PLEXTRAC EBOOK

10 Tips for Cutting Pentest Reporting Time in Half

Without sacrificing quality.

PlexTrac®

Unlock the power of automation to streamline the pentest findings delivery process, accelerate reporting cycles, and enhance the quality of deliverables.

Have It All with Pentest Reporting Automation

Pentest or assessment reports are a key deliverable for your clients or internal stakeholders. This document is vital for:

1. Communicating results/findings
2. Demonstrating expertise
3. Documenting work performed
4. Differentiating your service provider practice (if applicable)
5. Prioritization of remediation efforts

Despite being vital, manually creating reports can be tedious. For pentesters, the process often involves context switching, taking them away from time spent hacking.

Reporting automation improves efficiency and delivers substantial time savings. See how PlexTrac makes it easy to build a report in 5 minutes or less. Efficient reporting processes boost pentester morale, ensure deadlines are met, and increase service margins for service providers.

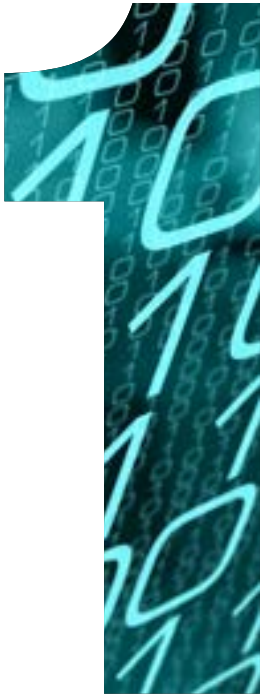
> "By utilizing PlexTrac we've seen up to 60% reduction in the amount of time our practitioners spend writing reports." — PenTest Team Lead, Herjavec Group

Speed is important, but it's not the only factor when it comes to successfully meeting the five objectives of quality pentest reports. Both the practitioners who perform pentests and write reports, and the practice managers who are responsible for driving business growth should place a high priority on both efficiency and quality. Fortunately, a mature pentest reporting automation solution can deliver both significant time savings and higher-quality deliverables.

How does pentest reporting automation enable higher quality findings delivery? ***Here are 10 benefits security service providers and enterprise teams can realize by implementing an automation solution and how reporting automation makes them possible.***

> "PlexTrac enables the team to produce higher quality findings to our stakeholders faster. Our internal processes have been changed to take advantage of this capability."
> — Fortune 100 Apparel Company

Automate for Thorough Data Aggregation and Analysis



Pentesters use a variety of tools to support their work, whether for data gathering or exploitation. These tools produce a tremendous amount of baseline data that informs the results of their work. Unfortunately, managing information from disparate sources is not only a time suck but also leads to missed detail or errors.

A reporting automation platform solves this problem by serving as a central location to easily upload results from all standard pentesting tools. Those raw data files can then be parsed and analyzed with no information loss.

Automate for More Consistent Findings Writeups

Another significant pain point for testers occurs in the writeup of their findings analysis. Technical snippets are a critical component of the report. However, they often are repetitive as similar findings come up in many different engagements. But copying and pasting from old reports or Word document repositories often leads to errors and inconsistencies — not to mention the time it takes to find the right snippets.

A reporting automation solution that includes a powerful content management module can transform the quality and consistency of finding writeups. It enables you to store QAed writeups in organized repositories directly in the reporting platform for single-click, permission-based access. Saving your writeups directly in the platform makes it easy to pull them into a report and further customize the writeup as needed. Junior testers or less experienced writers can use common writeups from the organization's library to ensure consistency and quality across all reports.

Automate for Streamlined Content Archiving

It's not just findings writeups that present issues. All reusable content components in a report benefit in terms of accessibility, quality, and consistency from a reporting automation solution.

Archive, access, and customize standard narratives, boilerplates, bios, etc., in repositories with permission-based access controls to save time and ensure consistency regardless of who creates the report. Additionally, avoid embarrassing mistakes by using short codes to customize client or department names and other variable text in the final report without tedious "find-and-replace" work.

Automate for Easy Artifact Capture

The written content of a report cannot stand alone. A quality report must also include visual evidence that supports the findings and recommendations. This evidence usually takes the form of screenshots, code snippets, photos, or even video artifacts. Capturing these items during an exploit is essential, but keeping track of them to include in the report adds complexity and makes errors more likely.

A reporting automation solution facilitates the capture and storage of all the artifacts and evidence needed for the final report. It also makes adding and formatting them into the document simple and quick. An automated report delivery platform even facilitates dynamic delivery options that support evidence, such as video.

Automate for Better QA Processes

Many inefficiencies in the report creation process happen during collaboration. Collaboration, particularly for QA, is essential for effective reports. Even superior content creators can't effectively edit their own work to perfection.

Reporting automation facilitates collaboration and QA processes to save time and improve the final product. Commenting and change tracking in the same place where reusable content is housed and the report is produced greatly reduces context shifting and version-control issues.

Automate to Improve Templates

The report template is the secret sauce for many pentesters. For a service provider, the security report is often a major differentiator for the business. And the branding of the report is also essential for marketing purposes. Formatting those unique templates again and again is both time-consuming and fraught with the potential for errors.

The ability to create the template once and automate the inclusion of content and formatting is a game changer for ensuring quality and consistency with every deliverable. Whether you need a fully customized template to represent your service provider's unique perspective or are seeking multiple standardized templates for different types of security reports, a reporting automation platform will keep branding and content consistent with company standards every time — with much less effort for everyone involved.

Automate for More Comprehensive Reports

Penetration testing produces myriad data. Analyzing and prioritizing that information for clients or internal stakeholders is critical. Report writers must continuously make decisions about what to include and how to prioritize the material.

Reporting automation makes it much easier to include more information without requiring more time to prepare it. Scaling an engagement and a report without expending more resources is only possible with automation. Additionally, a reporting automation platform that can support secure dynamic findings delivery gives clients or internal stakeholders access to in-depth information — and even raw data findings — without making the report cumbersome or unreadable.

Automate for Secure Findings Delivery

Secure delivery of reports must always be a top priority. This often requires encryption or use of a file-sharing platform. For service providers, these steps often create friction that discourages frequent communication and collaboration with clients about the results of an engagement.

A reporting automation platform with a secure, permission-based portal ensures simple secure delivery of the report along with more efficient communication throughout the engagement. Communicate scoping questionnaires, provide results throughout the engagement, and deliver the final recommendations securely — all without added tools, steps, or processes.

Automate for More Actionable Insights

Ultimately, service providers and enterprise security teams have the same goal of improving security posture. Completing annual testing and finding the same issues engagement after engagement, for example, is frustrating for testers. While a service provider can't control the actions a client takes after receiving a report, and pentesters at enterprise security teams can't hand hold through the remediation process, they can help move the needle with more actionable findings and clearer prioritization.

Automation in the reporting process supports this goal by enabling dynamic findings delivery. When all stakeholders use a reporting automation platform, recommendations can be immediately turned into remediation tickets and assigned and tracked, whether through the platform itself or integrations with tools such as Jira and ServiceNow. Even if the client or stakeholder doesn't use the reporting automation solution, a portal to view findings and update those that have been resolved creates a greater sense of urgency than a static document.

Automate for Better Stakeholder Differentiation

To truly be effective, a pentest report must communicate to several different stakeholders. One report can and should accomplish this with high-level overviews for executives and sections of extensive technical detail for IT experts. However, giving all the potential audiences the amount of detail they desire and communicating it in the most effective manner is a delicate art.

A reporting automation platform makes the differentiation of content for various stakeholders more of a science. For example, reusable standard narrative content that's been reviewed and edited for a specific audience ensures consistency among report writers and in multiple reports for the same client. Storing those narratives for easy access and customization in the reporting platform makes them available with a click.

The ability to create analytics and data visualizations is another feature of a robust reporting platform that makes data more accessible to readers of varying technical skill. Finally, providing access to raw data and all the findings via a portal delivers all the detail technical readers need to understand and act on the results.

Deliver Higher Quality in Half the Time with PlexTrac

PlexTrac is the premier pentest reporting automation solution. Streamline the full pentesting life cycle in a robust platform built by a pentester *for* pentesters. By eliminating process pain points and building efficiency and consistency throughout the workflow, pentesters are relieved of tedious tasks, improve the quality of their deliverables.

If you are ready to save valuable time and produce higher-value reports, request a customized demo to see PlexTrac in action.

PLEXTAC.COM/DEMO

> **"We were looking for a way to streamline and expedite our own reporting process while also giving our clients a better reporting product and new way to interact with our findings and recommendations. We found that in PlexTrac."**
> **— Will Keppler, Security Specialist, Cyzen**

PlexTrac is the premier penetration test reporting, collaboration, and management platform designed to automate planning, documentation, communication, and remediation tracking, allowing service providers to enhance margins and client outcomes and enterprises to demonstrate the value of internal pentesting efforts and improved security posture.

www.plextrac.com

PlexTrac®