ATTACKFORGE

Centralized Enterprise Management of Penetration Testing Program

ATTACKFORGE WHITE PAPER
JANUARY 2020

>50 PENETRATION TESTS A YEAR LARGE SCALE PEN TESTING PROGRAM

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Traditionally, penetration tests (or pentests) are commissioned and performed on a per-project basis. The results of each pentest are provided as reports in various static formats, requiring considerable time and effort to compare results, track remediation activities and address vulnerabilities. There is also the challenge of vendors using different methodologies. In an organization that requires more than fifty (50) pentesting engagements on an annual basis, these challenges are exacerbated. A large-scale pentesting program requires consistency and scalability. A centralized pentesting management system - specifically designed for penetration testers, engineers, and business - ensures collaboration between different stakeholders in the company will provide better operational efficiency and reduced mean time to remediate vulnerabilities.

ORGANIZATIONAL SECURITY REQUIREMENTS

CHALLENGES FACING A LARGE-SCALE PENETRATION TESTING PROGRAM

Pentesting is typically performed towards the end of the software development project life cycle. It takes weeks from the time that the pentesters (persons performing the penetration test) discover the vulnerabilities - until the engineers receive the details. Depending on the workload and project priorities, it may take weeks before the developers can fix the issue. This can cause delays to product launches and delivery pipeline, resulting in lost business opportunities and increased project burn rate.

Providers and even pentesters themselves tend to use different methodologies and terminologies. This makes it difficult for organizations that commissioned the pentests, to compare results between a previous report and a current one. This leads to a lack of visibility on what has been tested. Furthermore, using different terminologies leads to confusion in understanding the vulnerability terms and language used by various providers and pentesters.

Companies that have a large-scale pentesting program will find it nearly impossible to do cross-analysis of the results of the pentests. A large-scale pentesting program is defined as having more than fifty (50) pentests done over a 12-month period. Without a centralized system to manage all these results, coupled with the differences in methodologies and terminologies - an overall analysis of the results and return of investment into the program will require a separate project by itself.

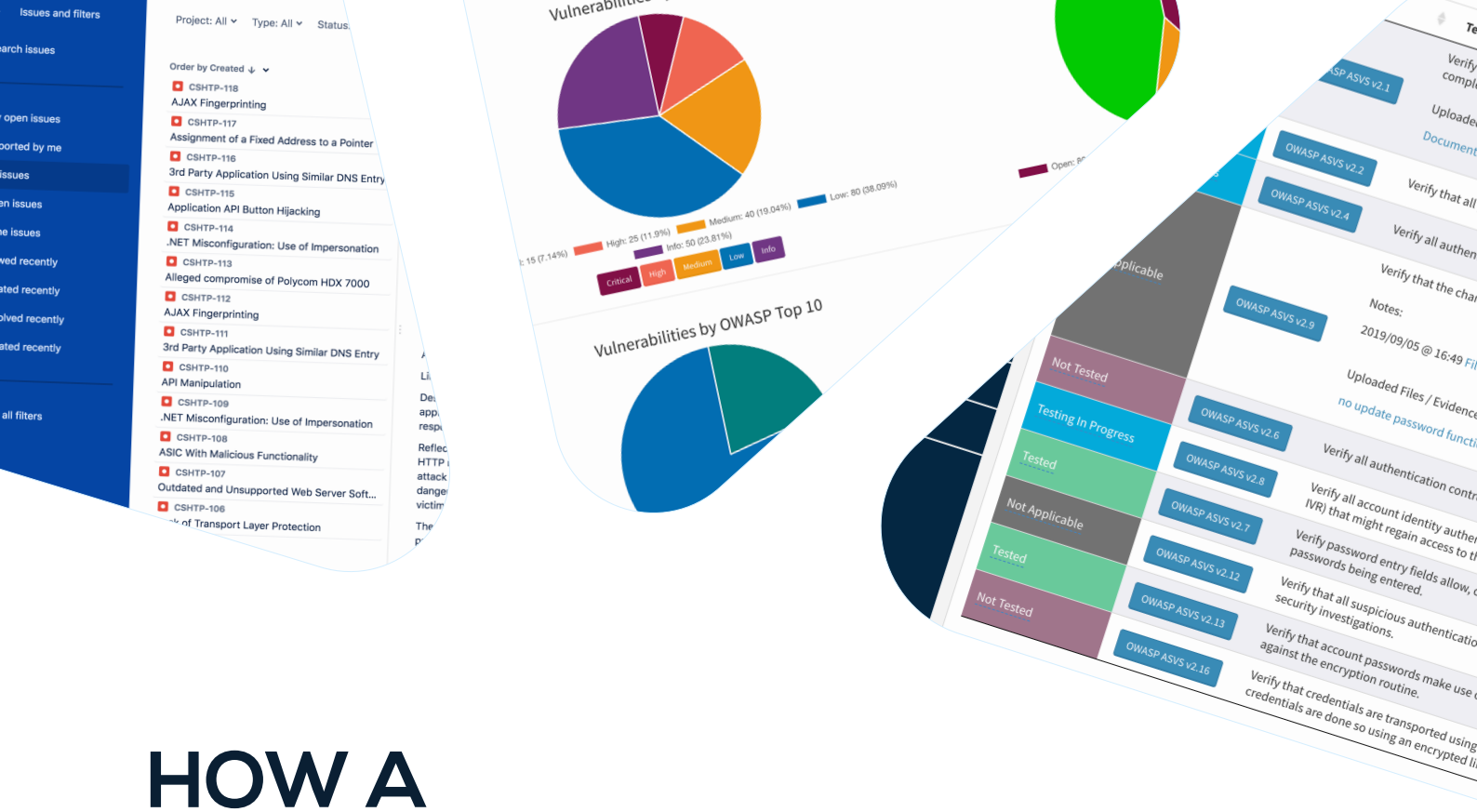
HIGHER MEAN TIME TO REMEDIATE (MTTR)

The final pentesting results are provided in various formats such as Word documents, PDF files or Excel spreadsheets. These are then shared via email or online file storage. Tracking all these reports and trying to find a pattern of prevalent vulnerabilities or insecure coding practices will be time consuming and inefficient.

From the time that a pentester finds the vulnerability, to the time that the report is written and submitted to their client and such until the time it finally reaches the engineer, a vulnerable system may have been compromised or exposed. Should the pentesting be done on a greenfield solution, the delay in getting the information to the engineers will delay the product launch and increase the project burn rate (that is, the rate at which the project budget is being spent).

SHIFTING SECURITY TO THE LEFT

The rise in the adoption of several Agile methodologies for software development means there is a requirement for continuous collaboration by different teams in an organization, and that testing is done earlier in the project lifecycle. This paradigm of shifting to the left has also influenced stakeholders to involve the security team early on. There is a greater need to have technology, business and security teams collaborating together. Both internal pentesters and external vendors are increasingly being utilized to find security issues or vulnerabilities before the final software product is shipped.



HOW A COMPREHENSIVE SOLUTION SOLVES THESE PROBLEMS

The AttackForge Enterprise platform solves these problems by bringing the vulnerabilities to the forefront, where engineers can easily see them and fix them in near-real time. This platform provides pentesters with a common set of methodologies and vulnerability language. By using this common and standardized approach, the art of pentesting can now become the science of pentesting - where there is a mature and repeatable process - allowing an enterprise to compare results from multiple vendors or pentest teams across different periods of time.

All the reports and findings are now stored, easily searched and compared - in a single platform. This provides a single pane of glass for different stakeholders – project managers, software developers, quality analysts, security team members, and executives – that allows them to collaborate to determine root causes/issues, to identify vulnerability trends within the enterprise, and to find effective solutions to address these issues.

REDUCTION OF COST AND EXPOSURE WHILST REMEDIATING VULNERABILITIES FASTER

The AttackForge Enterprise platform provides an easy-to-use interface that lets:

- business stakeholders track the progress of a pentesting project and get their systems into production faster. They also get to understand how a vulnerability can lead to a business impact by looking at the associated attack chain for the vulnerabilities discovered.
- pentesters document their findings efficiently and effectively by leveraging the built-in, centralized vulnerability library.
- engineers see the findings immediately, communicate directly with pentesters, collaborate on solutions to address the vulnerabilities, track remediation efforts and retesting, all whilst the pentesting is still being executed.

The wait for manually created reports is now over. All reports are available to project teams on demand, when they need it. The days of having to go through intermediaries and getting worried about potential data leakage via emailing of the pentest reports, is now replaced with peace of mind. Each project in AttackForge has a dedicated workspace and private communication channels to make collaboration easy and effective.

With these features, AttackForge Enterprise enables the organization to be faster and more agile in releasing products, to reduce their unnecessary vulnerability exposure and to reduce costs of project delays due to the time it takes for vulnerabilities to be remediated. It is estimated that AttackForge Enterprise reduces go-to-market lead time on average by up to fifteen (15) days.

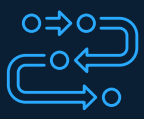
15

DAYS ESTIMATED GO-TO-MARKET LEAD TIME REDUCTION WITH *ATTACKFORGE*

TRANSPARENCY, CONSISTENCY AND STANDARDIZATION

AttackForge Enterprise provides a platform that delivers industry accepted methodologies and flexibility to modify the methodologies to fit the organization's needs, or even create new ones that will align to the compliance requirements or organizational goals - at the time, and into the future.

AttackForge Enterprise provides the following features for transparency, consistency and standardization:



Methodologies are represented as Test Suites which are assigned to, and executed on every pentesting project. Test Suites consist of a set of test cases that guide the pentester on what must be tested.

There is a large number of pre-populated industry accepted methodologies, including OWASP Application Security Verification Standard (OWASP ASVS), Penetration Testing Execution Standard (PTES), Open Source Security Testing Methodology Manual (OSSTMM) and others. The use of these methodologies provides consistency in the execution of pentesting, ensuring a thorough approach that is independent from provider/vendor, delivery team or individual pentester.

Should the company require Test Suites that are aligned to a specific regulatory requirement or that must be aligned to their custom methodologies in the areas of IoT, Red Team, OSINT, Physical Security, SCADA or others - the Test Suite Builder feature will provide the flexibility to create custom methodologies. These tailored methodologies can then be approved and used by project team members on every pentesting engagement - to ensure maximum testing coverage, every time.

The built-in centralized vulnerability library allows the enterprise to apply a consistent set of vulnerability terminology across multiple providers and pentesters. This leads to consistency in the pentesting report and communication of findings, even when the vendor or team has changed.

Auditing of the pentest results is done properly. Once a test case is completed, it is time-stamped, user-stamped and logged, with the ability to attach evidence to ensure compliance to different regulatory requirements.

PENETRATION TESTING ANALYTICS

The AttackForge Enterprise platform provides organizations with hard data on the effectiveness of their penetration testing programs. The organization can analyze the pentesting results across the entire enterprise, business units, external providers and even across time periods. There are analytics provided to identify overall trends, assist root cause discovery and objectively evaluate external pentesting providers. When time is of the essence, the analytics feature of AttackForge Enterprise will show the "Top 10 Most Frequent Vulnerabilities" and "Top 10 Test Cases Leading to Vulnerabilities" which the organization can prioritize in their remediation efforts and training budgets. With data provided in real-time, organizations can plan remediation effectively and fix security issues efficiently.

CONCLUSION

Penetration tests can be tedious activities, and results may not be immediately available to the right team member at the right time. In order to get the most value out of the different sets of pentests done across the years, an organization needs a tool that can efficiently and effectively manage a large-scale pentesting program.

AttackForge Enterprise has been created by pentesters and engineers who understand all the challenges involved in creating secure software that needs to be tested and shipped as per the project deadlines.

INFORMATION

For more information or for demo requests, contact us at *info@attackforge.com.*

AttackForge

Level 9, 167 Queen Street
Melbourne, Australia, 3000

Produced in Melbourne, Australia
January 2020

ATTACKFORGE