Recon

DNS Discovery

Name	Link
Sublist3r	https://github.com/aboul3la/Sublist3r
enumall	https://github.com/jhaddix/domain/
massdns	https://github.com/blechschmidt/massdns
altdns	https://github.com/infosec-au/altdns
brutesubs	https://github.com/anshumanbh/brutesubs
dns-parallel-prober	https://github.com/lorenzog/dns-parallel-prober
dnscan	https://github.com/rbsec/dnscan
Knockpy	https://github.com/guelfoweb/knock

Port scan

Name	Link
nmap	https://nmap.org
masscan	https://github.com/robertdavidgraham/masscan

Screenshots

Name	Link
EyeWitness	https://github.com/ChrisTruncer/EyeWitness
httpscreenshot	https://github.com/breenmachine/httpscreenshot/

Web Discovery

Name	Link
DirBuster	https://sourceforge.net/projects/dirbuster/
dirb	http://dirb.sourceforge.net/
ilebuster	https://github.com/henshin/filebuster
gobuster	https://github.com/OJ/gobuster
dirsearch	https://github.com/maurosoria/dirsearch

Github

Name	Link
Gitrob	https://github.com/michenriksen/gitrob
git-all-secrets	https://github.com/anshumanbh/git-all-secrets
truffleHog	https://github.com/dxa4481/truffleHog

Name	Link
git-secrets	https://github.com/awslabs/git-secrets
repo-supervisor	https://github.com/auth0/repo-supervisor

S3

Name	Link
sandcastle	https://github.com/yasinS/sandcastle
bucket_finder	https://digi.ninja/projects/bucket_finder.php

Google Dorks

Name	Link
Goohak	https://github.com/1N3/Goohak/
GoogD0rker	https://github.com/ZephrFish/GoogD0rker/

Hidden parameters

Name	Link
parameth	https://github.com/mak-/parameth

Old content

Name	Link
Wayback Machine	https://web.archive.org
waybackrobots	https://gist.github.com/mhmdiaa/2742c5e147d49a804b408bfed3
waybackurls	https://gist.github.com/mhmdiaa/adf6bff70142e5091792841d4b3
Google (with the time filter on)	https://google.com

Asset identification

Name	Link
Shodan	https://shodan.io/
Internet Wide Scan Data	http://Repositoryscans.io
censys	https://censys.io
Hurricane Electric	http://bgp.he.net/

Frameworks

Name	Link
Kubebot	https://github.com/anshumanbh/kubebot
Intrigue	https://github.com/intrigueio/intrigue-core
Sn1per	https://github.com/1N3/Sn1per/

Name	Link
scantastic-tool	https://github.com/maK-/scantastic-tool/
XRay	https://github.com/evilsocket/xray
datasploit	https://github.com/DataSploit/datasploit
Inquisitor	https://github.com/penafieljlm/inquisitor
Spiderfoot	https://github.com/smicallef/spiderfoot

Exploiting & Scanning

XSS

Name	Link
XSS-Radar	https://github.com/bugbountyforum/XSS-Radar
XSSHunter	https://github.com/mandatoryprogrammer/xsshunter
xsshunter_client	https://github.com/mandatoryprogrammer/xsshunter_clier
domxssscanner	https://github.com/yaph/domxssscanner
XSSer	https://github.com/epsylon/xsser
BruteXSS	https://github.com/rajeshmajumdar/BruteXSS
XSStrike	https://github.com/UltimateHackers/XSStrike
XSS'OR	http://xssor.io/

SQLi

Name	Link
sqlmap	http://sqlmap.org/

XXE

Name	Link
oxml_xxe	https://github.com/BuffaloWill/oxml_xxe/
XXE Injector	https://github.com/enjoiz/XXEinjector

SSRF

Name	Link
ssrfDetector	https://github.com/JacobReynolds/ssrfDetector
ground-control	https://github.com/jobertabma/ground-control

SSTI

Name	Link
tplmap	https://github.com/epinna/tplmap

LFI

Name	Link
LFISuit	https://github.com/D35m0nd142/LFISuite

File upload

Name	Link
gen_xbin_avi	https://github.com/neex/ffmpeg-avi-m3u-xbin/

Exposed Git/SVN directory

Name	Link
GitTools	https://github.com/internetwache/GitTools
dvcs-ripper	https://github.com/kost/dvcs-ripper

Subdomain takeover

Name	Link
tko-subs	https://github.com/anshumanbh/tko-subs
HostileSubBruteforcer	https://github.com/nahamsec/HostileSubBruteforcer
second-order	https://github.com/mhmdiaa/second-order

Race conditions

Name	Link
Race the Web	https://github.com/insp3ctre/race-the-web

CORS misconfiguration

Name	Link
CORStest	https://github.com/RUB-NDS/CORStest

Struts

Name	Link
RCE struts-pwn	https://github.com/mazen160/struts-pwn

Serialization

Name	Link
ysoserial	https://github.com/GoSecure/ysoserial
PHPGGC	https://github.com/ambionics/phpggc

Known vulnerable software

Name	Link
retire-js	https://github.com/RetireJS/retire.js
getsploit	https://github.com/vulnersCom/getsploit
Findsploit	https://github.com/1N3/Findsploit

Default/config files

Name	Link
bfac	https://github.com/mazen160/bfac

CMS

Name	Link
WPScan	https://wpscan.org/
CMSMap	https://github.com/Dionach/CMSmap
joomscan	https://github.com/rezasp/joomscan

JWT

Name	Link
The JSON Web Token Toolkit	https://github.com/ticarpi/jwt_tool

Fuzzing & Bruteforcing

General

Name	Link
wfuzz	https://github.com/xmendez/wfuzz/
patator	https://github.com/lanjelot/patator

Name	Link
hydra	https://github.com/vanhauser-thc/thc-hydra
changeme	https://github.com/ztgrace/changeme

Fingerprinting

Server Software

Name	Link
whatweb	https://github.com/urbanadventurer/whatweb
wappalyzer	https://wappalyzer.com/
builtwith	https://builtwith.com/

WAF

Name	Link
wafw00f	https://github.com/EnableSecurity/wafw00f

decompilers

Flash

Name	Link
Show My Code	http://www.showmycode.com/
JPEXS Free Flash Decompiler	http://www.showmycode.com/

Proxy Plugins

Burp suite

Name
backslash-powered-scanner
reflected parameters

Name
SAML Encoder/Decoder
Bypass WAF
CVSS Calculator
Java deserialization Scanner
Autorize
BurpSmartBuster
Content Type Converter
JSON Beautifier
PsychoPATH
Retire-js
J2EEScan
SAML Raider
Active Scan++
UUID Detector
Additional Scanner Checks
CO2 Flow

Name
Hackvertor
Meth0dMan
Paramalyzer

Monitoring

General

Name	Link
assetnote	https://github.com/infosec-au/assetnote

JS Parsing

Beautification

Name	Link
jsbeautifier	http://jsbeautifier.org/

endpoint extraction

Name	Link
LinkFinder	https://github.com/GerbenJavado/LinkFinder

Mobile testing

Frameworks

Name	Link
MobSF	https://github.com/MobSF/Mobile-Security-Framework-MobSF/

Emulators

Name	Link
GenyMotion	https://www.genymotion.com/
Android Studio	https://developer.android.com/studio/

Decompilers

Name	Link
Apktool	https://github.com/iBotPeaches/Apktool
dex2jar	https://sourceforge.net/projects/dex2jar/
jd-gui	https://github.com/java-decompiler/jd-gui

Misc

Name	Link
idb	https://github.com/dmayer/idb