October - December 2025

VULNERABILITY REPORT

Report & Trends

OUR MISSION IS SIMPLE

To combine the best possible customer experience, with market leading delivery for every client, every time.

Contact

Phone	+44 (0)1789 608708
Website	www.istormsolutions.co.uk
Email	info@istormsolutions.co.uk

iSTORM®

Privacy • Security • Pentesting

Quarter 4 Vulnerability Report

Summary

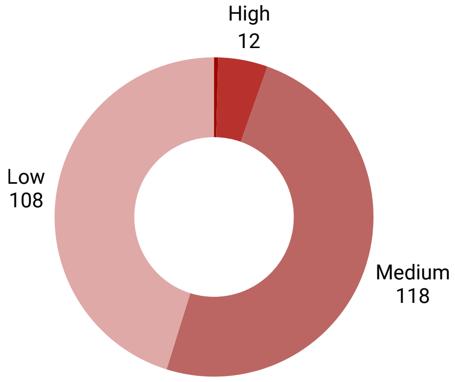
From 1st October 2025 to the 31st December 2025, a total of 250 vulnerabilities were identified, categorised by severity as follows:

Critical: 1

High: 12

Medium: 118

Low: 108



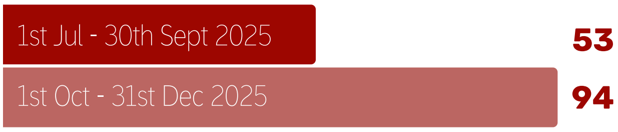
Vulnerabilities by Type

Of these vulnerabilities: 94 were associated with Web Applications, 36 External Infrastructure, and 27 were Cloud related.

Top Testing Type: Web Application

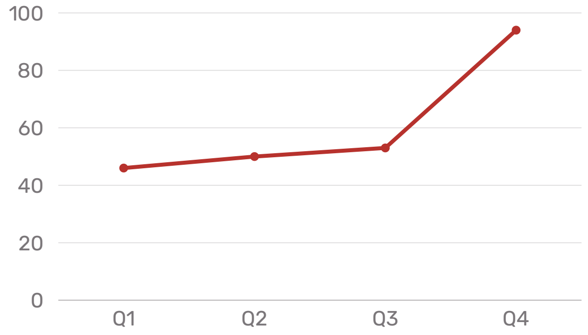
During the final quarter of 2025, our web application security assessments identified 94 vulnerabilities, a 77.3% increase compared to the previous quarter. This significant rise highlights a continued upward trend in the growing complexity of modern web applications and reinforces the critical importance of proactive security reviews to keep pace with emerging threats.

Common findings included high-risk issues such as broken access control, Defender for Azure API not being enabled, and outdated JavaScript libraries, all of which significantly increase exposure if left unaddressed.



94 vulnerabilities in the third quarter of the year. An increase of 77.3% on previous the 3 months

Quarterly Vulnerability Trend



Top Master Vulnerabilities

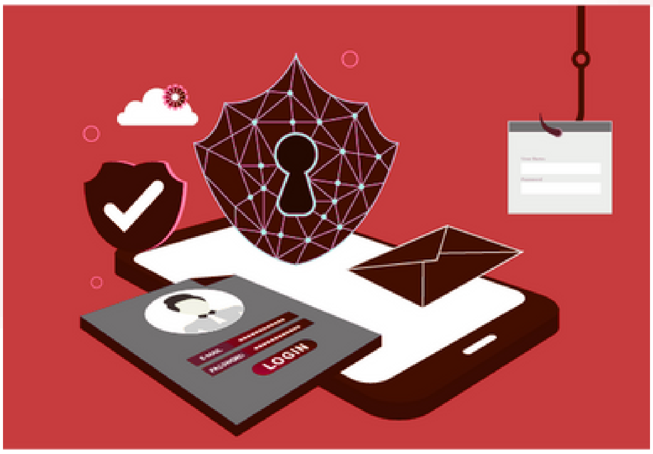
Of the vulnerabilities identified, the following were the most frequent or high-risk:

○ Access Control: Broken access control	**High**
○ Azure: Defender for Azure API not enable	**High**
○ Web Applications: Outdated Third Party Libraries in Use	**Medium**

Notable Trends

Phishing remains one of the most effective and widely used attack methods, and continues to be a primary entry point for broader security incidents. Attackers increasingly leverage convincing email content, cloned login pages, and trusted cloud services to trick users into disclosing credentials or approving malicious authentication requests. As a result, even well-secured environments can be compromised through a single successful user interaction.

Modern phishing campaigns are becoming more targeted and harder to detect, often using organisation-specific branding, language, and contextual detail to increase credibility. These attacks are no longer limited to emails, and now commonly extend to SMS (smishing), voice calls (vishing), and collaboration platforms, significantly increasing the likelihood of user engagement.



Technical controls alone are insufficient to fully mitigate phishing risk. While email filtering and domain protection reduce exposure, user awareness remains a critical defensive layer. Regular security awareness training, simulated phishing exercises, and clear reporting processes help reduce the likelihood and impact of successful attacks. Additionally, enforcing Multi-Factor Authentication, particularly phishing-resistant MFA, significantly reduces the risk of account compromise, even when credentials are exposed.

How can we help?

As a boutique consultancy, our business is really about people. We work with you to understand, your business, and your requirements. Our testing approach is driven by threat intelligence, incorporating insights from global and industry-specific cyber trends to ensure relevancy and accuracy in our assessments.

Threats are evolving rapidly—and staying ahead requires more than just reactive measures. Our team can help you proactively identify, assess, and mitigate risks before they impact your business.

Whether you're looking to strengthen your web applications, secure your infrastructure, or gain insight into emerging threats, we’re here to help.

For more information about how iSTORM can support your organisation, please contact us - info@istormsolutions.co.uk or call 01789 608708

iSTORM®

Privacy • Security • Pentesting