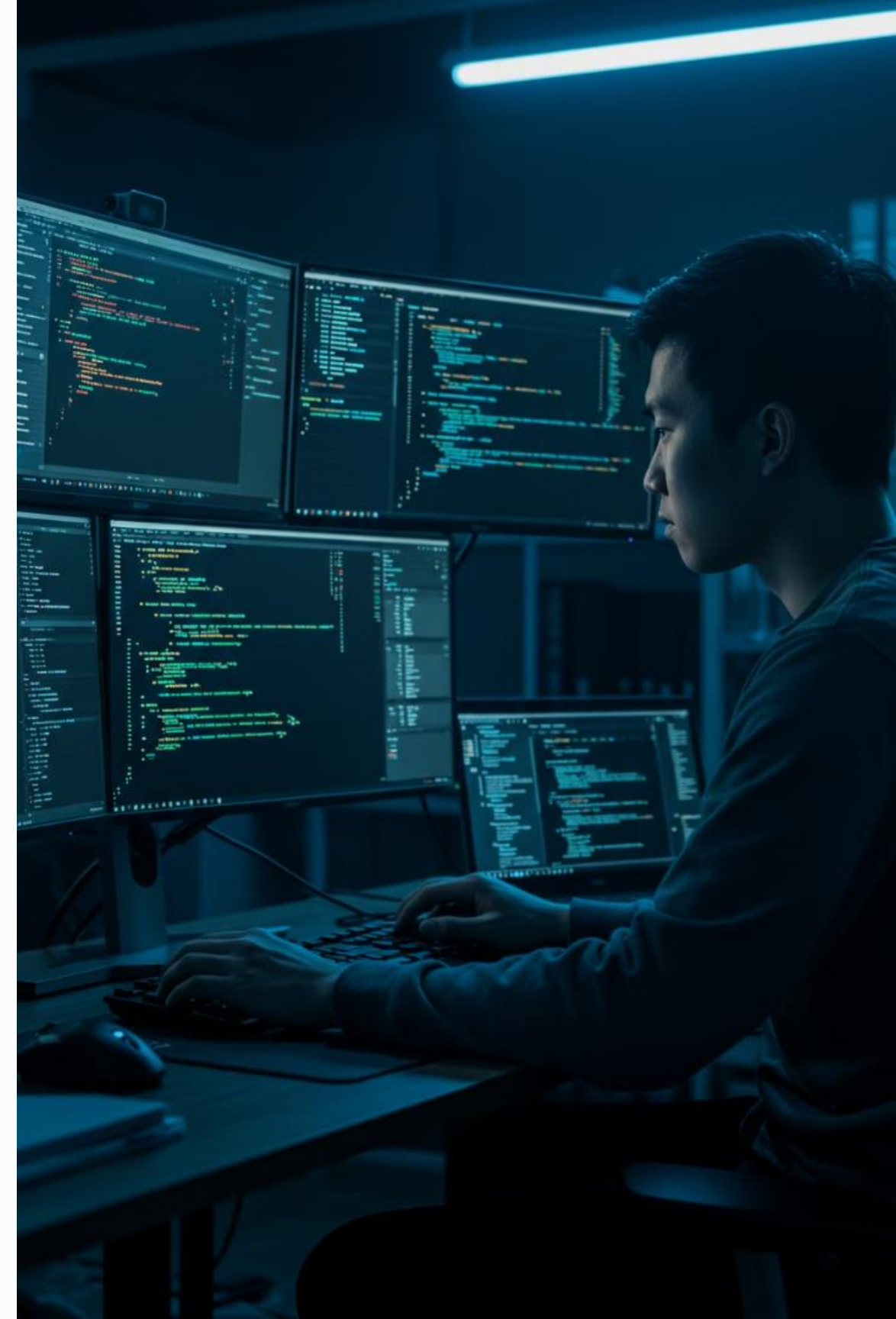


Web Application Penetration Testing

Our comprehensive security assessment methodology is designed to identify vulnerabilities in your web applications before malicious attackers can exploit them. By proactively uncovering security weaknesses, we help protect your sensitive data and maintain your customers' trust.

We follow industry-standard approaches based on OWASP (Open Web Application Security Project) guidelines, utilising specialised tools and techniques to thoroughly evaluate your web applications' security posture. Our expert team combines automated scanning with manual expertise to deliver actionable insights that strengthen your security defences.

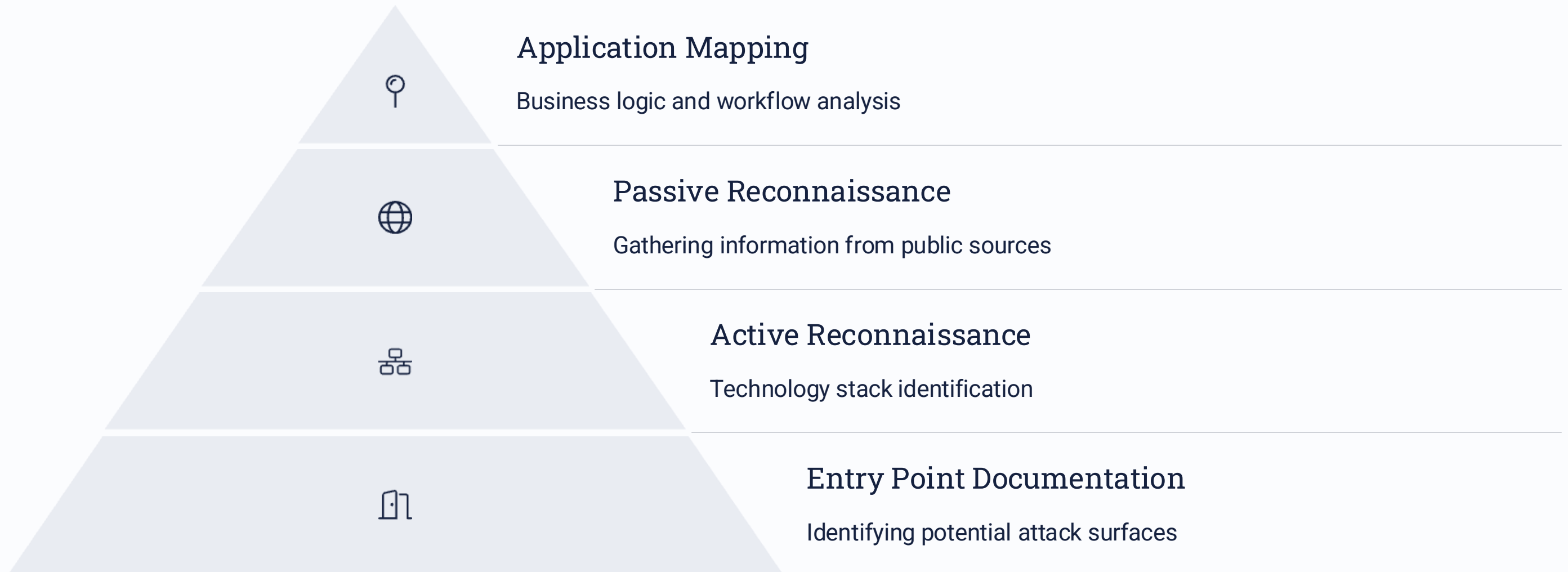


Our Penetration Testing Methodology



Our four-phase approach ensures comprehensive security testing by combining automated scanning with manual expertise. We align with the OWASP Application Security Verification Standard to simulate real-world attack scenarios, providing maximum protection for your web applications.


Phase 1: Information Gathering & Reconnaissance



The first phase establishes the foundation for our testing by defining the target scope and boundaries. We map the application's business logic and workflows to understand how it functions. This involves both passive information gathering using publicly available resources and active reconnaissance to identify the technology stack.



Phase 2: Scanning & Vulnerability Assessment

-  **Port Scanning**
Network enumeration using Nmap to identify open services and potential entry points
-  **Web Crawling**
Automated mapping of application structure and functionality
-  **Vulnerability Scanning**
Using specialised tools to identify potential security weaknesses
-  **Risk Prioritisation**
Categorising findings based on severity and exploitability

In the scanning phase, we employ a variety of tools to systematically identify potential vulnerabilities. This includes port scanning with Nmap, web crawling for application mapping, and targeted vulnerability scanning. Our team analyses each potential issue and prioritises them based on risk level and exploitability, creating a roadmap for further testing.

Phase 3: Exploitation & Research

Manual Verification

Our security experts manually verify each discovered vulnerability to eliminate false positives and confirm actual security issues. This hands-on approach ensures that only legitimate concerns are reported.

Business Logic Testing

We identify flaws in the application's business logic that automated tools might miss. This includes testing for insecure direct object references, privilege escalation, and workflow bypass vulnerabilities.

Authentication Testing

Comprehensive testing of authentication mechanisms to identify weaknesses in password policies, session management, and multi-factor authentication implementations that could lead to unauthorised access.

Input Validation

Thorough assessment of how the application handles various inputs, testing for vulnerabilities like SQL injection, cross-site scripting (XSS), and command injection that could compromise data security.

The exploitation phase involves attempting to leverage discovered vulnerabilities to determine their real-world impact. Our ethical hackers use controlled exploitation techniques to demonstrate how attackers might compromise your systems, providing concrete evidence of security weaknesses.

Phase 4: Reporting & Remediation

Vulnerability Documentation

Comprehensive documentation of all identified vulnerabilities, including detailed technical descriptions, impact assessments, and reproduction steps. Each finding is categorised by severity and exploitability.

Remediation Recommendations

Detailed, actionable guidance for fixing each vulnerability, including code examples, configuration changes, and best practices. Recommendations are tailored to your specific technology stack and environment.

Post-Remediation Support

Ongoing assistance during the remediation process, including verification testing to ensure vulnerabilities have been properly addressed. Our team remains available to answer questions and provide guidance.

The final phase delivers clear, comprehensive reporting that communicates findings effectively to both management and technical teams. Our reports include an executive summary with risk overview, alongside detailed technical documentation for developers. We prioritise vulnerabilities based on severity and provide specific remediation steps for each issue.

Tools We Utilise

Burp Suite Professional

Our primary web application testing platform, providing intercepting proxy capabilities, automated scanning, and a suite of specialised tools for manual testing. Enables our team to observe and modify traffic between browser and application.

OWASP ZAP

Open-source security tool that finds vulnerabilities in web applications during development and testing. Particularly effective for OWASP Top 10 vulnerability detection and automated scanning.

Specialized Tools

We employ various specialised tools including SQLMap for SQL injection testing, Metasploit for exploitation verification, and custom scripts developed for specific testing scenarios and unique application requirements.

Our toolset combines industry-standard solutions with custom-developed scripts to ensure comprehensive coverage. We continuously update our toolkit to address emerging threats and techniques used by malicious actors.

Sample Deliverables

Document Type	Target Audience	Key Contents
Executive Summary	Management & Stakeholders	Overview of findings, risk assessment, strategic recommendations
Technical Report	Security & Development Teams	Detailed findings, reproduction steps, code examples
Remediation Guide	Development Team	Step-by-step fix instructions, best practices, verification criteria
Retest Report	All Stakeholders	Validation of fixes, remaining issues, security posture improvement

Our comprehensive reporting provides clear documentation of all findings, with different formats tailored to various stakeholders. Executive summaries offer high-level risk assessments, while technical reports provide detailed evidence and reproduction steps. Each vulnerability includes specific remediation guidance and verification criteria.

After remediation, we provide retest validation to ensure issues have been properly addressed, completing the security improvement cycle.

Benefits of Our Approach



Comprehensive Security Coverage

Our methodology addresses all OWASP Top 10 vulnerabilities plus numerous other security risks, providing thorough protection for your web applications.



Continuous Improvement

Our framework enables ongoing security enhancement through actionable guidance and knowledge transfer to your team.



Business Logic Expertise

We go beyond automated scanning to identify complex business logic flaws that tools alone cannot detect, finding the vulnerabilities that matter most.



Regulatory Compliance

Our testing helps meet requirements for PCI DSS, HIPAA, GDPR, and other regulations, reducing compliance risks and potential penalties.

By partnering with our penetration testing team, you gain access to security expertise that substantially reduces the risk of data breaches and security incidents. Our approach provides actionable insights that not only address immediate vulnerabilities but also strengthen your overall security posture for the long term.

The detailed remediation guidance we provide helps your development team implement fixes correctly the first time, minimising security-related rework and ensuring efficient use of resources.