Sales Engineer - Penetration Testing Technical Guide

🔧 Technical Fundamentals

Vulnerability Prevalence

- **94%** apps have broken access control (A01:2021)[1]
- **75%** mobile apps contain vulnerabilities[2]
- **95%** organizations have API security issues[3]
- **10-15** exploitable findings from 100-200 scan results[4]

OWASP Top 10 Quick Reference

Category	Business Impact	Our Solution
Broken Access Control	Data breach, privilege escalation	IAM, Zero Trust
Cryptographic Failures	Data exposure, compliance fail	Encryption, HSM
Injection	Database compromise	WAF, Input validation
Insecure Design	Unfixable by implementation	Secure SDLC
Misconfiguration	Cloud exposure, breach	CSPM, Hardening

🛠️ Testing Methodologies

OWASP WSTG[5]

- PCI DSS 4.0 requirement
- Application focus
- Industry standard

NIST SP 800-115[6,7]

- Federal/regulated required
- 4 phases: Plan→Discover→Attack→Report
- Audit-ready format

PTES[8]

- 7 comprehensive phases
- Professional grade
- Vendor-agnostic

🔍Testing Types - Technical Details

Web Application Testing

- **Scope**: OWASP Top 10, business logic, authentication
- **Tools**: Burp Suite (£399/yr), OWASP ZAP (free)
- **Duration**: 7-10 days active testing
- **Output**: 10+ manual findings typical

Mobile Testing

- **iOS**: Secure Enclave, sandboxing, sideloading risks[9]
- **Android**: Fragmentation, 3rd party stores[10]
- **Tools**: MobSF, Frida, Charles Proxy
- **Focus**: API security, data storage, platform-specific

Network Testing

- **External**: Perimeter, exposed services
- **Internal**: Lateral movement, segmentation
- **Tools**: Nmap, Metasploit, Nessus
- **Timing**: 1-2 weeks per environment

API Testing

- **OWASP API Top 10**: BOLA, authentication, rate limiting[11]
- **Tools**: Postman, Burp, custom scripts
- **Issues**: 10x more data exposed than web breaches[12]

📊Technical Approach Comparison

Approach	Info Provided	Coverage	Authenticity	Cost

Approach	Info Provided	Coverage	Authenticity	Cost
Black Box	None	Limited	Maximum	High
Gray Box	User access	Balanced	Good	Medium
White Box	Everything	Maximum	Limited	Low/scan

Key: 66% prefer Gray Box for balance[13]

🔬 Tool Categories & Leaders

Commercial (28% organizations use none)[14]

- **Burp Suite Pro**: Web app gold standard
- **Nessus**: 60K+ vuln signatures
- **Metasploit Pro**: 2,300+ exploits
- **Checkmarx/Veracode**: SAST integration

Open Source (72% rely on these)[14]

- **OWASP ZAP**: Free Burp alternative
- **Nmap**: 100% of network tests
- **SQLMap**: Database testing
- **MobSF**: Mobile all-in-one

PTaaS Trends

- Market: £118M→£301B by 2029[15,16]
- Benefits: 31% cost reduction, 96% higher ROI[16]
- Limits: No business logic, needs manual supplement

🎯 Quality Indicators

High-Quality Test Markers

✅ Manual validation (not just scan)
✅ Business logic testing
✅ Exploitation evidence (PoC)

✅CVSS + business context
✅Detailed remediation steps
✅Compliance mapping

Red Flags

❌Scanner output only
❌No manual findings
❌Generic recommendations
❌Missing evidence/PoC
❌No retest included

🔗Finding-to-Solution Mapping

Finding Type	Technical Detail	Our Solution
SQL Injection	DB query manipulation	WAF rules, parameterized queries
XSS	Script injection	CSP headers, output encoding
Broken Auth	Session/password issues	MFA, SSO, session management
API Abuse	Rate limiting, BOLA	API Gateway, throttling
Misconfig	Default settings, exposure	CSPM, hardening guides

📋Scoping Checklist

- □ Number of applications/APIs/IPs
- □ Authentication requirements
- □ Testing window constraints
- □ Production vs staging
- □ Data sensitivity levels
- □ Compliance requirements
- □ Previous findings to verify

🚀 Advanced Topics

Business Logic Examples

- Price manipulation (negative quantities)
- Workflow bypass (skip payment)
- Race conditions (double-spend)
- Authorization flaws (IDOR)[17,18]

Purple Teaming Value

- 30-40% detection improvement[19]
- Real-time blue/red collaboration
- 150-200% Year 1 ROI[19]
- MITRE ATT&CK aligned

Certifications That Matter

- **OSCP**: Gold standard, hands-on[20]
- **GWAPT**: Web app specialist
- **GPEN**: Network focus
- **CEH**: Entry level, DoD approved

💡 Technical Differentiators

1. Manual validation beyond scanning
2. Business logic focus
3. Chained exploit demonstration
4. Platform-specific expertise
5. Remediation verification included

🎪 Demo Talking Points

- Show scan vs manual finding comparison
- Explain false positive reduction
- Demo exploitation path (safely)
- Map findings to compliance
- Calculate specific customer ROI

References

1. OWASP Top Ten Project
2. Build38 - Mobile App Security Statistics 2024
3. Salt Security - API Breaches 2024
4. Industry analysis of vulnerability scanning vs. penetration testing
5. OWASP Web Security Testing Guide
6. NIST SP 800-115
7. RSI Security - NIST Penetration Testing
8. Penetration Testing Execution Standard
9. McAfee - iOS vs Android Security
10. Promon - Android vs iOS Security
11. OWASP API Security Top 10 2023
12. Salt Security - Gartner Market Guide
13. TestDevLab - Box Testing Types
14. Astra Security - Penetration Testing Statistics
15. Markets and Markets - PTaaS Market
16. BreachLock - CISO's Guide to PTaaS
17. Qwiet AI - Business Logic Testing
18. OWASP - Business Logic Vulnerability
19. Industry reports on purple teaming effectiveness
20. Offensive Security certification requirements