INSIGHTS FROM WASP

The State of Penetration Testing in 2024

The State of Penetration Testing in 2024

INSIGHTS FROM WASP

By OP Innovate Research Team

The State of Penetration Testing in 2024 offers a comprehensive analysis of the vulnerabilities uncovered by OP Innovate and its partners over the past year. These findings stem from our meticulous human-led penetration testing efforts coupled with the advanced capabilities of our innovative Web Application Security Platform (WASP).

WASP is a comprehensive security platform that integrates continuous automated testing with expert-driven manual penetration testing, offering a complete view of vulnerabilities to help organizations identify, prioritize, and remediate potential security risks.

Drawing on data from engagements of OP Innovate and its partners, along with customer-submitted findings, this report offers strategic insights to help organizations mitigate risks and enhance their security postures by analyzing key vulnerabilities, their business impacts, and the trends shaping cybersecurity practices.

This year's analysis identified vulnerabilities across a range of asset types, from web applications to cloud services and APIs.

The findings highlight the growing importance of automation in streamlining security operations, with nearly 80% of vulnerabilities detected using WASP's automated tools, complemented by manual penetration testing to uncover complex and nuanced security risks.

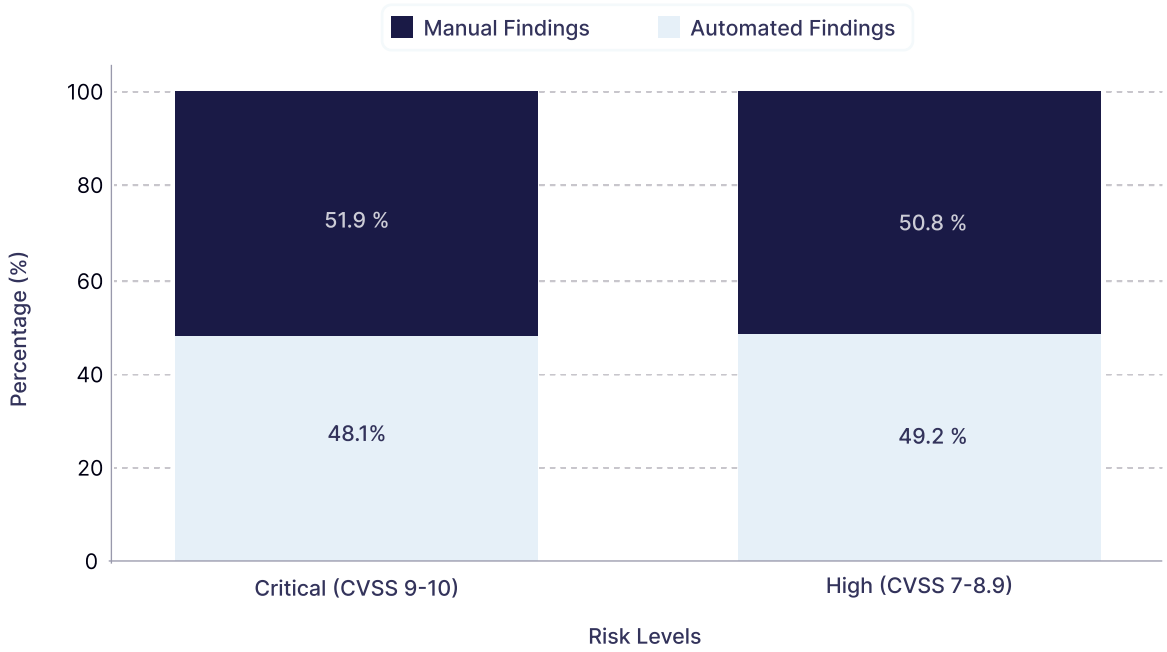
The findings and recommendations presented in this report are intended to guide cybersecurity leaders in refining their strategies and achieving a more resilient security posture in the coming year.

Note: The findings presented in this document are solely derived from the vulnerabilities identified through our work and that of our partners over the past year. They do not take into account third-party threat data or external efforts.

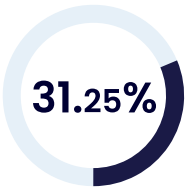
Executive Summary

78.9% of the discovered vulnerabilities were identified through the automated tools integrated within our WASP platform, while the remaining 21.1% were discovered via manual penetration testing efforts conducted by our highly certified team.

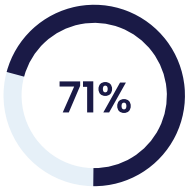
Although the majority of our findings were generated through automated testing, manual penetration testing played a much more significant role in identifying more nuanced, higher risk vulnerabilities, accounting for nearly 85% of all identified high and critical-risk vulnerabilities.



It's also worth pointing out that a significant portion of automated findings (both critical and high) were either false positives or dismissed. Manual testing was crucial for filtering these out and identifying actionable vulnerabilities that automated systems missed or misclassified.



of automated high-severity findings dismissed or FP vs 7.8% of manual high-severity findings



of automated critical-severity findings dismissed or FP vs 0% of manual critical-severity findings

Combining the speed and scale of automation with the expertise of manual testing delivers unmatched efficiency and depth in vulnerability management.

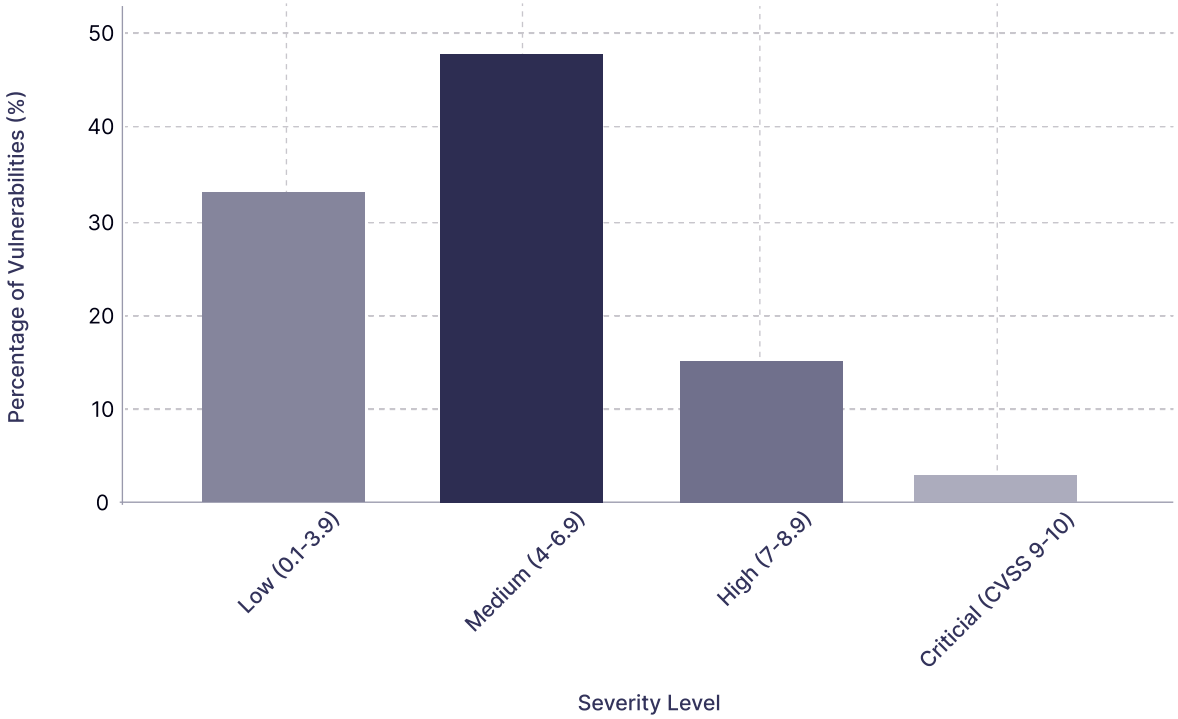
Vuln. IDs:

1,223

unique vulnerability titles highlight a wide range of issues.

Of all the vulnerabilities identified by OP Innovate and our partners in 2024, almost 15% were high-risk or above. These findings are in line with other industry reports, which suggest that around 80% of vulnerabilities are informational or low-severity, highlighting the disparity between the sheer volume of findings and the truly urgent threats.

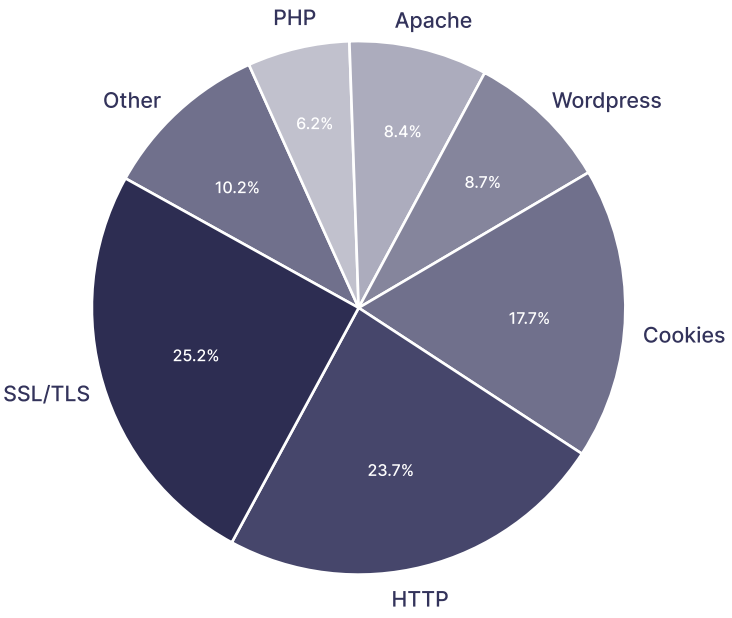
Here is the severity distribution of vulnerabilities in WASP with a CVSS score:



Targeted Asset and Service Types

Over one-third (38.2%) of all identified vulnerabilities were discovered in web applications, underscoring their critical role in business operations and their high exposure as a primary attack surface for threat actors. With their reliance on APIs and cloud integrations, these applications are increasingly vulnerable to sophisticated attacks.

API endpoints account for 16.1% of the vulnerabilities, while cloud services make up 5.6%



Assets with most vulnerabilities:

1. **Web applications**
2. **API endpoints**
3. **Cloud services**

When it comes to the most “vulnerable” technologies, the top three were:

1. **SSL/TLS**
2. **HTTP**
3. **Cookies**

Automated vs. Manual Findings

SSL/TLS vulnerabilities often stem from outdated encryption protocols, misconfigured certificates, or the absence of secure headers like HSTS. These issues leave applications exposed to attacks such as man-in-the-middle (MITM) and eavesdropping.

Most SSL/TLS vulnerabilities were discovered via automated testing, where the two most common issues were:

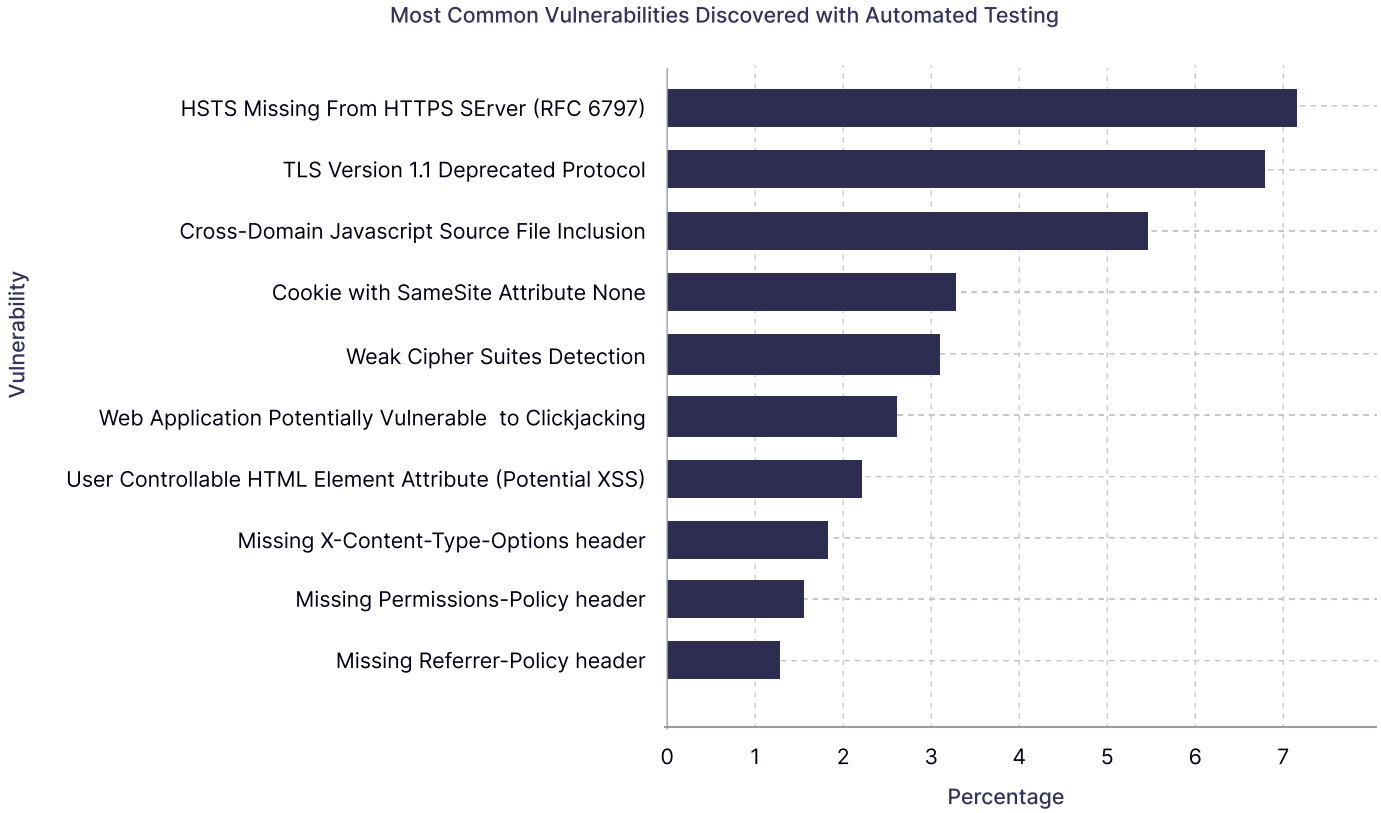
HSTS Missing From HTTPS Server

Represents approximately 7.1% of all automated findings.

TLS Version 1.1 Deprecated Protocol

Accounts for around 6.8% of all automated findings.

This highlights the prevalence of specific SSL/TLS issues among vulnerabilities detected through automation.



While automated tools excel at identifying vulnerabilities quickly, manual efforts remain indispensable for uncovering nuanced, context-specific risks.

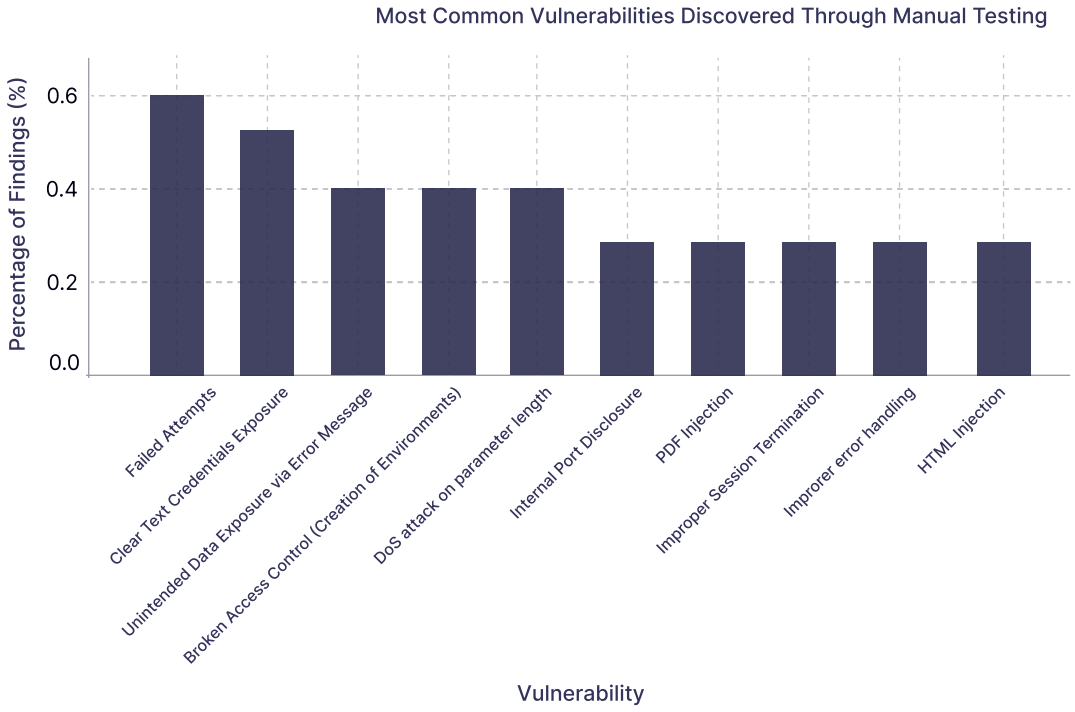
One thing to note about the above vulnerabilities, and most others identified with automated scanning, is that while they technically present a risk, the practical exploitability is often limited by high attack complexity.

For example, vulnerabilities like HSTS and TLS1.1 are associated with man-in-the-middle (MITM) attacks. Exploiting these vulnerabilities requires the attacker to intercept and manipulate (not merely read) data between the user and the vulnerable website.

To achieve this, the attacker would need to position themselves within the same local Wi-Fi network or have access to the ISP, which significantly raises the complexity of the attack. As a result, the practical risk of such exploits is often too minimal to warrant concern in most scenarios.

Over the past year, the OP Innovate team and partners uncovered some recurring high-risk issues through manual testing, all closely related to the top 10 vulnerabilities identified by OWASP:

- **Broken Access Control:** Vulnerabilities that permitted unauthorized users to perform actions such as creating, modifying, or deleting resources, potentially compromising sensitive data or system integrity.
- **Unintended Data Exposure via Error Message:** Misconfigured error messages inadvertently disclosed internal information, creating opportunities for attackers to exploit system weaknesses.
- **Input Validation (such as XSS):** Improper input handling allowed attackers to inject malicious scripts,resulting in data theft, account compromise, or other unauthorized actions.
- **Inadequate Handling of Failed Attempts:** Repeated unsuccessful actions exposed potential weaknesses, such as system behavior patterns or poorly managed error responses.
- **Clear Text Credentials Exposure:** Unencrypted credentials left sensitive information vulnerable to interception or unauthorized access.



Balanced Approach: Automated tools quickly identify widespread issues, while manual testing zeroes in on complex, high-impact threats.

Recurring Weaknesses

The data revealed several recurring vulnerabilities across various industries, many of which remain unaddressed due to their perceived low urgency, despite being relatively easy to resolve. Analyzing the cost of remediation reveals that addressing these issues often requires minimal effort, making them a valuable opportunity to significantly enhance overall security.

- **Missing Security Headers:** Common issues included missing configurations such as HSTS and SameSite cookies. These vulnerabilities are frequently overlooked but can typically be resolved with a simple configuration update or by enabling a checkbox in the settings
- **Outdated JavaScript Libraries:** Libraries like DOMPurify and moment.js, which are no longer actively maintained, contributed to a significant number of high-severity findings. While considered lower priority, replacing these libraries is straightforward and helps maintain both security and compliance.
- **Cross-Site Scripting (XSS) and Injection Vulnerabilities:** These risks persist due to recurring coding errors and inadequate input validation. Addressing these issues often involves adopting secure coding practices or enabling existing safeguards, such as input sanitization functions.

Many of these vulnerabilities are easy targets that attackers exploit repeatedly, yet they can often be resolved quickly with the implementation of proper processes.

The Impact of High and Critical-Severity Findings

Top High-Severity Vulnerabilities by Title

Based on our data, the following are the most frequently observed high-severity vulnerabilities:

1. **Potential Organizational Credential(s) Leaked**
2. **Deprecated JS package vulnerabilities (DOMPurify, nextjs, moment.js)**
3. **Webflow Subdomain Takeover Vulnerability**

Our **deep web scanner** frequently identifies potentially leaked credentials exposed on the Dark Web. These credentials are sometimes sold, potentially granting malicious actors access to sensitive organizational systems. Additionally, our **threat intelligence capabilities** enable us to detect infostealer-based credential leaks and trace their origins, including the specific breached machine, within hours of the breach - often before they appear on Dark Web marketplaces.

Deprecated JavaScript Packages pose a significant risk because they are no longer actively maintained or supported by developers. While not inherently vulnerabilities, these packages can quickly become threats if a zero-day exploit is discovered, as there is no longer anyone to patch or fix the issue.

To mitigate this risk, organizations should conduct regular dependency audits using tools like **npm audit** or **Snyk** to identify and replace outdated or vulnerable libraries.

Additionally, misconfigurations in web applications and cloud services are pervasive. Leveraging configuration scanning tools, such as those available in **WASP**, can help identify and remediate insecure settings, reducing exposure to potential attacks.

Top High-Severity Vulnerabilities by Title

On several occasions, high-severity vulnerabilities we uncovered were linked to known CVEs. The most common ones were:

1. **CVE-2024-4580**
   The Master Addons plugin for WordPress is vulnerable to stored cross-site scripting (XSS) via several parameters.
2. **CVE-2023-4629**
   A vulnerability in Next.js versions up to 13.4.20 which allows attackers to bypass certain security restrictions.
3. **CVE-2022-2478**
   A vulnerability in Moment.js allows for regular expression denial of service (ReDoS) attacks.
4. **CVE-2022-3112**
   A vulnerability in Webflow's subdomain management could allow attackers to perform subdomain takeovers.

To stay updated with the latest threats and exploited CVEs, follow our Cyber Threat Intelligence (CTI) updates.

Vulnerability Detection and Remediation Times

The Cybersecurity and Infrastructure Security Agency (CISA) recommends the following remediation timeframes:

Critical Vulnerabilities
Remediate within 15 calendar days of detection.

High-Severity Vulnerabilities
Remediate within 30 calendar days of detection.

However, many organizations struggle to meet these benchmarks. According to Edgescan's 2023 Vulnerability Statistics Report, the Mean Time to Remediate (MTTR) for high and critical severity vulnerabilities ranges from 45 to 51 days. This means high-risk vulnerabilities often go unaddressed for over two months, leaving organizations exposed to potential exploitation.

In contrast, **WASP customers** achieved a significant reduction in their MTTR for high and critical severity vulnerabilities, averaging just below **31 days.**

31 days

MTTR for critical vulnerabilities in WASP

A report by the Cloud Security Alliance found that over half of the vulnerabilities addressed by organizations tend to recur within a month of remediation, highlighting the challenges of achieving long-term resolution.

These statistics underscore the importance of enhancing vulnerability management processes to reduce remediation times and prevent the reoccurrence of issues.

Note: Dynamic environments add another layer of complexity to vulnerability management. Even after vulnerabilities are identified and addressed, changes to software, configurations, or integrations can cause them to reappear. Regular retesting is essential to ensure vulnerabilities remain resolved over time.

Managing all vulnerabilities on a single platform, like **WASP**, significantly improves MTTR by seamlessly integrating with developers' ticketing systems and fostering direct communication between pentesters and developers. Transitioning from siloed solutions to a managed platform has been shown to **reduce MTTR by up to 80%.**

WASP customers have achieved exceptional results, with an average **MTTR ranging between 21 and 28 days**, showcasing the platform's ability to streamline vulnerability remediation processes. These fast remediation times are further supported by **manual arbitrage**, which removes false positives and irrelevant findings, ensuring users can focus exclusively on addressing real issues.

These fast remediation times are further improved by a superior MTTD (Mean Time to Detect), which is less then 24h if working with the hybrid approach. In contrast, traditional penetration testing models often leave organizations waiting for the next testing cycle - **sometimes up to 11 months** - before vulnerabilities are identified and addressed.

WASP's continuous approach ensures vulnerabilities are detected and remediated promptly, reducing exposure time and improving overall security posture.

21 to 28 days

the average MTTR for WASP customers

Looking Ahead: Best Practices for 2025

Continuous testing remains a cornerstone of effective cybersecurity in 2025. Combining **scheduled manual testing with automated, ongoing scans** ensures comprehensive coverage of both known and emerging vulnerabilities. Organizations should also embrace Vulnerability Disclosure Programs (VDPs) to engage external researchers and ethical hackers in identifying vulnerabilities that might otherwise go unnoticed.

For more info, please visit https://op-c.net/vulnerability-disclosure-program-vdp/

Takeaway: A hybrid approach—**blending automation, manual testing, and external input via VDPs**—empowers organizations to proactively identify and address vulnerabilities.

Manual testing provides the in-depth analysis and human expertise required to uncover complex or context-specific issues, such as logic flaws or business logic vulnerabilities, that automated tools might miss. In contrast, automated testing offers scalability and speed, identifying the majority of vulnerabilities across systems in real-time.

To achieve optimal results, organizations should:

- **Schedule penetration tests** to uncover deep-rooted vulnerabilities. The testing frequency should be tailored correctly to match the organization's security needs.
- **Deploy automated vulnerability scanning tools,** such as those provided by OP Innovate's WASP platform, to maintain continuous visibility into their security landscape.
- **Integrate these testing practices with regular patch management** cycles to ensure discovered vulnerabilities are addressed promptly.
- **Prioritize high-risk vulnerabilities** based on their potential impact and likelihood of exploitation, along with an efficient method to mitigate them in a timely manner.

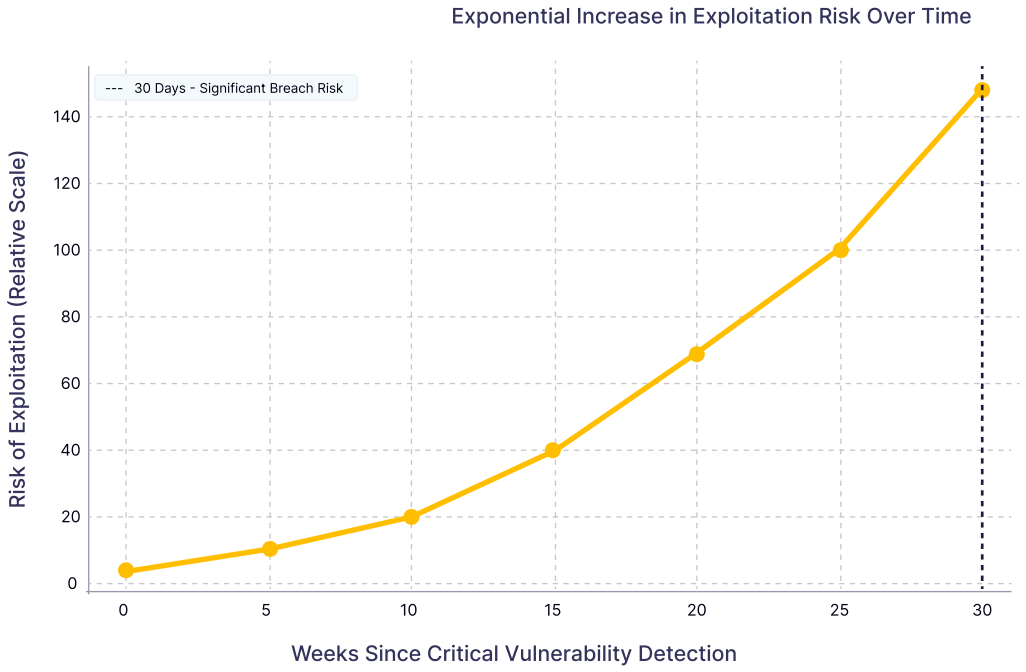
It's essential to implement both manual and automated retesting cycles to address the dynamic nature of modern software systems. Even when vulnerabilities are resolved, system updates or environmental changes can inadvertently reintroduce similar issues.

Why Prioritization Matters

Most organizations face dozens, if not hundreds, of unique vulnerabilities, which can quickly overwhelm even the most well-equipped security teams.

However, not all vulnerabilities carry the same level of risk. To mitigate threats effectively, organizations must adopt a robust prioritization strategy that focuses efforts on the most critical and exploitable vulnerabilities. This ensures that resources are allocated to areas where they can deliver the greatest impact.

The urgency of addressing critical vulnerabilities cannot be overstated. For every week a critical vulnerability remains unpatched, the risk of exploitation grows exponentially. Research shows that organizations failing to remediate critical vulnerabilities within the first 30 days experience a significantly higher likelihood of breaches, underscoring the importance of timely action.

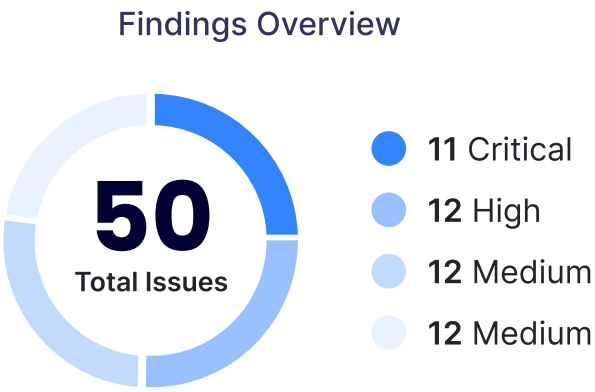


CISA recommends that critical vulnerabilities be remediated within 15 calendar days of detection, and high-severity vulnerabilities within 30 days.

How OP Innovate Prioritizes High-Severity Issues

At OP Innovate, we help organizations cut through the noise and focus on addressing high-severity issues that pose the most significant risks.

The WASP platform automatically categorizes vulnerabilities based on severity (ranging from informational to critical). This allows teams to easily identify where the biggest risks lie, and act quickly to remediate them.



Thanks to the various third-party integrations, teams can connect their existing tools with the WASP platform for improved collaboration and operational efficiency, significantly reducing their mean time to remediation (MTTR).

Case in Point: A client facing alert fatigue reduced their remediation time by 75% thanks to WASP's ability to seamlessly integrate with dev workflow tools.

All of our findings come with detailed vulnerability descriptions, as well as mitigation steps. Additionally, our clients have the full support of our CREST-certified team, who can help them dive deep into findings and provide remediation guidance.

Summary and Key Takeaways

The State of Penetration Testing in 2024 provides an in-depth analysis of vulnerabilities identified by OP Innovate through a combination of manual penetration testing and the automated capabilities of the WASP platform. Key findings reveal critical insights into the types of vulnerabilities, their distribution across asset types, and the growing importance of automation in vulnerability detection.

Impact of Automation:

Automation accounted for nearly 80% of detected vulnerabilities, underscoring its efficiency and scalability. Manual testing remains crucial for identifying nuanced and context-specific risks, as almost 50% of high and critical severity issues through manual testing efforts.

Remediation Challenges:

Organizations struggle to meet recommended remediation timelines, with critical vulnerabilities often remaining unaddressed for over two months. Recurrent vulnerabilities highlight gaps in sustainable resolution strategies.

Prioritization is Essential:

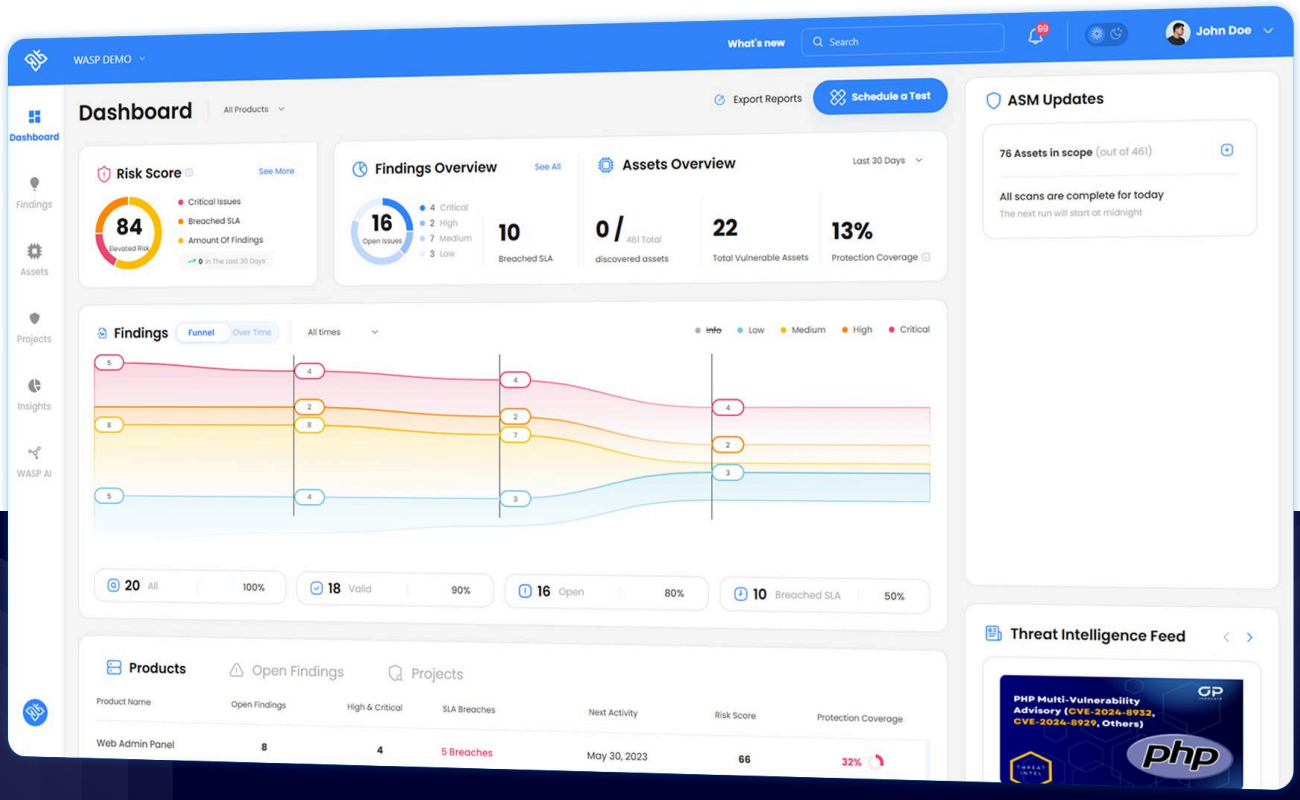
Effective prioritization ensures that high-risk vulnerabilities are addressed promptly, reducing the risk of exploitation. Tools like the WASP platform streamline prioritization by categorizing vulnerabilities and integrating with existing workflows.

Appendix: About WASP and OP Innovate

OP Innovate was established in 2014 to defend global enterprises from the increasing challenges of organizational cybersecurity. Our experience in the field is extensive with unmatched expertise in penetration testing, incident response, cyber research, training and forensics.

With headquarters in Israel, we rub shoulders with the best-of-breed in the field of cybersecurity, exposed to cutting-edge responses to today's most critical cybersecurity concerns. This knowledge allows us and our customers to remain ahead of the curve.

In 2019, we introduced our all-in-one PTaaS platform, WASP. This platform revolutionizes the penetration testing process by combining advanced automation with expert analysis, enabling continuous vulnerability detection, real-time remediation insights, and seamless collaboration. With WASP, organizations can proactively address vulnerabilities and adapt to the rapidly changing threat landscape with confidence.



Want to experience the power of WASP for yourself?

Register for your FREE account now

REGISTER NOW

OP INNOVATE

WASP