PSICURITY™

BARR ADVISORY

2025 Whitepaper

Identifying Quality Web Application Penetration Tests:

A Practical Guide for Customers and Auditors

Table of Contents

2 | Introduction
3 | Audience
4 | Overview of Web Application Pentesting
5 | Choosing a Quality Pentest Provider
7 | How to Identify a Quality Pentest Report
9 | Conclusion
10 | Our Partnership

Introduction

With a majority of new applications today being specifically architected to use a web browser as the primary user interface, it has become a standard requirement for many companies to perform third-party **web application penetration tests** (or "pentests"). Globally, web application developers check-in countless millions of lines of new code each day. From a security perspective, this new code is effectively "new attack surface" (i.e., code that has never been tested before).

With the widespread adoption of AI-generated code, the creation of vulnerable attack surface is also quickly accelerating. A recent study of popular code generation models showed that,

> **"...almost half of the code snippets produced by five different models contain bugs that... could potentially lead to malicious exploitation."**

As a result, third-party web application pentests are increasingly more necessary to discover vulnerabilities before the attackers do.

The Problem with Pentests

Organizations face an overwhelming number of options when choosing a pentest provider. Unfortunately, it is common for providers to market "comprehensive" pentests, while instead giving their customers an automated scan report using off-the-shelf tools and passing it off as a penetration test. These providers may charge high fees, and claim to use advanced techniques like manual exploit testing. However, such claims are often superficial, or even misleading.

In other cases, pentesters may fail to scope the entire attack surface, leaving significant portions untested. Some providers may find important vulnerabilities, yet deliver vague reports that leave customers unsure about what was done and whether it was complete.

Such low-quality pentests create a false sense of security, leaving organizations exposed to unauthorized access, data theft, and fraud. While low-quality pentests may succeed in checking a compliance box, they can result in undiscovered vulnerabilities that compound over time into serious organizational risk.

This whitepaper addresses the following two issues regarding pentest quality:

1. **How do you choose a quality pentest provider?**

2. **How do you identify a quality pentest by reading the report?**

[1] https://github.blog/news-insights/research/survey-ai-wave-grows/ A 2024 survey by Github shows that "97% of respondents reported having used AI coding tools at work at some point", and that "59-88% of respondents... reported that their companies are either 'actively encouraging' or 'allowing' the use of these tools."

[2] https://cset.georgetown.edu/wp-content/uploads/CSET-Cybersecurity-Risks-of-AI-Generated-Code.pdf, Center for Security and Emerging Technology, Georgetown University.

Audience

Pentest Customers: Pentest customers are responsible for selecting a qualified pentest provider and ensuring that a thorough, standards-based assessment is performed.

Auditors: It is the auditor's responsibility to review an organization's pentest reports to determine control success. If a pentest is found to cut corners on effort, or omit key attack surfaces from the scope, the auditor may need to flag a deficiency or control failure.

Third-Party Risk Analysts: These analysts are responsible for evaluating vendor risks as a part of their due diligence program. It is essential to identify whether quality pentests were performed by partners and vendors prior to engaging with them.

Overview of Web Application Pentesting

Before defining what makes a pentest "high quality," it is essential to understand the pentest process and its related benefits.

Pentest Process

A web application pentest is typically performed on an annual basis, or after significant changes, and utilizes the following high-level methodology:

1. **Discover:** Discover and validate vulnerabilities.
2. **Exploit:** Attempt to exploit those vulnerabilities like a hacker would.
3. **Document:** Document all pentest findings, and recommend fixes to the customer.
4. **Remediate:** The customer performs remediation of vulnerabilities.
5. **Re-test:** The pentest provider performs a re-test to validate customer fixes.

Pentest Benefits

An effective pentest will help:

- Protect your organization against data theft, revenue loss, and reputation damage.
- Assure your customers and partners that their data is actively safeguarded.
- Reduce overall risk to the company, its customers, and partners.
- Support compliance with relevant security standards, such as ISO 27001, SOC 2 Type 2, PCI DSS, etc.

Note Regarding the Types of Penetration Tests

We recommend the approach in this whitepaper because it is the most effective way to identify the maximum number of vulnerabilities within the time and budget available. Hackers have unlimited time to discover and exploit weaknesses; therefore, it is essential to perform pentests that maximize vulnerability discovery and validation. That said, we recognize that other approaches may be appropriate, depending on the requirements for a specific pentest, such as when a Red Team is used for testing the readiness and response of a Blue Team, etc.

Because this document is solely focused on web application penetration tests, any isolated use of the term "pentest" hereafter will relate specifically to web applications. Pentests for network, Wifi, social engineering, mobile, etc., are not covered in the scope of this whitepaper.

The use of color-coded terms for pentests (such as whitebox, blackbox, or greybox) is avoided in this paper, as their use may vary depending on the scope of each engagement.

Choosing a Quality Pentest Provider

When scoping a web application pentest, the following checklist can be used to help with choosing a quality provider:

- **Detailed Methodology:** A quality provider should supply a clear and detailed methodology. Look for the following:
  - Testing and documentation processes are guided by a recognized industry standard, such as OWASP's "Application Security Verification Standard" (ASVS) or a similar standard.
  - Advanced techniques are described, such as manual exploit testing, etc.
  - A formal risk rating system is applied (e.g. CVSS).
  - Testing limitations and constraints are disclosed upfront.

- **Manual Testing:** The methodology should clearly state that advanced exploitation attempts will be performed using manual testing techniques. This demonstrates that they are not just running automated scans with boilerplate reports. While automated tools cannot replace a real human tester, such tools may still be used for surface discovery and parameter fuzzing. But these are only preliminary steps in the testing process. Manual techniques remain essential for validating the findings and emulating real-world attacks.

- **Pentest is Standards-based:** Does the methodology utilize a recognized industry standard to guide the process of testing and documentation?

  Here's what to know:

  - **OWASP ASVS is recommended:** The OWASP ASVS is regarded by many as the gold standard for web application pentests. It is a detailed set of application tests comprising over 250 controls spread across 17 categories. Auditors will especially appreciate the "control-like" structure of an ASVS-based report, while customers will enjoy how it provides a comprehensive snapshot of their application's security posture.

  - **What about the OWASP Top 10?** Pentest providers often cite the "OWASP Top Ten" as the basis for a web application pentest. However, the OWASP Top Ten is not a testing standard, but is meant to be an "awareness tool." It is helpful for communicating vulnerability types, but it is not sufficient for structuring a pentest.

- **Thorough Scope of Work:** The penetration test should be scoped so that all relevant application surfaces (including APIs) will be thoroughly covered. API documentation should be requested to ensure they are thoroughly tested. Simply fuzzing API surface without documentation is likely to result in false negatives. Furthermore, application workflows should be communicated to the pentesting team to ensure that all logical paths can be exercised, particularly if intervention is required by a business unit to complete a workflow. Please see the next section for red flags with scoping.

- **Comprehensive Documentation:** An ASVS standard-based report should provide comprehensive documentation of every single test that was performed, including both good and bad findings. This is called a "positive findings model" and demonstrates that a thorough test was performed.

- **Skilled Testers:** Providers should employ skilled analysts. Things to look for include industry certifications (OSCP, GPEN, CRTP, CEH, CISSP, etc.), equivalent work experience, and security-related achievements and accolades. Degrees in cybersecurity from accredited institutions are also appropriate.

- **Next-level Customer Service:** A good pentest provider values your time, and will promptly address your needs throughout the engagement, like an extension of your team. After the report is delivered, they will promptly answer questions about remediation steps. In short, they will "give you the time of day."

- **Cooperative vs. Adversarial:** Look for pentest providers who prefer a cooperative approach to testing, rather than adversarial. They should ask for as much access to the application and artifacts (e.g. API definitions, source code, etc.) as you are willing to give them. This will help analysts provide the most complete and thorough testing possible within the time allotted and allow analysts to minimize false positives and negatives and recommend specific fixes for affected code.

How to Identify a Quality Pentest Report

Customers and auditors must review web application pentest reports carefully to understand the vulnerabilities and remediation steps. They must also recognize telltale signs that a test was rushed, incomplete, or lacking sufficient depth.

When reviewing a pentest report, use the following checklist to help determine its quality:

Signs of Quality Work

- **Positive Findings Model:** The report documents all tests that were performed, including “pass” or “fail” results for each.
- **Standard-Based Reporting:** The most thorough documentation will be structured using a testing standard, such as ASVS.
- **Findings are Validated:** All findings have been checked for accuracy. False positives, if any, will be few and far between. If the testing is incomplete due to time or budget constraints, it should be documented in the report, as this may result in undiscovered vulnerabilities (or “false negatives”). The location of this un-tested surface should also be well-documented in the report.
- **Findings are Business-Context Aware:** Vulnerability descriptions should demonstrate awareness of business context, and the severity of each finding should be based on actual risk to the application. Sometimes, a vulnerability may seem like a High Severity issue, but it may not actually lead to a meaningful compromise, depending on where it exists in the application.
- **Pentest Utilizes Credentials:** Credentialed penetration testing should be used to map the attack surface and systematically test it, when applicable. This will ensure the application’s attack surface is thoroughly assessed—especially given the limitations on time and budget. Credentialed testing assumes a “threat model” wherein the application will be attacked not only by outside hackers, but also by those who may have authenticated access to the application. This can include threats such as malicious insiders, customers of the product, vendors, and partners (who already possess login credentials).
- **Detailed Recommendations:** The report provides detailed recommendations for remediation, including settings, parameters, or code modifications specifically tailored to your application, when applicable. If a vulnerability is exploitable, the report should provide step-by-step instructions to help engineers reproduce the problem.

Indicators of Low-Quality or Superficial Pentests

- **Limited Scope:** The scope of a pentest may be severely limited. For instance, a pentest might include the login page of a web application, but in some cases, the attack surface occurring after the login may not get tested. In these instances, a report might claim that the whole web application was in-scope, while less than 1% of the attack surface was actually tested. APIs can be overlooked, unless they are specifically scoped. This is especially a concern when the API endpoints are undocumented or intended for programmatic access only.

- **Lacks a Documented Methodology:** The report lacks a clear, structured testing methodology and does not reference testing standards, such as ASVS. This may indicate that testing is improvised or relies too much on automation.

- **Automated Scan Reports:** The following red flags indicate that automated scanning tools may have been overly relied upon, and that no significant manual testing was performed:
  - **Unvalidated Findings (False Positives):** Excessive false positives indicate that no real work has been done to validate the findings. Automated reports often list vulnerabilities with obvious inaccuracies. In some cases, these reported vulnerabilities may not exist at all.
  - **Exaggerated Severity Ratings:** Watch for findings that are rated with higher severities than they should be. For instance, Medium and Low Severity issues are instead reported as High and Critical Severity. Informational issues may be cited as Low and Medium Severity.
  - **Report Findings are Excessive:**
    - The report may list dozens or even hundreds of vulnerabilities, while no attempts have been made to condense them into a more concise and readable format.
    - Informational findings may be excessive and lack any useful purpose for the customer.
    - The report may be excessively long, sometimes running into hundreds of pages. An average ASVS-based report will be only 35 to 60 pages.
  - **Boilerplate Language:** Automated reports often have:
    - Overly broad or generic language.
    - Bad grammar and typos in vulnerability descriptions.
    - Stock references to the names of scanning tools that were used.

- **Report is a Negative Findings Model:** A report with a “negative findings model” will only list “what was found.” It does not provide a list of all tests performed or the results for each. The pentest may have been thorough, but there is no way to know it by reading the report.

- **Certificate is Provided Instead of a Real Report:** Companies may sometimes present a so-called “certificate” to demonstrate that a pentest has been performed. However, a certificate is not a real report if it does not provide a summary of vulnerabilities, severity assignments, remediation details, and methodology. Certificates are effectively useless without this added detail. Calling it a “certificate” may also create the illusion that the company was “certified.” This is misleading at best, and deceptive at worst, depending on how the certificate is “framed” by the party providing it.

Conclusion

When selecting a web application pentest service provider and assessing the quality of their work, you can't rely on a price tag, verbal assurances, or marketing claims. As this guide has shown, quality pentests are grounded in a clearly defined methodology, robust manual testing (using automation to enhance accuracy and thoroughness), comprehensive testing standards (such as the OWASP ASVS), and thorough reporting.

Low-quality pentests should be avoided, as they create a false sense of security and an unacceptable risk of compromise, including unauthorized access, data theft, and fraud. While a poorly scoped pentest may succeed in checking the compliance box, it creates new risks that accumulate over time, endangering the organization as a whole.

A quality pentest will help improve your web application’s security posture, reducing organizational risk and building trust with both customers and partners.

Whether you are selecting a provider or reading a pentest report, careful review is essential. This practical guide has been provided to help you with that process.

If you have further questions, or would like to scope out a web application pentest, feel free to contact us directly.

Our Partnership

To best serve our clients, BARR Advisory and Psicurity have closely partnered to provide comprehensive cybersecurity and compliance solutions. Our partnership enables organizations to access BARR's expert attestation and consulting services along with Psicurity's full suite of penetration testing services, while working as a single, unified team.

BARR ADVISORY

BARR Advisory is a security and compliance solutions provider specializing in cybersecurity and compliance for organizations with high-value data that serve regulated industries such as healthcare, financial services, and government. A trusted advisor to some of the fastest growing cloud-based organizations around the globe, BARR simplifies compliance across multiple regulatory and customer requirements. Learn more at barradvisory.com.

PSICURITY

Founded in 2003, Psicurity helps organizations adapt to the ever-changing threat landscape through dedicated, quality services including standards-based penetration testing, and remediation advice. We respect each client as a partner with whom we share trade secrets, develop security strategies, and implement new defensive techniques. Learn more at psicurity.com.