Enhancing Web Application Security through Proactive Vulnerability Monitoring and Open Disclosure Tracking

Vivek Somi

somivivek@gmail.com

Abstract

This paper analyses the opportunities that proactive vulnerability monitoring and open disclosure tracking offer to improve web application security. Vulnerability scanning entails a constant search for vulnerability, while open vulnerability reporting entails reporting these vulnerabilities with less severity. When applied together with web application penetration testing, these practices will help establish an effective security model to help organizations to detect and provide solutions to vulnerabilities within their systems. This paper also reviews the advantages, disadvantages and the way forward on vulnerability monitoring together with other trends that are trending now such as artificial intelligence, blockchain, and zero-trust architecture. These are improvements that are likely to transform how organizations inspect and counter risks and guarantee the continuity of security to corporate resources.

Keywords: Vulnerability Monitoring, Open Disclosure, Web Application Security, Penetration Testing, Cybersecurity, Artificial Intelligence, Blockchain, Zero Trust Architecture, Threat Detection, Proactive Security

Introduction

Web application security is now among the critical issues in the current computer environment given that more organizations depend on Web applications as channels through which customers access products and services, manage internal business processes, and store information. Nevertheless, with the emergence of new web applications, related threats in such systems have increased significantly. Since Web applications deal with strict information such as and personal details, financial information it is very important that they are secure.

Of all the approaches used to reduce these threats effectively, the most viable one is vulnerability monitoring proactively. As a result, potential threats are detected and mitigated proactively without waiting for hackers to use them to their advantage by penetrating the workflow of the organization and compromising web applications. In such regard, the utilization of open disclosure tracking as an organization's feature is established as an essential factor in an organization's cybersecurity framework. It enables organizations to report security weaknesses that they find and to have them fixed and a secure environment is achieved.

Inthis study, the significance of vulnerability monitoring in web application security will beanalysed, and how practising open disclosure tracking can improve vulnerability management vastly will be also explained at length. This study will also discuss how vulnerability monitor fills the gaps of traditional penetration tests, it also provides useful tips for good security programs, challenges and future development of the vulnerability monitor.

Understanding Vulnerability Monitoring

Definition and Purpose

Vulnerability monitoring refers to continuously scanning for flaws in webapplications that malicious attackers can exploit[1]. This method is of the utmost importance in web application security since it provides instantaneous awareness of potential vulnerabilities so organizations will be able to repair them before it is attacked. Some of the cyber-attacks that represent a risk to an organization's integrity are data breaches and unauthorized access, that's why vulnerability monitoring exists to feed up all these risks[2]. This paradigm shift pulls security out of the reactive mode (where vulnerabilities become fixed once they're exploited) and over closer to the proactive space (detect and fix vulnerabilities at the earliest possible time)[3].

A feature of a web application by design, it is an easy attack target and exposed to the internet[4]. The ability to monitor vulnerabilities continuously is more important than ever in today's hyper-connected world, where organizations more and more rely on web-based platforms. Vulnerability monitoring helps the organization stay alert to the latest threat and ready with a response to swiftly[5]. As it monitors vulnerabilities in real-time, vulnerability monitoring reduces the chance of exploitation and frees up security team resources to focus on mitigation instead of being crippled by a potential cyberattack.

Key Components of Effective Vulnerability Monitoring

While an effective vulnerability monitoring system is not a one-size-fits-all model, it is a combination of tools, practices, and policies that all work together to provide complete coverage of security[6]. Automated vulnerability scanning tools are important in order to find known vulnerabilities because they scan web applications networks or databases continuously to find the things which are not much known to the common people. Unfortunately, these automated tools, on their own, are not enough to identify complex issues, and this is where knowledgeable security professionals come in to provide manual assessments[7].

Figure 1: Web Security Threats and Best Practices

Source: Adapted from [7]

Considering both the manual assessments and the human element they introduce to the process of monitoring vulnerabilities, gives experts the ability to analyse the application logic as well as identify flaws that were missed by automated scanners, and perform more sophisticated testing. It especially useful for catching the kind of business logic vulnerabilities and flaws in the application in which the way it works is exploited, as opposed to flaws in the underlying code are business logic vulnerabilities[8].Another necessary

feature is the real-time alerts and notifications integration. An effective monitoring system should be an instant alert to security teams on newly found vulnerabilities so that they can take quick action upon it. Such a timely response is essential for blocking attackers' exploitation of weaknesses. Additionally, threat intelligence, that is, acquiring information on unknown threats from external sources in order to monitor the presence of new vulnerabilities within the wider cybersecurity landscape, has played a role in keeping organizations updated on newer vulnerabilities in the general cybersecurity arena[9].

The backbone of an effective vulnerability monitoring system is continuous monitoring. Continuous monitoring addresses the drawback of periodic assessments in that there are no wide gaps between evaluations, and thus vulnerabilities are discovered as soon as they appear. In the case where new code is frequently deployed into high-traffic environments, this is very important as it increases the chance of security flaws.

Open Disclosure Findings

Explanation of Open Disclosure

Open or Responsible disclosure is a practice whereby the hacker informs the owner of the webpage with the leak, of the vulnerability and even demonstrates the vulnerability but does not exploit it to the public. This gives the organisation ample time to close this hole before anyone can take advantage of it. That is why once such a threat is addressed, its details together with the solution are released into the public domain so that the companies and the security community can work together.The open-disclosure culture is an important aspect of today's cybersecurity as so as has shown it motivates ethical hackers to engage in the proper development of web applications[10]. They can also find weaknesses that insiders might overlook so that external researchers are beneficial to organizations.

Benefits and Potential Risks of Open Disclosure Practices

The key advantage of open disclosure is that an organisation can address weaknesses that it has in place before others capitalize and publicize on them. This approach also countermeasures the risks as well as cultivates trust between the firms and users/ stakeholders. Most organizations have adopted bug bounty programs, in order to encourage ethical hacking since members get rewarded when they discover more vulnerabilities.Open disclosure has its drawbacks; for instance,disclosure of the vulnerabilities before a solution has been developed exposes organizations to being attacked[11]. If the vulnerability is announced and there is not enough time to act upon it, the attackers will be able to use the flaw and produce a lot of harm. Such scenarios can be avoided by organizations which need to act swiftly on vulnerability reports.

How Open Disclosure Findings Tracking Enhances Vulnerability Monitoring

Overlying open disclosure findings enhances vulnerability analysis since it remits findings to the organizations about existing vulnerabilities. Therefore, enriching these monitoring tools with the presented findings will help companies improve the detection of new threats[12]. For instance, using open disclosure where a given vulnerability affects a popular framework, an organization employing the framework can immediately focus on the vulnerability by scanning for similar problems in its system.Open disclosure findings provide insights into the types of vulnerabilities actively being targeted by attackers, allowing organizations to adjust their security strategies accordingly[13]. Integrating these findings into automated monitoring tools ensures that both known and newly discovered vulnerabilities are identified and addressed promptly.

Integration with Web Application Penetration Testing

How Vulnerability Monitoring Enhances Penetration Testing

Vulnerability monitoring and penetration testing are two related techniques of information security. While penetration testing assumes an attacker's position on the web application in order to expose each of the possible flaws, vulnerability monitoring constantly searches for vulnerabilities online. Combining these practices makes the security stronger since by use of monitoring in case there is a creation of another security hole after a penetration test, it will be noticed[14].Vulnerability monitoring also has its benefit for penetration testing since it supplies a lot of relevant information about the systems in the organization. For instance, monitoring tools may be used to point out the aspect of the web application that seems to be most susceptible to attacks; penetration testers, therefore, should consider focusing on such areas[15]. This is bound to enhance the approaches used in penetration tests since it will be done with the recent information regarding the security state of the application.

Practical Steps for Integration

To include vulnerability monitoring to penetration testing, the schedules for testing need to be harmonised with continuous monitoring. This guarantees that penetration tests are going to be conducted on the current vulnerability data and therefore a better approximation of the application is achieved. Organizations should use the monitoring data to inform the penetration testing activity to be conducted in an organization[16]. These risk slots can be formulated by vulnerability monitoring, which will enable penetration testers to brainstorm more intensely on these areas. A correlation test should be with the monitoring team in a way that the monitoring tools and procedures are to be updated after every test is conducted.The patch management tools and the system used to determine vulnerabilities should be compatible with monitoring tools to begin patching as soon as they are identified[17]. It helps to ensure that the time difference between the discovery of a weakness and the time the patch to the weakness is implemented is reduced hence reducing the exploit time space.

Key Strategies for Effective Vulnerability Monitoring

To bring into effect the most suitable vulnerability monitoring program it is necessary to follow certain steps. As a result of the factors discussed, other automated tools should also be integrated with the manual solutions to achieve adequate coverage. Static analysis tools are used to identify known weaknesses and dynamic tools enable the identification of other harder-to-find problems.

Organizations should also make sure that tools which are used to monitor are adequately updated so that they can suit the current threats. Threat landscapes change over time quickly; by doing frequent updates with the tools available, new emerging threats are recognized and resolved on time[18]. Also, there is the need to assess priorities because all the vulnerabilities are not equal and do not even necessarily constitute equal threats. Such vulnerabilities with high-risk ratings, which include the risk of data or service loss, must be fixed first.This makes it possible to have a clear record of audit and it also makes it possible to avoid leakage of certain types of security breaches.

Figure 2: Strategies for Vulnerability Monitoring

Source: Adapted from [18]

Tips for Implementing a Robust Monitoring Program

For organizations that have not implemented vulnerability monitoring before, then the best approach is to begin with a small scope and build-up. It is suggested to start with the simple monitoring of the key systems and then gradually develop this program. Training of the security teams is also crucial as well to know how to read the results of monitoring and how to react[19].Organizations should also develop ways of working with external conveyors of the vulnerability by creating bug bounty programs or vulnerability disclosure policies. This makes it easy for outsiders to report cases of vulnerabilities which enhances the organization's security. Lastly, incorporating monitoring tools into other security systems including intruder detection systems and security information as well as event management systems offers a better look at an organization's security solutions.

Challenges and Limitations

Common Obstacles in Vulnerability Monitoring

A potential problem is alert overloading, wherein security teams, through monitoring systems, may receive an excess of alerts rather than solely pertinent ones. It can have the consequence of accomplishing significant vulnerabilities that are of terminal importance[20]. As a result, the said problem should be solved by categorizing different alerts taking into consideration their risk and severity levels.Another limitation is the question of resource limitation, most noticeable in organizations with limited resources. Real-time vulnerability scanning, for instance, comes with the cost of implementing new systems and instrumentations, staff recruitment or training, among others[6]. Realistically and sadly, smaller organizations may not be able to invest adequate resources toward owning a functioning monitoring provision.

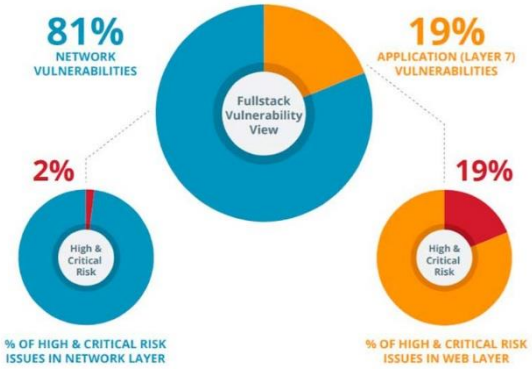

Figure 3: Threats in Vulnerability Monitoring

Source: Adapted from [21]

Monitoring is more difficult because the requirements for modern web applications are higher than for legacy systems. Since a considerable number of applications employ a variety of programming languages, various frameworks, and third-party libraries, each of them is potentially flawed[21]. It can be seen that such systems are best supervised by highly skilled professionals as well as possessing unique features.

Potential Drawbacks and How to Mitigate Them

A major weakness of vulnerability monitoring is that it often results in high false positives, where normal activity is seen as a threat. Doing so can be a complete waste of time and effort. To address this, the organizations should leverage the automated tools to identify the vulnerabilities while doing a follow-up verification done through other means hand.Another is the increased probability of over-dependency on the systems[22]. Although using automated tools for monitoring is valuable when dealing with a broad range of sources, human supervision cannot be avoided. Several automation issues have to be solved through manual assessment for example I/O injections, SQL payload injection, time of check to time of use, cross-site scripting, business logic vulnerabilities, multiple input fields and complicated interactions within the application[23].

One of the major risks is if alerts are issued and not responded to in good time. Although such a mechanism is reasonably effective, some organisations may not pay adequate attention to addressing the identified weaknesses. That is why, defining clear response processes and delegating responsibility for vulnerability management can reduce this risk.

Future Trends

Emerging Technologies in Vulnerability Monitoring

Concerning the field of vulnerability monitoring is dynamically developing, and the usage of new technologies during the creation of vulnerability detection and counteraction systems is constantly increasing. The most appealing advancement documents the use of artificial intelligence and machine learning in vulnerability trackers. Such systems could also make evaluations, assessments and forecasts concerning large amounts of data, tendencies and probable risks before they are being exploited[24]. With the help of switching to AI and ML, it is possible to recognize complex attacks that are not revealed by regular monitoring.

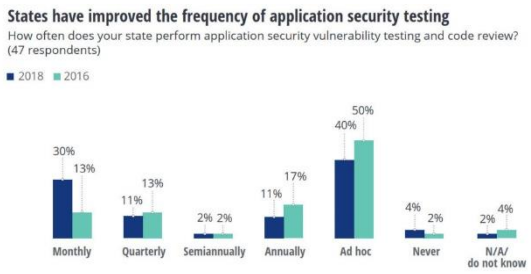

Figure 4: Emerging Technologies in Vulnerability Monitoring

Source: Adapted from [24]

Self-tracking may also be revolutionized by the use of blockchain technology regarding vulnerability monitoring. The use of Blockchain technology as a platform for recording vulnerability data is convenient because it is decentralized and cannot be tampered with. Blockchain has the potential to enhance the vulnerability management process by enabling the creation of an unalterable ledger that contains all the vulnerabilities and how they will be addressed. This could be particularly useful in fields with specific regulatory demands which inputs a necessity to prove compliance with security standards for instance the finance or the health care sector.

Another nascent trend that may revolutionize vulnerability monitoring is zero-trust architectures[25]. This approach postulates that the network perimeter and the users and devices inside and outside this perimeter are intrinsically malicious. This approach expects the certification of all access requests without favouring internal or external origin. Incorporation of the zero-trust concept on the vulnerability scanners can improve the ability of an organization in identifying insider threats, compromised computers, and unauthorized access among others.

Predicted Developments in the Field

The future of vulnerability monitoring looks ahead, including several developments that can affect the future program. While AI and ML technologies get better, organizations will increasingly rely on automated tools that will automatically detect and respond to vulnerabilities in real-time. Organizations that intend to beat cyber threats will start getting involved in automated patch management systems, real-time vulnerability tracking and AI-driven threat detection[26].

A significant advance will be in integrating vulnerability scanning even closer with DevSecOpspractices. DevSecOps means to incorporate security into each stage of the software development lifecycle such that, instead of being identified and resolved after the deployment, they are detected and remediated during the course of development[27]. When organizations embrace DevSecOps, vulnerability monitoring will be a critical part of the development continuum, allowing continuous security assessments across the entire life cycle of the application.

However, vulnerability monitoring efforts will increasingly leverage collaboration between organizations, and with the cybersecurity community. As bug bounty programs, responsible disclosure policies and partnerships with external researchers increase in popularity organizations will have a broader pool of expertise to call upon.Developing this together will ensure that vulnerabilities are found sooner and the security of web applications is better overall when vulnerabilities are found sooner.

Conclusion

Considering the expanding threats in cyberspace, organizations need to take preventive measures to shield their web applications as well as the very data they handle. By making open their vulnerabilities, organisations also get the tools and insight to find, assess and eliminate their security weaknesses before such vulnerabilities are used by attackers. To have effective vulnerability monitoring, it needs to be based on a layered approach combining automated tools, manual assessments, real-time alerts, continuous updates, infrastructure monitoring, and other tools which are used for vulnerability management. While there is a narrowpath forward filled with false positives, alert fatigue, and resource constraints, it is nonetheless possible for organizations to negotiate this path through strategic planning, investment in appropriate technologies, and working with the cybersecurity community.

Looking ahead, advancements in AI, blockchain, and zero-trust architectures will transform the vulnerability monitoring sector. These technologies will only further gain in development so that organizations will be better able to detect and how to respond to vulnerabilities in real time to maintain secure web applications in an increasingly complex threat environment. With vulnerability monitoring coupled with penetration testing and having best practices for continuous improvement in place, organizations can see ahead of potential threats coming, and keep their digital assets intact.

Bibliography

[1] S. Bairwa, B. Mewara, and J. Gajrani, "Vulnerability Scanners: A Proactive Approach to Assess Web Application Security," *International Journal on Computational Science & Applications*, vol. 4, no. 1, pp. 113–124, Feb. 2014, doi: https://doi.org/10.5121/ijcsa.2014.4111.

[2] S. Gupta and B. B. Gupta, "Detection, Avoidance, and Attack Pattern Mechanisms in Modern Web Application Vulnerabilities," *International Journal of Cloud Applications and Computing*, vol. 7, no. 3, pp. 1–43, Jul. 2017, doi: https://doi.org/10.4018/ijcac.2017070101.

[3] Q. Chen, "Proactive Vulnerability Discovery and Assessment in Smart, Connected Systems Through Systematic Problem Analysis," *Deep Blue (University of Michigan)*, Jan. 2018.

[4] H. H. Jazi, H. Gonzalez, N. Stakhanova, and A. A. Ghorbani, "Detecting HTTP-based application layer DoS attacks on web servers in the presence of sampling," *Computer Networks*, vol. 121, pp. 25–36, Jul. 2017, doi: https://doi.org/10.1016/j.comnet.2017.03.018.

[5] S. UMRAO, M. KAUR, and G. K. GUPTA, "VULNERABILITY ASSESSMENT AND PENETRATION TESTING," *International Journal of Computer and Communication Technology*, pp. 200–203, Jul. 2016, doi: https://doi.org/10.47893/ijcct.2016.1367.

[6] E. Zio, "Challenges in the vulnerability and risk analysis of critical infrastructures," *Reliability Engineering & System Safety*, vol. 152, pp. 137–150, Aug. 2016, doi: https://doi.org/10.1016/j.ress.2016.02.009.

[7] S. Chen, "10 Cybersecurity Statistics in 2019 [Infographic]," *TitanFile*, Nov. 05, 2019. https://www.titanfile.com/blog/cybersecurity-statistics-2019/

[8] M. Sharma and S. Singh Tomar, "Attack Detection and Security in Remote Code Execution," *International Journal of Computer Applications*, vol. 114, no. 14, pp. 9–15, Mar. 2015, doi: https://doi.org/10.5120/20045-1475.

[9] S. Brown, J. Gommers, and O. Serrano, "From Cyber Security Information Sharing to Threat Management," *Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security*, Oct. 2015, doi: https://doi.org/10.1145/2808128.2808133.

[10] A. Maurushat, "Ethical Hacking," 2019. Available: https://library.oapen.org/bitstream/handle/20.500.12657/87998/9780776627922.pdf?sequence=1

[11] "Information disclosure attacks in web applications," Invicti. [Online]. Available: https://www.invicti.com/blog/web-security/information-disclosure-issues-attacks/.

[12] F. Li *et al.*, "You've Got Vulnerability: Exploring Effective Vulnerability Notifications You've Got Vulnerability: Exploring Effective Vulnerability Notifications," 2016.[Online]. Available: https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_li.pdf

[13] M. Cadariu, E. Bouwers, J. Visser, and A. van Deursen, "Tracking known security vulnerabilities in proprietary software systems," *2015 IEEE 22nd International Conference on Software Analysis, Evolution, and Reengineering (SANER)*, Mar. 2015, doi: https://doi.org/10.1109/saner.2015.7081868.

[14] J. Doshi and B. Trivedi, "Comparison of Vulnerability Assessment and Penetration Testing," *International Journal of Applied Information Systems*, vol. 8, no. 6, pp. 51–53, Apr. 2015, doi: https://doi.org/10.5120/ijais15-451326.

[15] F. Jeremy, "Penetration Tester's Open Source Toolkit," *Google Books*, 2016. https://books.google.com/books?hl=en&lr=&id=avWcBAAAQBAJ&oi=fnd&pg=PP1&dq=How+Vulnerability+Monitoring+Enhances+Penetration+Testing&ots=yD_RZPeGNq&sig=NaUtIQWWVtob5UcR4i5_R_1Q2o0.

[16] V. Chang and M. Ramachandran, "Towards Achieving Data Security with the Cloud Computing Adoption Framework," *IEEE Transactions on Services Computing*, vol. 9, no. 1, pp. 138–151, Jan. 2016, doi: https://doi.org/10.1109/tsc.2015.2491281.

[17] M. Kumar and A. Sharma, "An integrated framework for software vulnerability detection, analysis and mitigation: an autonomic system," *Sādhanā*, vol. 42, no. 9, pp. 1481–1493, Jul. 2017, doi: https://doi.org/10.1007/s12046-017-0696-7.

[18] Testbytes, "Testbytes: Software Testing and QA Consulting Company," *Testbytes*, 2019. https://www.testbytes.net/resource/cyber-security-statistics-2019/

[19] I. Kirlappos, S. Parkin, and M. Sasse, "Learning from 'Shadow Security': Why understanding non-compliant behaviors provides the basis for effective security," 2014, doi: https://doi.org/10.14722/usec.2014.23%3C007%3E

[20] To Be Appear At: Ieee, Communications, V. Tutorials, Xx, and X. No, "Security of the Internet of Things: Vulnerabilities, Attacks and Countermeasures," 2019. Available: https://arxiv.org/pdf/1910.13312

[21] N. Sanyal, "Web application security facts to consider for 2019," *Devhelperworld.in*, 2019. https://www.devhelperworld.in/2019/06/web-application-security.html.

[22] B. Ali and A. Awad, "Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes," *Sensors*, vol. 18, no. 3, p. 817, Mar. 2018, doi: https://doi.org/10.3390/s18030817.

[23] M. Abomhara and G. M. Koien, "Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks," *Journal of Cyber Security and Mobility*, vol. 4, no. 1, pp. 65–88, 2015, doi: https://doi.org/10.13052/jcsm2245-1439.414.

[24] B. Ventures, "2019 RANSOMWARE STATISTICS – Business Ventures," *Business Ventures*, 2019. https://businessventures.com.mt/cyber-crime/2019-ransomware-statistics/

[25] N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," *Telecommunications Policy*, vol. 41, no. 10, pp. 1027–1038, Nov. 2017, doi: https://doi.org/10.1016/j.telpol.2017.09.003.

[26] G. Nagar, "The Evolution of Security Operations Centers (SOCs): Shifting from Reactive to Proactive Cybersecurity Strategies," *International Journal of Scientific Research and Management (IJSRM)*, vol. 6, no. 09, pp. 100–115, Sep. 2018, doi: https://doi.org/10.18535/ijsrm/v6i9.ec03.

[27] L. Williams, F. Massacci, and G. Synopsys, "Secure Software Lifecycle Knowledge Area Issue," 2019. Available: https://cybok.org/media/downloads/Secure_Software_Lifecycle_issue_1.0.pdf