

● OFFENSIVE SECURITY CAPABILITIES // GENERAL EDITION

Comprehensive Penetration Testing Proposal

“Reaching Beyond the Limits of Automated Scanners.”

A rigorous, manual offensive security evaluation designed to identify, exploit, and eliminate high-impact vulnerabilities across your critical digital assets before real-world threat actors strike.

PRIMARY OBJECTIVE

**Risk Reduction &
Vulnerability Elimination**

Pre-Emptive Threat & Breach
Prevention

ASSESSMENT SPECTRUM

**Web, API, Network, Active
Directory & Cloud**

Full Attack Surface Evaluation

PRIMARY ENGAGEMENT CONTACT

pentest@rootmare.com

WhatsApp: +966 50 454 6141



DOCUMENT CLASSIFICATION

**Commercial & Technical
Offer**

Confidential & Restricted
Distribution

01 Executive Summary & Battle-Tested Track Record

We are pleased to present this technical penetration testing proposal on behalf of **RootMare Cyber Operations**. Unlike standard automated compliance scanners that only scratch the surface and flood teams with false positives, RootMare focuses entirely on **advanced manual offensive exploitation** that mirrors the tactics, techniques, and procedures (TTPs) of sophisticated modern threat actors.

Our operators bring hands-on offensive mastery forged in competitive global bug bounty programs and enterprise adversarial engagements. We identify architectural flaws, chain multi-tier attack vectors, and prove business risk with reproducible Proofs-of-Concept before real attackers strike.

Every finding is vetted by senior offensive security engineers, accompanied by pinpoint code-level remediation steps and backed by an inclusive re-testing cycle to ensure permanent vulnerability mitigation.

370+

Verified Vulnerabilities Responsibly Disclosed
Across Major Global Platforms

Top Tier

Global Bug Bounty & Corporate Hall of Fame
Standing Worldwide

02 Approach & 4-Phase Offensive Methodology

RootMare employs an adversarial 4-phase offensive methodology engineered to simulate sophisticated real-world threat actors with zero automated noise:

Phase 01

Planning & Reconnaissance

Scoping alignment, intelligence gathering, OSINT analysis, attack surface enumeration, and communications setup.

- Asset mapping & port fingerprinting
- API schema ingestion & endpoint discovery
- Safe harbor and rules of engagement

Phase 02

Vulnerability Analysis & Exploitation

Deep manual offensive testing targeting business logic, authentication bypasses, chained privilege escalation, and custom exploits.

- Manual parameter & token tampering
- Chaining low/medium bugs into critical RCE
- True positive exploit validation

Phase 03

Reporting & Risk Assessment

Synthesis of verified vulnerabilities into an executive briefing alongside detailed engineering remediation documentation.

- CVSS v3.1 scoring & risk prioritization
- Step-by-step reproducible PoCs & curls
- Actionable source code fix guidance

Phase 04

Post-Fix Verification (Re-Test)

Rigorous follow-up re-testing of remediated endpoints within 30 days to verify and certify complete resolution.

- Regression testing against bypasses
- Final Verification Letter of Attestation
- Confirmed security posture upgrade

03

Key Deliverables & Indicative 10-Day Timeline

DELIVERABLE 01

Comprehensive Pentest Report

Executive presentation for C-level leadership alongside an exhaustive technical breakdown for engineers: CVSS v3.1 scores, verified Proof-of-Concepts (PoCs), attack chain narratives, and pinpoint code remediation guidance.

DELIVERABLE 02

Developer Remediation Debrief

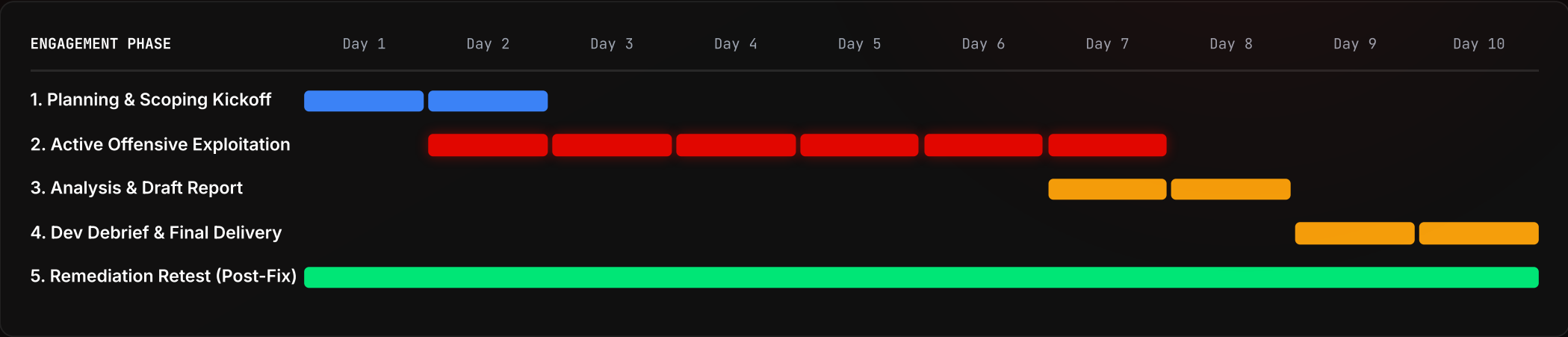
Interactive engineering workshop with RootMare offensive operators. We walk your engineering team through root causes, review fix implementations, and eliminate risk regressions before going live.

DELIVERABLE 03

Post-Fix Verification & Re-Test

A comprehensive follow-up assessment executed after fixes are deployed to verify that every reported vulnerability has been effectively closed. We issue an official *Letter of Attestation* for client audits.

INDICATIVE 10-DAY ENGAGEMENT SCHEDULE:



04 The Engagement Team & Security Leadership

Our 6 dedicated offensive security operators bring specialized expertise across cloud architectures, enterprise networks, Active Directory topologies, web/API systems, and technical engagement advisory:



Ahmed Tamer

Principal Penetration Tester & Lead

Cloud Pentest

Active Directory

Network Pentest

Web Pentest

API Pentest

Specialized in complex Active Directory forest compromise, multi-cloud IAM privilege escalation, and deep web/API vulnerability analysis. Uncovered over 70+ verified vulnerabilities in bug bounty programs.



Mostafa Nasser

Senior Offensive Security Engineer

Mobile Pentest

Cloud Pentest

Web Pentest

API Pentest

Network Pentest

Senior offensive researcher specializing in mobile application reversing (iOS/Android), cloud security evaluations, and deep web API exploitation. Discovered over 100+ verified vulnerabilities.



Seif Mohammed

Penetration Tester & Vulnerability Researcher

Web Pentest

API Pentest

Network Pentest

Cloud Pentest

Offensive penetration tester specialized in complex business-logic flaws, authentication bypasses, and network lateral pivoting. Disclosed over 70+ verified vulnerabilities in enterprise environments.



Youssef Mohammed

Penetration Tester & Infrastructure Analyst

Web Pentest

API Pentest

Network Pentest

Cloud Pentest

Focuses on modern microservice architectures, API authorization auditing (BOLA/BFLA), container security, and network infrastructure penetration testing with manual exploit analysis.



Sami Alhosani

Primary Engagement Contact & Specialist

Web Pentest

API Pentest

Cloud Pentest

Directs technical engagement scoping, risk assessment communication, and client remediation roadmaps. Based in Riyadh with expertise aligning penetration testing with regional compliance standards.



Youssef Ghareeb

Technical Engagement & Solutions

Scoping & Discovery

Technical Advisory

Client Relations

Bridges the gap between technical offensive operations and business stakeholders. Specializes in translating complex client infrastructure requirements into actionable testing scopes, ensuring seamless engagement lifecycle management from initial discovery to executive debriefs.

05

Companies We Helped Securing

As an elite offensive collective, RootMare operators have been officially acknowledged and inducted into the Corporate Halls of Fame for global institutions, government agencies, and Fortune 500 industry leaders:

Microsoft

Security Hall of Fame

Gov. of Singapore

GovTech Vulnerability
Disclosure

NASA

Vulnerability Acknowledgment

Atlassian

Corporate Hall of Fame

PepsiCo

Responsible Disclosure
Acknowledged

Mars

Corporate Hall of Fame

GEICO

Vulnerability Disclosure
Acknowledged

Wix

Security Researcher Hall of
Fame

Initiate Your Security Assessment

Connect directly with our penetration testing team to discuss scope, timelines, and deliverables.



Chat on WhatsApp



pentest@rootmare.com