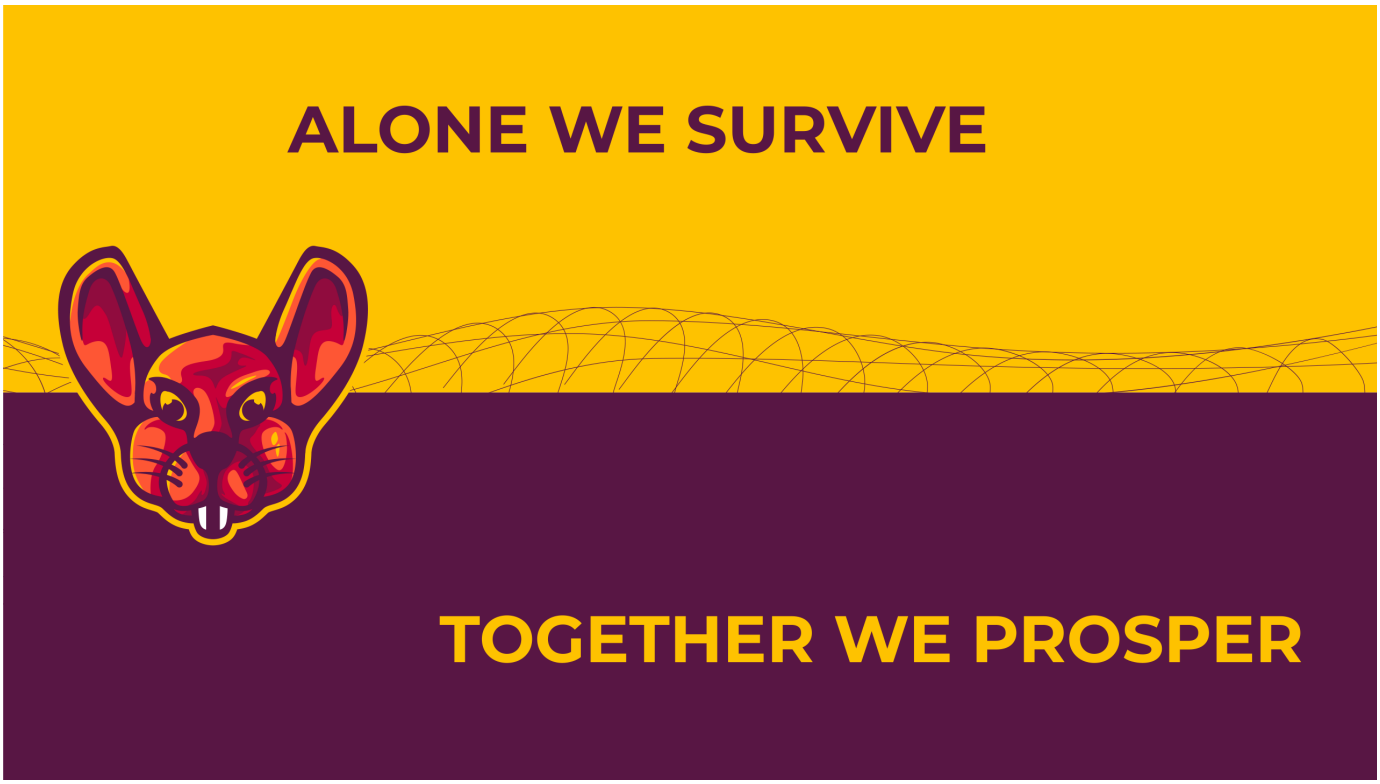
Checklist: Tool selection



Info gathering

General

1. Google Search - https://www.google.com/
2. Shodan - https://www.shodan.io/
3. Maltego - https://www.maltego.com/
4. Recon-ng - https://github.com/lanmaster53/recon-ng
5. theHarvester - https://github.com/laramies/theHarvester
6. FOCA - https://github.com/ElevenPaths/FOCA
7. SpiderFoot - https://www.spiderfoot.net/
8. OSINT Framework - https://osintframework.com/
9. Metagoofil - https://github.com/laramies/metagoofil
10. Tinfoleak - https://github.com/vaguileradiaz/tinfoleak

Portscanning tools

1. Google Search - https://www.google.com/
2. Shodan - https://www.shodan.io/
3. Maltego - https://www.maltego.com/
4. Recon-ng - https://github.com/lanmaster53/recon-ng
5. theHarvester - https://github.com/laramies/theHarvester
6. FOCA - https://github.com/ElevenPaths/FOCA
7. SpiderFoot - https://www.spiderfoot.net/
8. OSINT Framework - https://osintframework.com/
9. Metagoofil - https://github.com/laramies/metagoofil
10. Tinfoleak - https://github.com/vaguileradiaz/tinfoleak
11. Nmap
12. Naabu
13. Masscan
14. Netcat
15. AngryIP

OSINT

1. Censys - https://censys.io/
2. Foca Pro - https://www.elevenpaths.com/es/soluciones/foca-pro/index.html
3. Datasploit - https://github.com/DataSploit/datasploit
4. Sherlock - https://github.com/sherlock-project/sherlock
5. PhoneInfoga - https://github.com/sundowndev/PhoneInfoga
6. Sn1per - https://github.com/1N3/Sn1per
7. Photon - https://github.com/s0md3v/Photon
8. Infoga - https://github.com/m4ll0k/Infoga
9. Gitrob - https://github.com/michenriksen/gitrob
10. Amass - https://github.com/OWASP/Amass

Checking if domain live

1. Ping - https://en.wikipedia.org/wiki/Ping_(networking_utility)
2. Curl - https://curl.se/
3. Wget - https://www.gnu.org/software/wget/
4. Telnet - https://en.wikipedia.org/wiki/Telnet
5. Netcat - https://en.wikipedia.org/wiki/Netcat
6. Traceroute - https://en.wikipedia.org/wiki/Traceroute
7. Nmap - https://nmap.org/
8. Hping - http://www.hping.org/

Subdomain flyover tools

1. Sublist3r - https://github.com/aboul3la/Sublist3r
2. Recon-ng - https://github.com/lanmaster53/recon-ng
3. Amass - https://github.com/OWASP/Amass
4. Subfinder - https://github.com/projectdiscovery/subfinder
5. Aquatone - https://github.com/michenriksen/aquatone
6. Knockpy - https://github.com/guelfoweb/knock
7. theHarvester - https://github.com/laramies/theHarvester
8. Subbrute - https://github.com/TheRook/subbrute
9. dnsrecon - https://github.com/darkoperator/dnsrecon
10. EyeWitness - https://github.com/FortyNorthSecurity/EyeWitness
11. Fierce - https://github.com/mschwager/fierce

Code review

1. ESLint - https://eslint.org/
2. JSHint - https://jshint.com/
3. Retire.js - https://github.com/RetireJS/retire.js
4. Brakeman - https://brakemanscanner.org/
5. SonarJS - https://www.sonarqube.org/features/security/
6. Snyk - https://snyk.io/
7. jsprime - https://github.com/dpnishant/jsprime
8. QL for Javascript - https://www.semanticscholar.org/paper/QL-for-JavaScript%3A-Principles-and-Applications-Ferrari-Palomba/b2a73e71b3c2dcebe83f16a75711c290b8032029
9. CodeQL - https://securitylab.github.com/tools/codeql/
10. Jscrambler - https://jscrambler.com/

Content discovery

1. DirBuster - https://sourceforge.net/projects/dirbuster/
2. DirSearch - https://github.com/maurosoria/dirsearch
3. Gobuster - https://github.com/OJ/gobuster
4. wfuzz - https://github.com/xmendez/wfuzz
5. Arjun - https://github.com/s0md3v/Arjun
6. ffuf - https://github.com/ffuf/ffuf
7. Dirb - https://sourceforge.net/projects/dirb/
8. Nikto - https://cirt.net/nikto2
9. Wfuzz - https://github.com/xmendez/wfuzz
10. Skipfish - https://github.com/spinkham/skipfish

Vulnerability scans

Web app vulnerability scans

- [ ] Burp suite pro
- [ ] OWASP ZAP
- [ ] Nuclei
- [ ] Nikto
- [ ] Acunetix
- [ ] Nessus
- [ ] Netsparker
- [ ] OpenVAS
- [ ] Qualys Web Application Scanning
- [ ] Rapid7 AppSpider
- [ ] Security Compass
- [ ] Trustwave App Scanner
- [ ] Veracode Dynamic Analysis

API vulnerability scanners

1. OWASP ZAP - https://www.zaproxy.org/
2. Postman - https://www.postman.com/api-security/
3. Insomnia - https://insomnia.rest/
4. SoapUI - https://www.soapui.org/api-testing/
5. Burp Suite - https://portswigger.net/burp/api-scanning
6. Rest-Assured - https://github.com/rest-assured/rest-assured/wiki/Usage
7. Checkmarx - https://www.checkmarx.com/products/api-security-testing/
8. Fortify - https://www.microfocus.com/en-us/products/fortify-application-security-testing/overview/api-testing
9. Netsparker - https://www.netsparker.com/api-security/
10. SecureLayer7 - https://www.securelayer7.net/api-security-testing/

External tools

Out of band servers

1. RequestBin - https://requestbin.com/
2. ngrok - https://ngrok.com/
3. Hookbin - https://hookbin.com/
4. Beeceptor - https://beeceptor.com/
5. Pipedream - https://pipedream.com/
6. Webhook.site - https://webhook.site/

Fuzzers

1. AFL (American Fuzzy Lop) - http://lcamtuf.coredump.cx/afl/
2. Peach Fuzzer - https://peachfuzzer.com/
3. Spike - https://github.com/aramosf/spike
4. Sulley - https://github.com/OpenRCE/sulley
5. OWASP ZAP Fuzzer - https://www.zaproxy.org/docs/desktop/addons/fuzzer/
6. Wfuzz - https://github.com/xmendez/wfuzz
7. Fuzzbox - https://github.com/fuzzbox-ws/fuzzbox
8. Radamsa - https://github.com/aoh/radamsa
9. BooFuzz - https://github.com/jtpereyda/boofuzz
10. Powerfuzzer - https://github.com/carlosmiranda/powerfuzzer
11. PeachPy - https://github.com/peachpiecompiler/peachpy

XSS scanners

1. Acunetix - https://www.acunetix.com/
2. AppScan - https://www.ibm.com/security/application-security/appscan
3. Arachni - https://www.arachni-scanner.com/
4. Burp Suite - https://portswigger.net/burp
5. Detectify - https://detectify.com/
6. Fortify - https://www.microfocus.com/en-us/products/application-security-testing/overview
7. IBM Security AppScan - https://www.ibm.com/security/application-security/appscan
8. Netsparker - https://www.netsparker.com/
9. Nikto - https://cirt.net/Nikto2
10. OWASP ZAP - https://www.zaproxy.org/
11. Qualys Web Application Scanning - https://www.qualys.com/apps/web-app-scanning/
12. Retina - https://www.beyondtrust.com/products/retina-network-security-scanner/
13. Rapid7 AppSpider - https://www.rapid7.com/products/appspider/
14. Skipfish - https://tools.kali.org/web-applications/skipfish
15. Vega - https://subgraph.com/vega/
16. Veracode Dynamic Analysis - https://www.veracode.com/products/dynamic-analysis

Blind XSS

1. XSS Hunter - https://xsshunter.com/
2. Blind XSS Injector - https://github.com/cujanovic/Blind-XSS-Injector
3. Sleepy Puppy - https://github.com/Netflix/sleepy-puppy
4. XSStrike - https://github.com/s0md3v/XSStrike
5. XSStrumer - https://github.com/Manas-Harsh/XSStrumer
6. Wfuzz - https://github.com/xmendez/wfuzz
7. BruteXSS - https://github.com/shawarkhanethicalhacker/BruteXSS
8. Dalfox - https://github.com/hahwul/dalfox
9. Fiddler - https://www.telerik.com/fiddler
10. Burp Suite - https://portswigger.net/burp

SQL scanners

1. SQLMap - http://sqlmap.org/
2. Havij - http://www.itsecteam.com/en/projects/project1.htm
3. DorkNet - https://github.com/NullArray/DorkNet
4. NoSQLMap - https://github.com/codingo/NoSQLMap
5. jSQL Injection - https://github.com/ron190/jsql-injection
6. Blind SQL Injector - https://github.com/UltimateHackers/sqlmate
7. SQLMate - https://github.com/UltimateHackers/sqlmate
8. SQLNinja - https://github.com/sqlninja/sqlninja
9. BBQSQL - https://github.com/Neohapsis/bbqsql
10. SQLSentinel - https://github.com/xxlegendriderx/SQLSentinel