JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Fortifying Cybersecurity: VAPT Strategies with OWASP and Django Framework

Dr. Rajini S - (B.E., M.Tech., Ph.D)
Department of Information Science Engineering
Vidyavardhaka College of Engineering
Mysuru, India

Chiranth K N
Department of Information Science Engineering
Vidyavardhaka College of Engineering
Mysuru, India

Darshan A S
Department of Information Science Engineering
Vidyavardhaka College of Engineering
Mysuru, India

Darshan G R
Department of Information Science Engineering
Vidyavardhaka College of Engineering
Mysuru, India

Guru Pruthvi J M
Department of Information Science Engineering
Vidyavardhaka College of Engineering
Mysuru, India

***Abstract*—In This survey delves into the increasing complexity of computer systems and interconnected networks, heightening their vulnerability to cyber threats and necessitating robust cybersecurity measures. Focusing on the pivotal role of Vulnerability Assessment and Penetration Testing (VAPT), the paper navigates through the systematic life cycle of VAPT, elucidating key phases like reconnaissance, scanning, gaining access, maintaining access, and analysis. By emphasizing the significance of OWASP Zed Attack Proxy (ZAP) and the Django framework, the study presents a comprehensive framework for identifying, addressing, and preventing vulnerabilities in web applications, adding an extra layer of protection through Django's renowned security features. The operational scheme of VAPT underscores meticulous planning, execution, result analysis, and reporting. Additionally, the paper reviews the OWASP Top Ten vulnerabilities, with a specific focus on injection and cross-site scripting, culminating in the amalgamation of penetration testing methodologies supported by Django and OWASP tools as a dynamic defense against evolving cyber threats. Despite not explicitly incorporating the Raspberry Pi 3b+, the paper highlights practical application and adaptability, recognizing the ongoing evolution of these methodologies as crucial for effective cybersecurity in the dynamic landscape.**

Keywords- VAPT: Vulnerability assessment (VA), Penetration testing (PT), OWZAP, ZAP.

I. INTRODUCTION

The ubiquity of computers, interconnected systems, and intricate software has accentuated the susceptibility of systems to cyber threats. Vulnerabilities, denoting weaknesses in applications, present substantial risks to system security and information assurance. As assailants exploit these vulnerabilities to gain unauthorized access and information, the imperative for robust cybersecurity measures becomes undeniable.

Vulnerability Assessment and Penetration Testing (VAPT) have emerged as indispensable components of cyber defense technology. VAPT entails the systematic evaluation and testing of systems to identify weaknesses and potential exploits. While achieving a 100% vulnerability-free system may be an elusive goal, regular and efficient VAPT can significantly diminish the risk of cyber-attacks, fortifying overall system security and information assurance.

This paper delves into VAPT as a proactive cyber defense technology, underscoring its paramount importance amid the escalating cyber threats. The life cycle of VAPT is expounded upon, encompassing various techniques employed in vulnerability assessment and penetration testing. Notably, VAPT serves as a proactive measure, helping identify cyber threats and vulnerabilities under controlled circumstances, allowing organizations to preemptively address and eliminate potential risks before malevolent actors exploit them.

The existing body of research in vulnerability assessment sheds light on important regularities and interdependencies among vulnerabilities. The paper meticulously reviews studies on web vulnerability scanners, topological vulnerability analysis approaches, and comprehensive investigations of specific vulnerabilities. Additionally, the integration of VAPT into a structured approach for cybersecurity is underscored, emphasizing the need for a holistic defense strategy.

The comprehensive paper is meticulously organized into sections, commencing with an introduction to VAPT, followed by a detailed exploration of its life cycle, presentation of prevalent techniques and tools, and a discussion on its pivotal role as an effective cyber defense technology. The paper systematically unfolds, elucidating the dynamic nature of cyber threats and the ongoing necessity for VAPT to adapt and evolve in tandem.

In the introductory section, the paper underscores the increasing prevalence of cyber threats due to the widespread use of computers, interconnected systems, and complex software. It highlights the significance of vulnerabilities, defined as weaknesses in applications, as potential entry points for attackers seeking unauthorized access and information. The urgency for effective cybersecurity measures is emphasized as a countermeasure to mitigate the risks posed by these vulnerabilities.

Moving on to the life cycle of VAPT, the paper meticulously details the systematic evaluation and testing processes involved. It explicates how VAPT aims to identify weaknesses and potential exploits in systems, acknowledging the practical challenge of achieving a completely vulnerability-free system. The paper underscores the preventive nature of VAPT, enabling organizations to proactively address and eliminate potential risks before they are maliciously exploited.

The subsequent sections delve into existing research on vulnerability assessment, providing insights into important regularities and interdependencies among vulnerabilities. The paper reviews studies on web vulnerability scanners, which play a crucial role in identifying and assessing vulnerabilities in web applications. Topological vulnerability analysis approaches are explored, shedding light on comprehensive studies that analyze specific vulnerabilities in-depth.

Throughout the paper, the integration of VAPT into a structured approach for cybersecurity is a recurring theme. The importance of adopting a holistic defense strategy is emphasized, recognizing that VAPT is just one facet of a comprehensive cybersecurity framework. The conclusion reiterates the dynamic nature of cyber threats and emphasizes the perpetual need for VAPT. Future research directions are suggested, underlining the evolving landscape of cyber threats and the continuous adaptation required in the realm of vulnerability assessment and penetration testing.

II. TYPES OF VULNERABILITY

Vulnerabilities in computer systems represent flaws or weaknesses that can be exploited, potentially leading to security breaches. Once an attacker identifies and exploits these vulnerabilities, the confidentiality, integrity, and availability of a system's resources become at risk. Attackers often employ specific tools and strategies to identify and compromise application vulnerabilities. The OWASP Top 10 vulnerability list, along with Common Weakness Enumeration (CWE) associations, provides insights into the most prevalent vulnerabilities related to web application security.
The OWASP Top 10 2013 list includes various vulnerabilities, each associated with a specific CWE rank:

1. Injection (CWE-929)
2. Broken Authentication and Session Management (CWE-930)
3. Cross-Site Scripting (XSS) (CWE-931)
4. Insecure Direct Object Reference (CWE-932)
5. Security Misconfiguration (CWE-933)
6. Sensitive Data Exposure (CWE-934)
7. Missing Function Level Access Control (CWE-935)
8. Cross-Site Request Forgery (CWE-936)
9. Using Component with Known Vulnerability (CWE-937)
10. Invalidated Redirects and Forwards (CWE-938)

Injection vulnerabilities and Cross-Site Scripting (XSS) are particularly highlighted as significant threats. XSS vulnerabilities involve injecting client-side scripts into web pages, executed when viewed by other users. These vulnerabilities can lead to bypassing Same Origin Policy, identity theft, data exposure, session hijacking, malware attacks, website defacement, and denial of service.

Cross-Site Scripting attacks come in two forms:
Persistent XSS: Malicious code submitted by an attacker is stored on the server, allowing victims to retrieve the unsafe data.
Non-Persistent XSS: Attacker-crafted URLs trick victims into clicking links, sending injected code to the server, which reflects the attack back to the victim's browser for execution.

III. PENETRATION TESTING

Process of Penetration Testing

Figure 1 General scheme of the process of penetration testing.

Penetration testing, a crucial component of Vulnerability Assessment and Penetration Testing (VAPT), involves a systematic process aimed at assessing the security posture of a system or network. The first phase, Reconnaissance, involves determining the scope and objectives of the test while gathering intelligence to gain a comprehensive understanding of the target. Subsequently, Scanning is conducted through static analysis, inspecting an application's code to predict its behaviour, and dynamic analysis, examining the code in a running state for a real-time view of application-performance.

Upon identifying vulnerabilities, the process moves to Gaining Access, where external testing focuses on visible internet assets, such as web applications and Domain Name Servers, with the goal of extracting valuable data. Internal testing simulates insider attacks, reflecting scenarios where a person with internal access breaches the system, and Blind
Testing provides a realistic perspective by giving testers only the target name. Double-blind testing simulates real-world attacks with no prior knowledge, and Targeted testing involves mutual information sharing between the tester and the target, offering valuable real-time feedback.

Maintaining Access is a critical step to assess the system's susceptibility to ongoing threats and establish a strong presence within the exploited system. The subsequent Analysis phase utilizes the generated data to configure the system for enhanced security. A comprehensive report is then produced, detailing specific vulnerabilities exploited, any unauthorized access to sensitive data, and the duration of testers' undetected presence in the system.

Examining the Pros of Penetration Testing, it proves advantageous as it imitates real attackers, chains together vulnerabilities to demonstrate in-depth risks, eliminates false positives across all layers, and provides realistic evidence of security issues. However, Cons include the need for time and expertise, potential dangers if handled by inexperienced testers leading to data loss and corruption, high costs, Labor intensiveness, and the exposure of source code to third parties.

The Operational Scheme of VAPT, depicted in Figure 3, outlines the process. Testers first determine the scope, choosing between Black box, grey box, or White box approaches. Reconnaissance follows, involving the gathering of information about the network, IP addresses, and system configurations. Vulnerability detection then utilizes techniques from the Vulnerability Assessment (VA) phase to identify weaknesses. Information Analysis and Planning involve analysing VA results to devise a penetration testing plan. Penetration testing is executed according to the devised plan, with Privilege Escalation occurring after successful penetration to enhance reach, ease, and persistence.

Result Analysis involves a detailed examination of all test outcomes, and Reporting includes the documentation of findings, recommendations, and solutions to address identified vulnerabilities. Finally, the Clean-up phase ensures the system is restored to its pre-VAPT state. This holistic approach to VAPT provides a structured and thorough assessment of security measures, enabling organizations to proactively identify and address potential vulnerabilities, ultimately enhancing their overall cybersecurity posture.

IV. OVERVIEW OF OWZAP TOOL

The device ZAP tool is a open source, single-board, credit The Open Web Application Security Project (OWASP) is a global non-profit organization focused on improving the security of software. Established in 2001, OWASP has become a leading authority in the field of application security, providing resources, tools, and guidelines for organizations to enhance their web application security posture. One of the critical aspects of OWASP's contribution is its comprehensive list of security risks and vulnerabilities known as the OWASP Top Ten.

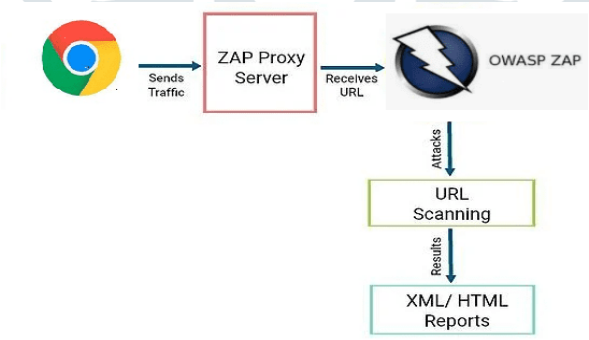

Figure 2 Mechanism of Action: Understanding the Operation of Zap

The OWASP Top Ten serves as a crucial reference for penetration testers, developers, and security professionals, highlighting the most prevalent and impactful security issues in web applications. This list is regularly updated to reflect the evolving threat landscape, ensuring its relevance in the face of emerging cyber threats.

Penetration testing, a crucial component of a robust security strategy, involves simulating real-world attacks to identify and address vulnerabilities before malicious actors can exploit them. OWASP plays a pivotal role in penetration testing by offering a range of resources and tools that aid security professionals in conducting thorough assessments.

OWASP provides a wealth of information, but one notable tool that stands out is OWASP Zed Attack Proxy (ZAP). ZAP is an open-source security testing tool designed for finding vulnerabilities in web applications during the development and testing phases.

It provides automated scanners and various tools for both beginners and experienced testers, making it a versatile choice for penetration testing.

At its core, ZAP functions as a proxy between the tester's browser and the target application. This intermediary position allows ZAP to intercept and inspect the traffic between the two, enabling detailed analysis and identification of potential vulnerabilities. The tool supports various automated scanners for common vulnerabilities such as SQL injection, cross-site scripting (XSS), and security misconfigurations.

One of ZAP's notable features is its user-friendly interface, making it accessible to both novice and expert users. The tool offers a range of automated scanners for quick assessments and also allows manual testing for a more in-depth analysis. ZAP's extensibility is another key strength, as it supports add-ons and plugins, allowing users to customize and extend its functionality according to their specific testing requirements.

ZAP's active community contributes to its continuous improvement and evolution. Regular updates and enhancements ensure that ZAP remains aligned with the latest security challenges and testing methodologies. The community-driven nature of ZAP encourages collaboration and knowledge sharing among security professionals worldwide.

For penetration testers, integrating ZAP into their testing toolkit provides a valuable asset for identifying vulnerabilities early in the development lifecycle. Its ability to generate detailed reports simplifies communication with development teams, facilitating the timely resolution of security issues.

V. LITERATURE SURVEY

Author	Methodology	Advantages	Disadvantages	Summary
Jai Narayan Goel, BM Mehtre	The VAPT methodology involves scope definition, reconnaissance, vulnerability assessment, penetration testing, privilege escalation, results analysis, reporting, remediation, and verification.	VAPT provides proactive cyber defence, identifies system weaknesses, and helps in preventing potential cyber-attacks.	VAPT can be time-consuming, costly due to tool requirements, and may require significant expertise for effective execution.	VAPT is a comprehensive process for identifying and addressing system vulnerabilities, ultimately contributing to strengthened system security and proactive cyber defence.
M. Mehtre	The VAPT methodology involves multiple sub-processes and the use of open source and commercial tools to analyse the cyber security arrangements of the entire system	VAPT helps organizations assess the effectiveness of their security infrastructure, enabling them to install patches and adopt required security measures to safeguard themselves from cyber-attacks.	Limitations of VAPT include the need for clear rules of engagement, potential impact on third parties, and the possibility of false positives during the testing process.	The paper aims to create a high level of cyber security awareness and importance at all levels of an organization, enabling them to adopt required up-to-date security measures and remain protected from various cyber attacks
Hermawan Setiawan, Lytio Enggar Erlangga, Ido Baskoro	Combines dynamic and static analysis to test applications for vulnerabilities.	Provides greater test accuracy compared to other approaches.	May require specific tools and expertise for implementation.	The IAST approach, utilizing Jenkins, API ZAP, and SonarQube, aims to establish a web-based government application vulnerability analysis system, identifying 249 risks.
Rajiv Pandey, Vutukuru Jyothindar, and Umesh K Chopra	The vulnerability assessment and penetration testing as key methodologies for network security. It suggests using a portable solution with Raspberry Pi 3b+ for conducting these tests.	The portable solution offers cost-effective and flexible testing of network security, with easy customization using Raspberry Pi 3b+.	Potential disadvantages include high false positive rates, detectability by intrusion systems, and limitations in identifying the latest vulnerabilities.	The study emphasizes the importance of vulnerability assessment and penetration testing, highlighting the benefits of a portable solution for conducting these tests.

Prashant S. Shinde and Shrikant B. Ardhapurkar	The paper discusses the use of Vulnerability Assessment and Penetration Testing (VAPT) techniques to identify security loopholes in web applications and install security patches.	VAPT provides a comprehensive application evaluation, detailed view of threats, and helps in preventing financial losses and preserving corporate image.	Penetration testing requires more time and effort than vulnerability assessment, and it is unlikely to provide information about new vulnerabilities.	The paper emphasizes the importance of cyber security awareness and the need for organizations to adopt up-to-date security measures to stay protected from cyber-attacks.
Pulei Xiong, Liam Peyton, SITE	The proposed approach integrates penetration testing into the Software Development Life Cycle, emphasizing collaboration with developers and utilizing a model-driven approach with automation for test campaigns.	The framework offers a repeatable, systematic, and cost-efficient penetration testing approach, enabling regular testing personnel involvement while still requiring security professionals' expertise. The implemented prototype demonstrates feasibility and efficiency	The document does not explicitly mention any identified disadvantages of the proposed model-driven penetration test framework.	A model-driven penetration test framework for web applications, integrating testing into the development life cycle, fostering collaboration with developers, and employing grey-box testing. The implemented prototype validates the framework's feasibility and efficiency
Prof. Sangeeta Nagpure and Sonal Kurkure	Two testing methods are explored—vulnerability assessment for identifying security loopholes and penetration testing for actively exploiting vulnerabilities.	Manual penetration testing is deemed more accurate, while automated testing is efficient for quick vulnerability detection in web applications.	Automated vulnerability assessment tools lack 100% accuracy, potentially missing some vulnerabilities.	The document underscores web application security, compares vulnerability assessment and penetration testing, and recommends an integrated approach combining manual and automated testing for comprehensive security analysis.
Hessa Mohammed Zaher Al Shebli, Babak D. Beheshti, PhD	The penetration testing process involves three phases: test preparation, test implementation, and test analysis, which include information gathering, vulnerability analysis, and reporting. These phases are crucial for systematically conducting and documenting the outcomes of penetration tests.	The paper discusses the importance of penetration testing, its benefits, strategies, tools, and ethical competency required for conducting penetration tests.	It consumes time and effort, and the exploitation phase poses potential risks to the targeted system.	The paper provides a comprehensive overview of penetration testing, including its significance, benefits, strategies, tools, and ethical considerations, emphasizing the importance of maintaining security while conducting tests.
Sandhya	The methodology involves using Wireshark as a packet sniffer to capture and analyze live network traffic during the login process on a vulnerable website, aiming to identify security vulnerabilities at the user authentication level.	Enables swift detection of security vulnerabilities in user authentication, ensuring adherence to required standards. Powerful in live network analysis, providing successful identification of vulnerabilities.	Requires technical expertise, potentially overwhelming for beginners. Not ideal for large-scale network analysis due to possible performance is	Wireshark in penetration testing swiftly identifies authentication vulnerabilities, ensuring standards adherence, but demands technical expertise and may be overwhelming for beginners, limiting its suitability for large-scale network analysis.

Arvind Goutam and Vijay Tiwari	The paper focuses on vulnerability assessment and penetration testing of a financial web application, and proposes a framework for secure access to the application. The methodology involves planning, discovery, vulnerability exploitation, and data extraction, followed by analysis and development of new strategies based on the results.	The proposed framework can act as a blueprint for upcoming websites to create a more secure environment against attacks. The paper ensures that the developed project will be more secure than the running project in the finance sector.	The paper does not provide a detailed analysis of the vulnerabilities discovered during the testing process. The proposed framework may not be applicable to all types of web applications.	The paper highlights the importance of information security in the finance sector and provides a methodology for vulnerability assessment and penetration testing. The proposed framework can help organizations create a more secure environment for their web applications.

VI. CONCLUSIONS

This survey extensively investigates the integration of the Django framework and the OWASP scanning tool in the domain of penetration testing, presenting a robust strategy to bolster cybersecurity against evolving threats. Underscoring the indispensable role of Vulnerability Assessment and Penetration Testing (VAPT) as a proactive cyber defense technology, the paper navigates through the systematic VAPT life cycle, emphasizing key stages such as reconnaissance, scanning, gaining access, maintaining access, and analysis. The synergy between these stages, coupled with OWASP Zed Attack Proxy (ZAP) and Django, forms a comprehensive framework for identifying, addressing, and preventing vulnerabilities in web applications, with a specific focus on critical OWASP Top Ten vulnerabilities like injection and cross-site scripting. The incorporation of Django, celebrated for its security features, adds an additional layer of protection to developed web applications. The outlined operational scheme of VAPT stresses the importance of meticulous planning, execution, result analysis, and reporting. Although not incorporating the Raspberry Pi 3b+ in this context, the paper maintains its focus on practical application and adaptability. In conclusion, the amalgamation of penetration testing methodologies, supported by Django and OWASP tools, presents a dynamic defense against cyber threats, with the ongoing evolution of these methodologies remaining crucial for organizations to effectively safeguard their systems and networks in the dynamic landscape of cybersecurity.

VI. REFERENCES

[1] A model-driven penetration test framework for Web applications. (2010, August 1). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/5593250

[2] Cyber security analysis using vulnerability assessment and penetration testing. (2016, February 1). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/7583912

[3] Goel, J. N., & Mehtre, B. M. (2015, January 1). Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology. Procedia Computer Science. https://doi.org/10.1016/j.procs.2015.07.458

[4] Safitra, M. F., Lubis, M., & Widjajarto, A. (2023, March 24). Security Vulnerability Analysis using Penetration Testing Execution Standard (PTES): Case Study of Government's Website. https://doi.org/10.1145/3592307.3592329

[5] Vulnerability Analysis Using the Interactive Application Security Testing (IAST) Approach for Government X Website Applications. (2020, November 24). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/9332116

[6] Vulnerability Assessment and Penetration Testing: A portable solution Implementation. (2020, September 25). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/9242640

[7] Shah, S., Mehtre, B.M. An overview of vulnerability assessment and penetration testing techniques. J Comput Virol Hack Tech 11, 27–49 (2015). https://doi.org/10.1007/s11416-014-0231-x

[8] H. M. Z. A. Shebli and B. D. Beheshti, "A study on penetration testing process and tools," 2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT), Farmingdale, NY, USA, 2018, pp. 1-7, doi: 10.1109/LISAT.2018.8378035.

[9] S. Sandhya, S. Purkayastha, E. Joshua and A. Deep, "Assessment of website security by penetration testing using Wireshark," 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2017, pp. 1-4, doi: 10.1109/ICACCS.2017.8014711.

[10] Goutam and V. Tiwari, "Vulnerability Assessment and Penetration Testing to Enhance the Security of Web Application," 2019 4th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 2019, pp. 601-605, doi: 10.1109/ISCON47742.2019.9036175.

[11] S. Nagpure and S. Kurkure, "Vulnerability Assessment and Penetration Testing of Web Application," 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA), Pune, India, 2017, pp. 1-6, doi: 10.1109/ICCUBEA.2017.8463920.

[12] Shah. Sugandh. and B.M. Mehtre. "A Modern Approch to CyberSecurity Analysis Using Vulnerability Assessment and Penetration Testing" NCRTCST - 2013, Nov. 2013, Hyderabad (A.P), India.

[13] Shah, Sugandh, and B. M. Mehtre."A Reliable Strategy for Proactive Self-Defence in Cyber Space using V APT Tools and Techniques", "School of Computer and Information Sciences, University of Hyderabad, Hyderabad, India." Computational Intelligence and Computing Research (ICCIC), 2013 IEEE International Conference on.

[14] Shah, S.; Mehtre, B.M., "An automated approach to Vulnerability Assessment and Penetration Testing using Net-Nirikshak 1.0," in Advanced Communication Control and Computing Technologies (ICACCCT), 2014 International Conference on, vol., no., pp.707-712, 8-10 May 2014 doi: 10.1109/ICACCCT.2014.7019182

[15] Kranthi Kumar, K. Srinivasa Rao," A Latest Approach to Cyber Security Analysis using Vulnerability Assessment and Penetration Testing", International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-3, Issue-4

[16] Urmi Chhajed, Ajay Kumar, "A Critical Review on Detecting Cross-Site Scripting Vulnerability", ISSN: 2319-8753 International Journal of Innovative Research in Science, Engineering and Technology, Vol 3, Issue $, April 2014

[17] Owasp.org, "OWASP", 2016. [Online]. Available: https://www.owasp.org/index.php/Main_Page. [Accessed: 15- Feb- 2016].

[18] Kieyzun, A.; Guo, P.J.; Jayaraman, K.; Ernst, M.D., "Automatic creation of SQL Injection and cross-site scripting attacks," Software Engineering, 2009. ICSE 2009. IEEE 31st International Conference on, vol., no., pp.199,209,16-2410.1109/ICSE.2009.5070521M