



The BreachLock Penetration Testing Intelligence Report 2023

2nd Annual Penetration Testing Report

Table of Contents

Foreword	3
Highlights	4
Introduction	5
Methodology and Scope	6
Demographics	7
Industry Insights	8
OWASP Top 10 - What haunts your systems?	9
Assets	11
Web Applications	12
Networks	15
APIs	18
Mobile	20
Cloud	22
Industries	24
Computer Software and Technology	26
Banking and Financial Services	28
IT Services & Consulting	30
Retail and eCommerce	32
Healthcare	34
Conclusion	36
Why BreachLock	39

FOREWORD



Seemant Sehgal
Founder & CEO, BreachLock

We have one common enemy – cybercriminals.

Over the past five years, BreachLock has emerged as a global leader in Cyber Security Validation. We have successfully aided numerous clients in their pursuit of ongoing attack surface management and continuous security validation.

We also realize that we have common adversaries, understanding that the power of our defense lies in the unity of our security community.

The BreachLock Penetration Testing Intelligence Report 2023 represents our initiative to give back to this community. Each year, we dedicate substantial effort to distill insights that empower CISOs and cybersecurity professionals to elevate their defense strategies. This year's report draws from a rich dataset of over 3,000 penetration tests, offering comprehensive insights across applications, networks, APIs, and cloud infrastructures. Notably, the report includes industry-specific benchmarking data enabling you to contextualize the threats your peers may be confronting.

In a landscape where the efficacy of security tools alone is increasingly questioned, this report arrives at a crucial juncture. The boardroom acknowledges that validating investments is essential for optimizing Return on Investment (ROI). In 2023, security validation solutions, including Pen Testing as a Service, have earned a place in three Gartner Hype Cycles: Security Operations, Everything as a Service, and Application Security. This underscores the convergence of defensive and offensive investments, promising a balanced approach to cybersecurity.

By sharing this report, we reaffirm our commitment to making cyberspace safer for all stakeholders. We extend our gratitude to our clients, dedicated Security and IT professionals, and the public, for your unwavering support in this endeavor. It is our sincere hope that this report equips you and your teams to bolster cyber resilience today and prevent breaches in the future.

Thank you for your continued partnership. Together, we stand against the tide of cyber threats, united in our pursuit of a safer digital realm.

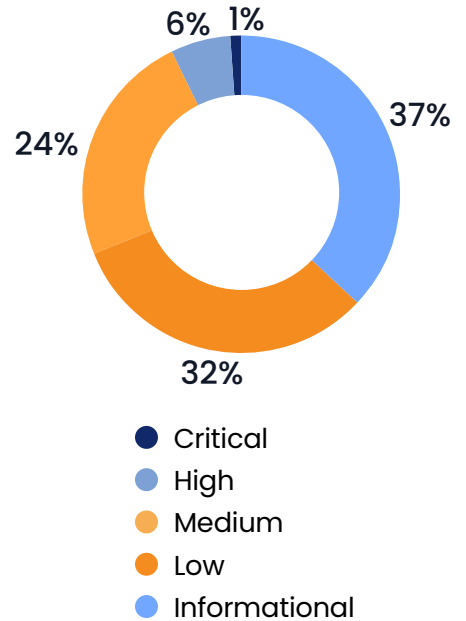
Seemant Sehgal

HIGHLIGHTS

In a digital world, attack surfaces are expanding, and organizations are becoming perimeterless. Organizations today must manage hundreds of evolving risks continuously across full-stack systems to secure web applications, network infrastructures, multi-cloud environments, APIs, mobile apps, wireless networks, IoT – and the list continues to grow.

In our 2023 report, BreachLock security researchers analyzed anonymized, aggregated data from over 3000 penetration tests to highlight the current state of security risks by taking an in-depth look at the most exploited OWASP Top 10 categories by industry and asset-specific vulnerabilities.

Overall Risk Severity of Vulnerabilities



BreachLock has identified these as the top trends and recommendations to enable organizations to develop impactful security strategies for 2023 and beyond.

TOP 5 IMPACTED INDUSTRIES

1. Computer Software & Technology
2. Banking and Financial Services
3. Professional Services
4. Retail & eCommerce
5. Healthcare

TOP 5 OVERALL SECURITY ISSUES IN WEB APPLICATIONS

1. Cross-Site Scripting (XSS)
2. Outdated Software Versions
3. Insecure Direct Object References (IDOR)
4. Lack of Security Headers
5. Insecure Secure Sockets Layer (SSL) and Transport Layer Security (TLS) Protocols

TOP 3 CRITICAL SEVERITY FINDINGS

1. SQL Injection
2. Broken Authentication
3. Remote Code Execution (RCE)

TOP 3 HIGH SEVERITY FINDINGS

1. Cross-Site Scripting (XSS)
2. CSV Injection
3. Cross site Request Forgery (CSRF)

Introduction

Welcome to the BreachLock Penetration Testing Intelligence Report 2023.

In today's modern security operations center, an organization's attack surface has become endless, as every endpoint and associate represents a 'branch of one.' A data breach caused by a known vulnerability may cost up to \$4.45M USD in 2023 (global average cost)*.

As a follow-up to BreachLock's inaugural report, the 2023 report aims to demonstrate the state of full-stack security based on thousands of pentests performed globally, across assets, industries, and geographies.

These statistics presented in the report, when combined with security validation functions, such as penetration testing and vulnerability assessments, can accelerate remediation activities for DevSecOps teams.

By establishing these along with compliance readiness, DevSecOps teams can take action to secure digital systems, users, and applications.

**Source – IBM's Cost of a Data Breach Report 2023*



METHODOLOGY AND SCOPE

Cyber attackers scanning the internet are looking for commonly exploited vulnerabilities. Their goal? Find the vulnerable components and weaknesses for an easy and profitable cyber attack to achieve their objective.

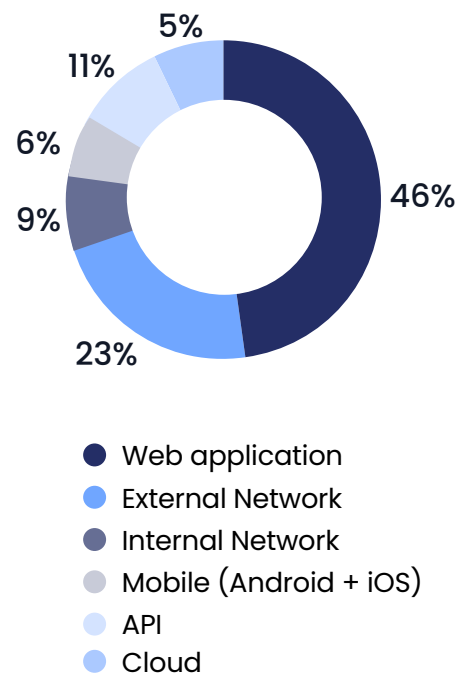
In every pentesting engagement, BreachLock offers visibility into the “hacker’s perspective.” Backed with AI and automation capabilities, our in-house, certified pentesters work with security researchers to showcase the attacker’s view of organizations’ digital environments.

This report is based on the data collected from over 3,000 penetration tests performed over a 12-month period between 2022 and 2023. The data has been sanitized to remove all identifiable information and aggregated for analysis to share insights with the broader cybersecurity community.

The analysis contains data points from small organizations to global enterprises with varying security maturity across industries. Data is organized by industry-specific findings with the top vulnerabilities discovered by asset type. Where relevant, OWASP Top 10 category mapping is also provided.

Report Scope	
Timeframe	12 Months
Total Number of Pen Tests	3,300 global penetration tests
Assets Included	<ul style="list-style-type: none"> Applications <ul style="list-style-type: none"> • Web Applications • APIs • Mobile Applications Networks <ul style="list-style-type: none"> • External Network • Internal Network Cloud
Industries Covered	<ul style="list-style-type: none"> Banking and Financial Services Computer Software and Technology Education Government Healthcare Manufacturing Media Services Professional Services Public Sector Retail & Ecommerce Telecommunications Travel and Hospitality

Assets Tested from 2022 - 2023

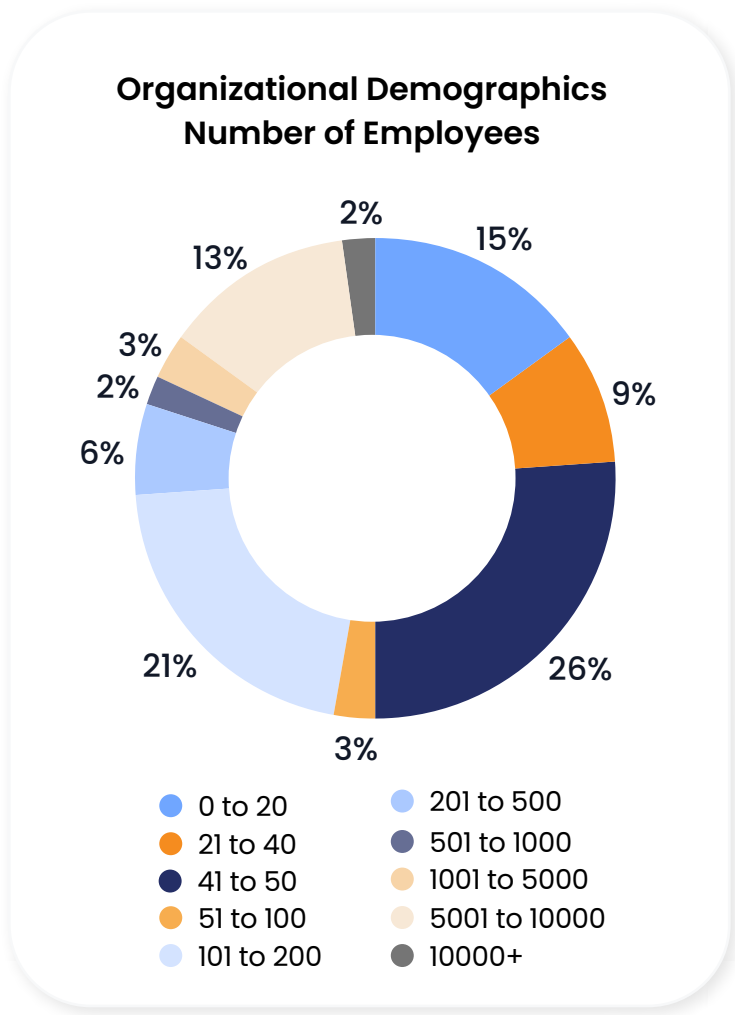


DEMOGRAPHICS

The dataset analyzed for this report addresses organizations of all sizes. BreachLock primarily focuses on the mid-size to large enterprise segments, which account for the majority of the data analyzed in this report.

Mid-size organizations: 100 to 1000 employees represent 29% of the organizations in the mix
Large organizations: 1001 to 10000 employees represent 16%

This is a positive trend in the industry and infers that organizations of every size and maturity are working on implementing the basics of cybersecurity and regularly testing IT systems. On the other hand, the ripple effect impacts of the global pandemic have continued to amplify cybercrime. Many organizations have restructured their teams with hybrid working environments – demonstrating that remote work is here to stay. Meanwhile, security teams continue to grapple with the question of how to protect remote assets and secure critical data in hybrid ecosystems.



INDUSTRY INSIGHTS

Insights from multiple industry verticals and geographies are included in the report's findings

- 46%** of the organizations belong to the Computer Software and Technology industry.
- 17%** of the organizations come from the Banking and Financial Services domain. Cyber adversaries commonly target this industry because of the wealth of information it possesses and the high value of financial data on the dark web.
- 12%** of the organizations come from the IT Services & Consulting domain, as IT landscapes are borderless. One exposure can provide an attacker with limitless possibilities to move laterally through the network potentially leading to a supply chain attack if third-party data is exfiltrated.
- 10%** of the organizations are from the Retail and eCommerce industry, which is digitally transforming how goods and services are exchanged online while increasing security and compliance risks.
- 8%** of the organizations are from the Healthcare industry bound by HIPAA compliance and security requirements to protect and defend patient care and PHI from cybercriminals.

The remaining **13%** of the organizations, including Media Services, Government, Travel and Hospitality, Manufacturing, Public Sector, Education, and Telecommunications, are referred to as "Other".

Observations

The percentage of the Computer Software & Technology Industry investing in penetration testing services has significantly increased due to the following factors:

- Today's Supply Chain is Vulnerable:** With the global spike in supply chain attacks in recent years, organizations that provide software and technology products in the supply chain are taking steps to manage the risks prior to the sharing and exchange of services and information.
- Third-Party Security has become a Market Force:** Organizations are now requiring certifications and accreditations to ensure digital suppliers are not introducing downstream risks into their environments. It's common for a new client to request an independent, certified pentest report from a computer software or technology vendor before signing a deal.

OWASP TOP 10 – WHAT HAUNTS YOUR SYSTEMS?

The OWASP Top 10 framework is widely recognized as one of the industry’s leading security frameworks. In this section, we present the risks identified in the OWASP Top 10, along with data observations and recommendations.

The analysis resulted in factual evidence that security misconfigurations are the most common risk, as it allows an attacker to easily hack a system and exploit its weaknesses resulting in greater and more impactful harm.

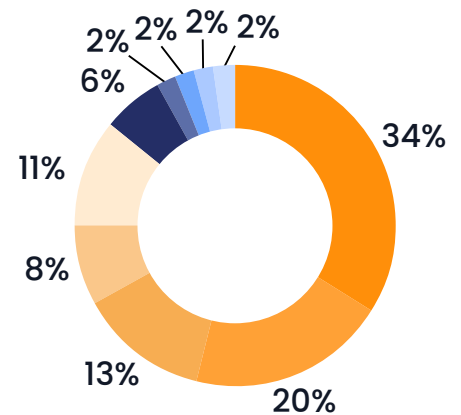
The top 5 risks most identified across web applications by OWASP aligned with BreachLock’s top 5 findings as follows:

1. A05:2021 – Security Misconfiguration
2. A02:2021 – Cryptographic Failures
3. A01:2021 – Broken Access Control
4. A04:2021 – Insecure Design Injection
5. A03:2021 – Injection

These top 5 categories aggregated together cover over 85% of the findings and security weaknesses in the report’s full data set.

Distribution of findings mapped to OWASP Top 10

- Security Misconfiguration
- Cryptographic Failures
- Broken Access Control
- Insecure Design
- Injection
- Vulnerable and Outdated Components
- Identification and Authentication Failures
- Server-Side Request Forgery (SSRF)
- Software and Data Integrity Failures
- Security Logging and Monitoring Failures



Observations

The table below shows a comparison of the Top 5 OWASP risks compared to BreachLock’s findings. The only difference is the order of the categories, except for Cryptographic Failures (20%), which held the number two spot on both sides of the comparison.

OWASP 2021 Top 5 ranking 2021	Observed Top 5 categories
A01:2021–Broken Access Control	Security Misconfiguration: 34%
A02:2021–Cryptographic Failures	Cryptographic Failures: 20%
A03:2021–Injection	Broken Access Control: 13%
A04:2021–Insecure Design	Insecure Design: 8%
A05:2021–Security Misconfiguration	Injection: 11%

OWASP Top 5 ranking vs Observed (by BreachLock) Top 5 categories

source: <https://owasp.org/Top10/>

- 🔴 Security misconfigurations ranked fifth in the OWASP Top 10 for 2021 and was the most identified category in BreachLock's 2023 findings. This contributes to 34% of the overall risk categories observed.
- 🔴 Cryptographic failures, the second-ranked risk on the OWASP list, also ranked second in this year's findings. It was previously referred to as 'sensitive data exposure' and ranked third in OWASP Top 10 for 2017.
- 🔴 Broken access control, insecure design, and injection, which are among OWASP's Top 5 most critical categories, were also trending in our findings, albeit, in a slightly different order.

As seen in the OWASP Top 10 2021 update from 2017, this analysis reveals that some of the top categories are trending upward indicating a direct proportional relationship with the weaknesses and vulnerabilities identified by BreachLock.

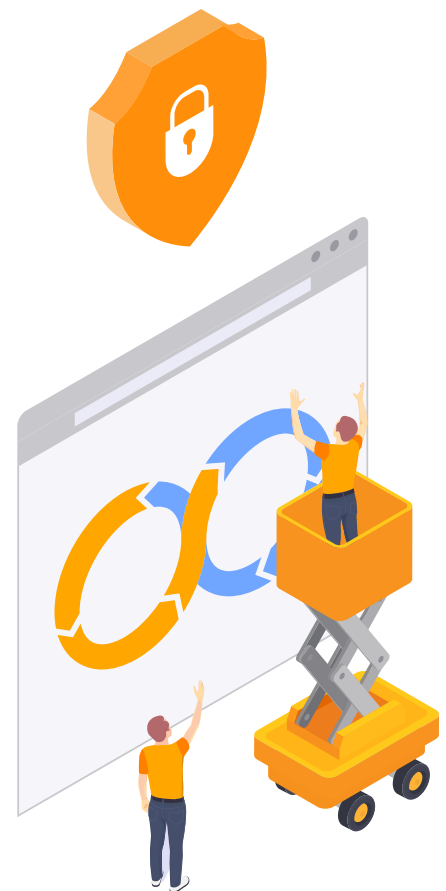
The paradigm has not shifted drastically over the last two years. However, attackers are getting more creative as they interlink weaknesses and vulnerabilities to launch sophisticated targeted attacks. These attack paths can lead to expensive, impactful breaches.

Recommendations

Based on the top 5 findings identified above, DevSecOps teams can reduce possible exposures by creating a strategic, accelerated plan to address these risks proactively.

- ✅ **Assess AppSec Risks:** Application security leaders should take proactive steps to assess and implement secure coding practices, use threat models to identify risks, and deploy WAF (Web Application Firewalls) to secure web applications.
- ✅ **Conduct a Penetration Test:** Consider an in-house or external pentesting provider for a targeted gray box or black box penetration test to identify these specific risks in all applications paired with a proactive remediation plan.

By following these recommendations, organizations can act on these critical and common security risks revealed in this analysis, reinforcing the importance of using an industry framework like OWASP Top 10. These strategic investments strengthen security posture, mitigate potential vulnerabilities, and protect applications from preventable breaches.









ASSETS

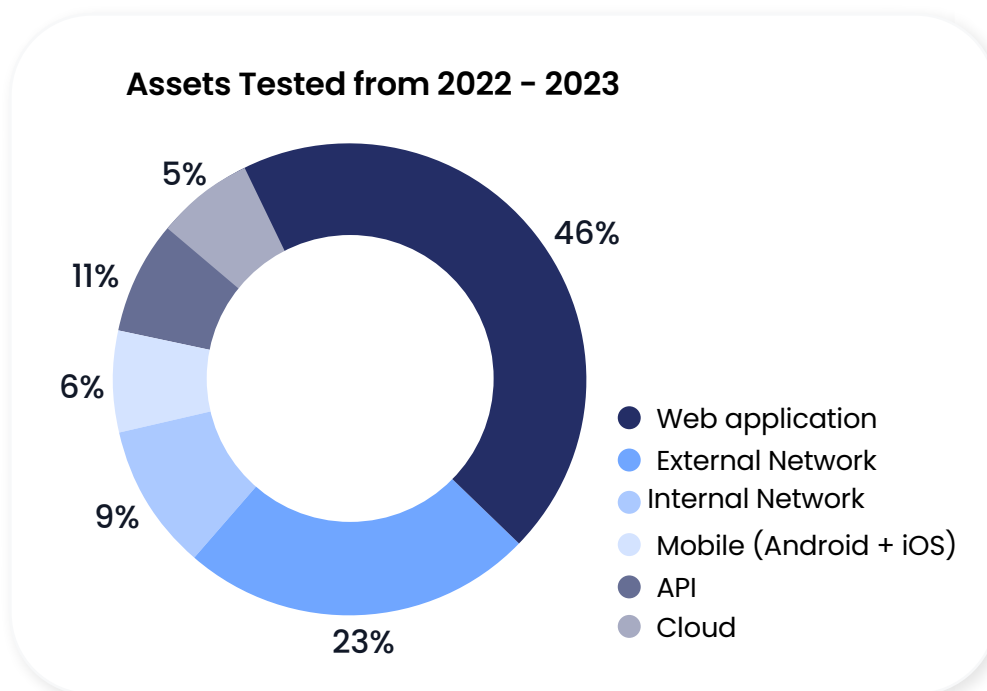
BreachLock provides full-stack penetration testing and vulnerability assessments in 20+ countries and a variety of industries around the world.

Based on experience and expertise in testing a variety of assets, BreachLock has devised a proven methodology that is flexible to fit the needs of our clients across highly regulated industries.

The asset types that resulted in the greatest number of findings are ranked as follows:

- | | | | |
|---|----------------------|---|--|
|  | 1. Web Applications |  | 4. Internal Networks |
|  | 2. External Networks |  | 5. Mobile Applications (Android and iOS) |
|  | 3. APIs |  | 6. Cloud Environments |

Taking a closer look at the next pages, these asset-focused insights provide valuable guidance for any DevSecOps team to take action now.



WEB APPLICATIONS

Web applications sit at the core of digital businesses and are accessible to clients, partners, vendors, and employees.

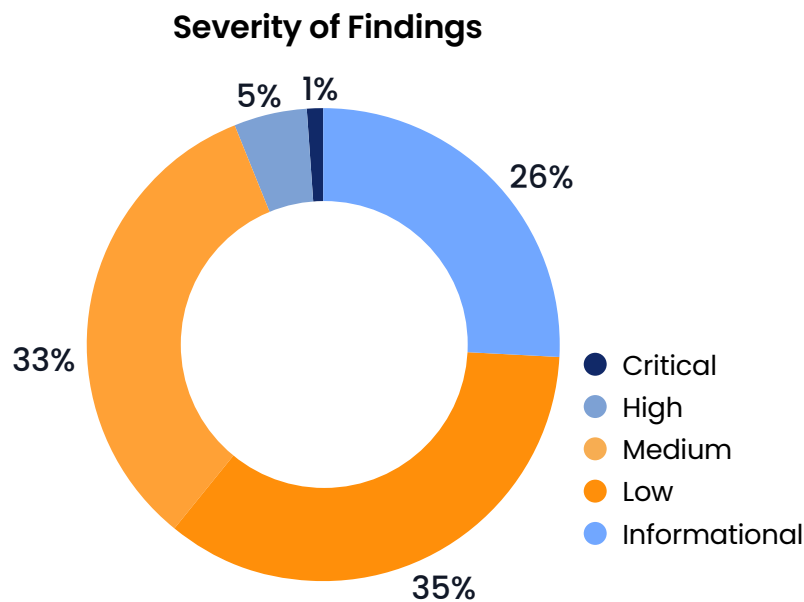
Cybercriminals target web applications due to their vulnerabilities and potential for unauthorized access. Industry statistics highlight that web applications are among the most targeted assets across various sectors. Organizations that prioritize web application security have an edge over threat actors, as they are better prepared to protect sensitive data, minimize the external attack surface, and prevent potential breaches.

Spanning across all industries, web applications make up 48% of the overall assets tested. These stats advocate for web apps to be appropriately secured, as they are accessible to the outside world and can open doors for an attacker.

Overall Risk Ratings of Findings

Risk Severity Analysis: The data reveals the distribution of risk findings in web applications, with Critical findings being 1%, High findings at 5%, and Medium findings at 35%. **The number of Medium-risk findings is significantly higher per application in comparison to High and Critical findings.**

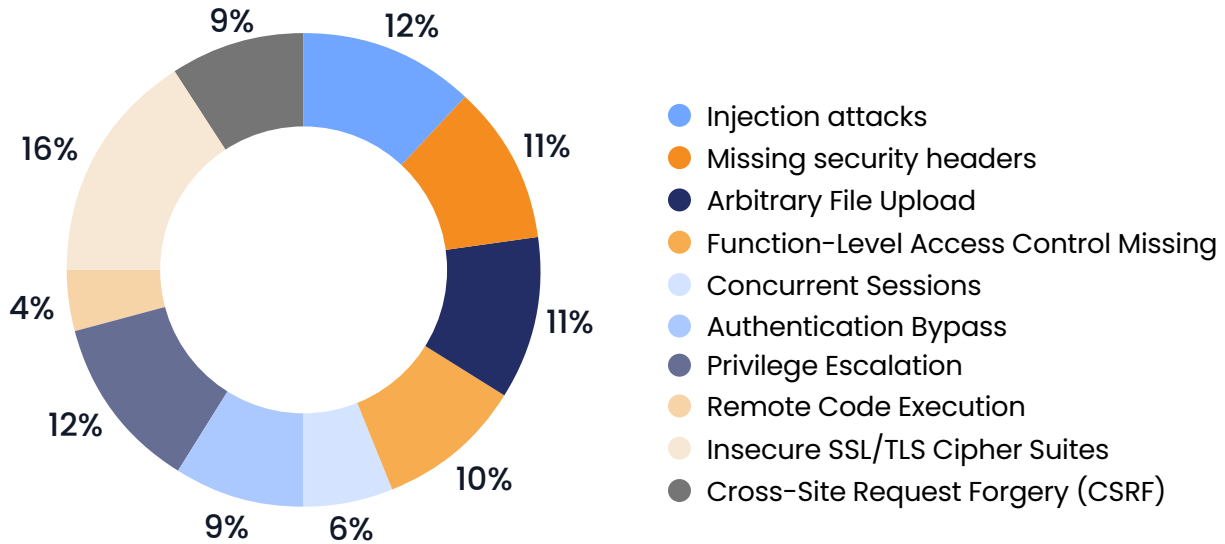
On the positive side, the share of Critical and High findings among total findings is relatively smaller, which also reinforces the fact that most organizations invest in penetration testing before releasing a product into production.



Top 10 Critical Vulnerabilities in Web Apps

The top 10 critical vulnerabilities in web applications are displayed below. The root cause of several OWASP Top 10 vulnerabilities such as Injections, arbitrary file upload, and Cross-Site Request Forgery (CSRF) is the same - lack of input sanitization. One fix can remediate over 30% of the Critical vulnerabilities.

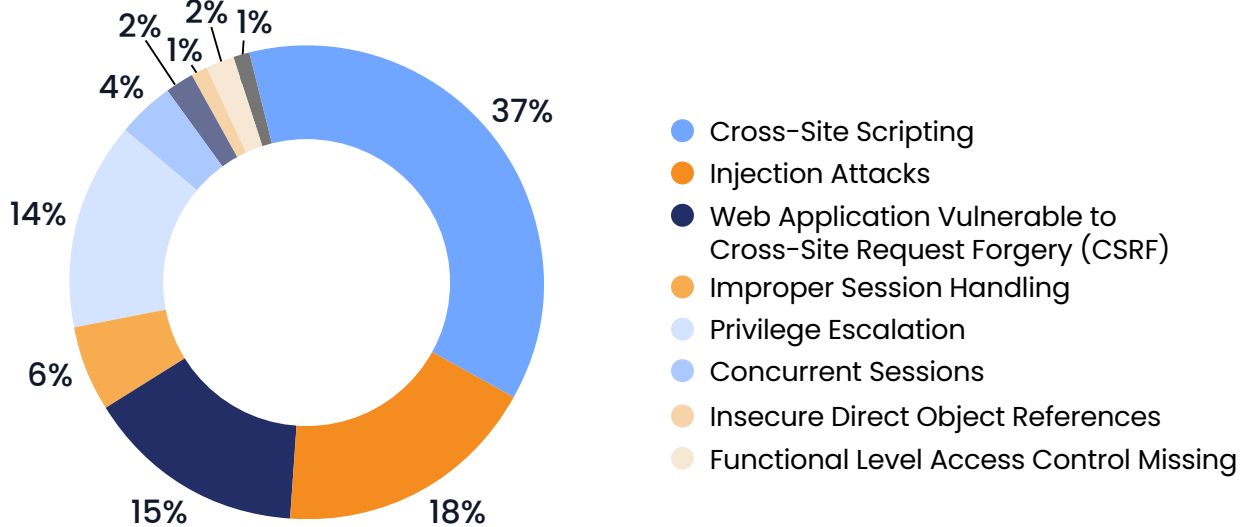
Top 10 Critical findings in Web applications



Top 10 High Vulnerabilities in Web Apps

It's alarming to see Cross Site Scripting (XSS) contributing to 37% of the total high findings. This trend indicates that applications are not implementing client-side and server-side validation holistically. Developers often take the 'deny list' approach to data validation over the 'allow list' approach, which leads to new data exploiting the cross-site scripting vulnerabilities.

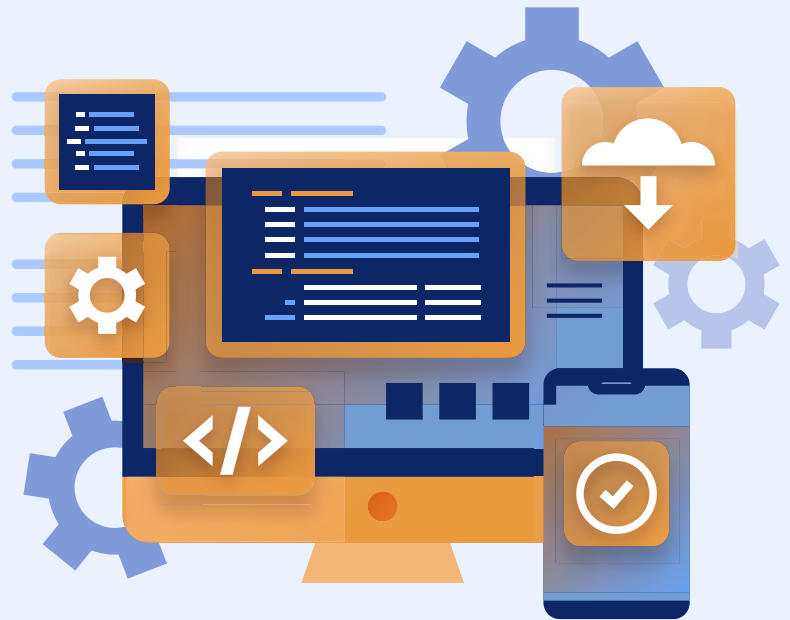
Top 10 High findings in Web applications



Observations

On average, web application security programs across various organizations are effectively managing **Critical and High risks**. However, there is still room for improvement, particularly in addressing Medium and Low-risk findings.

Furthermore, the top three findings in the OWASP Top 10 resulting in **Critical and High vulnerabilities** (**Security Misconfiguration, Cryptographic Failures, and Broken Access Control**) highlight how the OWASP Top 10 categories can be used as a framework to prioritize web app remediation efforts.



Recommendations

Though the distribution of risk and findings tilt towards Medium and Low severity vulnerabilities, that does not outweigh the following requirements:

- ✔ **Mitigate Findings to Improve Web App Security:** Organizations should prioritize web app remediation based on the business criticality, accessibility of the application, and severity of the findings. DevSecOps teams can effectively reduce the overall risk exposure of their web applications by continuing to remediate Medium and Low-risk findings with a prioritized approach.
- ✔ **Use OWASP Top 10 Categories for Continuous Testing:** Organizations can continuously monitor web apps for the OWASP Top 10 Categories - a proactive mechanism to secure and improve the overall security of web applications.
- ✔ **Direct DevOps Integration:** Incorporate pentesting to support your Secure Development Lifecycle (SDL) by ensuring that the software developed is inherently secure across all phases of software development and deployment.
- ✔ **Conduct Third-Party Penetration Testing in Test Environments:** Select a qualified, reputable third-party assessor to conduct an independent web app pentest within the test environment before releasing the application into production.

NETWORK INFRASTRUCTURE

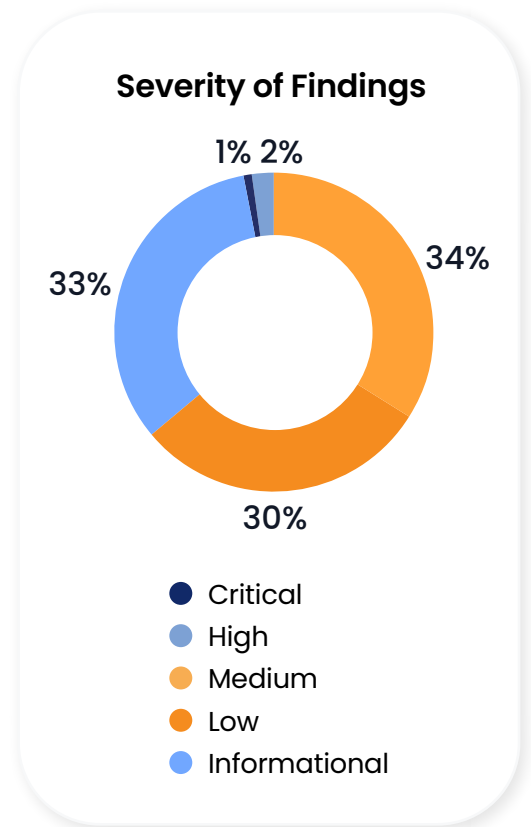
Organizations rely heavily on both external and internal networks for operational purposes, making network security crucial to protect and defend against persistent cybercriminals and ransomware attacks.

Securing external and internal networks continues to be a top priority for organizations. Furthermore, as organizations seek to manage overall risks in hybrid environments, securing both the cloud environment and the network is vital.

Collectively, network penetration testing represents 34% of the complete data set.

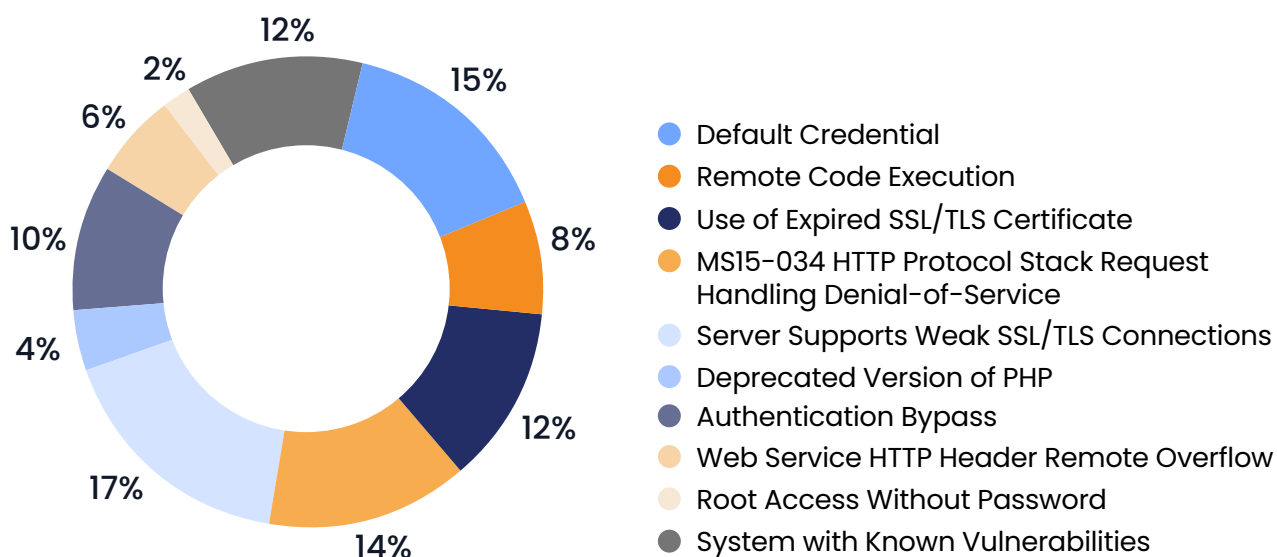
Overall Risk Ratings of Findings

Risk Severity Analysis: The risk distribution shows an insignificant number of Critical (1%) and High (2%) findings, respectively. Meanwhile, Medium findings account for 33%, Low findings for 30%, and Informational findings for 34%.



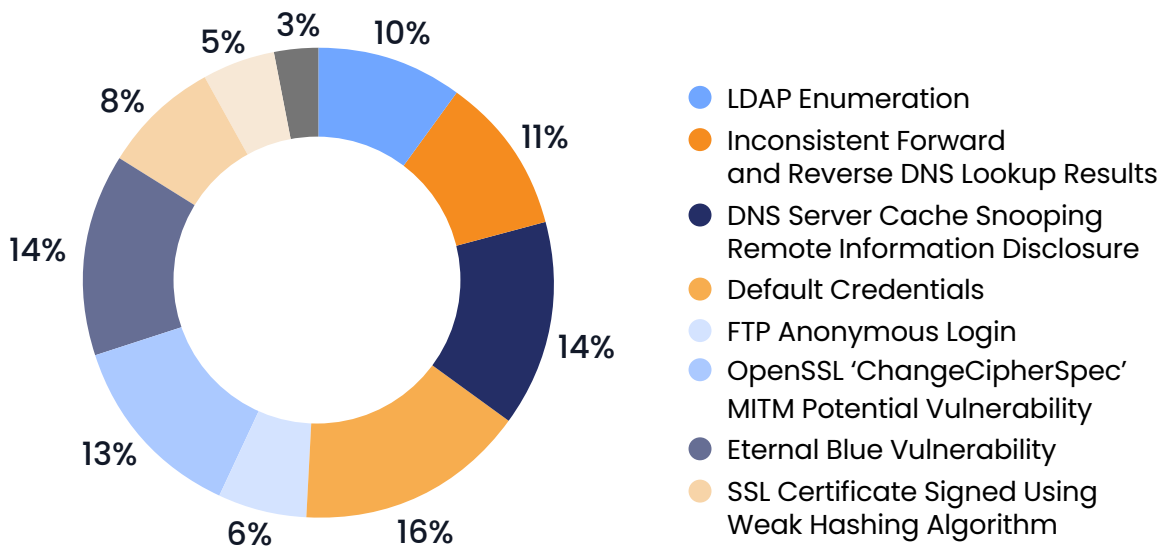
Top 10 Critical Vulnerabilities in Networks

OpenSSL findings on external-facing infrastructure are very common across systems, which leave communications prone to Man-In-The-Middle (MITM) attacks, as do default credentials found in both external and internal-facing networks.



Top 10 High Vulnerabilities in Networks

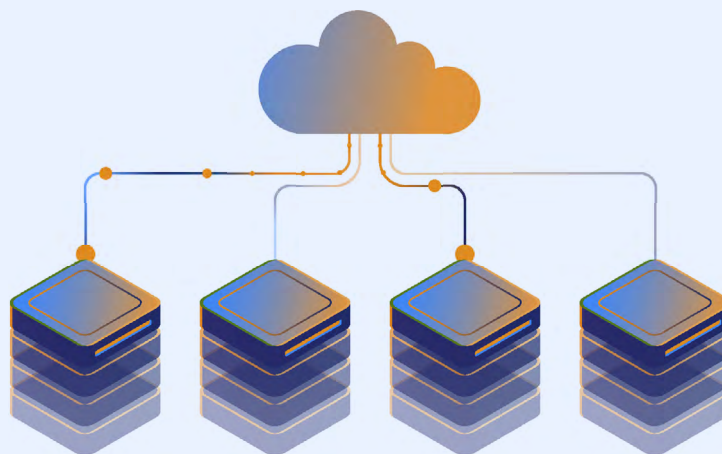
Default credentials are the highest contributor to the vulnerabilities identified in networks, both internal and external - making systems vulnerable to attackers intelligent enough to know the default credentials to the target system.



Observations

These network vulnerability findings indicate a renewed focus on the security of both external and internal networks is needed across industry verticals.

The total number of unique **Critical findings in External Networks is less than in Internal Networks**. This indicates organizations are focusing more heavily on vulnerabilities in their external network and adding more rigor in managing the external-facing vulnerabilities. This is primarily because of the notion that threats come from external-facing assets - such as web applications and systems. Hence, calculated planning is needed to secure external-facing assets.



Recommendations

Based on the data observations and the importance of network security, the following remediation priorities are suggested:

- ✔ **Continuously Evolve the Security program:** Organizations should adapt and stay in sync with the evolving threat landscape. The security team should adopt an attacker's mindset by leveraging daily intelligence feeds, trending breach headlines, and OSINT to bolster defenses proactively.
- ✔ **Manage Risks Associated with Insider Threats:** Cybercriminals do not always come from external facing assets; in some cases, they collude with internal resources to extend the target landscape by many folds. In other words, internal networks require the same level of protection as that of external networks.
- ✔ **Fortify Defense-in-Depth Controls:** Establish and maintain defense-in-depth best practices for networks, including network segmentation, hardened ingress points, encryption, and identity & access management controls. Regularly review and update these measures to ensure that the internal and external networks are protected from advanced persistent threats.

These results demonstrate that prioritizing the security of networks across all risk levels is crucial for both internal and external networks. By addressing the top 10 network vulnerabilities shown here, remediating Medium and Low-risk findings, and fortifying security controls, security leaders can strengthen their network security program and protect their digital assets from potential cyber threats.



External vs. Internal Networks

EXTERNAL NETWORKS:

The external network is the first line of defense against cyber threats. Securing it against potential attacks is crucial to safeguard sensitive data and assets. By prioritizing security, organizations can thwart external threats and minimize the risk of data exposure or compromise.

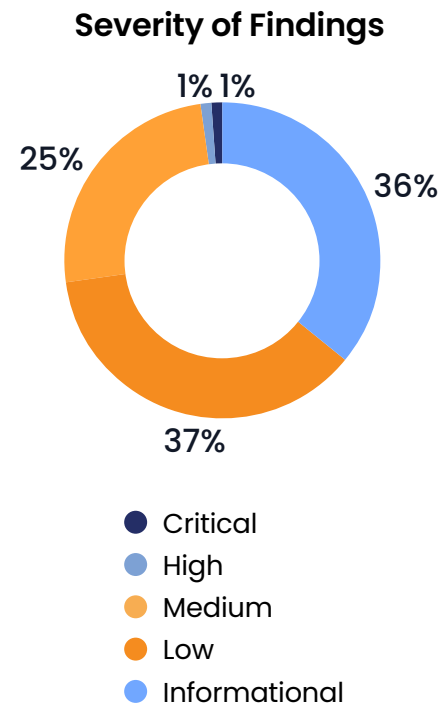
INTERNAL NETWORKS:

Even internal network can be susceptible to security breaches. Preventing unauthorized access and implementing stringent security protocols are Critical to safeguard valuable information from insider threats and other malicious actors.

APIs

APIs are one of the major enablers of digitalization across businesses, as they connect one application with another to appear as one single workflow. Meanwhile, as APIs offer a seamless experience to users and businesses, they present opportunities for cybercriminals, who can exploit endpoints to gain footholds, establish persistence, and move laterally across networks.

APIs essentially work the same way as web applications but in a headless manner. Many vendors and applications take an API-first approach. As APIs have become a core component of enabling digitalization, it is equally important to secure them as well. Despite growing awareness of API security, these breaches continue to occur.



Overall Risk Ratings of Findings

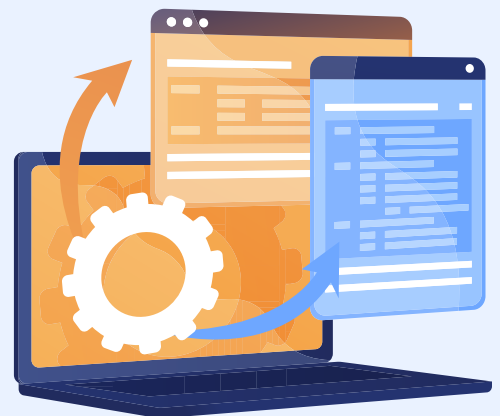
Risk Severity Analysis: The data reveals the distribution of risk findings in APIs, with Critical findings at 1%, High findings at 1%, Medium findings at 25%, Low at 37%, and Informational at 36%.

Considering the number of Medium and Low-risk findings, the highest contributor for APIs are Low-risk findings. However, it's important to understand that a 'Low' finding is not directly proportional to 'no risk'. Once an adversary has an entry point, they have the means and expertise to exploit it to the fullest.

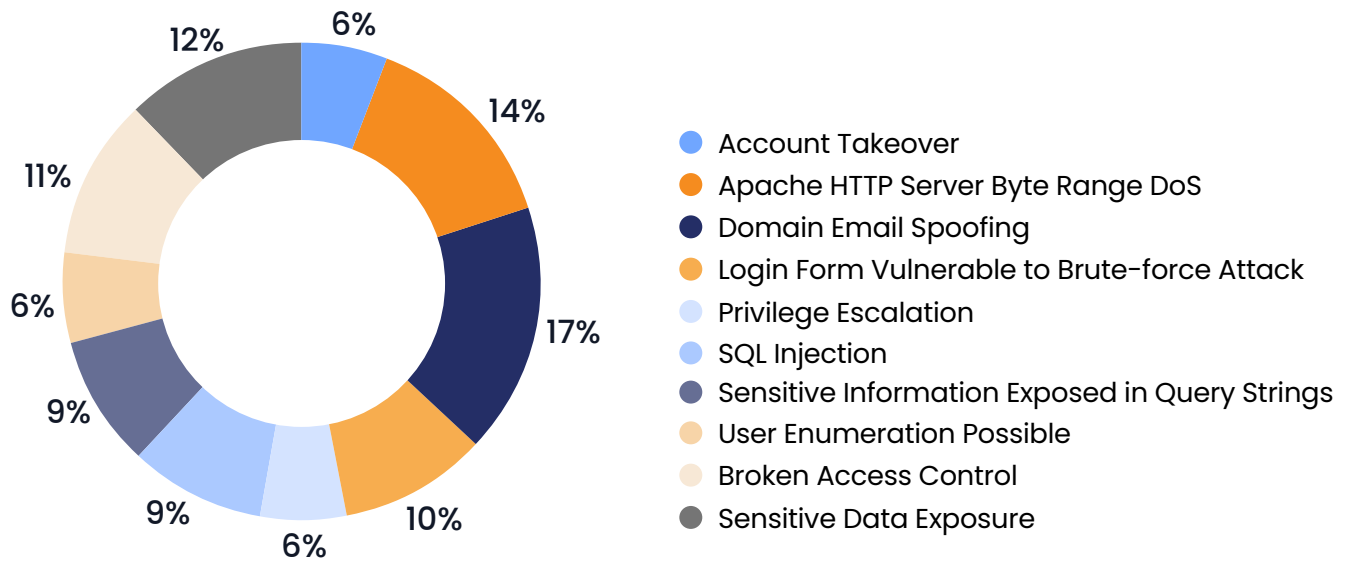
Top 10 Critical and High Vulnerabilities in APIs

The top 10 vulnerabilities in APIs are displayed below, with the top 3 vulnerabilities as follows:

- Domain Email Spoofing
- Apache HTTP Server Byte Range DoS
- Sensitive Data Exposure



Top 10 Critical and High Vulnerabilities in API



Observations

Medium and Low-risk findings contribute to over 60% of the overall API-related findings. Incorporating API security testing into all aspects of the Software Development Life Cycle has become a clear necessity, as they provide a lucrative gateway to data and systems.

The Security Misconfigurations risk is at the top of the API security leaderboard, showing that organizations can do more to mitigate this and prevent an API attack.

Recommendations

Though the distribution of risk and findings lean towards Low vulnerabilities, that does not override these requirements:

- ✓ **Conduct API Penetration Testing:** Include API pentesting in the same scope as web applications to ensure a comprehensive vulnerability assessment.
- ✓ **Enforce HTTPS Across all APIs:** Mitigate this risk to prevent Man-In-The-Middle (MITM) attacks and sensitive data leakage by implementing strict HTTPS requirements for all API communication.

MOBILE

Global organizations have witnessed a consistent rise in the usage of mobile applications especially in the age of digital transformation. Mobile apps are heavily focused and designed to deliver a specialized and targeted user experience.

Mobile apps also have compliance requirements to maintain overall security and ensure sensitive data is protected from unauthorized access, use, or disclosure. As with other assets, these compliance requirements will vary across industries and geolocations.

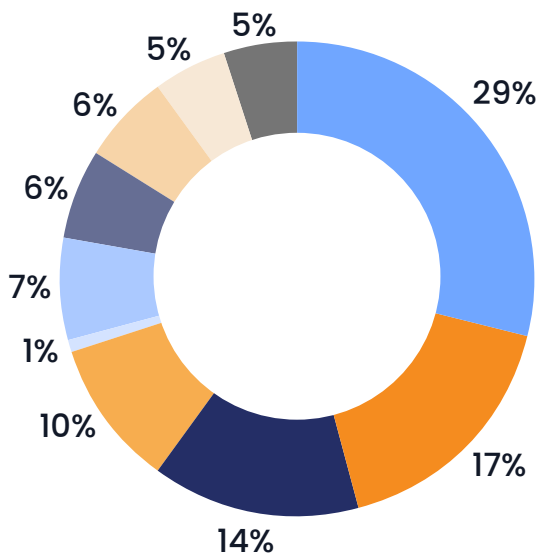
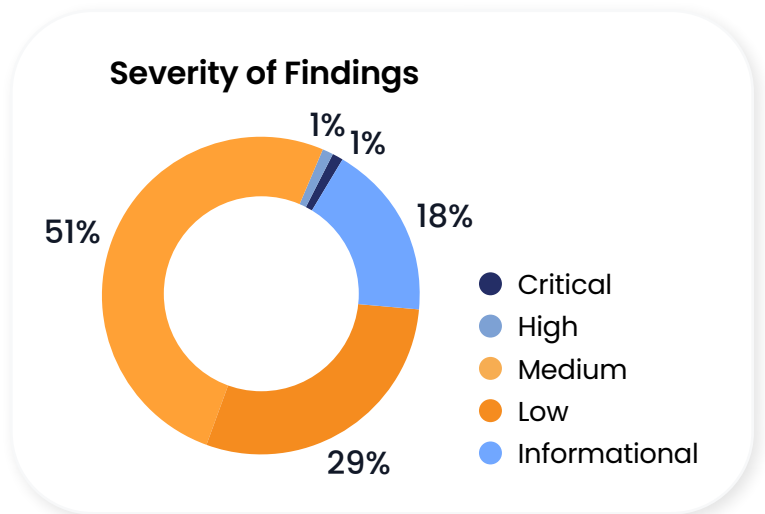
Overall Risk Ratings of Findings

Risk Severity Analysis: The data reveals the distribution of risk findings in mobile applications, with Critical findings being 1%, High findings at 1%, Medium findings at 51%, Low findings at 29%, and Informational findings at 18%.

Top 10 Vulnerabilities in Mobile Applications

The top 10 vulnerabilities in mobile applications are displayed below, with the top 4 vulnerabilities as follows:

1. Application Does Not Implement Certificate Pinning
2. Misconfigured Launch Mode Attribute
3. Janus Vulnerability



- Application Does Not Implement Certificate Pinning
- Misconfigured Launch Mode Attribute
- Janus Vulnerability
- Application Transport Security (ATS) Disabled
- No Rate Limiting Implemented
- Application Allows Backups Over ADB
- Sensitive Data Exposure
- User Enumeration Possible
- Insecure Data Storage
- User Enumeration Possible

Observations

It is observed that iOS applications have marginally fewer numbers of Critical and High findings compared to Android. However, both platforms' findings reveal similar risk scores and vulnerabilities.

Overall, 29% of the findings are related to **Certificate Pining**, which surfaces the risk of Man-In-The-Middle attack (MITM). Meanwhile, 17% of the findings are related to a **Misconfigured Launch Mode Attribute**, which exposes mobile applications to the risk of task hijacking.



Recommendations

Though the distribution of risk and findings lean toward Medium and Low severity vulnerabilities, that does not outweigh the importance of the following requirements:

- ✓ **Instill the SDLC in Mobile Application Development:** Adhere to the principles set forth for the SDLC, especially within the Continuous Integration and Continuous Development (CI/CD) pipeline.
- ✓ **Harden Mobile Apps using Industry Standards:** Use industry standards, such as the OWASP Mobile Application Security Verification Standard (MASVS), to ensure mobile applications are hardened and aligned with mobile security best practices.
- ✓ **Improve Mobile App Security with Threat Modeling:** Establish and enforce threat modeling techniques for a cyber-resilient, secure mobile application.

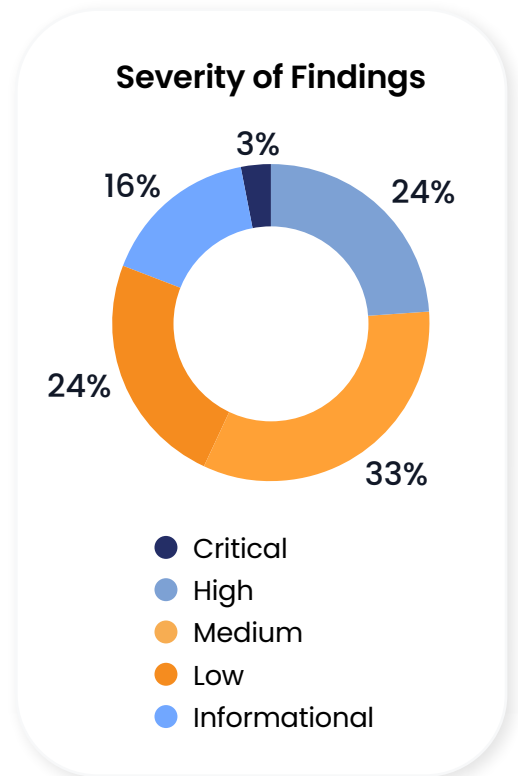
CLOUD

Cloud computing systems have become a vital part of modern business operations. However, with the increasing reliance on cloud services, new security challenges arise. Furthering the complexity, a cloud practitioner today may inadvertently contribute to the risks in cloud environments due to this complexity and ongoing evolution of the cloud.

Cloud compliance and security requirements in today's ever-evolving threat landscape have also made cloud security incredibly challenging. The following insights can help Cloud Security teams uncover common misconfigurations and risks associated with cloud environments.

Overall Risk Ratings of Findings

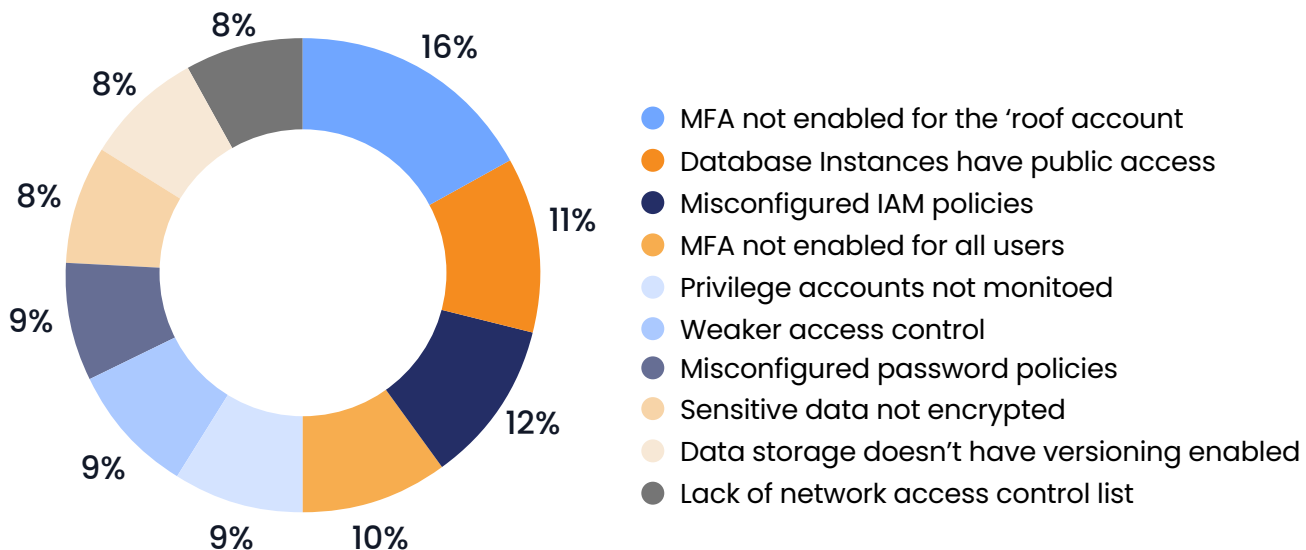
Risk Severity Analysis: The data reveals the distribution of risk findings in cloud security, with 3% Critical and 24% High findings. Meanwhile, Medium findings account for 33%, while Low findings are 24% and Informational findings are 16%, respectively.



The Top 10 Cloud Misconfigurations

The top 10 cloud misconfigurations are shown below, with the top three cloud misconfigurations as follows:

1. Multi-Factor Authentication (MFA) Not Enabled for the 'Root' Account
2. Misconfigured IAM Policies
3. Database Instances Have Public Access

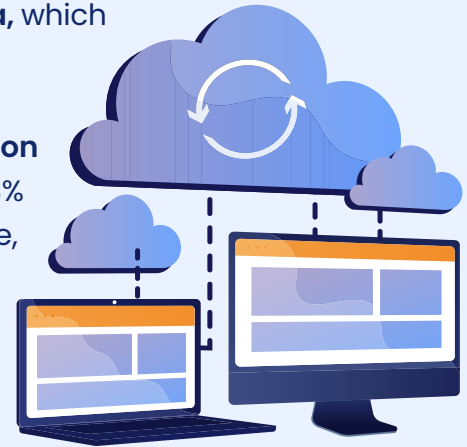


Observations

Access control acts are the baseline to guard entry points from attackers. However, in cloud services, **Access Control-related issues contribute to up to 38% of the overall findings.**

Another finding not far behind is the **Exposure of Sensitive Data**, which totals up to 27% of the overall findings.

And whether it's lacking entirely or simply inadequate, **Encryption of Sensitive Data** is another security requirement, revealed in 8% of the findings. As the security needs of an organization change, encryption is a central mechanism that protects data transfer in IT systems and digital acceleration initiatives.



Recommendations

Using the following recommendations, CloudSec teams can strengthen their cloud security, mitigate risks, and ensure the resilience of their critical business systems in cloud and hybrid environments.

- ✔ **Implement a Cloud Security Framework:** Organizations should adopt a cloud security framework aligned with industry best practices, such as the Cloud Security Alliance (CSA) Cloud Controls Matrix or the National Institute of Standards and Technology (NIST) Cloud Computing Security Reference Architecture. This type of framework will provide guidance on implementing security controls across various cloud service models.
- ✔ **Regularly Assess and Remediate Vulnerabilities:** Conduct regular assessments to identify misconfigurations and insecure cloud applications, and cloud audits to identify and address security weaknesses in cloud environments. Promptly remediate any identified vulnerabilities to maintain a secure cloud infrastructure.
- ✔ **Identity and Access Management:** Enforce strong Identity and Access Management (IAM) policies and align them with the principles of least privilege and need-to-know.
- ✔ **Educate and Train Cloud Practitioners:** Invest in training and awareness programs to ensure that cloud practitioners can securely configure and manage cloud resources. This includes training on cloud security best practices, cloud configurations, shared responsibility models, and incident response procedures.
- ✔ **Establish Incident Response and Disaster Recovery Plans:** Develop and regularly test incident response and disaster recovery plans specific to cloud environments. This ensures a swift and effective response to security incidents to minimize the impact on business operations and data integrity.

When cloud security is prioritized, organizations can ensure the security of their data and digital assets in the cloud, maintain customer trust, and prevent potential security breaches due to cloud misconfigurations.

INDUSTRIES

In this year's report, the data showed a wide range of industries conducting penetration testing. Private and public organizations of all sizes globally are represented in this report, including those from the Computer Software and Technology, Banking and Financial Services, Professional Services, Retail, eCommerce and Education, Public Sector, and Healthcare industries.

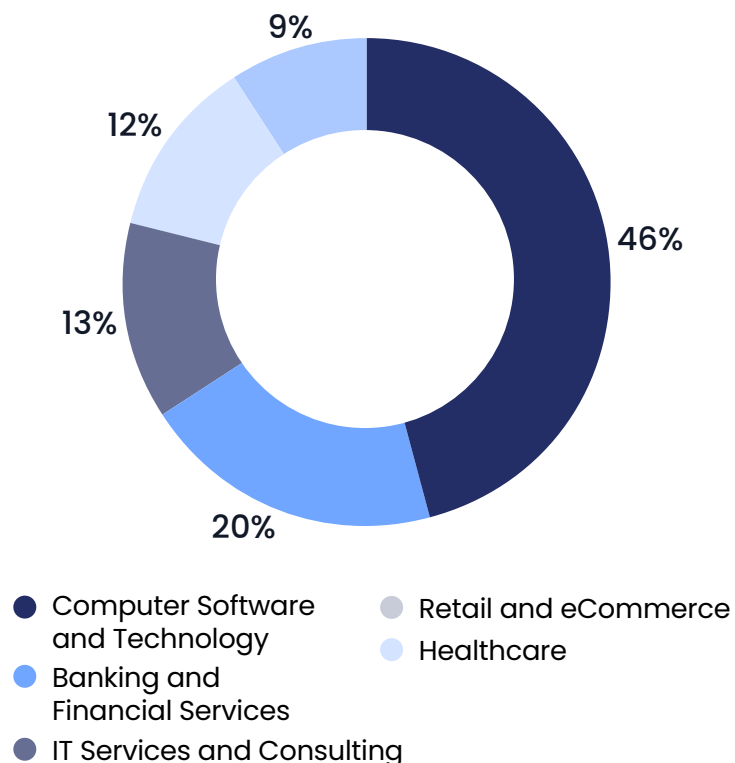
In the next pages, take a closer look at the top 5 industry pentest findings for specific risks and patterns.

Significant Industry Findings

The report focuses on the top 5 industries with the most findings, indicating their significance in terms of cybersecurity risks and regulatory requirements:

1. Computer Software and Technology
2. Banking and Financial Services
3. IT Services and Consulting
4. Retail and eCommerce
5. Healthcare

Top 5 Industries with the Most Findings



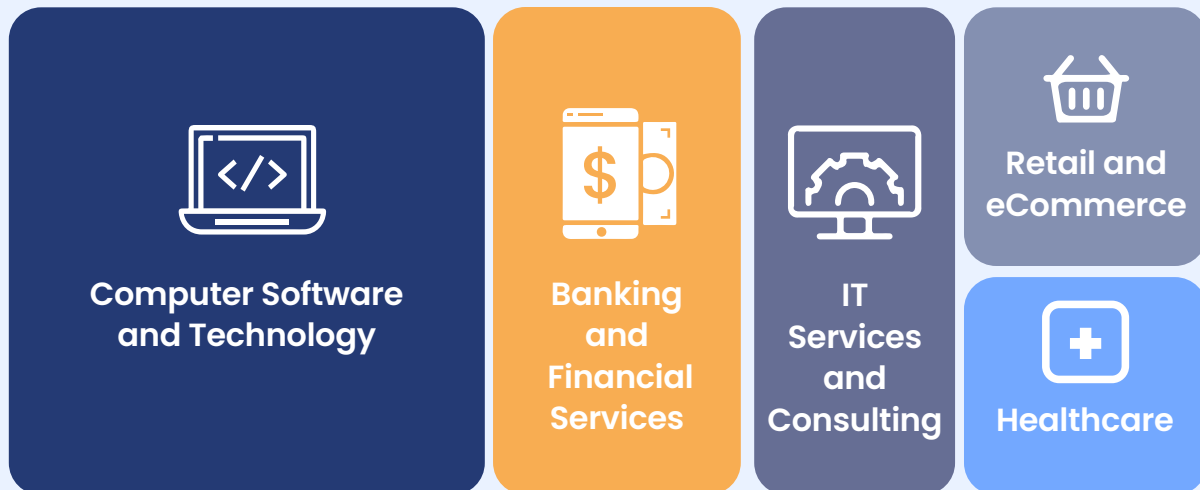
Recommendations

Based on the data observations, organizations across all industries should consider the following recommendations to enhance their cybersecurity posture:

✔ **Tailored Penetration Testing Approach:** Organizations should seek penetration testing services that offer comprehensive risk assessment and third-party certifications to meet the specific regulatory requirements of their industry. A tailored approach ensures that the unique risks and challenges of highly regulated organizations are adequately addressed.

✔ **Act with Industry-Focused Insights:** DevSecOps teams should closely examine the industry-focused insights provided in this report. These insights offer relevant findings specific to each industry, enabling teams to take immediate action to mitigate risks and strengthen security measures.

Top 5 Industries Tested 2022-2023



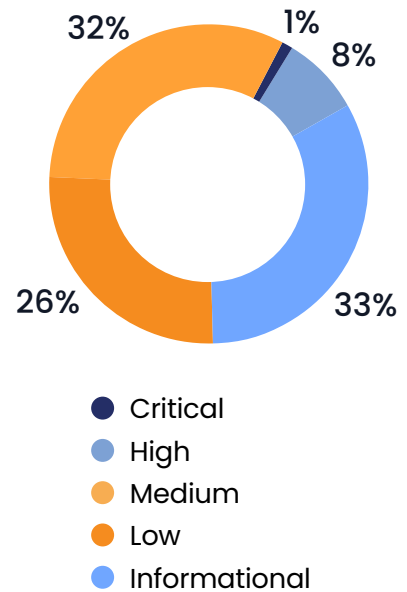
Industry Verticals that Resulted in the Highest Number of Findings

COMPUTER SOFTWARE AND TECHNOLOGY

The Computer Software and Technology industry is of paramount importance in supporting the security of the digital supply chain and ensuring third-party security. Because this industry owns the digital highway for the global supply chain, these businesses are responsible for securing their products as they connect individuals, communities, and organizations around the world.

To ensure security, computer software and technology products require secure design to preserve data confidentiality and integrity while maintaining system functionality. Technology manufacturers of physical components, such as network servers and IoT devices, have components that require ongoing patch management and firmware updates. Software products have equally vital maintenance requirements, including secure coding practices, thorough code reviews, and regular software updates to prevent vulnerabilities in operating systems and applications.

Severity of Findings

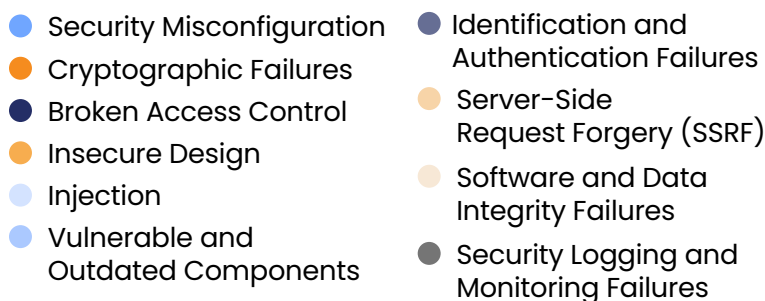


Overall Risk Ratings of Findings

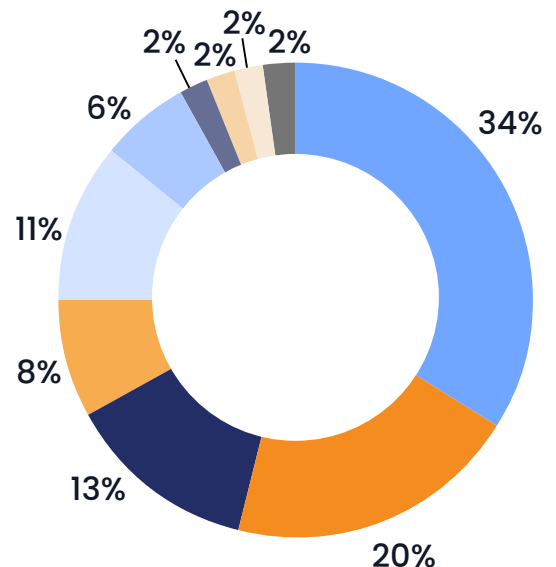
Risk Severity Analysis: The report reveals that Critical findings account for only 1% of the total findings, while High findings make up 8%. Medium findings represent the largest portion at 32%, followed by Low findings at 26% and Informational findings at 33%.

Top 3 Risks on OWASP Top 10: When mapped to the OWASP Top 10, the report identifies the top 3 categories resulting in Critical and High vulnerabilities as follows:

1. Security Misconfiguration
2. Cryptographic Failures
3. Broken Access Control



Findings categorized with OWASP TOP 10



Observations

The Computer Software and Technology industry is a key player in the cybersecurity industry. As the strength of the digital environment relies on every component, even one misconfiguration can have a domino effect on the entire supply chain. Therefore, businesses in this industry have a responsibility to secure their products to prevent downstream third-party security impacts.

Businesses in this industry compete in a fast-paced environment, and teams face constant demands for new software assets, frequent releases, and patch updates. Velocity is often prioritized over security, as goals are set to capitalize on the dynamic business landscape and grow revenue. These pressures can lead to products being released before they are adequately tested and increases the likelihood of a critical vulnerability occurring in production. This can lead to expensive breaches, revenue losses, and widespread supply chain attacks.

Recommendations

Based on the data observations and the importance of the Computer Software and Technology industry in strengthening the supply chain and third-party security, the following recommendations are suggested:

- ✓ **Balance Speed and Agility with Security:** The industry should find a fine balance between the speed of business and release with secure software releases.
- ✓ **Shift Security Left in the SDLC:** Security is not an afterthought. Security best practices, such as security testing in the SDLC, should be baked in from the inception of the development process. This leads to a stronger foundation to withstand the rigors of cyber warfare in the modern world.
- ✓ **Enforce Third-Party Security:** Given the industry's significant role in supply chain security, organizations should proactively conduct thorough vendor assessments to confirm that they meet security requirements. This will help maintain a strong supply chain and shrink the attack surface.
- ✓ **Common Criteria Certifications:** Adherence to guidelines specified for evaluating information security products help organizations build products that adhere to baseline security standards and ensure layered defenses within the digital environment.



Supply Chain Security

Supply chain security refers to the protection of assets and data shared and exchanged by third-party supply chain vendors, suppliers, and customers in order to maintain business operations.

Third parties within the supply chain have a responsibility to ensure the integrity and security of their systems and products in order to prevent vulnerabilities that could impact the supply chain and compromise sensitive information.

BANKING AND FINANCIAL SERVICES

Financial Service Institutions (FSIs) which include major banking, finance services (FinServ) and financial technology (FinTech) providers, is one of the most heavily targeted industries by cyber criminals. Because FSIs handle vast amounts of financial data and Personally Identifiable Information (PII) daily, FSIs are an extremely attractive target. Last year was no different as FSIs experienced a multitude of serious global cybersecurity incidents, leading to compromised data, including exposed customer payment card information, credentials, personal data, and other sensitive information.

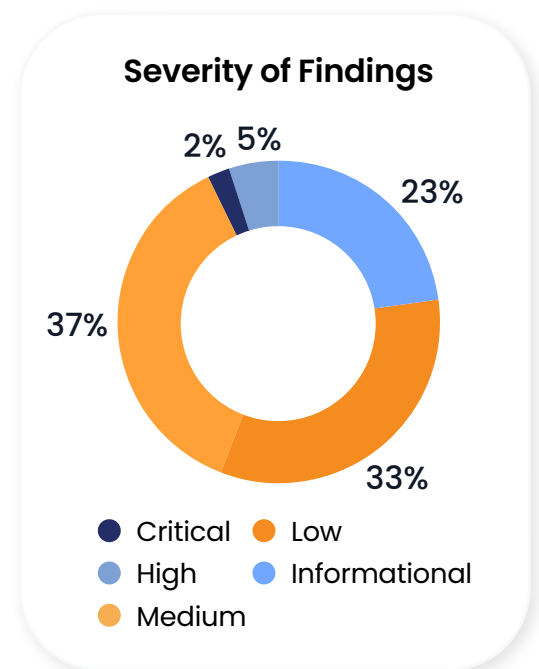
To counteract security risks and protect financial data, FSIs must adhere to stringent security standards, including the Payment Card Industry Data Security Standard (PCI DSS), for which v4.0 will be in effect in early 2025. PCI DSS compliance is essential for protecting sensitive financial information and securing the cardholder data environment (CDE).

Overall Risk Ratings of Findings

Risk Severity Analysis: The report reveals that Critical findings account for only 2% of the Total findings, while High findings make up 5%. Medium findings represent the largest portion at 37%, followed by Low findings at 33% and Informational findings at 23%.

Top 3 Risks on OWASP Top 10: The report maps the Critical and High vulnerabilities to the OWASP Top 10 categories, revealing the top 3 categories as follows:

1. Security Misconfiguration
2. Injection
3. Broken Access Control



Observations

FSIs are subject to more complex regulations with each passing year, due to the high-impact risks these businesses must manage. When a reportable breach occurs, they face revenue losses and compliance fines facing multiple risks due to the data value it holds.

Exposed Attack Surfaces: To meet customers' demands, FSIs are increasingly leveraging new applications and infrastructure. This increases their attack surface and exponentially raises the probability of misconfigurations and their digital footprint.

Excessive Access Authorization: Interacting with customers globally, organizations face challenges in finding the right balance between user experience and restricting authorized user activities. When the principle of least privilege is not enforced, excessive access authorizations can lead to unauthorized user activities and data breaches.

Recommendations

Based on the data observations, organizations should consider the following actions to improve their security posture:

✔ **Invest in Regular Evaluations and Security Automation:**

Organizations that undergo periodic security evaluations, and implement security automation, save an average of \$3M USD per breach* compared to firms that do not assess their security posture.

✔ **Prepare for PCI DSS 4.0:** Preparing to meet PCI DSS 4.0 compliance readiness will help organizations take the necessary steps to update their security systems to meet the new cardholder data environment requirements. With full compliance required by March 2025, the time to prepare is now.

What's coming with PCI DSS 4.0?

Here's what's changing regarding penetration testing and vulnerability scanning:

- **Frequency of Penetration Testing:** Penetration testing is now required quarterly, or more frequently if required by the organization's risk assessment.
- **Scope of Penetration Testing:** Penetration testing must now be performed on all systems and applications that are in the scope of PCI DSS. This includes systems and applications in the cloud, as well as those that are connected to the cardholder data environment (CDE).
- **Qualifications of Penetration Testers:** Penetration testers must now be qualified to perform PCI DSS penetration testing. This means that they must have the necessary experience, knowledge, and skills to identify and exploit vulnerabilities in PCI DSS environments.
- **Reporting Requirements:** The reporting requirements for penetration testing have also been updated in PCI DSS 4.0. The penetration test report must now include more detailed information about the vulnerabilities that were identified, as well as the steps that have been taken to remediate them.

PCI DSS 4.0 also introduces new requirements for vulnerability scanning that includes:

- **Qualified Scanner:** Vulnerability scanning must now be performed using a qualified scanner.
- **Certified Results:** The results of vulnerability scanning must now be reviewed by a qualified security professional.
- **Continuous Scanning:** Vulnerability scanning must now be performed regularly, as determined by the organization's risk assessment.

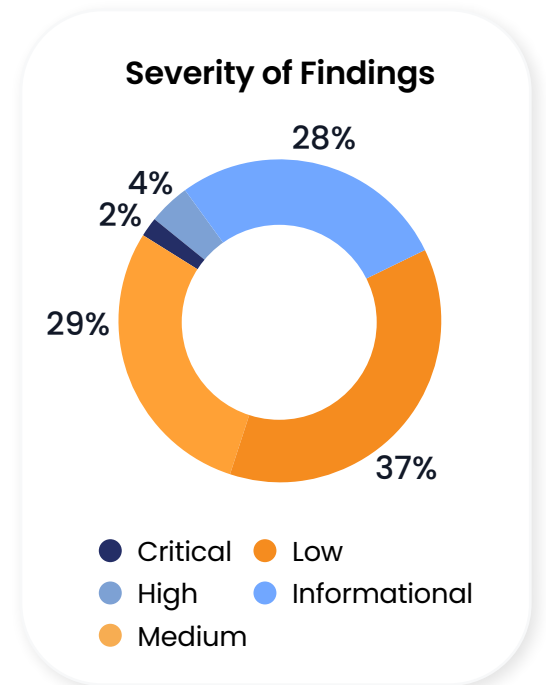
*Source – IBM's Cost of a Data Breach Report 2023



PCI DSS 4.0

PCI DSS 3.2.1 requirements are changing, and PCI DSS 4.0 will be required by March 2025.

The upcoming changes for the 4.0 penetration testing and vulnerability scanning requirements are designed to improve the security of PCI DSS environments. This includes requiring more frequent penetration testing and vulnerability scanning, as well as by specifying the qualifications of penetration testers and the content of penetration test reports.



Due to the nature of work, IT Services & Consulting and Managed Security Service Providers (MSSPs) have access to receive, and store highly confidential sensitive information relating to their clients. As such, they have become increasingly attractive targets for cybercriminals, as breaching into one service provider will help them gain access to the MSSP's customer environments as well. MSSPs are no longer immune to a singular breach as just one incident can affect a multitude of customers and organizations emphasizing the need for stringent security controls.

Overall Risk Ratings of Findings

Risk Severity Analysis: The report highlights the significant difference between the number of Critical risk findings (2%) and the total of High-risk findings (4%). Medium-scored findings make up the largest portion (29%), followed by Low (37%) and Informational (28%) findings.

Top 3 Risks on OWASP Top 10: The report maps the Critical and High vulnerabilities to the OWASP Top 10 categories, revealing the top 3 findings as follows:

1. Security Misconfiguration
2. Broken Access Control
3. Cryptographic Failures

Observations

IT Services and Consulting firms as well as MSSPs are responsible for providing highly specialized services to their clients. Due to the speed and agility in which these businesses must deliver, this industry sector has more findings in this year's report for both internal and external infrastructure.



The findings indicate that these businesses are facing security challenges in several key areas. First, remote work security has become a major concern as the working environment has expanded beyond traditional borders, making it difficult to secure the growing attack surface. This is due to evolving security and privacy requirements, as well as restrictions on cross-border data transfers. Secondly, unsuspecting employees are falling prey to phishing and social engineering attacks. The lack of employee security awareness can inadvertently lead to data breaches. Lastly, these businesses face substantial risks that can impact the supply chain, along with the challenge of meeting the third-party security requirements of their customers and partners. The findings demonstrate the complex risks these businesses have to manage.

Recommendations

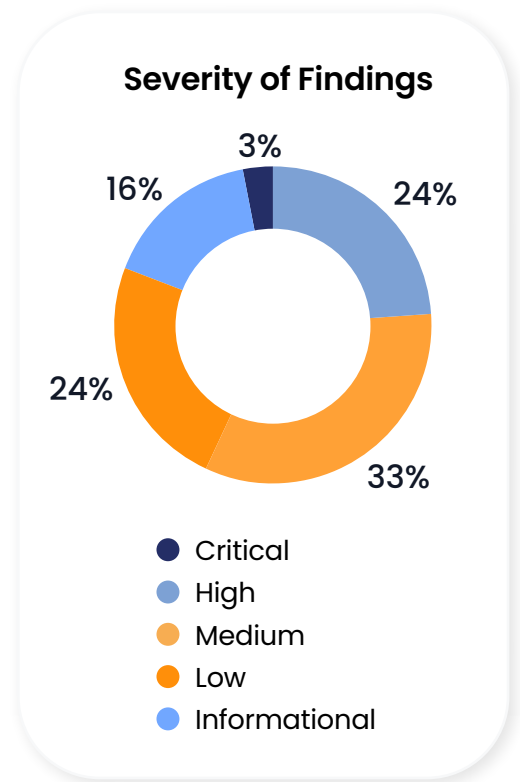
Based on the data observations, IT Services & Consulting organizations should consider the following actions to improve their security posture and ensure regulatory compliance readiness:

- ✔ **Establish Defenses for Sensitive Data Leakage:** Due to the requirement of handling sensitive datasets, Data Leakage Prevention (DLP) solutions can protect against the leakage of sensitive information, in addition to intentional or unintentional exfiltration.
- ✔ **Security Awareness Training:** Security awareness training is a central component of an organization's security-first culture. These regular trainings help keep employees apprised of the ever-changing threat landscape and trained on how to report suspicious emails to security operations.
- ✔ **Enforce Third-Party Security:** Threat actors in recent years have put IT Services and Consulting businesses on notice, due to the profitable targets within their customer databases. Therefore, such businesses as MSP/MSSPs and even Managed Detection and Response (MDR) providers must hold themselves to a higher standard to proactively protect and defend their IT environment against potential attacks that could ultimately affect their customers' overall security.
- ✔ **Conduct Penetration Testing Aligned with Your Risk Tolerance:** Regularly conduct penetration testing to meet the risk objectives of an organization. This proactive approach, with the right penetration testing provider, helps IT Services and Consulting firms identify and remediate security risks consistently and effectively. This will help organizations stay ahead of emerging threats, maintain compliance readiness for auditing, and accelerate timely remediation activities identified by the certified pentester.

RETAIL AND ECOMMERCE

The Retail and eCommerce industry has experienced significant digital transformation due to technological advancements and changing consumer behavior. These changes are a double-edged sword that enhances convenience but also increases security concerns. As digital platforms have become increasingly vital for shopping and touchless payments, this industry faces various cybersecurity challenges and strict compliance requirements to conduct business online and in physical stores. Regulations, such as the Payment Card Industry Data Security Standard (PCI DSS), General Data Protection Regulation (GDPR), and the California Consumer Privacy Act (CCPA), are top compliance priorities.

To protect customer data, maintain trust, and enforce compliance, Retail and eCommerce businesses must prioritize security investments, manage financial security and privacy requirements, and test systems routinely. By fostering a compliance-ready and security-conscious culture, these businesses can enhance their security posture, safeguard customer data, and maintain compliance.



Overall Risk Ratings of Findings

Risk Severity Analysis for Retail & eCommerce: The report highlights the number of Critical risk findings (1%) and the total of High-risk findings (2%). Informational-scored findings make up the largest portion (37%), followed by Medium (30%) and Low (37%) findings.

Top 3 Risks on OWASP Top 10: The report maps the critical and high vulnerabilities to the OWASP Top 10 categories, revealing the top 3 findings as follows:

1. Security Misconfiguration
2. Cryptographic Failures
3. Broken Access Control



Observations

The data indicates Retail & eCommerce businesses follow a very similar pattern to other industries in this report. While Critical and High findings are rapidly remediated, Medium and Low-risk vulnerabilities are not mitigated at the same pace.

To succeed in this extremely competitive industry, businesses are deploying feature-rich, user-friendly web applications designed to grow maximum revenue. However, when convenience is prioritized over security, security requirements can take a back seat. This approach creates the perfect storm for Medium and Low-risk findings to remain open and on the backlog. Left unmitigated, a large volume of these types of risks can increase the overall risk of a cyber attack, as they can collectively form attack chains that pose imminent threats in the right circumstances.



Recommendations

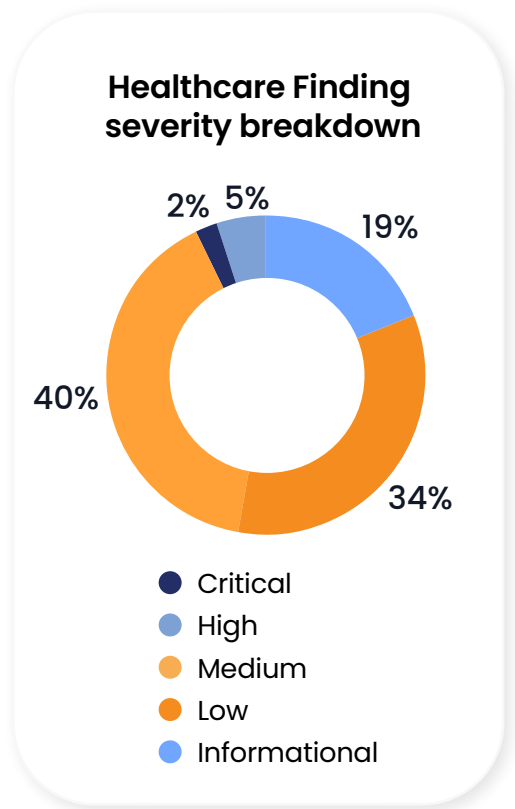
Establishing a core **cybersecurity** program focused on compliance readiness and security preparedness is crucial for Retail and eCommerce businesses. In order to grow revenue, these businesses should consider the following recommendations to build safe and secure retail operations.

- ✔ **Improve Web App Security:** Prioritize web application security to protect sensitive customer data. Implement secure coding practices to overcome risks such as Cross-site Scripting (XSS), SQL injections, prevention from brute force, etc. by continuously assessing the application against OWASP Top 10.
- ✔ **Implement SSL Certificates:** Secure Sockets Layer (SSL) certificates verify a website's identity and serve as an encrypted connection. SSL certificates protect credit card details and other potentially sensitive transactions facilitated on e-commerce websites and prevent hackers from using websites as part of a phishing attack.
- ✔ **Secure APIs:** Retail and eCommerce applications have a plethora of capabilities, including processing payments, invoking third-party APIs, etc. Assessing third-party API libraries for known vulnerabilities can save a lot of time and effort in preventing and recovering from an API-related cyber attack.
- ✔ **Use Multi-layer Security:** Multi-layer security adds more obstacles making it more difficult to access sensitive information, such as MFAs, CDNs, Firewalls, IDS/IPS, etc. These measures will slow down an attacker and raise sufficient alarms for the organization to either react or proactively stop an attack.
- ✔ **Focus on PCI DSS 4.0 Compliance Readiness:** By proactively preparing for PCI DSS 4.0 and any compliance-related requirements, such as GDPR and CCPA, Retail and eCommerce businesses can secure data, PII, and the cardholder data environment to meet regulations on time. Areas to focus on include security and privacy policies, access controls, data protection measures, such as encryption and pseudonymization, and routine compliance assessments.

HEALTHCARE

In the healthcare sector, patient care is number one. Therefore, cybersecurity is critical for healthcare organizations and their affiliates as they protect and defend patient care. The security of IT systems, data, and users is paramount for operational continuity and compliance of critical medical systems, devices, and patient records that comply with HIPAA (Health Insurance Portability and Accountability Act). As a result, the healthcare industry continues to be a prime target for cybercriminals due to the sensitive, life-saving nature of the day-to-day operations, equipment, and sensitive data that must be stored, shared, and managed.

Healthcare facilities store vast repositories of patient information, making them lucrative targets for cyberattacks. As healthcare cyber attacks can directly impact human life, these findings highlight the urgent need for strengthening cybersecurity measures to enforce HIPAA compliance, safeguard patient privacy, and protect patient care.



Overall Risk Ratings of Findings

Risk Severity Analysis for Healthcare: The report highlights the number of Critical risk findings (2%) and the total of High-risk findings (5%). Medium-scored findings make up the largest portion (40%), followed by Low (34%) and Informational (19%) findings.

Top 3 Risks from OWASP Top 10

The report maps the Critical and High vulnerabilities to the OWASP Top 10 categories, revealing the top 3 findings as follows:

1. Security Misconfiguration
2. Cryptographic Failures
3. Broken Access Control



Observations

The data reveals that healthcare organizations should prioritize addressing Medium and High-risk findings, as they make up a significant portion of the total findings. The lower percentage of Critical risk findings suggests that organizations may already be focusing on mitigating these risks, but there is still room for improvement.



Moreover, the top 3 OWASP categories with the highest number of Critical and High vulnerabilities should be prioritized for remediation. Security Misconfiguration, Cryptographic Failures, and Broken Access Control risks can lead to severe consequences if exploited by attackers, such as unauthorized access to sensitive data, system compromise, and loss of data integrity. If compromised, HIPAA-compliant healthcare organizations and their affiliates have to report breaches to the U.S. Office of Civil Rights, per the HIPAA Breach Notification Rule. For example, a U.S. Department of Health and Human Services' Office for Civil Rights (OCR) investigation could ensue due to breaches of protected health information (PHI) and trigger an audit to determine whether the privacy and security of patients' health information has been properly secured.

Recommendations

Based on the data observations, healthcare organizations should consider the following actions to improve their security posture and ensure HIPAA compliance readiness:

- ✔ **Invest in Cybersecurity:** The repercussions of a breached PHI record are higher than the investment to secure it; hence, healthcare organizations should invest more in cybersecurity to reduce the risks of cyber attacks.
- ✔ **Prioritize Medium and Low-Risk Findings:** Allocate resources to address Medium and Low-risk findings, as they make up a significant portion of the total findings. This will help reduce the overall risk exposure and strengthen the organization's security posture.
- ✔ **Enforce HIPAA Compliance Requirements:** Ensure that all systems and processes are compliant with HIPAA regulations. This includes implementing appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of electronic protected health information (ePHI).
- ✔ **Conduct routine HIPAA Penetration Testing:** Regularly conduct HIPAA penetration testing to identify and remediate security risks related to ePHI. This will help organizations stay ahead of emerging threats, enforce HIPAA compliance, and secure patient data.

By following these recommendations, healthcare organizations can improve their security posture, ensure HIPAA compliance readiness, and protect sensitive patient data from potential cyber threats.

CONCLUSION

The latest trends in cybersecurity reveal that the threat landscape is continuously evolving, with ransomware attacks on the rise and bad actors employing increasingly sophisticated tactics, techniques, and procedures (TTPs). Persistent cyber criminals are becoming more emboldened, the dark web is getting darker, and publicly available AI tools are presenting new risks organizations must manage.

The purpose of this report is to provide the security community with a comprehensive overview of internal and external assets and the most common associated vulnerabilities via pentesting. The report provides insights and broader context into these CVEs in hopes of facilitating continued collaboration and a holistic approach to defending your overall security ecosystem.

As cybersecurity is increasingly democratized and shared among teams as a collective responsibility, it is essential for all industries and organizations of all sizes and geographies to unite in their efforts to create a more secure digital environment for everyone.

KEY TAKEAWAYS



Reflecting on this year's analysis, these are the key insights, actions, and takeaways to share with your security teams and stakeholders. Use these insights to update your security program's roadmap for success

Security Maturity Costs Significantly Less Than a Data Breach:

Due to an all-time high of continued ransomware attacks and incidents in 2023, the overall costs for victims to recover from a successful breach has reached \$4.45M globally and a staggering \$9.48M for U.S. organizations.* The cost of a mature security program pales by comparison to the average cost of a successful attack.

Secure the Supply Chain with Third Party Security Risk Management:

The supply chain is a critical component of ensuring successful operations within all service organizations. However, supply chain vendors, partners, and contractors also pose the most significant risk. It is important that organizations invest not only in securing their own IT environment, but those of existing and new supply chain partners requiring regular testing and assessment of security controls as a cost of conducting business together.

*Source – IBM's Cost of a Data Breach 2023

💡 Securing the Software Development Life Cycle (SDLC):

DevOps teams must drive faster more secure release cycles to accelerate innovation for their organizations, but it also poses significant risk. Security teams must identify and understand the impact of runtime vulnerabilities in their production environments through routine security testing, while avoiding backlogs, in order to gain visibility across all stages of SDLC to mitigate risk.

💡 Improve Security in Hybrid and Remote Working Environments:

While hybrid and remote work environments offer flexibility for employees and employers, they introduce new risks. Common remote work security risks include accessing sensitive data through unsafe Wi-Fi networks, using personal devices for work, using weak and reused passwords, and practicing unencrypted file sharing. By implementing strong network security controls, such as segmentation, VPN, and DLP, organizations can substantially reduce risks and decrease the probability of a breach.

💡 Enhance Cloud Security:

Cloud security is essential to safeguard sensitive data, applications, and services stored in and accessed through cloud environments. Using continuous security validation tools like pentesting can protect against unauthorized access, data breaches, and malicious activity.

💡 Proactively Reduce IoT Risk:

The connected IoT market is expected to reach \$75B by 2025*. But IoT environments connected to critical infrastructure industries are prime targets for cyber criminals. Utilities, Oil & Gas, and manufacturing are just a few industries that have experienced expensive security incidents. Proactive security testing and vulnerability management will help identify vulnerabilities in your inter-connected IoT security environment.

💡 Continuous Penetration Testing and Vulnerability Assessments:

The growth of an organization's digital footprint directly correlates with an increased attack surface. Proactive mechanisms, such as continuous penetration testing and vulnerability assessments, provide remediation roadmaps to security assets, systems, and data while establishing compliance readiness.

*Source – [statista.com](https://www.statista.com)

BreachLock is committed to helping you 'Find and Fix the Next Cyber Breach.'

We hope this report has helped to provide new insights and guidance to address the ever-evolving changes in the cybersecurity landscape. By working together, we can collectively strengthen cybersecurity and create a safer digital world for all.



Disclaimer

This report is intended for informational purposes only and is not a substitute for (1) professional advice, or (2) penetration testing conducted for a specific business. Although BreachLock believes the data presented in this report is appropriate for generalization purposes, BreachLock makes no claims that the findings of this report are indicative of all vulnerabilities generally nor vulnerabilities in any particular industry. BreachLock does not accept any legal responsibility for errors, omissions, or claims, nor does it provide any warranty, express or implied, as to the accuracy, adequacy, or completeness of any of the information contained herein.






Copyright ©2023 BreachLock Inc. All rights reserved.

The information, methodologies, data, and opinions contained or reflected herein are based on the anonymized, aggregated data of BreachLock customers and are therefore proprietary and may not be copied, distributed, or used for any commercial purpose. However, you may use its contents for non-commercial purposes that classify as "fair use," such as personal, educational, and research purposes, provided you cite BreachLock and make reference to its website: **breachlock.com**.

Why BreachLock




BreachLock offers fully automated, AI-enabled, and human-delivered pentesting solutions based on a standardized built-in framework and platform that enables consistent and regular benchmarks of attack techniques, security controls, and processes. By creating a standardized framework, BreachLock elevates your security validation process delivering enhanced predictability, consistency, and more accurate results in real-time, every time.

With BreachLock, you gain the following advantages:

-  **Expert Support and Advanced Controls:** DevOps and SecOps teams enjoy expert-led engagements, advanced security controls, and exceptional customer support without disrupting operations.
-  **Reduced Risks and Improved Compliance:** PTaaS clients can lower security risks and enhance compliance outcomes without additional expenses for personnel or tools.
-  **DevSecOps Integration:** BreachLock's PTaaS enables efficient remediation to support the DevSecOps process with API workflow and ticketing integrations.
-  **Faster Turnaround:** BreachLock's PTaaS accelerates pentesting with real-time results and access to in-house experts, ensuring quick vulnerability identification and remediation.
-  **Eliminate False Positives:** BreachLock's automated and human-delivered pentesting approach identifies and validates security findings with speed, eliminating false positives based on AI-driven contextual insights around the most exploitable points of interest by an attacker.

Start Your Next Pentest in One Business Day

BreachLock, the pioneer behind Pentesting as-a-Service (PTaaS), enables security leaders and their teams to take control of their penetration testing investments like never before. Unlike other platforms, BreachLock delivers fast and comprehensive an AI-driven penetration testing platform that offers a more advanced and nuanced approach to testing and deeper and more enriched contextual insights.

-  Simplify penetration testing with an easy-to-use portal, dedicated customer success team, and certified, in-house penetration testers.
-  Save time with faster pentests that can start in one business day, with in-house experts ready to provide full-stack, compliant penetration testing and red teaming services.
-  Maximize value with DevSecOps remediation supported by expert customer support, API ticketing integrations, retesting, reporting, and scanning benefits.