Penetration Testing Tools: Eine Übersicht für Anfänger und Fortgeschrittene

Webanwendungs-Penetrationstesting

Tool	Haupteinsatzgebiet	Besondere Stärke	Stärke im Vergleich zu anderen Tools	Vergleichbare Tools	Download
Burp Suite Pro	Umfassende Überprüfung der Sicherheit von Webanwendungen	Manuelle und automatisierte Tests, Intercepting Proxy, Scanner, Intruder, Repeater	Vielseitigkeit, Benutzerfreundlichkeit, große Community	OWASP ZAP, Acunetix, Netsparker	portswigger.net/burp
OWASP ZAP	Automatisierte Schwachstellenanalyse	Open Source, einfache Bedienung, Integration in CI/CD	Kostenlos, aktiv gepflegt	Burp Suite, Nikto, Arachni	owasp.org/www-project-zap/
Nmap	Netzwerk- und Portscanning	Vielseitigkeit, Skriptfähigkeit, große Community	Schnell, zuverlässig, plattformübergreifend	Masscan, Zenmap, Angry IP Scanner	nmap.org

Tool	Haupteinsatzgebiet	Besondere Stärke	Stärke im Vergleich zu anderen Tools	Vergleichbare Tools	Download
Nikto	Webserver-Scanning	Schnell, einfach zu bedienen, erkennt viele bekannte Schwachstellen	Open Source, spezialisiert auf Webserver	OWASP ZAP, Nmap, Nessus	cirt.net/nikto2
Acunetix	Automatisierte Schwachstellensuche	Umfangreiche Datenbank bekannter Schwachstellen, detaillierte Berichte	Hohe Genauigkeit, gute Skalierbarkeit	Burp Suite, Netsparker, Qualys Web Application Scanning	acunetix.com
HCL AppScan	Statische und dynamische Codeanalyse	Integration in SDLC, umfassende Sicherheitsüberprüfungen	Umfassende Analyse, gute Reporting-Funktionen	Checkmarx, Fortify, Veracode	hcltechsw.com/appscan
Wfuzz	Web Fuzzing	Flexibel, unterstützt verschiedene Protokolle	Effizient, anpassbar	ffuf, Burp Suite Intruder, DirBuster	github.com/xmendez/wfuzz
SQLMap	SQL Injection-Tests	Automatisierte Erkennung und Ausnutzung von SQL	Spezialisiert auf SQL Injection, effektiv	sqlmap-dev/sqlmap (GitHub), jSQL Injection	github.com/sqlmap-dev/sqlmap

Tool	Haupteinsatzgebiet	Besondere Stärke	Stärke im Vergleich zu anderen Tools	Vergleichbare Tools	Download
		Injections			
Amass	Information Gathering (OSINT)	Umfassende Sammlung von Informationen über ein Ziel	Effizient, liefert viele Datenpunkte	Sublist3r, theHarvester, Recon-ng	github.com/OWASP/Amass
Netsparker	Automatisierte Schwachstellensuche	Proof-of-Concept-Exploits, genaue Ergebnisse	Zuverlässig, minimal falsch-positive Ergebnisse	Acunetix, Burp Suite, Qualys Web Application Scanning	netsparker.com
Fortify WebInspect	Statische und dynamische Codeanalyse	Integration in SDLC, detaillierte Berichte	Umfassende Analyse, gute Skalierbarkeit	Checkmarx, HCL AppScan, Veracode	microfocus.com/en-us/products/static-code-analysis-sast/overview

Mobile App Penetrationstesting

Tool	Haupteinsatzgebiet	Besondere Stärke	Stärke im Vergleich zu anderen Tools	Vergleichbare Tools	Download
MobSF	Statische und dynamische Analyse	Umfassende Analyse, benutzerfreundlich	Open Source, unterstützt Android und iOS	QARK, Appknox, NowSecure	github.com/MobSF/Mobile-Security-Framework-MobSF
Frida	Dynamische Instrumentierung	Mächtige Skriptsprache, flexible API	Ermöglicht tiefe Einblicke in App-Verhalten	Xposed Framework, Cydia Substrate	frida.re
APKTool	Reverse Engineering	Dekompiliert APK-Dateien, ermöglicht Code-Analyse	Open Source, einfach zu bedienen	JADX, dex2jar, Baksmali	ibotpeaches.github.io/Apktool/
jadx	Java Decompiler	Dekompiliert Java-Code, gut lesbarer Output	Open Source, schnell	JD-GUI, Procyon, CFR	github.com/skylot/jadx
Magisk Root	Rooting	Systemloses Rooting, erhält SafetyNet	Flexibel, viele Module verfügbar	SuperSU, KingoRoot, CF Auto Root	github.com/topjohnwu/Magisk
APKK	APK-Inspektion und	Einfache Bedienung	Open Source,	APK Studio,	github.com/xxczaki/a

Tool	Haupteinsatzgebiet	Besondere Stärke	Stärke im Vergleich zu anderen Tools	Vergleichbare Tools	Download
	-Modifikation	, viele Funktionen	benutzerfreundlich	Lucky Patcher	
Android Studio/Genymotion	Entwicklung und Debugging	Umfassende Entwicklungsumgebung, Emulation	Mächtige Tools, gute Integration	Eclipse, IntelliJ IDEA, Xamarin	developer.android.com/studio / genymotion.com
Drozer	Interaktion mit Android-Geräten	Framework für Sicherheitsassessments, viele Module	Spezialisiert auf Android-Sicherheit	MobSF, QARK	github.com/FSecureLABS/drozer
mitmproxy	Man-in-the-Middle-Proxy	Abfangen und Modifizieren von Netzwerkverkehr	Flexibel, Skriptfähigkeit	Burp Suite, Charles Proxy, Fiddler	mitmproxy.org
objection	Interaktion mit mobilen Apps	Mächtige Skriptsprache, viele Funktionen	Ermöglicht tiefgreifende Analysen	Frida, Xposed Framework	github.com/sensepost/objection
adb	Interaktion mit Android-Geräten	Vielseitig, Kommandozeilen-Tool	Standard-Tool für Android-Debugging	-	developer.android.com/studio/command-line/adb

Tool	Haupteinsatzgebiet	Besondere Stärke	Stärke im Vergleich zu anderen Tools	Vergleichbare Tools	Download
Cycript	Skriptsprache für iOS	Mächtige Sprache, Echtzeit-Interaktion	Ermöglicht dynamische Analyse	Frida, Hopper	cycript.org
iOS Hook	Hooking in iOS-Apps	Modifizieren von App-Verhalten	Mächtig, flexibel	Theos, Frida	-
Needle	Interaktion mit iOS-Apps	Framework für Sicherheitsassessments	Spezialisiert auf iOS-Sicherheit	-	github.com/FSecureLABS/needle
class-dump	Analyse von iOS-Apps	Extrahiert Objective-C-Klasseninformationen	Hilfreich für Reverse Engineering	Hopper, IDA Pro	stevenygard.com/projects/class-dump
Objection Mobile Assistant	GUI für Objection	Benutzerfreundliche Oberfläche	Vereinfacht die Nutzung von Objection	-	-
SSL kill Switch	Deaktivieren von SSL/TLS	Ermöglicht Analyse von verschlüsseltem Verkehr	Hilfreich für Man-in-the-Middle-Angriffe	NoRoot Firewall, SSL Unpinning	-
iMazing	iOS-Gerät emanage	Umfassende	Hilfreich für	iTunes, 3uTools	imazing.com

Tool	Haupteinsatzgebiet	Besondere Stärke	Stärke im Vergleich zu anderen Tools	Vergleichbare Tools	Download
	ment	Funktionen, Backup und Restore	Forensik und Datenextraktion		

API Penetrationstesting

Tool	Haupteinsatzgebiet	Besondere Stärke	Stärke im Vergleich zu anderen Tools	Vergleichbare Tools	Download
Postman	API-Entwicklung und -Testing	Benutzerfreundlich, viele Funktionen	Umfassendes Tool, große Community	Insomnia, SoapUI, REST-assured	postman.com
Insomnia	API-Entwicklung und -Testing	Plattformübergreifend, Open Source	Flexibel, erweiterbar	Postman, Paw, HTTPie	insomnia.rest
42Crunch API Security	API-Sicherheitstests	Umfassende Plattform, automatisiert	Integriert in CI/CD, skalierbar	Salt Security, Noname Security	42crunch.com
Swagger	API-Testin	Einfache	Hilfreich	Postman,	swagger.io

Tool	Haupteinsatzgebiet	Besondere Stärke	Stärke im Vergleich zu anderen Tools	Vergleichbare Tools	Download
Inspector	g und -Debugging	Bedienung, integriert in Swagger	für RESTful APIs	REST Client	/tools/swagger-inspector/
Kite Runner	API-Sicherheitstests	Automatisierte Tests, erkennt viele Schwachstellen	Spezialisiert auf API-Sicherheit	OWASP ZAP, Burp Suite	-
SecApps Intercept	API-Traffic-Analyse	Abfangen und Modifizieren von API-Verkehr	Hilfreich für Man-in-the-Middle-Angriffe	Burp Suite, mitmproxy	-

Secure Code Review

Tool	Haupteinsatzgebiet	Besondere Stärke	Stärke im Vergleich zu anderen Tools	Vergleichbare Tools	Download
SonarQube	Codequalität und -sicherheit	Umfassende Analyse, integriert in CI/CD	Plattformübergreifend, viele Plugins	Code Climate, Codacy	sonarqube.org

Tool	Haupteinsatzgebiet	Besondere Stärke	Stärke im Vergleich zu anderen Tools	Vergleichbare Tools	Download
Snyk	Schwachstellenanalyse	Open Source, integriert in Entwicklungstools	Einfache Bedienung, fokussiert auf Open-Source-Abhängigkeiten	Dependabot, WhiteSource	snyk.io
Semgrep	Statische Codeanalyse	Flexible Regeln, schnelle Analyse	Effizient, anpassbar	Brakeman, ESLint	semgrep.dev
Checkmarx	Statische und dynamische Codeanalyse	Umfassende Analyse, detaillierte Berichte	Skalierbar, integriert in SDLC	Fortify, Veracode	checkmarx.com
Veracode	Statische und dynamische Codeanalyse	Cloud-basiert, skalierbar	Einfache Integration, umfassende Sicherheitsüberprüfungen	Checkmarx, Fortify	veracode.com
Fortify WebInspect Audit	Statische Codeanalyse	Integriert in Fortify WebInspect, detaillierte Berichte	Umfassende Analyse, fokussiert auf Webanwendungen	Checkmarx, SonarQube	microfocus.com/en-us/products/static-code-analysis-sast/overview

Tool	Haupteinsatzgebiet	Besondere Stärke	Stärke im Vergleich zu anderen Tools	Vergleichbare Tools	Download
CodeQL	Codeanalyse	Mächtige Abfragesprache, flexible Analyse	Ermöglicht tiefgreifende Sicherheitsüberprüfungen	Semgrep, Joern	-
Bandit	Python-Codeanalyse	Open Source, einfach zu bedienen	Spezialisiert auf Python, erkennt gängige Schwachstellen	Flake8, Pylint	github.com/PyCQA/bandit
FindBugs	Java-Codeanalyse	Open Source, findet viele Fehlertypen	Spezialisiert auf Java, gut etabliert	PMD, SpotBugs	findbugs.sourceforge.net
GitLeaks	Analyse von Git-Repositories	Open Source, erkennt Datenlecks	Hilfreich für Sicherheitsüberprüfungen von Open-Source-Projekten	TruffleHog, detect-secrets	github.com/zricethezav/gitleaks

Thick Client Penetrationstesting

Tool	Haupteinsatzgebiet	Besondere Stärke	Stärke im Vergleich zu anderen Tools	Vergleichbare Tools	Download
Fiddler	Web Debugging	Abfangen und Modifizieren von HTTP-Traffic	Benutzerfreundlich, viele Funktionen	Charles Proxy, mitmproxy	-
dnSpy	.NET Debugging	Dekompilieren und Debuggen von .NET-Anwendungen	Open Source, mächtig	ILSpy, dotPeek	github.com/0xd4d/dnSpy
IDA Pro	Reverse Engineering	Mächtiger Disassembler und Debugger	Umfassende Funktionen, viele Architekturen unterstützt	Ghidra, Binary Ninja	-
Ghidra	Reverse Engineering	Open Source, umfangreiche Funktionen	Gute Alternative zu IDA Pro, aktiv entwickelt	IDA Pro, Radare2	ghidra-sre.org
Process Explorer	Prozessanalyse	Detaillierte Informationen über laufende Prozesse	Mächtig, zeigt Abhängigkeiten zwischen Prozessen	Task Manager, Process Hacker	-

Tool	Haupteinsatzgebiet	Besondere Stärke	Stärke im Vergleich zu anderen Tools	Vergleichbare Tools	Download
CFF Explorer	PE-Analyse	Analyse von PE-Dateien, Editieren von Ressourcen	Hilfreich für Reverse Engineering	PEview, Stud_PE	-
OllyDbg	Debugging	Benutzerfreundlich, viele Plugins	Klassischer Debugger, gut für Anfänger	x64dbg, Immunity Debugger	ollydbg.de
x64dbg	Debugging	Open Source, unterstützt 64-Bit	Moderner Debugger, aktiv entwickelt	OllyDbg, WinDbg	x64dbg.com
Wireshark	Netzwerkprotokollanalyse	Mächtiger Protokollanalysator, viele Filter	Standard-Tool für Netzwerkanalyse	tcpdump, tshark	wireshark.org

Netzwerk-Penetrationstesting

Tool	Hauptein satzgebiet	Besondere Stärke	Stärke im Vergleich zu anderen Tools	Vergleichb are Tools	Download
Nmap	Netzwerk- und Portscanni ng	Vielseitigk eit, Skriptfähig keit, große Communit y	Schnell, zuverlässi g, plattformü bergreifen d	Masscan, Zenmap, Angry IP Scanner	nmap.org
Wireshark	Netzwerkp rotokollana lyse	Mächtiger Protokolla nalysator, viele Filter	Standard-Tool für Netzwerka nalyse	tcpdump, tshark	wireshark. org
Metasploi t Framewor k	Exploit-Ent wicklung und -Ausführun g	Umfangrei che Exploit-Dat enbank, flexible Framewor k	Mächtig, vielseitig	Canvas, Core Impact	metasploit. com
Nessus	Schwachst ellenscann ing	Umfangrei che Schwachst ellendaten bank, automatisi ert	Kommerzi ell, zuverlässi g	OpenVAS, QualysGu ard	-
OpenVAS	Schwachst ellenscann ing	Open Source, aktive Communit y	Kostenlos e Alternative zu Nessus	Nessus, Nexpose	greenbone .net

Tool	Haupteinsatzgebiet	Besondere Stärke	Stärke im Vergleich zu anderen Tools	Vergleichbare Tools	Download
Responder	LLMNR/NBT-NS Poisoning	Einfache Bedienung, effektiv	Spezialisiert auf Windows-Netzwerke	Inveigh, mitm6	-
CrackMapExec	Post-Exploitation	Automatisierte Passwort-Cracking-Angriffe	Effizient, unterstützt verschiedene Protokolle	Mimikatz, Impacket	github.com/byt3bl33d3r/CrackMapExec
BloodHound	Active Directory-Analyse	Visualisierung von Angriffswegen	Hilfreich für Penetrationstests in Active Directory-Umgebungen	PingCastle, ADExplorer	-
Netcat	Netzwerkverbindungen	Vielseitig, einfach zu bedienen	"Schweizer Taschenmesser" für Netzwerkaufgaben	Socat, Ncat	-
Bettercap	Netzwerk-Monitoring und -Manipulation	Mächtig, modular	Umfassende Funktionen, erweiterbar	Ettercap, Wireshark	bettercap.github.io

Cloud-Sicherheit

Tool	Haupteinsatzgebiet	Besondere Stärke	Stärke im Vergleich zu anderen Tools	Vergleichbare Tools	Download
Prowler	AWS-Sicherheitsüberprüfung	Open Source, einfach zu bedienen	Spezialisiert auf AWS, erkennt viele Fehlkonfigurationen	ScoutSuite, Pacu	github.com/toniblyx/prowler
ScoutSuite	Cloud-Sicherheitsbewertung	Unterstützt mehrere Cloud-Anbieter, detaillierte Berichte	Umfassende Analyse, modular	Prowler, CloudSploit	-
CloudSploit	Cloud-Sicherheitsbewertung	Open Source, einfach zu bedienen	Spezialisiert auf AWS, Azure und GCP	Prowler, ScoutSuite	-
Pacu	AWS Post-Exploitation	Mächtiges PowerShell-Skript, viele Module	Hilfreich für Penetrationstests in AWS-Umgebungen	Prowler, Metasploit	github.com/RhinoSecurityLabs/pacu
SteamPipe	AWS-Ressourcenauf	Schnell, effizient	Hilfreich für	aws-cli, CloudMap	-

Tool	Haupteinsatzgebiet	Besondere Stärke	Stärke im Vergleich zu anderen Tools	Vergleichbare Tools	Download
	zählung		Information Gathering	per	
CloudMapper	AWS-Ressourcen-Mapping	Visualisierung von AWS-Ressourcen	Hilfreich für Sicherheitsanalyse	Prowler, ScoutSuite	-
NCC Group Scout	Cloud-Sicherheitsbewertung	Umfassende Analyse, detaillierte Berichte	Kommerziell, zuverlässig	ScoutSuite, CloudSploit	-
kube-bench	Kubernetes-Sicherheitsüberprüfung	Open Source, einfach zu bedienen	Spezialisiert auf Kubernetes, prüft Best Practices	kube-hunter, sonobuoy	github.com/aquasecurity/kube-bench

Container-Sicherheit

Tool	Haupteinsatzgebiet	Besondere Stärke	Stärke im Vergleich zu anderen Tools	Vergleichbare Tools	Download
Trivy	Schwachstellenscann	Open Source,	Unterstützt Container und	Clair, Anchore	github.com/aquasecu

Tool	Haupteinsatzgebiet	Besondere Stärke	Stärke im Vergleich zu anderen Tools	Vergleichbare Tools	Download
	ing	schnell	Kubernetes	Engine	rity/trivy
Aqua Microscanner	Schwachstellenscanning	Integriert in CI/CD, schnell	Spezialisiert auf Container	Trivy, Clair	github.com/aquasecurity/microscanner
Falco	Laufzeitsicherheit	Open Source, erkennt verdächtiges Verhalten	Hilfreich für Intrusion Detection	Sysdig Falco, Anchore Engine	falco.org
Sysdig	Monitoring und Sicherheit	Umfassende Plattform, detaillierte Einblicke	Kommerziell, mächtig	Datadog, New Relic	sysdig.com
Snyk	Schwachstellenanalyse	Open Source, integriert in Entwicklungstools	Einfache Bedienung, fokussiert auf Open-Source-Abhängigkeiten	Anchore Engine, JFrog Xray	snyk.io
Bench	Sicherheitsüberprüfung	Open Source, einfach zu bedienen	Prüft Kubernetes Best Practices	kube-bench, kube-hunter	-
kube-hunter	Sicherheitsüberprüfung	Open Source, findet	Spezialisiert auf Kubernete	kube-bench, sonobuoy	aquasec.github.io/kube-hunter

Tool	Haupteinsatzgebiet	Besondere Stärke	Stärke im Vergleich zu anderen Tools	Vergleichbare Tools	Download
		Fehlkonfigurationen	s		
Clair	Schwachstellenscanning	Open Source, API-basiert	Flexibel, integrierbar	Trivy, Anchore Engine	github.com/quay/clair
Anchore	Sicherheitsanalyse	Umfassende Plattform, Policy-basiert	Kommerziell, skalierbar	Trivy, Clair	anchore.com
Docker	Containerisierung	Standard-Tool für Containerisierung	Open Source, große Community	Podman, LXC	docker.com