FROST & SULLIVAN

ICT Market Insights

The Rise of Hybrid Web Application Security Testing

Introduction

Web applications have become the de facto standard for all types of applications and usually have access (direct or indirect) to critical network resources such as databases and various back-end systems. Easy and cheap to develop and deploy, Web applications offer outstanding compatibility with all platforms, yet very few companies and organizations understand the risks they engender and may wrongly consider them simple front-end applications that can be hacked without consequences. As a result, many companies overlook Web application security processes. These vulnerable Web applications present easy targets that offer gateways to companies' most sensitive data and systems.

Today, almost every small and medium sized business (SMB) uses a number of Web applications daily, both internal and external, including customer relationship management (CRM), booking systems, eCommerce, social networks, and various customer and partner portals. These applications offer great opportunities for hackers whether they are developed and deployed by the company itself, by a third-party in the cloud, or based on a software-as-a-service (SaaS) Web platform. Though businesses spend a lot on defending against zero-day exploits[1] or sophisticated advanced persistent threats (APT), hackers can easily exploit a basic vulnerability in a Web application that can provide attackers with the same level of access to sensitive information.

The high cost and administrative complexity of penetration testing as well as the false-positives[2] and false-negatives[3] pervasive among automated scanning solutions hamper the adoption of Web application security testing. However, vendors are working to meet this market need with easy, cost-effective, and efficient solutions.

[1] Exploits a vulnerability before security vendors are aware of the vulnerability

[2] A false-positive in the context of Web application penetration testing refers to a situation where a vulnerability is reported to exist but, in fact, is not present. It is essentially a "false alarm."

[3] Conversely, a false-negative in this context means that a test indicates the absence of a vulnerability that, in fact, is present.

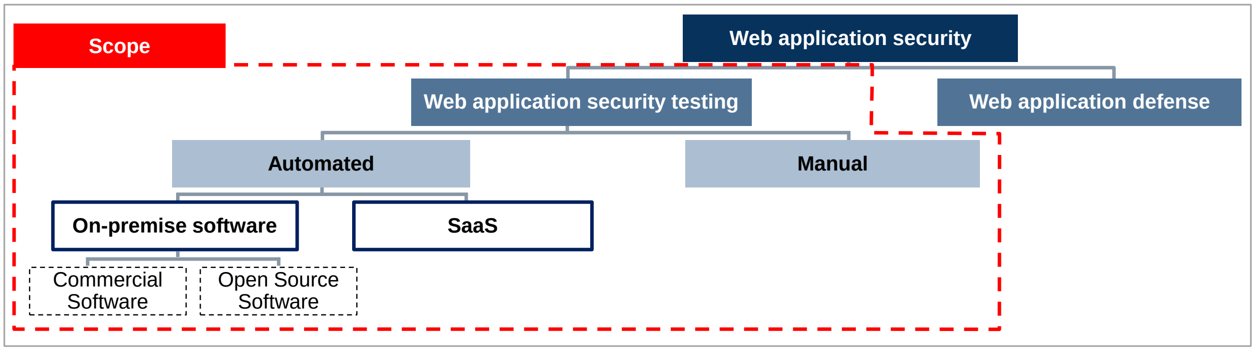
Awareness of Web Security

Unfortunately, businesses continue to underestimate the risk associated with unprotected Web applications. While there are many ways to gain illicit access into a company's network, a Web application is now a popular target. Industry research shows that Web site attacks and other hacking activities represent 40% of all tracked data breaches.[4] Hackers are likely to continue targeting this attack vector considering 4 out of 5 Web sites were found to have vulnerable Web applications.[5] Additionally, evidence shows that hackers are utilizing automated techniques to target a broad set of victims. In 2013, 30.5% of all Web site traffic was generated by malicious or unwanted bots, including automated hacking tools (which represented 4.5% of traffic).[6] Essentially, threat actors are using automated tools to test Web applications for vulnerabilities. Organizations require efficient and effective security solutions to be able to counter this threat.

Essential Web Application Security Practices

Businesses have many options available to keep their Web applications secure. There are two main branches of Web application security: proactive Web application security testing and reactive Web application defense. Web application security testing can be divided into two main approaches: automated (various tools, scanners, SaaS) and manual (penetration testing and security auditing). This Market Insight (MI) will focus on Web application security testing (see Figure 1). Discussion of Web application defense including various intrusion detection systems (IDS), intrusion prevention system (IPS), distributed denial of service (DDoS) mitigation solutions, and Web application firewalls (WAF) is not included in this MI.

Figure 1 – Web Application Security Segmentation



Source: Frost & Sullivan

[4] "Data Loss Statistics," The Open Security Foundation, accessed 21 February 2015.
[5] "Web Application Security is an On-going Commitment due to Highly Dynamic Hacking Risks," Frost & Sullivan, 2012.
[6] Zeifman, Igal, blogpost, "Report: Bot traffic is up to 61.5% of all website traffic," Incapsula's Blog, 9 December 2013.

Both Testing Approaches Perform Valuable Functions

Automated testing and manual penetration testing are both required in some capacity. Automated solutions search Web sites and applications for common security flaws, generate long lists of vulnerabilities, and provide much technical detail that can serve as the basis for prioritizing planning remediation. This is an important first step to Web application security testing as nearly all applications (96%) are vulnerable in some way, with about 14 vulnerabilities discovered per application on average.[7] Automated Web application testing solutions are provided by well-known vendors such as HP, IBM, Qualys, Acunetix, and Trustwave.

Manual Web application penetration testing relies on human analysis to identify, confirm, and exploit security vulnerabilities. Penetration testers utilize various automated tools to attain a baseline analysis of vulnerabilities in a Web site. These experts then analyze the scan results to eliminate false-positives, to exploit the vulnerabilities and see how far they can get in with it, and, probably the most important task, to identify vulnerabilities missed by automated solutions (false -negatives). Manual penetration testing provides the deep analysis and human insight necessary to find sophisticated vulnerabilities related to authentication by-pass, application logic, complex Web 2.0 vulnerabilities, or chained attacks.[8] Penetration testers can then properly prioritize the vulnerabilities by the factual risk to the customer's business continuity, integrity, and availability—something that automated solutions fail to do because they cannot take into consideration business context and environment. Penetration testers utilize a combination of commercial and open source tools, such as Core Impact and the Metasploit framework, or custom-built tools.

Both approaches provide valuable perspectives into the security posture of a Web site. Today, businesses attempt to use both automated tools and manual Web application penetration testing to ensure detection of the myriad small gaps as well as complex or severe Web site flaws.

Challenges to the Traditional Model of Web Application Security Testing

Automated Web application testing tools are a useful starting point, and many organizations subscribe to perform tests based on these tools on a regular or semi-regular basis. However, the long lists of results that these tools generate can easily become overwhelming and are often riddled with false-positives. These reports require extensive efforts to prioritize and remediate the vulnerabilities, with false-positives representing a time consuming and costly distraction. While the automated tool keeps costs low, the data is presented in a manner that is of limited value to customers, consequently demanding additional spending on security professionals to interpret and leverage the results.

[7] "Application Vulnerability Trends Report: 2014," Cenzic, 2014.

[8] Combining two or more vulnerabilities to gain access that would not otherwise be possible

Moreover, because of false-negatives many security tools provide customers with a false sense of security, provoking negligence and thus facilitating opportunities for hackers. Alibaba[9] and Delta Airlines[10] are two recent high profile examples of companies compromised by Web application logic vulnerabilities that were not detectable by any sort of automated solution, which could have led to a great compromise of confidential data and operations.

Automated solutions offered on a SaaS subscription base scan a Web application 24/7 and are capable of quickly notifying Web site owners about defacements, hacks, "obvious" vulnerabilities (e.g., Heartbleed or GHOST), or malware infections. This is something of which a penetration test cannot and is not intended to flag or to prevent in all cases. For example, if a Web site administrator PC is compromised or stolen, then a continuous monitoring solution would detect and report it. However, even the most sophisticated Web penetration test would not prevent this vector of attack.

On the other hand, manual Web application penetration testing cannot provide continuous monitoring at a justifiable cost, rather it provides deep and actionable analysis of the tested scope and perimeter. It is a labor-intensive process that requires significant knowledge and experience of application development, auditing, security practices, and standards. As a result, these tests are costly, which forces customers to drastically narrow the scope and frequency of their assessments—an annual assessment is considered a successful practice.

SaaS Delivery Models Enable the Emergence of Hybrid Security Assessment Solutions

Frost & Sullivan finds that both automated and manual testing are functions that assure the necessary level of Web application security. But for most businesses, automated solutions are too shallow, and manual Web application penetration testing is out of budget or is simply too infrequent to provide much security insight. What is required is a solution that blends the efficiency of automated tests with the effectiveness of a manual penetration test and delivers it as a SaaS.

Frost & Sullivan refers to this combination as an on-demand[11] hybrid Web application security assessment or on-demand hybrid Web application penetration test. That is, a hybrid Web security application assessment solution is neither a manual test nor an automated tool, but a combination of the two approaches balanced to maximize efficiency and effectiveness. Ideally, a hybrid Web application security solution reflects the following key characteristics:

1. it utilizes proprietary scanning technology that is actively used, supported, and improved by manual penetration testing experts in order to minimize false-positives and adapt to evolving hacking techniques;
2. manual penetration testing is delivered by in-house security experts who use and support the proprietary scanning technology and write custom, actionable reports tailored for the appropriate audience (developers, security specialists, IT generalists, or business users);

[9] Kovacs, Eduard, "Vulnerabilities in Alibaba Marketplace Exposed Buyer and Seller Accounts," SecurityWeek, December 11, 2014.

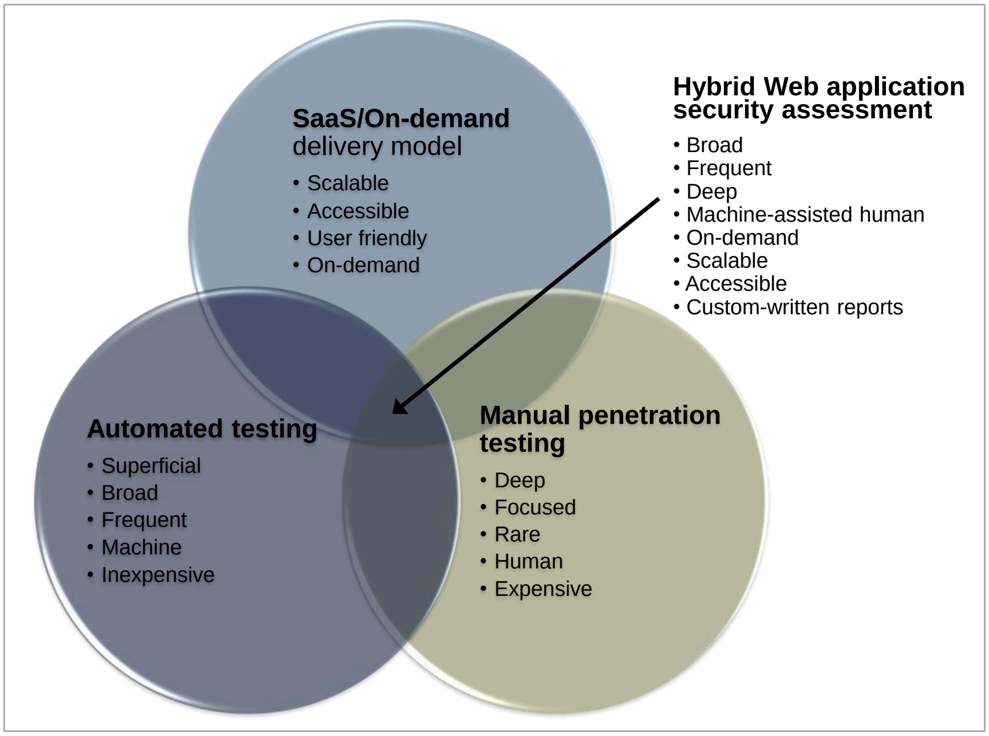
[10] Arce, Nicole, "Delta URL Bug Allowed Anyone to Access Anyone's Boarding Pass: Here's How (But it's Fixed Now)," Tech Times, December 18, 2014.

[11] On-demand means 24/7 availability where purchase, configuration, and management are possible entirely online.

3. hybrid Web application security assessment should also leverage a scalable on-demand SaaS model that enables simple, rapid, and transparent adoption by a broad range of users, including SMBs and enterprise customers.

Figure 2 illustrates characteristics of testing done through automated tools and manual penetration testing that hybrid SaaS Web application security testing strikes a balance between.

Figure 2 – SaaS Hybrid Application Security Assessment Characteristics



Source: Frost & Sullivan

Importantly, a true hybrid solution should integrate feedback from manual penetration tests to develop the automated technology further, while automated scanning gives more and more useful information to the (manual) auditors. The solution is analogous to a hybrid car wherein an electrical engine supports a fuel motor and vice-versa. This creates a virtuous circle of product development that improves the accuracy of the automated test as well as each subsequent test. As a result, the value created by a hybrid Web application security assessment is greater than the sum of its automated and manual testing components.

Furthermore, the SaaS model is vital to this definition in that it makes possible the on-demand nature of scanning for customers and instant feedback for the vendor. SaaS hybrid solutions enable the scalability and instant accessibility for use by a range of customer types. For vendors, the SaaS on-demand capability is critical to the process of quickly integrating feedback from manual penetration testers into the automated scanning tool.

The SaaS delivery model is a key point of differentiation between a hybrid assessment and classic penetration testing. Many automated solutions are delivered by a SaaS model, yet the potential to leverage insight gathered by hybrid SaaS assessments has been largely unrealized by security vendors.

Tracking the Emergence of Hybrid Assessment Solutions

The basic idea of hybrid assessment is to unify different testing methodologies into an integrated approach that leverages the advantages of each while minimizing the weaknesses. The idea of combining automated and manual methods is evolutionary rather than revolutionary. Consequently, multiple Web application security assessment solutions reflect some of this fundamental convergence.

Often, however, the integration of the two approaches is not emphasized or optimized. Currently, large, well-known vendors offer automated tools or manual penetration testing services that remain divided into separate business units or face other operational challenges to integrating the two testing techniques. This reflects the dual challenge of having to manage effective product development whilst cultivating the skills of an adept professional security service provider that few companies have taken on.

Instead, hybrid Web application security assessment is emerging as a separate category of solutions that has seen some security specialists such as High-Tech Bridge, Secfence Technologies, and Synercomm attribute similar labels of "hybrid" to their offerings. Synercomm and Secfence, respectively, describe their AssureIT Web application testing services and Web application penetration testing services as combining automated and manual testing techniques. Although the companies appear to have embarked on the path to offering a hybrid solution, both are restrained by a reliance on commercial automated tools that they did not develop, do not own, and do not offer as a SaaS delivery model.[12,13] Finally, some companies such as Whitehat Security offer many of the capabilities characteristic of the hybrid Web application security assessment category but do not actively position any solution as "hybrid."

High-Tech Bridge, in this respect, posits that its ImmuniWeb® on-demand Web penetration testing solution is a good example of a hybrid testing SaaS based on its proprietary ImmuniWeb scanner, which is used and supported by internal penetration testing experts and can be configured and managed through an online portal.[14] Of the solutions tracked as part of this research, High-Tech Bridge offers the most complete hybrid-labeled offering available today, having realized the importance of a hybrid approach and having the SaaS model needed to facilitate integration of manual penetration testing expertise into its proprietary scanning technology.

[12] Synercomm, "Web Application Testing," Synercomm Web site, accessed 25 February 2015.

[13] Secfence Technologies, "Web Application Penetration Testing," Secfence Technologies Web site, accessed 12 February 2015.

[14] High-Tech Bridge, "ImmuniWeb® On-Demand Web Penetration Testing Technology," High-Tech Bridge Web site, accessed 20 February 2015.

Summary and Conclusion

Automated testing is inexpensive, can be used continuously, and is scalable, but it is limited in its usefulness by producing false-positives and false-negatives. It tends to be too incomplete, especially as organization size and security needs increase. Manual penetration testing can deliver sophisticated and profound Web application security assessments, but it cannot be deployed continuously or exhaustively due to the cost of employing highly qualified human resources to do the actual work.

Combining the efficiency of automated testing and effectiveness of manual penetration testing in a hybrid solution and enabling these through a SaaS delivery model is a logical move toward achieving the greatest possible security from a limited budget, which will only increase in importance as Web applications and threats continue to grow in number and complexity. Frost & Sullivan anticipates that established vendors will increasingly recognize the value of hybrid solutions, though some are better positioned than others to bring a solution to market. Nevertheless, more will certainly be heard about hybrid solutions going forward.