EINPRESSWIRE

X Security Outlines 5 Key Sections a Pentest Report Must Have in 2022

One of the most important aspects of a pentest is the report delivered afterwards - Here we review what details should be in every report out there.

X Security

DOVER, DELAWARE, UNITED STATES, November 22, 2021 / EINPresswire.com/ -- Penetration testing doesn't have a reporting standard and that means that pentest firms deliver reports in all types of shapes, sizes, and quality. There are many important factors to evaluating pentest vendors, but one of the most important should be the the reporting content & structure. X Security, a whitelabel penetration testing firm for the channel community, recently outlined 5 key things that all pentest reports should have in 2022.

1. Executive Summary: Pentest reports contain a lot of technical details but should also have a section that provides value to non-technical leadership. Details such as overall strengths and weaknesses, industry comparisons, high level attack narrative, and actionable next steps help provide value to those who might not understand the technical findings during a pentest.

2. Business Impact: Most pentest reports do a satisfactory job at covering technical findings. What many miss the mark on is understanding and evaluating the business impact of vulnerabilities. The best pentest firms will be able to communicate the business impact of any given vulnerability, which helps the customer prioritize their remediation efforts. Business impact also helps non-technical viewers have a better grasp on the severity of technical findings.

3. Technical Findings: Every report needs to cover the technical findings of the assessment - but how those findings are conveyed and what is covered is critical. A quality pentest report will cover the technical details of the vulnerability & affected system(s), what the impact to the business is, and then steps to recreate the vulnerability.

4. Remediation Recommendations: The customer ultimately wants to know how to fix the findings from the pentest. All reports should provide prioritized & actionable remediation steps to ensure that the customer has a roadmap to improving their security posture.

5. Third Party Summary Report / Attestation Letter: Due to the sensitive information found in pentest report, customers should avoid sharing the full report with any third parties. To prove that a pentest has been performed, a summary report or attestation letter should be provided to customers in addition to the report for no extra cost.

6. Whitelabel Reporting Capabilities: MSPs that wish to provide pentesting services to their customers (without building an internal pentest team) can partner with pentest firms. Having the ability to whitelabel the pentest report is a plus for any business & it's branding.

Austin Harman
X Security
+1 302-232-3031
austin@xsecuritygroup.com
