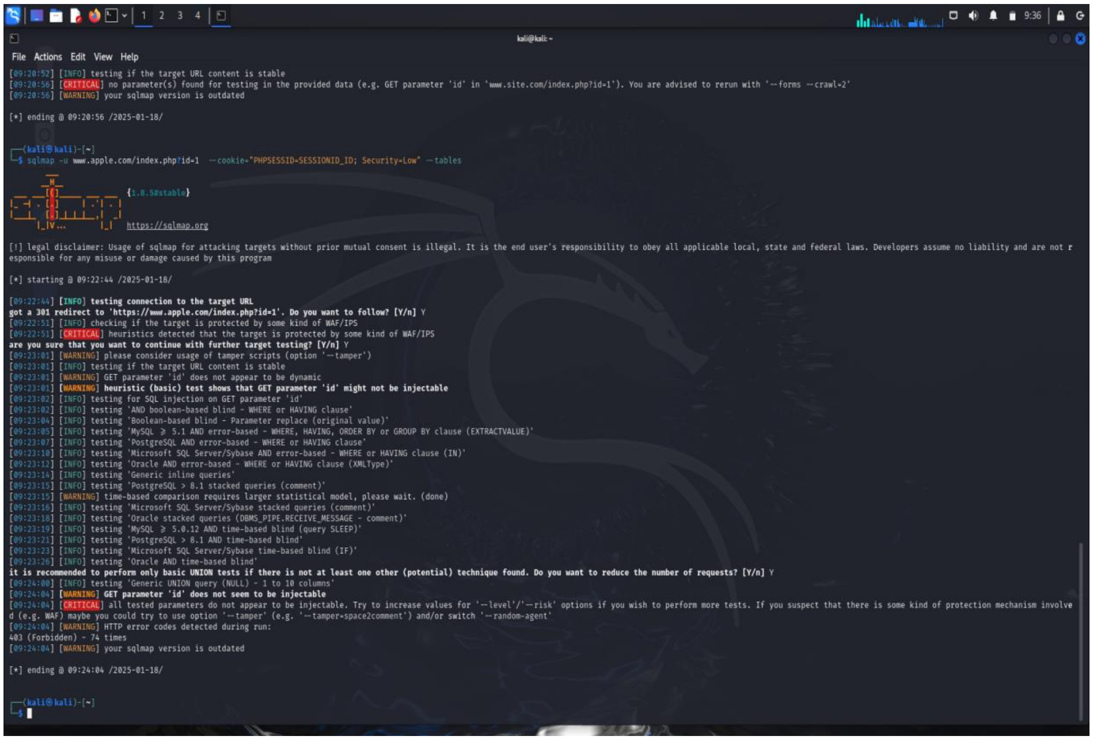
6.SQL Injection Testing

➢ Sqlmap

Purpose:This tool is helps to identify the SQL injection vulnerabilities in identified parameters



```
┌──(kali㉿kali)-[~]
└─$ sqlmap --help
                                  {1.8.5#stable}

                                  https://sqlmap.org

Usage: python3 sqlmap [options]

Options:
  -h, --help            Show basic help message and exit
  -hh                   Show advanced help message and exit
  --version             Show program's version number and exit
  -v VERBOSE            Verbosity level: 0-6 (default 1)

  Target:
    At least one of these options has to be provided to define the
    target(s)

    -u URL, --url=URL   Target URL (e.g. "http://www.site.com/vuln.php?id=1")
    -g GOOGLEDORK       Process Google dork results as target URLs

  Request:
    These options can be used to specify how to connect to the target URL

    --data=DATA         Data string to be sent through POST (e.g. "id=1")
    --cookie=COOKIE     HTTP Cookie header value (e.g. "PHPSESSID=a8d127e..")
    --random-agent      Use randomly selected HTTP User-Agent header value
    --proxy=PROXY       Use a proxy to connect to the target URL
    --tor               Use Tor anonymity network
    --check-tor         Check to see if Tor is used properly

  Injection:
    These options can be used to specify which parameters to test for,
    provide custom injection payloads and optional tampering scripts

    -p TESTPARAMETER    Testable parameter(s)
    --dbms=DBMS         Force back-end DBMS to provided value

  Detection:
    These options can be used to customize the detection phase

    --level=LEVEL       Level of tests to perform (1-5, default 1)
    --risk=RISK         Risk of tests to perform (1-3, default 1)

  Techniques:
    These options can be used to tweak testing of specific SQL injection
    techniques

    --technique=TECH..  SQL injection techniques to use (default "BEUSTQ")

  Enumeration:
    These options can be used to enumerate the back-end database
    management system information, structure and data contained in the
    tables

    -a, --all           Retrieve everything
    -b, --banner        Retrieve DBMS banner
```

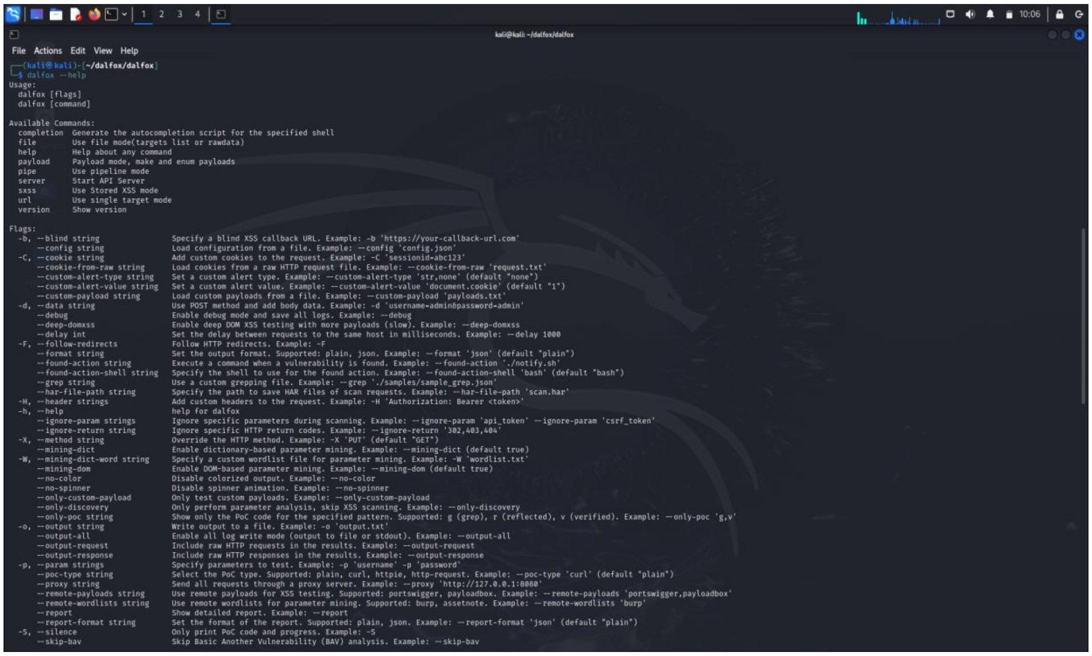


```
[09:20:52] [INFO] testing if the target URL content is stable
[09:20:56] [CRITICAL] no parameter(s) found for testing in the provided data (e.g. GET parameter 'id' in 'www.site.com/index.php?id=1'). You are advised to rerun with '--forms --crawl=2'
[09:20:56] [WARNING] your sqlmap version is outdated

[*] ending @ 09:20:56 /2025-01-18/


┌──(kali㉿kali)-[~]
└─$ sqlmap -u www.apple.com/index.php?id=1  --cookie="PHPSESSID=SESSIONID_ID; Security=Low" --tables
                                  {1.8.5#stable}

                                  https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not r
esponsible for any misuse or damage caused by this program

[*] starting @ 09:22:44 /2025-01-18/

[09:22:44] [INFO] testing connection to the target URL
got a 301 redirect to 'https://www.apple.com/index.php?id=1'. Do you want to follow? [Y/n] Y
[09:22:51] [INFO] checking if the target is protected by some kind of WAF/IPS
[09:22:51] [CRITICAL] heuristics detected that the target is protected by some kind of WAF/IPS
are you sure that you want to continue with further target testing? [Y/n] Y
[09:23:01] [WARNING] please consider usage of tamper scripts (option '--tamper')
[09:23:01] [INFO] testing if the target URL content is stable
[09:23:01] [WARNING] GET parameter 'id' does not appear to be dynamic
[09:23:01] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not be injectable
[09:23:02] [INFO] testing for SQL injection on GET parameter 'id'
[09:23:02] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[09:23:04] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[09:23:05] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[09:23:07] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[09:23:10] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[09:23:12] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[09:23:14] [INFO] testing 'Generic inline queries'
[09:23:15] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[09:23:15] [WARNING] time-based comparison requires larger statistical model, please wait. (done)
[09:23:16] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[09:23:18] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[09:23:19] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[09:23:21] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[09:23:23] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[09:23:26] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] Y
[09:24:00] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[09:24:04] [WARNING] GET parameter 'id' does not seem to be injectable
[09:24:04] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. If you suspect that there is some kind of protection mechanism involve
d (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent'
[09:24:04] [WARNING] HTTP error codes detected during run:
403 (Forbidden) - 74 times
[09:24:04] [WARNING] your sqlmap version is outdated

[*] ending @ 09:24:04 /2025-01-18/


┌──(kali㉿kali)-[~]
└─$
```

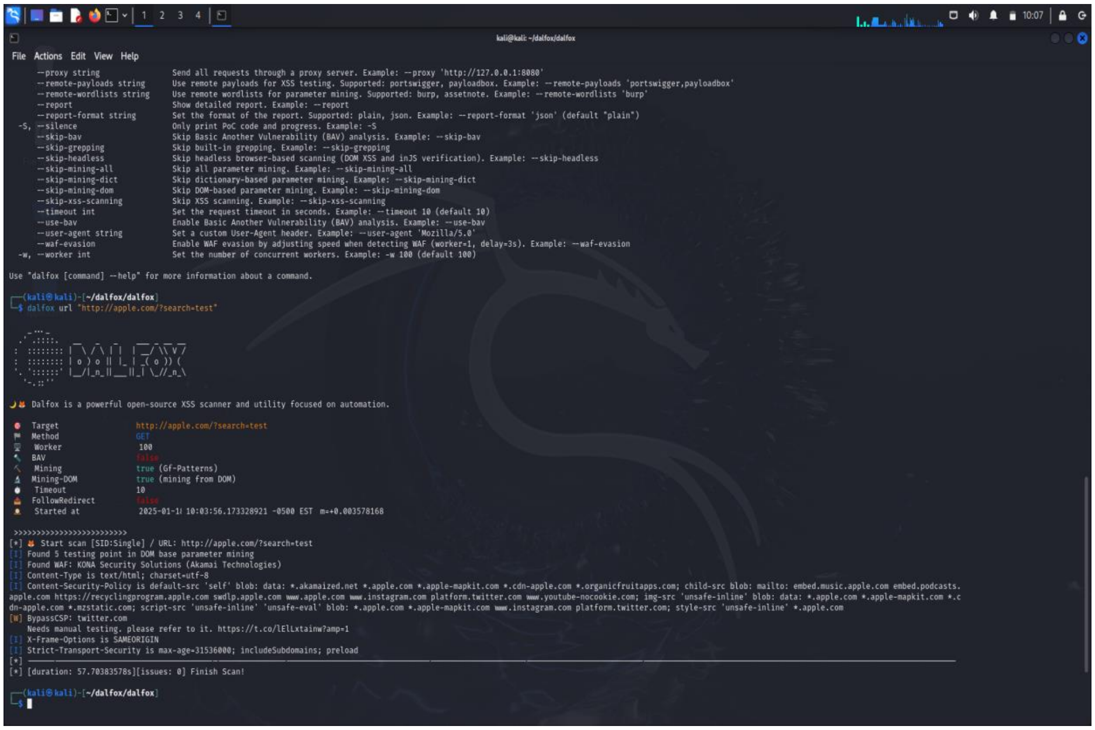
7.Cross-Site Scripting (XSS)

- Dalfox

  Purpose: This helps to test for XSS vulnerabilities



```
┌──(kali㉿kali)-[~/dalfox/dalfox]
└─$ dalfox --help
Usage:
  dalfox [flags]
  dalfox [command]

Available Commands:
  completion  Generate the autocompletion script for the specified shell
  file        Use file mode(targets list or rawdata)
  help        Help about any command
  payload     Payload mode, make and enum payloads
  pipe        Use pipeline mode
  server      Start API Server
  sxss        Use Stored XSS mode
  url         Use single target mode
  version     Show version

Flags:
  -b, --blind string                 Specify a blind XSS callback URL. Example: -b 'https://your-callback-url.com'
      --config string                Load configuration from a file. Example: --config 'config.json'
  -C, --cookie string                Add custom cookies to the request. Example: -C 'sessionid=abc123'
      --cookie-from-raw string       Load cookies from a raw HTTP request file. Example: --cookie-from-raw 'request.txt'
      --custom-alert-type string     Set a custom alert type. Example: --custom-alert-type 'str,none' (default "none")
      --custom-alert-value string    Set a custom alert value. Example: --custom-alert-value 'document.cookie' (default "1")
      --custom-payload string        Load custom payloads from a file. Example: --custom-payload 'payloads.txt'
  -d, --data string                  Use POST method and add body data. Example: -d 'username=admin&password=admin'
      --debug                        Enable debug mode and save all logs. Example: --debug
      --deep-domxss                  Enable deep DOM XSS testing with more payloads (slow). Example: --deep-domxss
      --delay int                    Set the delay between requests to the same host in milliseconds. Example: --delay 1000
  -F, --follow-redirects             Follow HTTP redirects. Example: -F
      --format string                Set the output format. Supported: plain, json. Example: --format 'json' (default "plain")
      --found-action string          Execute a command when a vulnerability is found. Example: --found-action './notify.sh'
      --found-action-shell string    Specify the shell to use for the found action. Example: --found-action-shell 'bash' (default "bash")
      --grep string                  Use a custom grepping file. Example: --grep './samples/sample_grep.json'
      --har-file-path string         Specify the path to save HAR files of scan requests. Example: --har-file-path 'scan.har'
  -H, --header strings               Add custom headers to the request. Example: -H 'Authorization: Bearer <token>'
  -h, --help                         help for dalfox
      --ignore-param strings         Ignore specific parameters during scanning. Example: --ignore-param 'api_token' --ignore-param 'csrf_token'
      --ignore-return string         Ignore specific HTTP return codes. Example: --ignore-return '302,403,404'
  -X, --method string                Override the HTTP method. Example: -X 'PUT' (default "GET")
      --mining-dict                  Enable dictionary-based parameter mining. Example: --mining-dict (default true)
  -W, --mining-dict-word string      Specify a custom wordlist file for parameter mining. Example: -W 'wordlist.txt'
      --mining-dom                   Enable DOM-based parameter mining. Example: --mining-dom (default true)
      --no-color                     Disable colorized output. Example: --no-color
      --no-spinner                   Disable spinner animation. Example: --no-spinner
      --only-custom-payload          Only test custom payloads. Example: --only-custom-payload
      --only-discovery               Only perform parameter analysis, skip XSS scanning. Example: --only-discovery
      --only-poc string              Show only the PoC code for the specified pattern. Supported: g (grep), r (reflected), v (verified). Example: --only-poc 'g,v'
  -o, --output string                Write output to a file. Example: -o 'output.txt'
      --output-all                   Enable all log write mode (output to file or stdout). Example: --output-all
      --output-request               Include raw HTTP requests in the results. Example: --output-request
      --output-response              Include raw HTTP responses in the results. Example: --output-response
  -p, --param strings                Specify parameters to test. Example: -p 'username' -p 'password'
      --poc-type string              Select the PoC type. Supported: plain, curl, httpie, http-request. Example: --poc-type 'curl' (default "plain")
      --proxy string                 Send all requests through a proxy server. Example: --proxy 'http://127.0.0.1:8080'
      --remote-payloads string       Use remote payloads for XSS testing. Supported: portswigger, payloadbox. Example: --remote-payloads 'portswigger,payloadbox'
      --remote-wordlists string      Use remote wordlists for parameter mining. Supported: burp, assetnote. Example: --remote-wordlists 'burp'
      --report                       Show detailed report. Example: --report
      --report-format string         Set the format of the report. Supported: plain, json. Example: --report-format 'json' (default "plain")
  -S, --silence                      Only print PoC code and progress. Example: -S
      --skip-bav                     Skip Basic Another Vulnerability (BAV) analysis. Example: --skip-bav
```



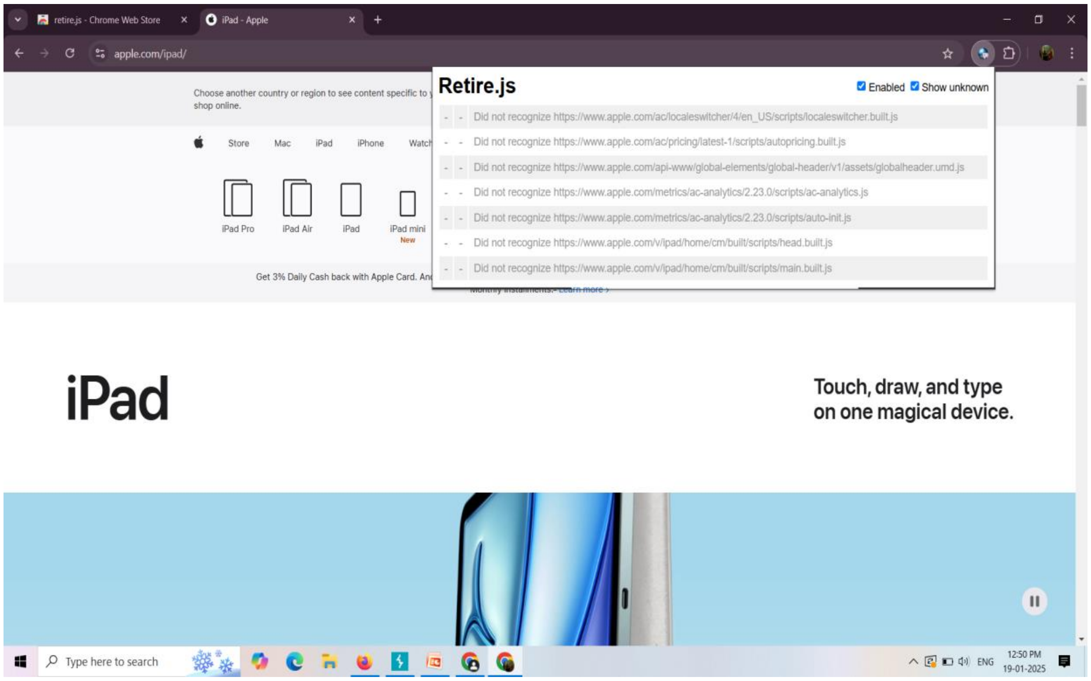
```
      --proxy string                 Send all requests through a proxy server. Example: --proxy 'http://127.0.0.1:8080'
      --remote-payloads string       Use remote payloads for XSS testing. Supported: portswigger, payloadbox. Example: --remote-payloads 'portswigger,payloadbox'
      --remote-wordlists string      Use remote wordlists for parameter mining. Supported: burp, assetnote. Example: --remote-wordlists 'burp'
      --report                       Show detailed report. Example: --report
      --report-format string         Set the format of the report. Supported: plain, json. Example: --report-format 'json' (default "plain")
  -S, --silence                      Only print PoC code and progress. Example: -S
      --skip-bav                     Skip Basic Another Vulnerability (BAV) analysis. Example: --skip-bav
      --skip-grepping                Skip built-in grepping. Example: --skip-grepping
      --skip-headless                Skip headless browser-based scanning (DOM XSS and inJS verification). Example: --skip-headless
      --skip-mining-all              Skip all parameter mining. Example: --skip-mining-all
      --skip-mining-dict             Skip dictionary-based parameter mining. Example: --skip-mining-dict
      --skip-mining-dom              Skip DOM-based parameter mining. Example: --skip-mining-dom
      --skip-xss-scanning            Skip XSS scanning. Example: --skip-xss-scanning
      --timeout int                  Set the request timeout in seconds. Example: --timeout 10 (default 10)
      --use-bav                      Enable Basic Another Vulnerability (BAV) analysis. Example: --use-bav
      --user-agent string            Set a custom User-Agent header. Example: --user-agent 'Mozilla/5.0'
      --waf-evasion                  Enable WAF evasion by adjusting speed when detecting WAF (worker=1, delay=3s). Example: --waf-evasion
  -w, --worker int                   Set the number of concurrent workers. Example: -w 100 (default 100)

Use "dalfox [command] --help" for more information about a command.

┌──(kali㉿kali)-[~/dalfox/dalfox]
└─$ dalfox url "http://apple.com/?search=test"

   _..._
 .' .::::.   __   _   _    ___ _ __ __
:  :::::::: |  \ / \ | |  | __/ \\ V /
:  :::::::: | o ) o || |_ | _( o )) (
'. '::::::' |__/|_n_||___||_| \_//_n_\
   '-.::''

🌙🦊 Dalfox is a powerful open-source XSS scanner and utility focused on automation.

 🎯 Target                 http://apple.com/?search=test
 🏁 Method                 GET
 🖥  Worker                 100
 🔦 BAV                    false
 ⛏  Mining                 true (Gf-Patterns)
 🔬 Mining-DOM             true (mining from DOM)
 ⏱  Timeout                10
 📤 FollowRedirect         false
 🕰  Started at             2025-01-1 10:03:56.173328921 -0500 EST m=+0.003578168

 >>>>>>>>>>>>>>>>>>>>>>>>>
[*] 🦊 Start scan [SID:Single] / URL: http://apple.com/?search=test
[I] Found 5 testing point in DOM base parameter mining
[I] Found WAF: KONA Security Solutions (Akamai Technologies)
[I] Content-Type is text/html; charset=utf-8
[I] Content-Security-Policy is default-src 'self' blob: data: *.akamaized.net *.apple.com *.apple-mapkit.com *.cdn-apple.com *.organicfruitapps.com; child-src blob: mailto: embed.music.apple.com embed.podcasts.
apple.com https://recyclingprogram.apple.com swdlp.apple.com www.apple.com www.instagram.com platform.twitter.com www.youtube-nocookie.com; img-src 'unsafe-inline' blob: data: *.apple.com *.apple-mapkit.com *.c
dn-apple.com *.mzstatic.com; script-src 'unsafe-inline' 'unsafe-eval' blob: *.apple.com *.apple-mapkit.com www.instagram.com platform.twitter.com; style-src 'unsafe-inline' *.apple.com
[W] BypassCSP: twitter.com
    Needs manual testing. please refer to it. https://t.co/lElLxtainw?amp=1
[I] X-Frame-Options is SAMEORIGIN
[I] Strict-Transport-Security is max-age=31536000; includeSubdomains; preload
[*] ──────────────────────────────────────────────────────────────────────────────────────────────
[*] [duration: 57.70383578s][issues: 0] Finish Scan!

┌──(kali㉿kali)-[~/dalfox/dalfox]
└─$ █
```

8.Identifying Outdated Libraries

➢ Retire.js

Purpose: This helps to scan for outdated JavaScript libraries on the target site.

Target site:apple.com



Retire.js ☑ Enabled ☑ Show unknown

```
- - Did not recognize https://www.apple.com/ac/localeswitcher/4/en_US/scripts/localeswitcher.built.js
- - Did not recognize https://www.apple.com/ac/pricing/latest-1/scripts/autopricing.built.js
- - Did not recognize https://www.apple.com/api-www/global-elements/global-header/v1/assets/globalheader.umd.js
- - Did not recognize https://www.apple.com/metrics/ac-analytics/2.23.0/scripts/ac-analytics.js
- - Did not recognize https://www.apple.com/metrics/ac-analytics/2.23.0/scripts/auto-init.js
- - Did not recognize https://www.apple.com/v/ipad/home/cm/built/scripts/head.built.js
- - Did not recognize https://www.apple.com/v/ipad/home/cm/built/scripts/main.built.js
```