breachlock

AUGUST
2025

Penetration Testing Intelligence Report

2025

A DATA-DRIVEN LOOK AT REAL-WORLD VULNERABILITIES FROM 4,200+ PENTESTS MAPPED TO MITRE ATT&CK® AND OWASP ACROSS KEY INDUSTRIES.

BreachLock.com

Table of Contents

FOREWORD

Agentic AI. Expanding Surfaces. No Excuses.

The pace of innovation has never been higher—and neither has the sophistication of adversaries. The emergence of **agentic AI** and **vibe coding** is transforming how applications are built, deployed, and ultimately exploited. These dynamic, automated development methods are expanding the attack surface at unprecedented speed—well beyond the scope of traditional security controls. Yet, many organizations are adopting them without fully understanding their security implications.

At BreachLock, we've conducted over **4,000 penetration tests** in the past 12 months. What sets our approach apart is how we **anchor our testing in real-world threat intelligence**, tailoring test cases and red team engagements to the unique business context, tech stack, and threat model of each client. This ensures our findings aren't just generic—they're strategically relevant and immediately actionable.

We've seen this pattern before. A decade ago, many resisted cloud adoption, citing concerns about data control and residency. Today, those same doubts are resurfacing with AI. But just as the cloud became an operational necessity, intelligent automation and agentic solutions will soon be indispensable to defend against ever-evolving threats. Security must evolve in lockstep—with humans and machines working together.

This **4th edition of the BreachLock Annual Penetration Testing Intelligence Report**, first published in 2022, goes beyond surface-level vulnerability reporting. It offers a data-driven blueprint for proactive defense, mapping out attacker behaviors, misconfiguration trends, and emerging exploit techniques observed across thousands of real engagements.

We're especially proud that our data contributed to the **2025 Verizon Data Breach Investigations Report (DBIR)**—a testament to the value and rigor of our insights.

Cybersecurity is no longer about reacting to yesterday's threats. It's about preparing for tomorrow's. That requires **continuous validation**, continuous learning, and continuous adaptation. We hope this report serves as a compass for CISOs and security leaders navigating an increasingly agentic and adversarial digital landscape.

Seemant Sehgal
Founder & CEO, BreachLock

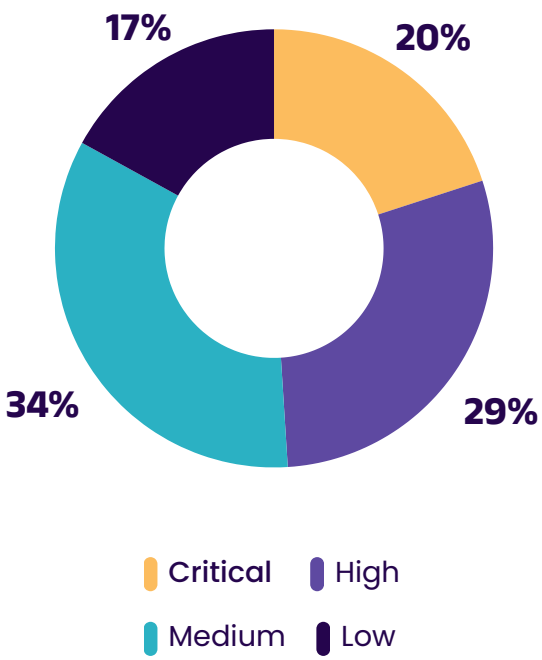
Seemant Sehgal

HIGHLIGHTS

In our 2025 report, BreachLock analyzed anonymized threat intelligence from over 4,200 global penetration tests conducted over the past 12 months. We examined affected assets and the prevalence and severity of their associated vulnerabilities across key industries, also taking enterprise size and geography into consideration to determine if there were related influencers.

We've chosen again this year to include MITRE ATT&CK® adversary tactics and techniques, which are a key component of the BreachLock framework, to demonstrate how our real-world observations and data align. We also examined and drew comparisons between BreachLock threat intelligence and exploits compared to OWASP Top 10 categories by asset-specific vulnerabilities across key industries.

Overall Risk Severity of Vulnerabilities



Key Findings

45% of findings (Critical + High) could lead to significant compromise without layered defenses.

- Remote code execution, unauthenticated admin access
- Broken access control, credential reuse, and SQL injection

Medium-risk issues often enabled privilege escalation or lateral movement during red team engagements.

- Insecure API endpoints, misconfigured permissions

Low and **Informational** findings are often overlooked but still aid reconnaissance and chaining.

- Information disclosure, outdated software (non-critical)
- Banner grabbing, exposed internal IPs, verbose errors

Top 5 Most Impacted Industries

Top 3 Critical Vulnerabilities

1	**Unauthenticated Remote Administrative Access**	• A01:2021 – Broken Access Control • A07:2021 – Identification & Authentication Failures • A05:2021 – Security Misconfiguration
2	**Remote Code Execution (RCE) Vulnerabilities**	• A1:2021 – Broken Access Control • A8:2021 – Software and Data Integrity Failures • A5:2021 – Security Misconfiguration
3	**Privilege Escalation via Misconfigured Access Controls**	• A1:2021 – Broken Access Control • A8:2021 – Software and Data Integrity Failures • A5:2021 – Security Misconfiguration

Top 5 Overall Security Issues in Web Applications

1. Broken Access Control
2. Injection Flaws (SQL, NoSQL, Command Injection)
3. Cross-Site Scripting (XSS)
4. Security Misconfiguration
5. Insecure Authentication and Session Management

OWASP Top 10 Mapping

OWASP®

Most Frequently Exploited Categories:

- **A01** (Broken Access Control)
- **A05** (Security Misconfiguration)
- **A02** (Cryptographic failure)

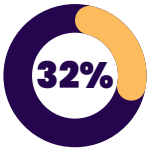
Emerging Focus Areas in 2025:

- **A04** (Insecure Design) due to poor architecture decisions in rapidly scaled SaaS environments.
- **A08** (Software/Data Integrity Failures) due to supply chain and CI/CD threats.

Risk Landscape Summary

Over the last year, penetration testing engagements across diverse industry sectors revealed a risk landscape heavily influenced by cloud adoption, remote access expansion, and legacy system exposure. A significant portion of tested environments exhibited vulnerabilities across both application and infrastructure layers, underscoring persistent gaps in access control, system hardening, and secure development practices.

Key Risk Observations



Broken Access Control emerged as the most prevalent and critical issue, accounting for **32%** of high-severity findings, often enabling unauthorized access and privilege escalation.

Security Misconfigurations were widespread in cloud and hybrid environments, with misconfigured storage, exposed administrative interfaces, and default credentials identified in **52%** of tested systems.

Authentication and Session Management Failures were frequently exploited, particularly in external assessments, where weak or missing multi-factor authentication and insecure token handling were observed.

Injection Attacks, especially SQL and command injections, remained relevant in poorly validated APIs and legacy applications, enabling direct compromise or data exfiltration.

Insecure Design and **Legacy Components** contributed to systemic risk, especially in organizations with rapid DevOps pipelines or unsegmented OT/IT infrastructure.

The convergence of these risks reflects a continued challenge in applying secure architecture principles and enforcing consistent security controls across modern, distributed environments. Notably, **red team simulations** revealed a **median time of 2.5 hours to achieve lateral movement**, highlighting the importance of detection and response maturity alongside preventative controls.

Industry Impact Highlights

Over the past 12 months, over 4,200 penetration testing engagements were conducted across a wide spectrum of industry sectors. The following summary outlines the proportional industry coverage and key exposure trends observed:

Industry	% of Total Engagements	Key Risk Exposures
Banking & Financial Services	**21%**	Insecure APIs, credential stuffing, and lateral movement
Healthcare	**11%**	Phishing success, unpatched systems, and flat networks
Technology & SaaS	**27%**	Cloud misconfigurations, token leakage, and weak IAM
Manufacturing	**3%**	Legacy SCADA, OT/IT bridging, and exposed services
Education	**4%**	Public admin panels, lack of MFA, and social engineering
Retail & Consumer Goods	**17%**	API rate limit abuse and insecure payment flows
Government & Public	**1%**	Authorization bypass and outdated protocols
Energy & Utilities	**9%**	Unsegmented networks and credential reuse
Logistics & Transport	**3%**	Wi-Fi exposure and weak physical security
Media & Entertainment	**4%**	Misconfigured CDNs and excessive permissions

Observational Summary:

- **Banking & Financial Services and Technology & SaaS sectors, together, accounted for 56%** of all penetration tests, driven by high compliance and threat exposure requirements.
- **Cloud-related vulnerabilities** were present in over **52% of all engagements**, particularly in Technology, Retail & Consumer Goods.
- **Manufacturing and critical infrastructure** showed significant weaknesses in legacy system protection and network segmentation.
- **Education and Government** faced elevated risks due to outdated authentication mechanisms and exposed admin interfaces.

INTRODUCTION

Welcome to the BreachLock Penetration Testing Intelligence Report, 2025.

This year's report draws from our largest and most diverse dataset to date, analyzing insights from 4,200+ penetration tests across a broad spectrum of industries, asset types, and global environments.

In 2025, real-world exploitability rose sharply across sectors, fueled by a convergence of outdated systems, cloud misconfigurations, and increasingly sophisticated multi-step attack chains.

While phishing has remained the most common entry point, credential abuse and lateral movement, such as OS credential dumping and valid account usage, continue to dominate post-compromise behavior.

As Penetration Testing as a Service (PTaaS) continues to gain traction, many organizations are shifting from periodic assessments to more integrated, ongoing testing strategies. This shift reflects a broader move toward continuous threat exposure management (CTEM), where pentesting plays a central role in proactively identifying exploitable risks. When paired with techniques like Adversarial Exposure Validation (AEV), testing can surface not just vulnerabilities, but the attack paths most likely to be exploited.

The findings in this report are intended to inform smarter risk decisions by highlighting which vulnerabilities are most likely to be exploited, where defensive gaps persist, and how adversary behavior is evolving. DevOps teams should be empowered to prioritize fixes based on impact, minimize noise from low-value findings, and adopt a more adaptive, threat-driven approach to defense. These results underscore the importance of penetration testing as more than a point-in-time activity, but a strategic mechanism for aligning security efforts with real-world risk.

Methodology & Scope

Over the past year, several key cybersecurity trends have significantly increased the demand for penetration testing (pentesting). These trends stem from evolving threats, stricter regulations, and emerging technologies such as:

1. Rapid Cloud Adoption & Misconfigurations: Organizations are increasingly shifting to multi-cloud and hybrid environments (AWS, Azure, GCP).

2. Proliferation of AI & LLMs: Companies deploying AI/LLM-based tools and APIs face new, poorly understood risks (e.g., prompt injection, data leakage).

3. API & Microservices Exposure: APIs have become the backbone of modern apps, and attacks targeting them (like Broken Object Level Authorization - BOLA) are rising.

4. Stricter Regulatory Requirements (e.g., DORA, NIS2, SEC Rules): New or updated regulations now require proactive threat testing and incident readiness.

5. More Sophisticated Phishing & Social Engineering: Deepfakes and AI-generated phishing have raised the bar.

REPORT SCOPE

4200+ PENTESTS
Performed Globally

12-Month Timeframe

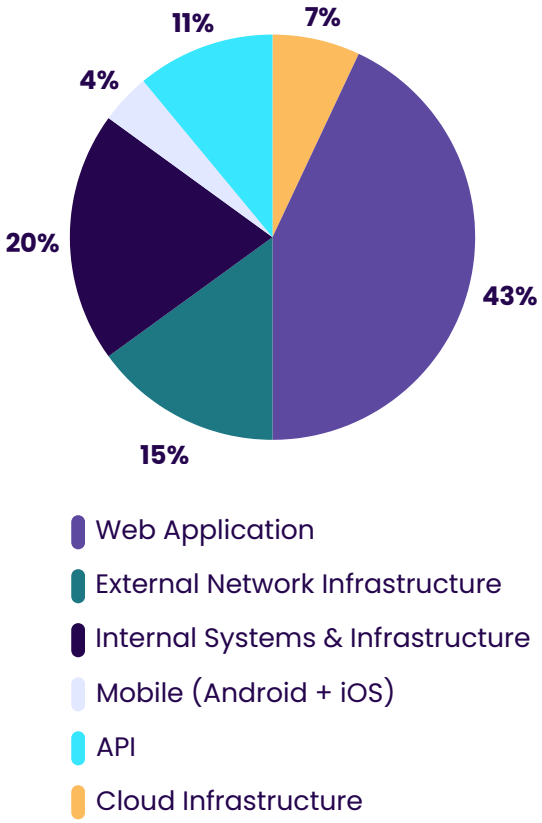
Assets Included

- Web Applications
- APIs
- Mobile Applications
- Cloud Infrastructure
- Internal Networks
- External Networks
- IoT Devices

Industries Covered

- Financial Services
- Education
- Healthcare
- IT & Prof. Services
- Manufacturing
- Media Services
- Public Sector
- Retail & eCommerce
- Telecommunications

Assets Tested in Last 1 Year



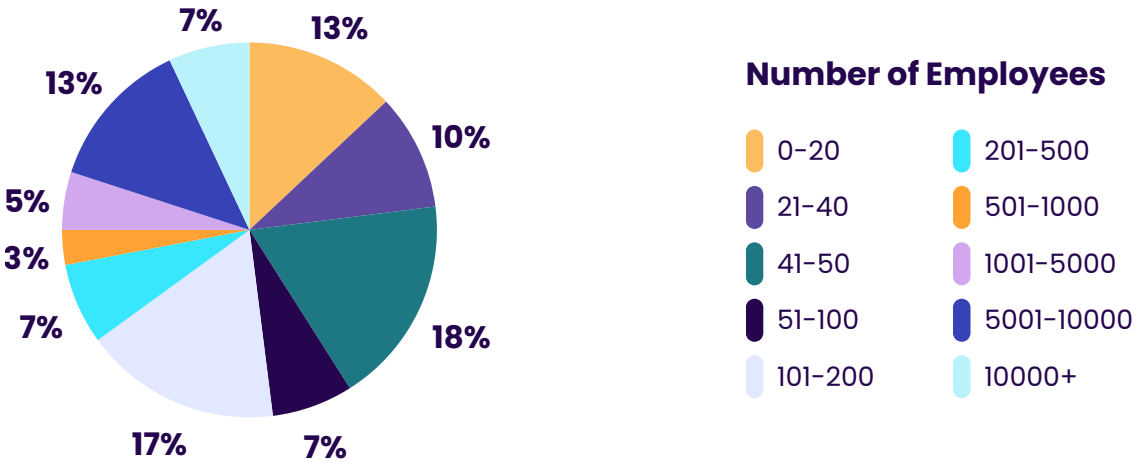
Demographics

When analyzing enterprise segments for a pentesting report, it's crucial to identify and evaluate the distinct areas within the organization that are most susceptible to cyber threats.

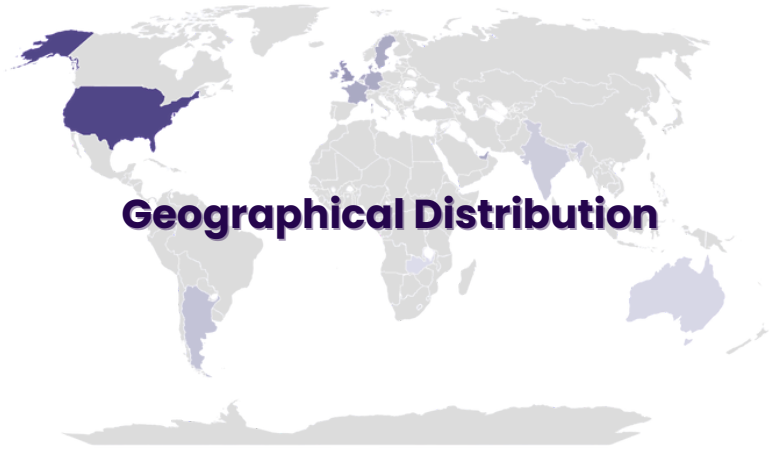
Over the past 12 months, similar to what we observed in 2024, we have seen a continued increase in interest from large enterprises to conduct penetration testing as part of their offensive security strategy. Large enterprises typically have vast and intricate IT infrastructures, including numerous applications, networks, and systems.

Continuous penetration testing can automate the pentesting process and handle this scale more efficiently, ensuring comprehensive coverage. This positive trend indicates an understanding that continuous Pentesting allows enterprises to identify and address vulnerabilities in real-time, perform tests much faster, and enable more frequent assessments, which is crucial when changes in IT environments occur regularly.

Company Size Distribution



Geographical Distribution



MITRE ATT&CK® Techniques

MITRE ATT&CK is a global knowledge base of adversary tactics and techniques based on real-world observations. BreachLock uses the latest ATT&CK data to enhance our pentesting methodologies. This allows certified pentesters to define multiple attack paths and provide a comprehensive overview of potential exploitation routes for critical vulnerabilities.

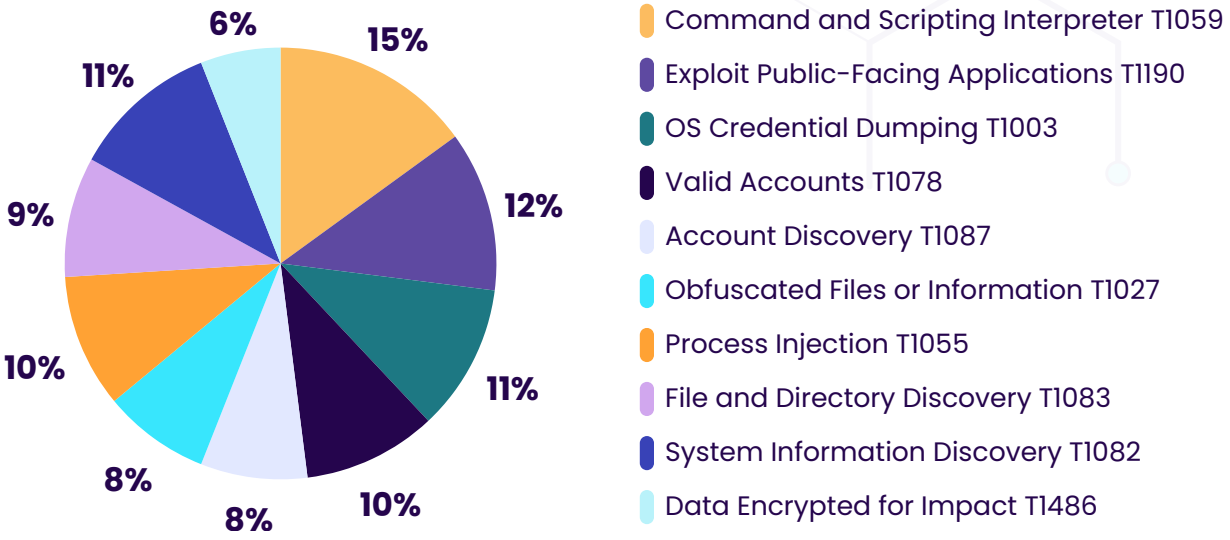
Alignment with ATT&CK Data

Below are ten of the most commonly exploited MITRE ATT&CK techniques discovered in our 2025 pentesting findings, along with the estimated prevalence by percentage.

Technique Name	Technique ID	Usage
Command and Scripting Interpreter	**T1059**	Used to execute PowerShell, Bash, CMD, etc. Very common in payload and post-exploitation scripting.
Exploit Public-Facing Applications	**T1190**	Attackers (and pentesters) exploit vulnerabilities in internet-facing services (e.g., web servers, APIs) to gain an initial foothold.
OS Credential Dumping	**T1003**	Used to extract credentials from memory
Valid Accounts	**T1078**	Pentesters often use harvested or reused credentials for lateral movement.
Account Discovery	**T1087**	Used to enumerate users and groups to find privileged accounts.
Obfuscated Files or Information	**T1027**	Techniques to make code/payloads harder to detect or analyze.
Process Injection	**T1055**	Used to run malicious code in the context of legitimate processes.
File and Directory Discovery	**T1083**	Lists and explores files and folders for sensitive data (e.g., credentials, financial info), config files.
System Information Discovery	**T1082**	Gathers basic host details: OS version, architecture, hostname, domain, logged-in user.
Data Encrypted for Impact	**T1486**	Typical ransomware behavior, but also simulated in pentests to test incident response.

Top 10 MITTE ATT&CK Techniques

Mapping to MITRE ATT&CK ensures that each finding reflects real-world attacker behavior. By aligning vulnerabilities with the most common and impactful techniques, organizations can prioritize remediation based on actual threat likelihood, validating the relevance and severity of our threat findings. By identifying vulnerabilities associated with the most common and impactful attack techniques, organizations can prioritize their remediation efforts to address the most critical and probable threats first. These are the most common techniques we identified in 2025.



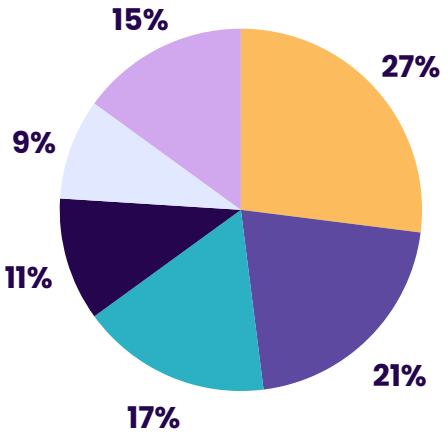
Industry Overview

Over the past year, penetration testing engagements across industries have revealed a consistent rise in real-world exploitability, driven by the convergence of outdated systems, cloud misconfigurations, and increasingly sophisticated attack chains. Phishing remains the most common initial access vector, while credential abuse and lateral movement techniques like OS credential dumping and valid account usage are frequently observed. Cloud environments continue to expose critical risks—especially in over-privileged IAM roles and exposed storage—while API testing uncovered rampant access control failures. Web application vulnerabilities, including injection flaws and business logic bypasses, remain widespread, despite increased developer awareness. These findings underscore a pressing need for proactive, threat-informed defense strategies and continuous security validation across the digital stack.

In the past year, offensive security requirements have evolved rapidly across sectors, shaped by unique threat landscapes and compliance demands. **Technology and SaaS providers** are emphasizing red teaming, cloud-native security testing, and AI/LLM abuse simulations to secure dynamic, multi-tenant environments. **Banking and financial services** demand advanced adversary emulation, phishing resilience assessments, and PCI-focused web/API testing due to heightened regulatory scrutiny.

Retail and consumer goods organizations prioritize API security, attack surface management, and social engineering defense amid increased digital transactions and omnichannel exposure. **Healthcare organizations**, facing sensitive data risks, are investing in medical device pentesting, ransomware simulations, and insider threat modeling. Meanwhile, **energy and utilities** firms are integrating OT/ICS penetration testing and scenario-based threat modeling into their programs to align with national critical infrastructure standards. This industry-specific focus reflects a broader shift from point-in-time testing to continuous, intelligence-driven offensive security.

Top 5 Most Impacted Industries



- **Technology & SaaS Providers**
- **Banking & Financial Services**
- **Retail & Consumer Goods**
- **Healthcare**
- **Energy & Utilities**
- **Other** (Education, Manufacturing, Gov. & Public Sector, Telecommunications, Media & Entertainment, etc.)

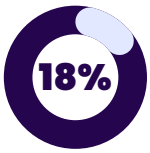
Industry Overview

In 2025, we observed an increased presence of **Security Misconfigurations** in **Technology & SaaS Providers,** identified in **24%** of applications in this sector. We also observed a **400% spike** in **critical API vulnerabilities**, highlighting poor access control, logic flaws, and insecure exposure.

The majority of vulnerabilities identified in the **Banking & Financial Services** sector fall within the OWASP Top 10 categories, with Broken Access Control, Injection flaws, and Security Misconfigurations representing the most prevalent. **Broken Access Controls** were present in **22%** of all applications within this sector.

This year, we observed a notable **increase in medium-level findings** in the **Retail & Consumer Goods** sector due to outdated third-party libraries and API misconfigurations in cloud-based retail services. **Cryptographic Failure**-related issues were also identified in **15%** of applications in this sector.

In the **Healthcare** sector, the **OWASP Top 10** categories most frequently identified —Broken Access Control (22%), Security Misconfiguration (17%), and Cryptographic Failures (14%)—underscore **systemic issues in identity management, data protection, and secure deployment practices**.



In the **Energy & Utilities** sector, **Medium and High** severity issues dominated due to widespread use of **legacy systems** and **inadequate OT security controls**. **Broken Access Control**-related issues were also identified in **18%** of applications in this sector.

Overall Recommendations

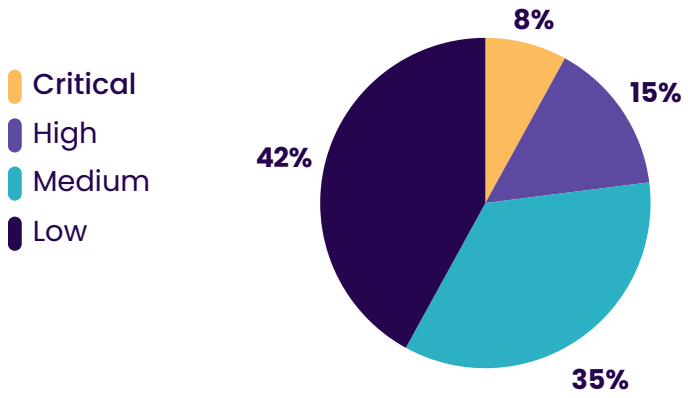
- Integrate ongoing pentesting, adversarial simulations, and threat-informed defense exercises into the software lifecycle.
- Prioritize API & Identity security by enforcing strict access controls, session management, and conducting API-specific testing as part of routine assessments.
- Prioritize remediation efforts based on risk context, focusing on high-impact, easily exploitable flaws like access control failures, insecure configurations, and exposed secrets first.

Technology and SaaS Providers

In the past year, Technology and SaaS companies have significantly expanded the depth and frequency of their penetration testing programs, driven by rapid cloud adoption, aggressive DevOps cycles, and growing customer demand for security transparency. There has been a notable shift from traditional perimeter testing to continuous, threat-informed assessments targeting CI/CD pipelines, third-party integrations, and multi-tenant cloud architectures. Red team simulations and assumed breach scenarios have become integral, focusing on post-compromise persistence, privilege escalation, and lateral movement across containerized and serverless environments. Additionally, SaaS providers increasingly require testing against modern threats such as business logic abuse, API over-permission, and AI/LLM prompt injections, reflecting the complexity of their platforms. This trend highlights a move toward proactive security validation embedded within development lifecycles, with pentesting now seen as a critical control for product assurance, compliance readiness, and enterprise trust.

Severity of Findings

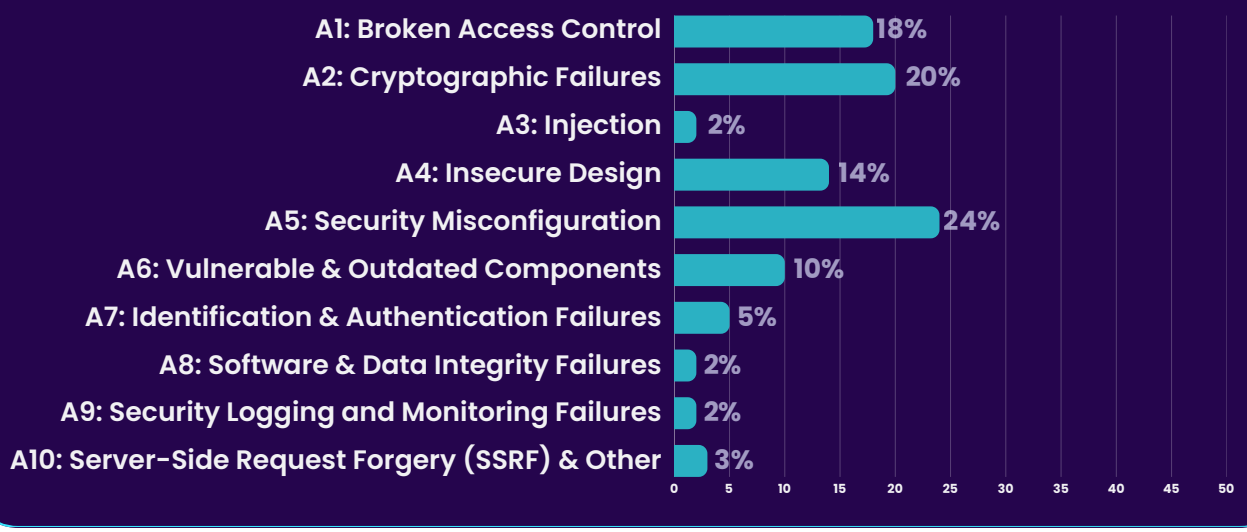
Across Technology & SaaS pentests, combining Web, Network, API, Cloud, and Mobile findings:



Risk Severity Analysis:

These ranges reflect higher-severity trend increases in network and API tests, balanced against lower-severity Web App results. The distribution underscores a “long tail” of medium and low findings that form the bulk of remediation efforts, with a notable rise in critical/high issues in APIs and networks.

OWASP Top 10 Prevalence: Technology & SaaS Providers



Sector-Specific Insights

Technology and SaaS Providers

APIs saw a 400% spike in critical vulnerabilities, highlighting poor access control, logic flaws, and insecure exposure.

CI/CD environments often lacked basic security controls, exposing pipelines to credential leaks and code tampering.

Authentication flows showed growing risk due to weak session handling in SPAs and fragmented identity layers.

Multi-tenant logic was a common weak point, particularly around role separation, provisioning flows, and resource scoping.

Over the last year, penetration testing engagements within the Technology and SaaS sector have revealed a marked increase in both the **complexity and criticality** of vulnerabilities, driven by rapid product innovation, cloud-native architectures, and expanded API ecosystems. **Security misconfigurations** (22–25%) and **cryptographic failures** (20–22%) emerged as the most prevalent OWASP-aligned issues, often stemming from fast-paced DevOps cycles and insufficient hardening of cloud resources. **Broken access control**, particularly in multi-tenant environments, remains a persistent risk, frequently enabling privilege escalation or unauthorized data access.

A sharp rise in **critical vulnerabilities** was observed in APIs (400% YoY) and internal/external network assets, reflecting increased attacker focus on integration points and infrastructure sprawl. The adoption of **containerized and serverless deployments** introduced new threat vectors, including insecure CI/CD pipelines, misconfigured IAM roles, and lateral movement paths within hybrid environments.

Notably, the majority of findings fell under the **medium to low severity** range (~60–70%), yet the impact of a small percentage of high/critical issues—especially around identity, encryption, and access logic—remained disproportionately significant. The sector is shifting toward **continuous, intelligence-driven security validation**, incorporating red teaming, business logic testing, and threat-informed simulations to stay ahead of evolving adversarial tactics.

Strategic Takeaways

- **Adopt Continuous Security Validation:** Move beyond periodic assessments by integrating ongoing penetration testing, adversary simulations, and threat-informed defense exercises into the software lifecycle.
- **Embed Security into DevOps (Shift-Left):** Incorporate secure coding, threat modeling, and automated security checks early in the CI/CD pipeline to detect and prevent vulnerabilities before deployment.
- **Prioritize API & Identity Security:** With APIs and authentication layers driving SaaS architectures, enforce strict access controls, session management, and API-specific testing as part of routine assessments.
- **Focus on Exploitability Over Volume:** Prioritize remediation efforts based on risk context—focusing first on high-impact, easily exploitable flaws like access control failures, insecure configurations, and exposed secrets.

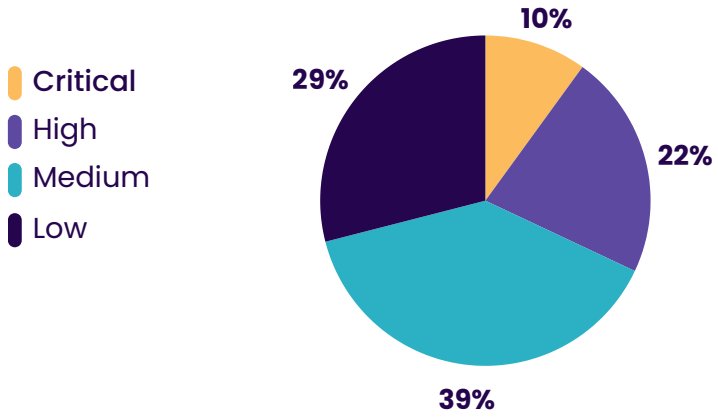
BANKING & FINANCIAL SERVICES

Over the past year, penetration testing in the banking and financial services sector has undergone a significant transformation driven by new regulatory mandates such as NIS2 and DORA.

These regulations have introduced more stringent cybersecurity and operational resilience requirements, compelling financial institutions to adopt more comprehensive and frequent penetration testing practices. The focus has expanded beyond traditional IT infrastructure to encompass critical payment systems, cloud environments, third-party vendors, and incident response capabilities. Compliance with these frameworks demands rigorous risk assessments, continuous monitoring, and detailed reporting to ensure robust protection against evolving cyber threats. As a result, penetration testing has become an integral component of financial institutions' security strategies, helping to safeguard sensitive data, maintain trust, and ensure regulatory compliance in an increasingly complex and hostile cyber landscape.

Severity of Findings

Across banking & financial services pentests, combining Web, Network, API, Cloud, and Mobile findings:

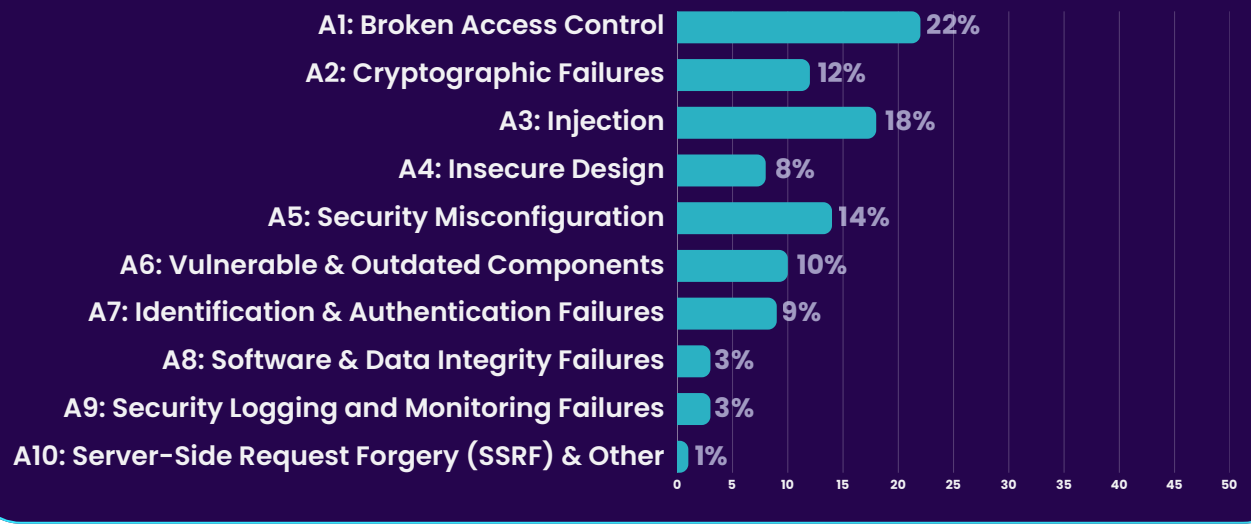


Risk Severity Analysis:

The distribution reflects increasing regulatory pressure (e.g., NIS2, DORA) pushing institutions to focus on early detection and mitigation of high-impact vulnerabilities.

Continuous pentesting and proactive vulnerability management have helped reduce the prevalence of critical issues over the year, though financial institutions still face complex threats requiring ongoing attention.

OWASP Top 10 Prevalence: Banking & Financial Services



Sector-Specific Insights

Banking & Financial Services

Over **70% of financial institutions** now conduct regular penetration tests to satisfy strict regulatory demands and manage growing cyber risks.

Stringent **regulation enforcement** has increased focus on Threat-Led Pentesting (TLPT / TIBER-EU), simulating real adversary TTPs to enhance resilience.

Pentesting is increasingly embedded in DevSecOps pipelines, using tools like SAST/DAST, secrets detection, and threat modeling supported through automated scanning tools.

Approximately **40% of financial firms** have moved to quarterly or continuous testing to keep pace with rapid IT changes and evolving threats.

This year, pentesting in the banking & financial services sector has highlighted critical security challenges amid an evolving threat landscape and stricter regulations. The majority of vulnerabilities identified fall within the OWASP Top 10 categories, with **Broken Access Control**, **Injection flaws**, and **Security Misconfigurations** representing the most prevalent of these high-impact risks.

Additionally, findings reveal persistent issues around **cryptographic failures** and **authentication weaknesses**, underscoring the ongoing need to strengthen data protection and identity management. While we've seen progress with logging and monitoring, gaps that could delay threat detection and response remain. The integration of cloud services and third-party dependencies has introduced new attack vectors, elevating risks related to insecure configurations and outdated components. Regulatory frameworks like **NIS2** and **DORA** have further driven organizations to adopt more rigorous, continuous, and risk-based penetration testing approaches.

Overall, the data underscores the imperative for financial institutions to maintain robust, adaptive security programs, prioritize early vulnerability detection, rapid remediation, and compliance alignment to safeguard customer trust and operational resilience.

Strategic Takeaways

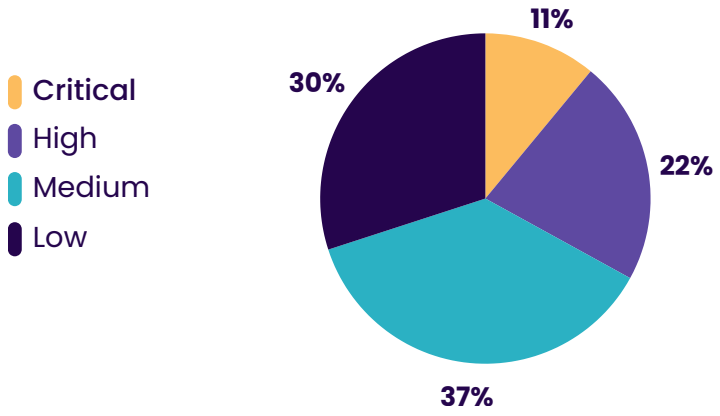
- **Prioritize Access Control and Authentication Hardening:** Broken access controls and authentication weaknesses remain the most exploited vulnerabilities. Strengthening identity and access management (IAM) frameworks, implementing multi-factor authentication (MFA), and enforcing least-privilege principles are essential to reduce risk.
- **Enhance Security Posture in Cloud and Third-Party Ecosystems:** With increased cloud adoption and reliance on third-party vendors, misconfigurations and supply chain vulnerabilities have become critical attack vectors. Financial institutions must invest in continuous configuration monitoring, third-party risk assessments, & enforce strict security standards across all external integrations.
- **Adopt Continuous and Risk-Based Penetration Testing:** Regulatory pressures and emerging threats require a shift from periodic to continuous, risk-driven pentesting. This ensures early detection of vulnerabilities and faster remediation, aligning security efforts with business priorities and compliance requirements.
- **Invest in Robust Logging, Monitoring, and Incident Response:** Gaps in security logging and monitoring impede timely threat detection and response. Enhancing visibility through centralized logging, real-time alerting, and well-practiced incident response plans will improve resilience against sophisticated cyberattacks.

RETAIL & CONSUMER GOODS

Over the past year, penetration testing requirements in the Retail and Consumer Goods sector have intensified significantly due to the sector's increasing reliance on digital platforms and e-commerce channels. With a surge in online transactions and customer data collection, retailers face heightened risks from sophisticated cyber threats targeting payment systems, supply chain logistics, and customer information databases. Regulatory pressures around data privacy, such as GDPR and CCPA, have also pushed companies to adopt more rigorous security assessments. As a result, penetration testing in this sector has evolved to focus not only on identifying traditional vulnerabilities but also on simulating advanced attack vectors like credential stuffing, ransomware, and supply chain compromises. Furthermore, with the rise of IoT devices in retail environments, such as smart shelves and connected point-of-sale terminals, pentesters are required to assess a broader attack surface that includes both digital and physical infrastructure, ensuring comprehensive risk mitigation in an increasingly complex ecosystem.

Severity of Findings

Across retail & consumer goods pentests, combining Web, Network, API, Cloud, and Mobile findings:

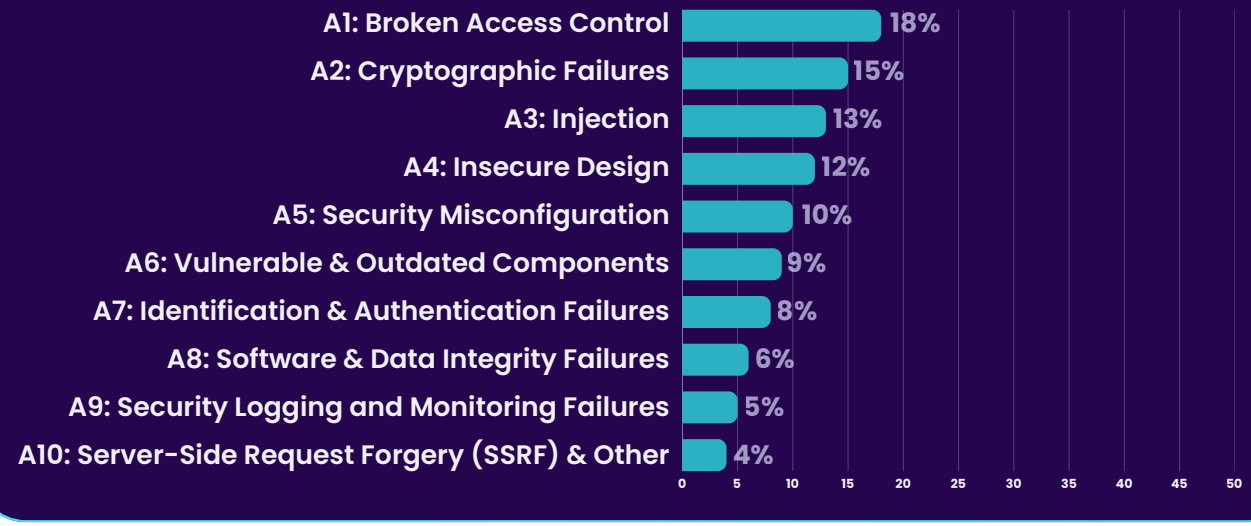


Risk Severity Analysis:

There has been a notable trend toward increased medium-level findings due to outdated third-party libraries and API misconfigurations in cloud-based retail services.

Critical and high-severity findings often correlate with a few core issues like poor input validation, authentication flaws, and encryption weaknesses.

OWASP Top 10 Prevalence: Retail & Consumer Goods



Sector-Specific Insights

Retail & Consumer Goods

68% of retail APIs suffered from misconfigured authorizations or excessive data exposure. When testing these clients' endpoints, we identified an average of 15 issues per engagement.

42% of organizations now combine SAST/DAST scans with regular pentests during development sprints for early detection.

There is a Frequency vs. Velocity Mismatch. **27%** still only conduct annual engagements, despite quarterly or more frequent release cycles for features and promotions. This gap leaves fast-changing Clients exposed for months without retesting.

Over the past year, penetration testing in the retail and consumer goods sector has revealed critical vulnerabilities, including security misconfigurations, cryptographic failures, and broken access controls. The industry has seen a 33% increase in cyberattacks, with 45% of organizations experiencing ransomware incidents, leading to an average recovery cost of $2.73 million. Despite significant investments in cybersecurity, challenges persist, with 68% of retailers reporting insufficient defences against current threats.

The predominance of these vulnerabilities highlights persistent weaknesses in access management, data protection, and input validation compounded by frequent security misconfigurations and the widespread use of outdated or vulnerable third-party components, reflecting gaps in secure deployment and maintenance practices. Emerging concerns around insecure design and inadequate logging indicate that many organizations are still maturing their security processes and threat modeling approaches. The evolving retail landscape—with increased e-commerce adoption, IoT integration, and complex supply chains—necessitates a holistic and proactive security posture. Comprehensive pentesting, rigorous secure coding standards, and continuous monitoring are imperative for safeguarding customer data, maintaining regulatory compliance, and preserving brand trust in an increasingly digital market environment.

Strategic Takeaways

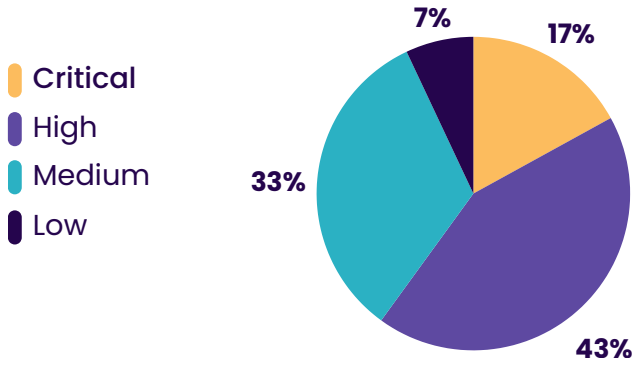
- **Strengthen Access Control Mechanisms:** Given the high prevalence of Broken Access Control vulnerabilities, organizations must prioritize implementing robust, role-based access controls and enforce strict authorization checks throughout all systems to prevent unauthorized data exposure and privilege escalation.
- **Enhance Cryptographic Practices and Data Protection:** Cryptographic Failures remain widespread, underscoring the need to adopt modern encryption standards, enforce secure key management, and ensure all sensitive data—both in transit and at rest—is adequately protected to maintain confidentiality and integrity.
- **Integrate Security Early in the Development Lifecycle:** The frequent findings of Insecure Design and Injection flaws indicate a critical need for embedding security into the software development lifecycle (SDLC) through comprehensive threat modeling, secure coding training, and automated security testing to reduce vulnerabilities from the outset.
- **Improve Asset Management and Patch Processes:** The significant use of vulnerable and outdated components highlights gaps in asset inventory and patch management. Retailers must implement continuous monitoring and timely patching strategies to mitigate risks arising from third-party libraries and frameworks.

Healthcare

Over the past year, the healthcare sector has witnessed a marked increase in penetration testing (pentesting) requirements, driven by a surge in cyber threats and regulatory pressure to secure sensitive patient data. With the expansion of telemedicine, electronic health records (EHRs), and interconnected medical devices, healthcare organizations have become high-value targets for ransomware and data breaches. Consequently, there has been a shift from basic vulnerability assessments to more rigorous, insight-oriented pentesting that includes simulated attacks on internal networks, APIs, and IoT-enabled medical devices. Regulatory frameworks such as HIPAA and the introduction of stricter compliance standards like HITECH and NIS2 in certain regions have further compelled healthcare providers to adopt continuous security testing. This trend underscores the growing recognition that proactive security validation is essential not only for compliance but also for safeguarding patient trust and ensuring uninterrupted clinical operations.

Severity of Findings

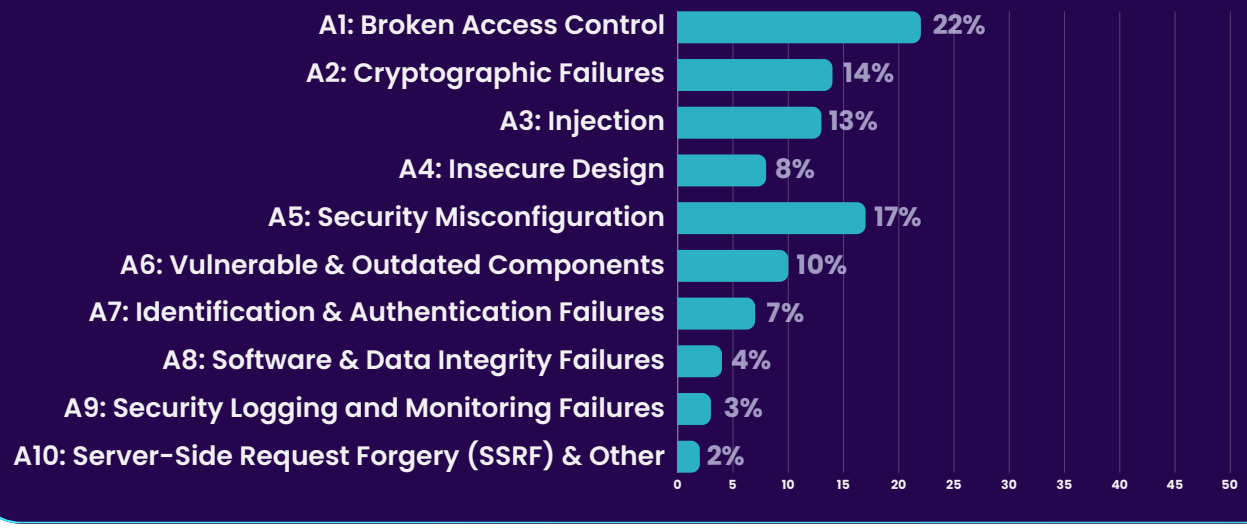
Across healthcare pentests, combining Web, Network, API, Cloud, and Mobile findings:



Risk Severity Analysis:

This distribution illustrates a pressing need for healthcare organizations to prioritize remediation strategies, particularly for high-risk vulnerabilities that have direct implications for data protection, regulatory compliance, and patient safety.

OWASP Top 10 Prevalence: Healthcare



Sector-Specific Insights

Healthcare

40% of Clients have shifted to quarterly or continuous testing to satisfy HIPAA, HITRUST, and emerging FDA Digital Health guidelines.

30% of pentesting engagements included AI/ML-powered support or triage systems. The top risks are prompt injection and insecure data pipelines.

With **25%** of healthcare clients migrating core services to public cloud, misconfiguration and overly provisioned IAM roles spiked as prevalent risks.

Over the past year, pentesting across the healthcare sector has revealed a consistent pattern of critical security weaknesses rooted in legacy infrastructure, misconfigurations, and insufficient access controls. High-risk vulnerabilities, particularly those related to broken access control, insecure APIs, and outdated software components, remain prevalent, highlighting a persistent gap between compliance efforts and real-world security readiness. The OWASP Top 10 categories most frequently identified—Broken Access Control (22%), Security Misconfiguration (17%), and Cryptographic Failures (14%)—underscore systemic issues in identity management, data protection, and secure deployment practices.

Healthcare environments continue to struggle with the secure integration of emerging technologies such as IoT medical devices and telehealth platforms, often lacking proper segmentation, patch management, and encryption standards. Additionally, many findings suggest that detection and response capabilities are underdeveloped, with logging and monitoring failures observed in several assessments. These trends emphasize the critical need for healthcare organizations to adopt a risk-based, proactive approach to cybersecurity beyond regulatory checkboxes, prioritizing continuous testing, secure design, and rapid remediation to protect sensitive patient data and ensure operational resilience.

Strategic Takeaways

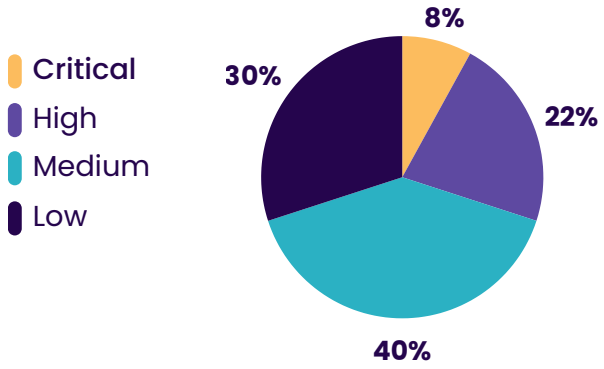
- **Prioritize Access Control Hardening:** Most critical vulnerabilities stemmed from broken access controls—including unauthorized access to patient data, misconfigured user roles, and weak authentication mechanisms. Healthcare organizations must strengthen identity and access management (IAM) systems, enforce least privilege principles, and mandate multi-factor authentication (MFA) across all critical systems.
- **Modernize and Patch Legacy Systems:** A large share of findings were linked to outdated software and unsupported infrastructure, common in healthcare environments due to long device lifecycles. There is an urgent need to implement robust patch management processes, decommission obsolete systems, and migrate to more secure, updatable platforms where feasible.
- **Secure Application Development and Deployment:** Frequent injection flaws, insecure APIs, & poor cryptographic practices point to gaps in secure coding & DevSecOps practices. Integrating application security testing (SAST/DAST) into the software development lifecycle (SDLC), along with secure architecture reviews, is essential for reducing risk in custom-built healthcare apps and portals.

Energy & Utilities

Over the past year, the energy and utilities sector has witnessed a significant increase in penetration testing (pentesting) requirements, driven by escalating cyber threats and stricter regulatory compliance mandates. With the growing integration of operational technology (OT) and information technology (IT) systems—particularly in smart grids, SCADA networks, and IoT-enabled infrastructure—the industry's attack surface has expanded dramatically. This convergence has made legacy systems more vulnerable to sophisticated cyberattacks, prompting energy providers to seek more frequent and specialized pentesting services. Additionally, global concerns over critical infrastructure security, spurred by high-profile cyber incidents and geopolitical tensions, have pushed regulators to enforce tighter cybersecurity frameworks, such as NERC CIP and IEC 62443. As a result, energy firms are now demanding comprehensive, scenario-based assessments that simulate advanced persistent threats (APTs), with a focus on lateral movement, privilege escalation, and real-world exploitation paths within hybrid IT/OT environments.

Severity of Findings

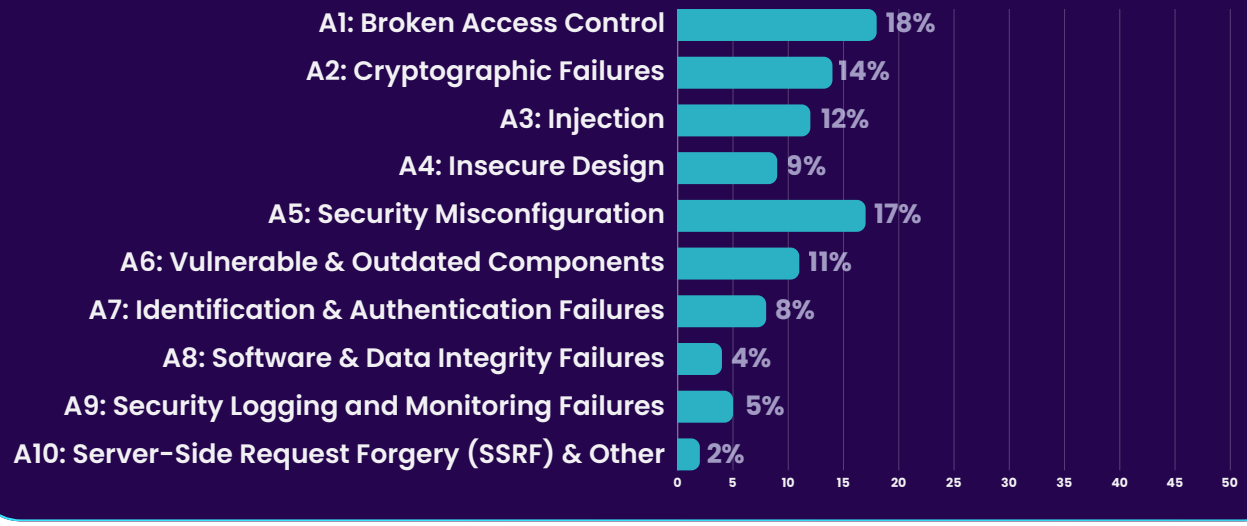
Across energy & utilities pentests, combining Web, Network, API, Cloud, and Mobile findings:



Risk Severity Analysis:

- **Medium and High-severity issues dominate**, due to widespread use of legacy systems and inadequate OT security controls.
- **Critical vulnerabilities**, though less frequent, pose major risks due to the potential impact on public infrastructure.
- There is **growing emphasis on OT-specific pentesting**, highlighting gaps between IT security maturity and OT resilience.

OWASP Top 10 Prevalence: Energy & Utilities



Sector-Specific Insights

Energy & Utilities

The increasing integration of **Information Technology (IT) and Operational Technology (OT)** systems has introduced new attack vectors.

Regulatory frameworks are driving security assessments - NERC CIP, and DOE cybersecurity initiatives are increasing pentest frequency.

The continued use of **outdated and insecure components** increases the risk of exploitation by malicious actors.

Legacy and vulnerable systems remain in use, exposing the environment to potential exploitation by threat actors

Over the past year, penetration testing within the energy and utilities sector has revealed a persistent and evolving threat landscape marked by a blend of legacy system vulnerabilities and emerging attack vectors. The convergence of IT and operational technology (OT) environments has significantly broadened the attack surface, exposing critical infrastructure to heightened risks. Testing outcomes consistently highlight a predominance of medium to high severity vulnerabilities, including insecure remote access, weak network segmentation, and outdated or unpatched control systems. Critical findings, though less frequent, underscore potentially catastrophic implications if exploited, particularly in SCADA and ICS components. Furthermore, the industry continues to grapple with inadequate security configurations and insufficient monitoring capabilities, reflecting gaps in both technical defenses and cybersecurity governance. These insights emphasize the urgent need for integrated, adaptive security strategies that address the unique challenges of hybrid IT/OT ecosystems and comply with evolving regulatory requirements, thereby safeguarding vital energy assets against increasingly sophisticated cyber threats.

Strategic Takeaways

- **Prioritize IT-OT Convergence Security:** The increasing integration of IT and operational technology systems demands a unified security approach. Organizations must strengthen network segmentation, implement robust access controls, and continuously monitor both environments to prevent lateral movement and contain breaches effectively.
- **Accelerate Patch Management & Legacy System Modernization :** A significant portion of vulnerabilities stem from outdated software, firmware, and legacy devices. Accelerating patch deployment and systematically upgrading or isolating legacy infrastructure is critical to reducing exploitable attack surfaces and enhancing overall resilience.
- **Enhance Identity and Access Management (IAM) Practices:** Weak authentication, lack of multi-factor authentication (MFA), and excessive privileges remain common findings. Implementing strict IAM policies, enforcing MFA, and regularly reviewing access rights are essential to mitigating risks related to unauthorized access and privilege escalation.
- **Invest in Proactive Detection and Response Capabilities:** Gaps in security monitoring and incident response impede timely threat detection and mitigation. Energy & utilities organizations should enhance logging, deploy advanced threat detection tools, and develop incident response plans tailored to OT environments to reduce dwell time and minimize operational impact during cyber incidents.

Threat Emulation & Red Teaming Insights

Executive Summary

Threat emulation and red teaming have become vital components of modern cybersecurity strategies. These proactive approaches simulate adversary tactics to identify weaknesses in an organization's detection and response capabilities. This report outlines key insights gained from recent threat emulation and red teaming exercises, focusing on common detection and response gaps, the application of the MITRE ATT&CK framework for technique mapping, and strategic recommendations to strengthen cybersecurity defenses.

Introduction

As cyber threats grow more sophisticated, organizations must adopt offensive security practices to test and improve their defenses. Threat emulation replicates attacker techniques in a controlled manner, while red teaming offers a comprehensive, adversary-like evaluation of security posture by combining technical exploits with social engineering and operational tactics. Both methodologies are instrumental in uncovering gaps in security monitoring, incident response, and overall resilience.

DETECTION AND RESPONSE GAPS

Detection Gaps:

One of the most frequent findings from threat emulation & red team engagements is the presence of significant detection blind spots. These gaps often result from:

- **Limited Telemetry Coverage:** Incomplete visibility across endpoints, networks, cloud workloads, and user activities hampers the ability to detect attacker behaviors such as lateral movement or privilege escalation.
- **Insufficient Behavioral Analytics:** Traditional signature-based detection methods fail to identify novel or subtle attacker techniques, especially those leveraging living-off-the-land binaries or fileless malware.
- **Underutilized Data Sources:** Critical logs or security data sources, such as PowerShell logging, Windows Event Logs, or DNS analytics, are often disabled or inadequately collected, limiting forensic & detection capabilities.

Response Gaps:

Red team operations also highlight response weaknesses, including:

- **Delayed Incident Recognition:** Teams frequently detect breaches late in the attack lifecycle, increasing attacker dwell time and potential damage.
- **Unclear Escalation Paths:** Ambiguities in incident handling responsibilities and escalation procedures cause delays in mobilizing the appropriate response teams.
- **Lack of Playbook Readiness:** Many organizations do not maintain or regularly test incident response playbooks tailored to specific attack scenarios, resulting in inconsistent or ineffective containment and recovery efforts.

MITRE ATT&CK TECHNIQUE MAPPING

The MITRE ATT&CK framework serves as a critical tool for aligning threat emulation and red team activities with known adversary tactics and techniques. This standardized knowledge base facilitates the identification of specific techniques successfully employed during simulations and those that evade detection.

- **Technique Coverage Analysis:** Mapping simulated attacks to ATT&CK techniques enables security teams to pinpoint detection strengths and weaknesses. For example, effective detection of phishing (Initial Access) may contrast with poor visibility into credential dumping (Credential Access).
- **Prioritizing Defense Enhancements:** Organizations can prioritize controls and monitoring based on the most relevant or frequently observed ATT&CK techniques targeting their sector or infrastructure.
- **Improving Incident Response Playbooks:** ATT&CK provides a structured vocabulary for designing incident response workflows, ensuring playbooks address the full range of adversary behaviors.

Using MITRE ATT&CK as a lens during red team exercises enhances communication between technical teams and leadership by framing findings in a clear, actionable context.

STRATEGIC TAKEAWAYS

The insights gained from threat emulation and red teaming yield several strategic lessons for cybersecurity improvement:

- **Enhance Telemetry and Visibility:** Comprehensive monitoring across all critical assets, including endpoints, network segments, cloud environments, and applications, is essential. Investments in Endpoint Detection and Response (EDR), Network Detection and Response (NDR), and cloud-native security monitoring should be prioritized.
- **Integrate Detection with Incident Response:** Tight coupling between detection alerts and response workflows accelerates incident handling. Automation and orchestration platforms (SOAR) can help streamline playbook execution and reduce manual delays.
- **Adopt Continuous Improvement Cycles:** Threat emulation and red teaming should be ongoing activities integrated into the security lifecycle, adapting to evolving attacker tactics and organizational changes.
- **Leverage MITRE ATT&CK Framework:** Utilizing ATT&CK for technique mapping and maturity assessments allows targeted investments, more effective training, and better risk communication.
- **Simulate Realistic, Contextual Threats:** Tailoring red team exercises to reflect actual threats and organizational context ensures findings are relevant and actionable.
- **Foster Cross-Team Collaboration and Executive Support:** Encouraging collaboration between blue teams, IT operations, and leadership ensures timely remediation and resource allocation based on risk-based priorities.

CONCLUSION

Threat emulation and red teaming are indispensable tools for identifying and addressing cybersecurity gaps. By uncovering detection blind spots, response inefficiencies, and leveraging the MITRE ATT&CK framework for systematic analysis, organizations gain critical insights that drive targeted improvements. Strategic investments in visibility, process integration, and continuous adaptation can transform these insights into enhanced resilience against increasingly sophisticated adversaries.

Large Language Model (LLM) Penetration Testing

Executive Summary

Large Language Models (LLMs) have rapidly become integral in various applications, including chatbots, code generation, and decision support systems. However, as their adoption grows, so do the security risks associated with their deployment. This report presents key insights from penetration testing exercises on LLM systems, focusing on identified vulnerabilities, mapping to the OWASP Top 10 security risks, and strategic takeaways to enhance LLM security and robustness.

Introduction

LLMs, powered by deep learning and vast training data, offer unprecedented natural language understanding and generation capabilities. Despite these benefits, their complex architectures and usage in critical systems expose new attack surfaces. Penetration testing of LLM environments aims to uncover exploitable weaknesses that could lead to data leakage, unauthorized actions, or manipulation of AI outputs. This report synthesizes the findings from such tests, aligning them with the OWASP Top 10 to provide a clear framework for risk assessment and mitigation.

IDENTIFIED VULNERABILITIES IN LLM SYSTEMS

Assessments of LLMs reveal a range of vulnerabilities that attackers may exploit:

- **Prompt Injection Attacks:** Adversaries craft inputs that manipulate the model's behaviour to bypass intended constraints, execute unauthorized commands, or reveal sensitive information.
- **Data Leakage:** LLMs unintentionally exposing training data or user-provided sensitive information, especially if proper data sanitization and access controls are lacking.
- **Model Poisoning and Backdoors:** Influence model training or fine-tuning phases, embedding malicious behaviors or biased outputs.
- **Authentication and Authorization Flaws:** Weak API protections allow unauthorized access to the LLM or its underlying infrastructure.
- **Insecure Logging and Monitoring:** Logs captured sensitive inputs or outputs without adequate protection, risking data exposure.
- **Insufficient Input Validation:** Malicious inputs that exploit the model's tokenization or parsing mechanisms can lead to unintended responses or denial of service.
- **Lack of Rate Limiting:** Excessive or automated queries can lead to service degradation or facilitate brute-force attacks.

OWASP TOP 10 MAPPING

Mapping these vulnerabilities to the OWASP Top 10 provides a structured view of risk areas:

OWASP Top 10 Category	Relevant LLM Vulnerabilities
A1: Broken Access Control	Weak API authentication enables unauthorized model usage
A2: Cryptographic Failures	Insecure transmission or storage of sensitive data
A3: Injection	Prompt Injection attacks manipulate model behavior
A4: Insecure Design	Lack of secure model training practices leading to poisoning/backdoors
A5: Security Misconfiguration	Insufficient logging protections and misconfigured rate limits
A6: Vulnerable and Outdated Components	Use of outdated ML frameworks or libraries with known vulnerabilities
A7: Identification and Authentication Failures	API key leakage or weak authentication mechanisms
A8: Software and Data Integrity Failures	Model poisoning and tampered training data
A9: Security Logging and Monitoring Failures	Logs exposing sensitive prompts or model outputs
A10: Server-Side Request Forgery (SSRF)	Indirect risks from LLM integrations that fetch external data

This mapping highlights that traditional web application security risks have direct analogs in LLM environments, often manifesting through novel attack vectors specific to AI systems.

STRATEGIC TAKEAWAYS

To mitigate these vulnerabilities and strengthen LLM security, organizations should consider the following strategies:

- **Robust Prompt Filtering and Validation:** Implement multi-layer input validation and prompt sanitization to prevent injection attacks and limit harmful queries.
- **Strong Access Controls:** Enforce stringent API authentication, role-based access control, and secure key management to prevent unauthorized use.
- **Secure Model Training Pipelines:** Adopt rigorous data provenance checks and model validation to detect and prevent poisoning or malicious training inputs.
- **Comprehensive Logging and Monitoring:** Ensure sensitive data is redacted in logs and establish real-time monitoring for anomalous query patterns indicative of attacks.
- **Rate Limiting and Throttling:** Protect LLM endpoints against abuse by limiting request volumes and detecting automated exploitation attempts.
- **Regular Security Assessments:** Conduct continuous penetration testing and vulnerability scans on LLM components and related infrastructure to detect emerging risks.
- **Incident Response Preparedness:** Develop and test incident response plans specifically tailored to AI-related security incidents, including data breaches and model integrity compromises.
- **User Awareness and Training:** Educate developers and users about the risks of prompt injection and secure usage practices to reduce accidental exposure.

CONCLUSION

As LLMs become embedded in critical applications, understanding and addressing their security vulnerabilities is paramount. Penetration testing reveals that many traditional web security risks apply in novel ways to LLM environments, necessitating both adapted defenses and AI-specific safeguards. By aligning vulnerabilities with the OWASP Top 10 framework and adopting strategic mitigations, organizations can better protect their LLM deployments from emerging threats, ensuring safe and trustworthy AI-driven services.

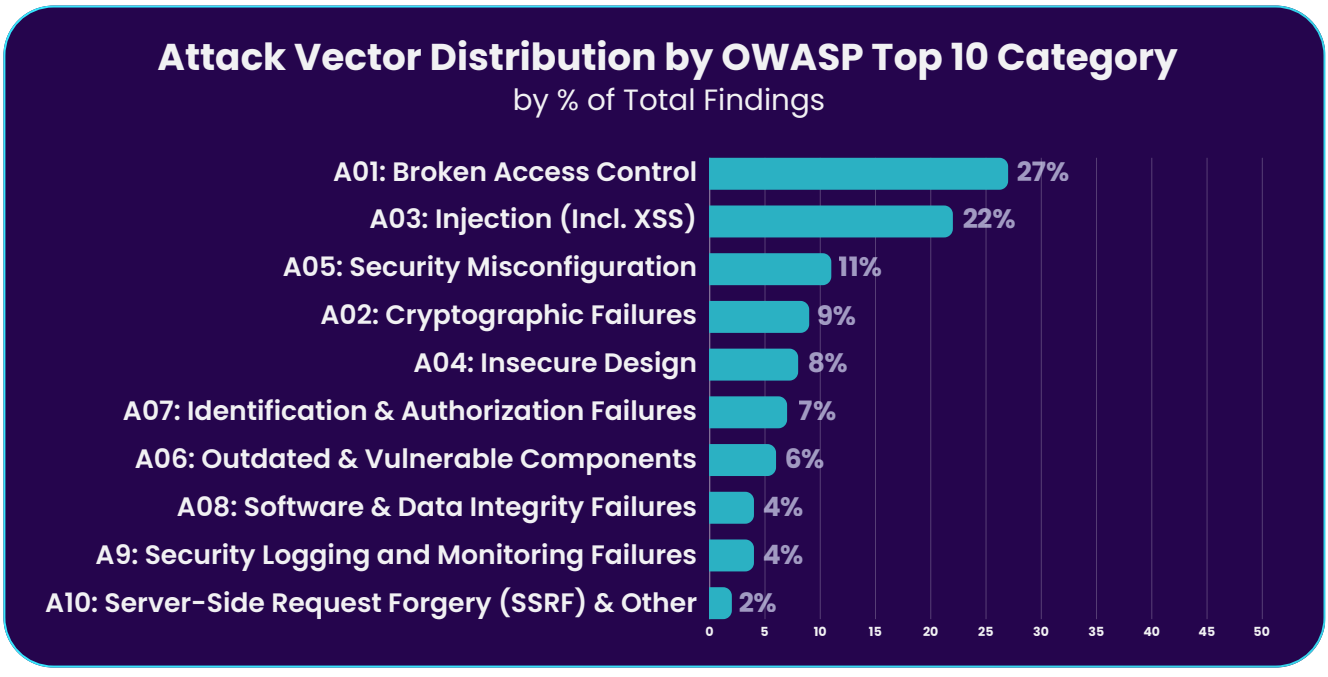
Attack Vectors & Exploitation Trends

Over the past year, penetration testing across diverse environments—including web applications, external networks, APIs, mobile applications, and cloud infrastructure—has highlighted consistent attack vectors and exploitation trends. Commonly exploited vulnerabilities include broken authentication and authorization mechanisms, injection flaws, misconfigurations, and others. Attackers increasingly leverage automation and supply chain weaknesses, particularly targeting third-party components and APIs to bypass traditional defences. Misconfigurations in cloud environments and excessive permissions remain significant risk factors for privilege escalation and data leakage. These trends underscore the critical need for rigorous security controls, continuous monitoring, and proactive vulnerability management to effectively reduce operational risk.

1. WEB APPLICATIONS

Over the past year, web application penetration testing has revealed consistent exploitation patterns aligned with the OWASP Top 10 framework. The most frequently targeted and successfully exploited categories remain Broken Access Control, Injection flaws, and Security Misconfiguration, which together represent more than 50% of all vulnerabilities. These attack vectors reflect persistent failures in authorization logic, input validation, and secure configuration.

As web applications increasingly rely on third-party services, CI/CD pipelines, and cloud-native deployments, less common but high-impact vectors—such as SSRF, Software/Data Integrity Failures, and Cryptographic Failures—are emerging more prominently in advanced threat scenarios.



KEY EXPLOITATION TRENDS

Authorization Bypass Attacks on the Rise

- IDOR and forced browsing remain top issues.
- APIs are especially vulnerable to broken access control due to poor object-level authorization.

Shift-Left Failures in Insecure Design

- Security is often absent from early design stages.
- Leads to exploitable logic flaws that are difficult to fix post-deployment.

Persistence of Classic Injection Vectors

- SQL, command, and XSS injections are still prevalent—especially in legacy or poorly maintained apps.
- Misuse of dynamic queries and unsensitized input is still widespread.

Cryptographic Missteps and Token Mismanagement

- Use of weak hashing (e.g., MD5, SHA-1), flawed JWT handling, and misconfigured TLS continue to expose sensitive data.

SSRF & Supply Chain Attacks Emerging

- As cloud-native and microservice architectures grow, SSRF and CI/CD injection flaws are surfacing more often.

STRATEGIC RECOMMENDATIONS

Access Control Failures Dominate Findings

- Emphasis should be placed on enforcing object-level authorization, validating session state transitions, and eliminating direct access to unlinked functions or records.

Injection Attacks Remain Pervasive & Impactful

- Despite awareness, injection flaws—particularly SQL injection and stored XSS—continue to affect a significant portion of applications.
- Proper implementation of parameterized queries, input sanitation, and secure templating frameworks is critical.

Insecure Design Reflects Gaps in Threat Modeling

- These findings stem from architectural or business logic flaws.
- Security must be integrated at the design level, with structured threat modeling and abuse-case analysis incorporated into development pipelines.

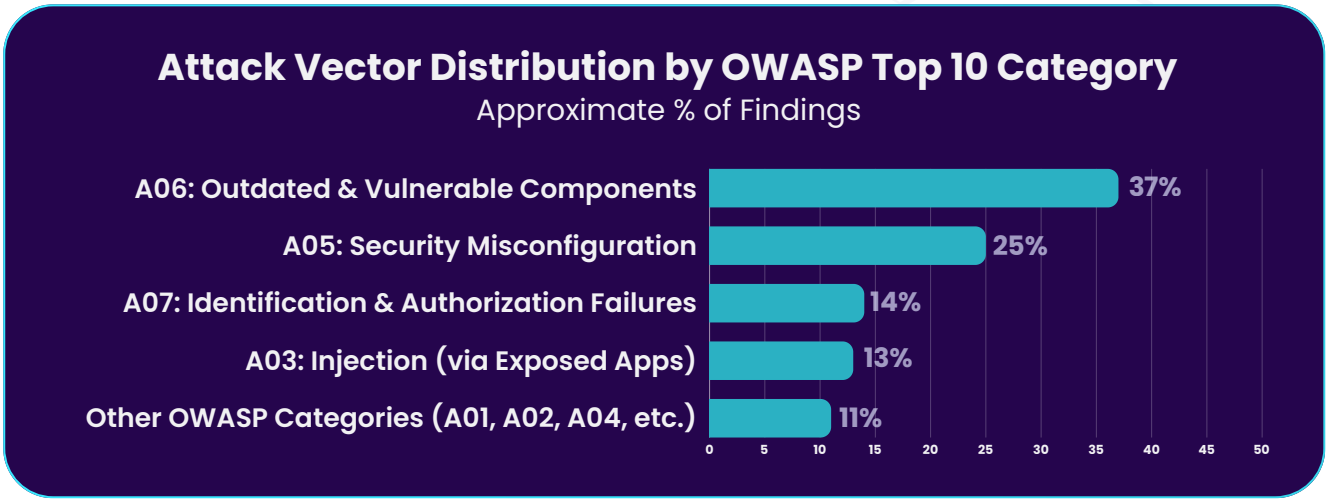
Dependency & Supply Chain Risks Are Escalating

- The exploitation of vulnerable third-party components and CI/CD misconfigurations is increasingly prevalent.
- Organizations must maintain SBOMs, perform regular dependency scanning, and implement integrity verification for software updates and build processes.

2. EXTERNAL NETWORKS

External network penetration tests over the past year continue to highlight critical weaknesses in perimeter-facing systems. Attackers most frequently exploited vulnerable third-party components, misconfigured services, and weak authentication mechanisms to gain initial access. These exploitation paths align with the OWASP Top 10 categories, with some adapted for the infrastructure and network layer.

The reliance on exposed remote access solutions (e.g., VPNs, Citrix, Exchange), unpatched services, and default credentials made these environments susceptible to compromise, often with minimal effort. In several assessments, successful external exploitation led directly to internal network pivoting and domain compromise within one or two attack steps.



KEY EXPLOITATION TRENDS

Unpatched Systems and Misconfigured Services are the #1 Entry Point

- Public-facing services and outdated components continue to be exploited via known CVEs.

Configuration Weaknesses Undermine Perimeter Defense

- Misconfigured services (e.g., open RDP, unprotected databases, exposed management interfaces) allowed external attackers to bypass intended controls.

Credential-Based Attacks Continue to Succeed

- Insecure password policies, missing MFA, and credential reuse enabled account takeover and built successful exploit chains.

Web Layer Code Flaws as Pivot Points

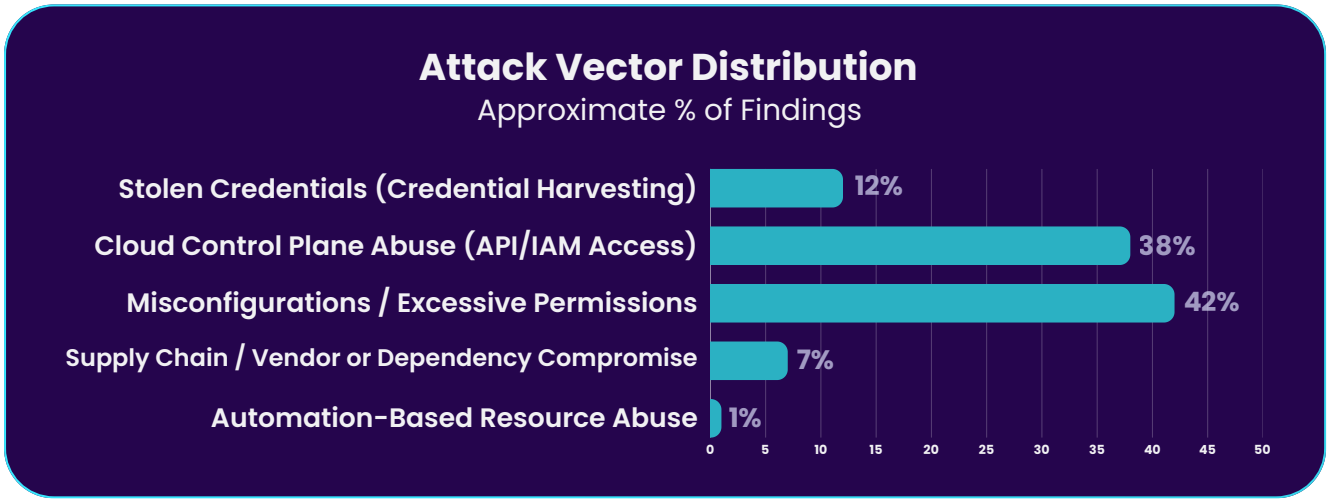
- Even in infrastructure-focused tests, poorly secured web applications (e.g., RCE via injection) were used to compromise back-end systems.

STRATEGIC RECOMMENDATIONS

- Automate patch management for external-facing systems using a prioritized CVE risk-based approach.
- Conduct regular perimeter configuration reviews, including cloud-exposed services.
- Enforce strong authentication (MFA, password hygiene, account lockouts) across all remote access points.
- Harden exposed web apps using WAFs, secure coding, and vulnerability scanning.

3. CLOUD INFRASTRUCTURE

Cloud environments have been targeted through highly efficient and diverse attack vectors, with adversaries leveraging automation, stolen credentials, misconfigurations, supply chain flaws, and unconventional AI misuse techniques. The shift to hybrid and multi-cloud identities, plus the rise of LLM usage, has widened the attack surface and complexity of defense.



KEY EXPLOITATION TRENDS

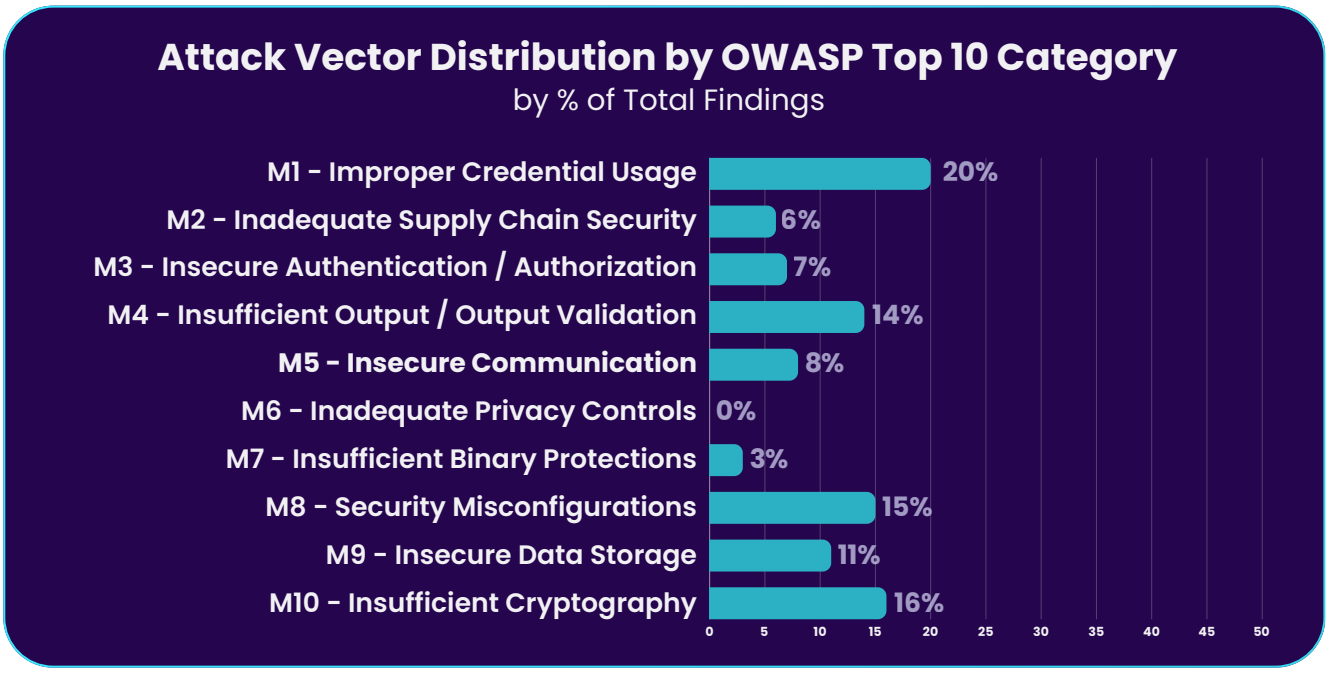
1. IAM Misconfigurations & Overprivileged Roles
2. Public Storage Exposure
3. Supply Chain Attacks
4. Zero Trust Violation
5. Serverless / Container Escape

STRATEGIC RECOMMENDATIONS

- **Enforce Zero Trust and Harden Identity:** Implement MFA, eliminate overly permissive IAM roles, segment access, and enforce least privilege for both human and machine identities.
- **Strengthen Anti-Phishing Defenses:** Deploy email filtering and protection, user training focused on credential theft prevention and AITM detection, and multi-factor authentication where possible.
- **Secure Cloud Control Planes:** Monitor IAM changes, audit API usage, detect creation of unauthorized users and suspicious persistent objects.
- **Continuously Remediate Misconfigurations:** Automate discovery and remediation of overprivileged access, public bucket exposure, insecure API endpoints, and third-party integrations.
- **Detect & Mitigate Automated Abuse:** Monitor for anomalous resource spin-up patterns, LLM model usage spikes, and unauthorized tool automation.

4. MOBILE APPLICATIONS

Mobile applications continue to be a lucrative target for adversaries, leveraging a diverse set of vectors including social engineering (phishing, smishing, vishing), malware-laced apps, and supply chain compromises. Rising device misconfigurations, outdated OS versions, and human-driven attack paths amplify the risk. These trends align with the OWASP Mobile Top 10 and broader enterprise attack patterns.



KEY EXPLOITATION TRENDS

Weak or Custom Cryptography Usage

- A majority of mobile apps (~36%) continue to use outdated, weak, or custom-built cryptographic mechanisms, exposing sensitive data to easy decryption and interception.

Security Misconfigurations and Insecure Data Storage

- About 20% of apps have misconfigurations like exposed debug modes, overly broad permissions, or store sensitive data (e.g., credentials) in plaintext on the device, increasing attack surfaces.

Authentication and Authorization Flaws

- Approximately 27% of apps suffer from broken authentication, token leakage, session management issues, and improper privilege controls, allowing attackers to bypass access restrictions.

Vulnerabilities in Third-Party SDKs and Supply Chain Components

- Around 15% of apps are impacted by vulnerable or outdated third-party SDKs, opening the door for supply chain attacks and code injection through untrusted dependencies.

STRATEGIC RECOMMENDATIONS

Enforce Strong, Standardized Cryptography

- Organizations must mandate the use of vetted, up-to-date cryptographic libraries and industry standard protocols (e.g., AES, TLS 1.3). Avoid custom or deprecated encryption methods to protect sensitive data against interception and tampering.

Strengthen Authentication and Authorization Controls

- Implement multi-factor authentication (MFA), secure token management, and robust session handling to prevent unauthorized access and privilege escalation. Regularly test authentication workflows for common weaknesses.

Harden App Configurations and Secure Data Storage

- Adopt secure coding and deployment practices by disabling debug modes in production, restricting app permissions to the minimum necessary, and encrypting sensitive data stored on-device to reduce exposure from misconfigurations.

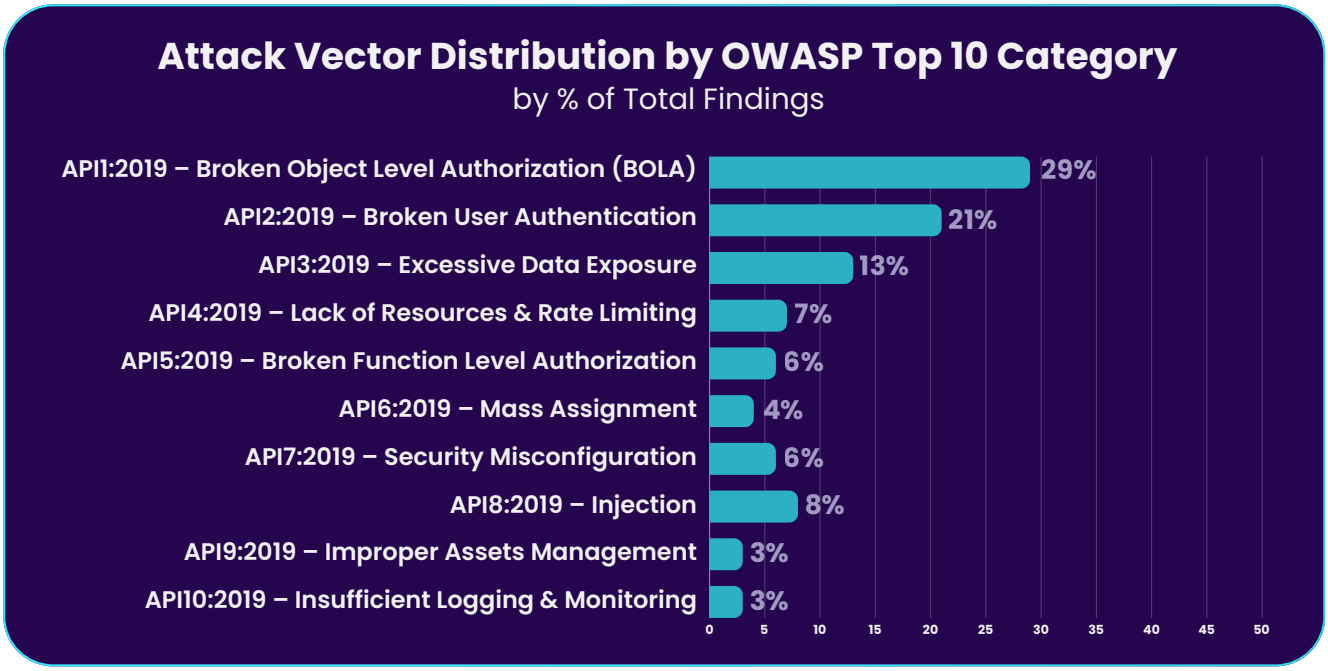
Monitor Third-Party SDKs Continuously

- Establish a rigorous process to evaluate the security posture of third-party SDKs and libraries, including regular patching and dependency scanning, to mitigate supply chain risks that can compromise app integrity.

5. APIS

APIs remain a critical attack surface as they expose backend services and sensitive data. The rise of microservices, mobile apps, and cloud-native architectures has driven explosive API usage, but also increased security challenges. Attackers increasingly target API endpoints to bypass traditional perimeter defences, steal data, and escalate privileges.

Over the past year, pentesting and threat intelligence have identified key attack vectors and exploitation trends affecting API security. Common issues include broken authentication, excessive data exposure, injection flaws, and inadequate rate limiting.



KEY EXPLOITATION TRENDS

Broken Object Level Authorization (BOLA)

- The most frequent vulnerability, BOLA, enables attackers to access or manipulate resources they don't own by manipulating object IDs or API parameters.

Excessive Data Exposure

- APIs often return more data than needed; attackers exploit this to harvest sensitive information.

Rate Limiting & Throttling Failures

- Absence or misconfiguration of rate limiting exposes APIs to brute force and denial-of-service attacks.

Broken Authentication & Session Management

- These flaws allow unauthorized access through token theft, weak credential policies, or improper session expiration.

Injection Attacks

- SQL, NoSQL, and command injection flaws remain prevalent in APIs lacking strong input validation.

STRATEGIC RECOMMENDATIONS

- Implement **strict authorization checks** at object and API parameter levels.
- Use robust **authentication frameworks** with token validation and MFA where applicable.
- Enforce **least privilege data exposure** by designing APIs to return only necessary information.
- Adopt **comprehensive input validation** to mitigate injection attacks.
- Configure **rate limiting and throttling** to prevent abuse and DoS attacks.
- Harden API gateways and servers to **minimize security misconfigurations** and information leakage.

M10 – Insufficient Cryptography 16%

Conclusion

In 2025, BreachLock's Penetration Testing Intelligence Report once again underscores a simple truth: attackers are innovating faster, and organizations are challenged to match or outpace that speed. This year's data reveals not only a continued rise in Critical and High-severity findings across industries, but also more complex exploit chains that blend multiple vulnerabilities for greater impact. APIs, cloud assets, and internet-facing systems remain top targets, reflecting an expanding and ever-shifting attack surface.

The widespread increase in the adoption of proactive, more frequent, and even continuous security testing signals to adversaries that security teams are more equipped than ever to find and remediate gaps before they do. Today's Offensive Security solutions like Penetration Testing as a Service (PTaaS), Adversarial Exposure Validation (AEV), and continuous pentesting give security teams the ability to identify real-world attack paths, validate risk against likely threats, and prioritize remediation that truly reduces exposures proactively.

At BreachLock, we believe in adopting an offensive mindset — not just detecting vulnerabilities, but anticipating how an attacker might exploit them, and neutralizing those opportunities before they become breaches. By combining deep human expertise with intelligent automation and AI, we provide a unified, actionable view of risk that helps organizations stay ahead of the threat curve.

The insights from this report serve as both a guide and a call to action. The threat landscape will only grow more sophisticated, but with the right offensive strategy, security teams can take back the advantage and stay ahead of evolving threats.

BreachLock is a global leader in offensive security, delivering scalable and continuous security testing. Trusted by global enterprises, BreachLock provides human-led and AI-powered attack surface management, penetration testing, red teaming, and adversarial exposure validation (AEV) services that help security teams stay ahead of adversaries. With a mission to make proactive security the new standard, BreachLock is shaping the future of cybersecurity through automation, data-driven intelligence, and expert-driven execution.

***Know Your Risk*. Contact BreachLock today!**

BreachLock Inc.
1350 Avenue of the Americas
2nd Fl., New York, NY. 10019

BreachLock NL B.V.
Kon. Wilhelminaplein 1, Tower 4
1062 - HG Amsterdam

hello@breachlock.com