INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT (IJSREM)
VOLUME: 05 ISSUE: 02 | FEB - 2021 ISSN: 2582-3930

Cyber Attack Prevention Using VAPT Tools

Abhilash Nair
Information Technology
Keraleeya Samajam(REGD) Dombivali's Model College)
Dombivali,India

Abstract— **Vulnerabilities are massive flaw in system security and data assurance. A vulnerability free system will offer a lot of info Assurance and system security, although it's virtually not possible to own 100 percent vulnerability free system, however by removing the maximum amount vulnerabilities as doable, we will increase system security.**

The need of Vulnerability Assessment and Penetration Testing is sometimes underestimated until currently. It's simply contemplate as a formality activity and use by terribly less individuals. By victimization regular and economical Vulnerability Assessment, we will scale back substantial quantity of risk to be attacked and have a lot of secured systems. We have a tendency to describe Vulnerability Assessment and Penetration Testing as a vital Cyber Attack interference Technology, by victimization VAPT as a Cyber Attack interference Technology we will take away vulnerabilities from our system and scale back chance of cyber-attack. Vulnerability Assessment and Penetration Testing may be a step by step method. Vulnerability assessment is that the method of scanning the system or computer code or a network to seek out the weakness and loophole in this. These loopholes will offer backdoor to aggressor to attack the victim. A system might have access management vulnerability, stipulation vulnerability, Input validation vulnerability, Authentication Vulnerabilities, Configuration Weakness Vulnerabilities, and Exception Handling Vulnerabilities etc.

Penetration testing is that the next step when vulnerability assessment. Penetration testing is to undertake to use the system in approved manner to seek out the doable exploits within the system. In penetration testing, the tester has the authority to try to penetration testing and he intently exploits the system and establish doable exploits. By applying VAPT technique user will establish the vulnerabilities those may end up in numerous severe attacks like - DDoS attack, RA flooding, artist poisoning etc.

When sorting out the vulnerabilities user will apply countermeasures. to form the system vulnerability free, Administrator ought to establish vulnerabilities in his own system/network. The administrator ought to apply complete vulnerability and penetration testing cycle the system/network.

Keywords—Vulnerability; threat; pen test; network security; assessment

I. INTRODUCTION

Vulnerability Assessment - A process to evaluate and review key systems, networks and applications:

• To identify vulnerabilities and configuration issues that may put the organization at risk of being breached or exploited
• Effective in identifying vulnerabilities, but it cannot differentiate between exploitable vs non-exploitable vulnerabilities
Penetration Testing :
• Goal-driven test focused on identifying all possible routes of entry an attacker could use to gain unauthorized entry into the target • Identifies the potential damage and further internal compromise an attacker could carry out once they are past the perimeter. • Proof of concept strategy to investigate, exploit and validate the extent of the identified vulnerability
• Testing from an external network with no prior knowledge of the internal network and system Black Box Testing
• Test being performed from within the network
• Prior knowledge of the network, architecture and system. White Box Testing :
• Testing from an internal or external network
• Partial knowledge of the internal network and system
• Combination of both white and black box testing Grey Box Testing Process Type:
• Network Vulnerability Assessment & Penetration Testing • Internal & External IPs • VoIP & Cloud ;Telephony
• Devices – Firewall, Switches, Routers, etc
• AWS Cloud Configuration Review
• AWS Cloud Assessment • Devices – Firewall, Switches, Routers, etc Objective - The scope will be scanned and tested for vulnerabilities using a wide variety of tools and techniques. The tools and techniques used will be consistent with current industry trends regarding exploitation of vulnerabilities. The tools and procedures are:
• Threat and attack vectors
• Combination of vulnerabilities exploited in a particular sequence • Business and operational impact of attacks
• Efficiency of the client's network and environment to detect and respond to attacks Areas of focused investment to reduce or mitigate risks Test Type
Objective – Key objective is to impersonate a real-world attacker and discover security issues within an application. We also want to assist the organisation in resolving the findings. We also want to provide a business case for investing in relevant security controls. Methodology – Industry standard test cases like, cookie attacks, sensitive data exposure, session management, data validation, business logic, security misconfigurations and much more. Evaluation – Impact and Risk Factor for the business. Remediation methods Application Security Test Type
8. Social Engineering Training USB Phishing Email Phishing Campaigns Objective – A simulated attack vector that relies heavily on human interaction and often involves manipulating people into breaking normal security procedures and best practices in order to gain access to systems, networks or physical locations. Methodology: Baiting – An attacker leaves a malware-infected physical device, such as a USB flash drive, in a place it is sure to be found. The finder then picks up

the device and loads it onto his or her computer, unintentionally installing the malware. Spear Phishing/Phishing – Phishing is when a malicious party sends a fraudulent email disguised as a legitimate email, often purporting to be from a trusted source. The message is meant to trick the recipient into sharing personal or financial information or clicking on a link that installs malware. Test Type

II. Material And Method

A. *Material Review*

There are various tools to conduct pen test, such as

• Nmap to find a web server. • Fiddler for web debugging proxy.

• Nikto to identify web server type, version, add on, configuration, and other interesting files.

• WebScarab as an interceptor for identifying new URLs on the test target, the session ID analyzer, and the parameter fuzzer. • w3af for vulnerability tester.

• Firefox extension, named firebug for inline editing, breaking forms, messing with JavaScript, making rogue sites, and man-in-the-middle component.

• Cenzic Hailstorm as a web vulnerability scanner.

• DOS, lastly, Metasploit Framework to develop and execute exploit code against a remote target machine. The penetration test can be performed in two models, both external and internal.

The penetration test for external networks has a function to show that there are known security vulnerabilities that can be exploited by attackers when they appear outside the network's boundaries, usually from the Internet. It includes the analysis of information available to the public, the network enumeration stages, and the behavior of the security agencies analyzed, which can be categorized as a traditional approach because related to server evaluation, technical infrastructure, and core software and without prior knowledge of the target environment. All web servers, mail servers, firewalls, routers, IDPs, and others must be subject to intrusion testing activities to assess security positions. On the other hand, the intrusion penetration test reveals a comprehensive view of the organization's security situation, which quite like the external evaluation. The test will be conducted through several network access points, representing each logical and physical network segment. It is used to determine whether an internal employee of an unsatisfied organization can break into the internal network with the amount of knowledge he/she has in the IT field. Commonly, it can occur through exposing the poor level of security or control in the environment for stealing sensitive information.

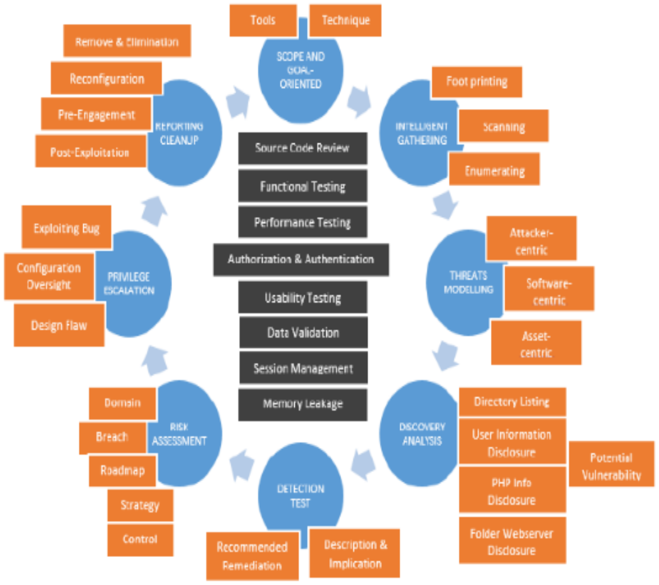


Fig. 2 VAPT Framework

III. Results And Discussion

A. *Directory Listing*

Penetration testing related to a simulation of the hacking process to identify security threats, which can be called ethical hacking. Importantly, there are specific points to be considered before conducting the testing, such as understanding the consequences of the risk related to the data stored and the test coverage to align with goal-oriented. In this VAPT, it is found that the folder in the Simpus application is not protected so that the attacker can view the contents of files from several folders such as /image/ and /assets/. The attacker also can see the contents of files contained in certain folders, so it is dangerous if the folder on the website has several confidential data such as databases and user passwords. This type of threats has a severity level of low, so the recommendations can be given by adding empty index.htm files to each folder.

B. *Full Path Disclosure:*

Full path disclosure vulnerabilities allow the attacker to know the information of the web path. This information will reveal a full error message to the attacker. By knowing the full error message, the attacker can predict the directory listed on that website. The attacker can also conduct direct access to the specific files on a directory. Another use of this full path this closure is predicting the directory of user information. The user information plays a critical role within companies, so the protection of personal data should be prioritized over the others. Unfortunately, Indonesia does not have specific legislation to administer and control personal data protection within an organization under government or private institution. This type of threat can be overcome by hiding error message with a certain code of error message, for example, by displaying Error 404.

C. PHPInfo Disclosure:

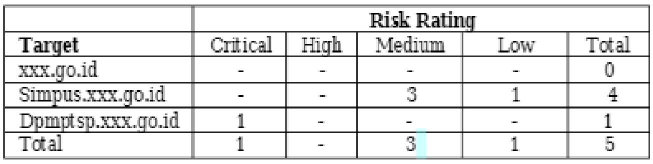
PHP Info is valuable to explain the compiled information about the server's environment, which controls processing information such as cookie, server, GET, POST, and others. In this vulnerability, there is a phpinfo.php file that can be accessed by everyone. This file is dangerous because it contains detailed information about the web server. An attacker can find out any information about the web server, such as the type of web server is used, the version, and the information in it. This type of threats has a severity level of medium, so the recommendation that can be given is to delete the phpinfo.php file. Commonly, unauthorized parties after finding certain exploitable weaknesses within the system, they will design and testing the performance of the attack within their system that has a similar attribute. Then, they will try to secure the line to obtain full access, and privilege together eliminates the possibility to track the source before conducting a cyber-attack and delete the recovery process.

IV. METHODOLOGY:

In the process of penetration testing, there are fully identified threats that can be verified and confirmed positively based on experiment and monitoring process, but there are also cases, in a certain condition where they cannot be fully explained. It is recommended to establish a further step to determine whether they exist or not when the authentication mechanism or trusted scanner can reveal the location or their cause. In this, VAPT found a blind SQL injection gap in the licensing file monitoring function. SQL injection occurs because there is no filter from user input so that it can perform database query injection. An attacker can see all the contents of the database from the website dpmptsp where the database contains confidential data in the form of usernames, passwords, employee data and permitted community data, and others. This kind of threats has a severity of critical while the recommendation that can be given is to use the filter function mysql_real_escape () on the parameter/variable that captures input from the user. This taken picture is the result of a dump database from the website dpmptsp, where the name of the database used is Sirindu. There are 89 tables in the sirindu database, which contain all confidential data such as users, passwords, permission data, complaint data and more

After conducting the VAPT, as it can be seen in table 1 about risk rating, which is defined four levels of categories: Critical, High, Medium, and Low, then this study identified five threats within three targets. In this case, critical level means an attack is expected that can endanger the resources and assets of the organization, while high level means an attack might disrupt the business process and operation, even the popularity. On the other hand, medium level defines that an attack is possible that can present certain profit loss while low level points out that an attack is unlikely but possible, which can reveal procedure about a specific project.

TABLE I
RISK RATING



	Risk Rating				
Target	Critical	High	Medium	Low	Total
xxx.go.id	-	-	-	-	0
Simpus.xxx.go.id	-	-	3	1	4
Dpmptsp.xxx.go.id	1	-	-	-	1
Total	1	-	3	1	5

V. CONCLUSION:

VAPT is a systematic process of deciding the weaknesses of an application that become popular and critical to promote security, reliability, and integrity. In the era of the technology advancement, which hacking become the trend among a society that threaten and endanger the harmony and business flow of a company, it is necessary to have standard to minimize risks and mitigate dangers. This study offers the developed framework to conduct VAPT to reduce the cost incurred and having a broad range of security measure and strategy for diverse application and IT resource, as well as to have a holistic view of the possibility of danger because of threats encountered within networks.

VI. REFFERENCES

[1] Symantec Corporation. 2017 Norton Cyber Security Insight Report Global Results. Retrieved at January 2019 from: https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf

[2] ITU-D. Global Cybersecurity Index (GCI) 2017. Retrieved at January 2019 from: https://www.itu.int/dms_pub/itu-d/opb/str/d-str-gci.01-2017-pdf-e.pdf

[3] Statista. Consumer Loss Through Cyber Crime Worldwide in 2017, by Victim Country (in billion US dollars). Retrieved January 2019 from: https://www.statista.com/statistics/799875/countries-with-the-largest-losses-through-cybercrime/

[4] R. Kuncoro. Current State of Cybersecurity Readiness and Cybercrime Enforcement Capability in Indonesia. Cybercrime Capacity Building Conference, 27-28 April 2010. Indonesiaan National Police.

[5] A.G. Bacudio, X. Yuan, B.T.B.Chu and M. Jones. An Overview of Penetration Testing. Int. Journal of Network Security & Its Applications 3(6), pp. 19-38, 2011.

[6] K. Palanisamy. Network Penetration Testing. White Paper: Happiest People Happiest Customer, 2014.

[7] T.S. Gunawan, M.K. Lim, M. Kartiwi, N.A. Malik and N. Ismail. Penetration Testing using Kali Linux: SQL Injection, XSS, Wordpress and WPA2 Attacks. Indonesian J. of Electrical Engineering and Com. Science, vol. 12(2), Nov., pp. 729-737, 2018.

[8] PTES Team. The Penetration Testing Execution Standard Documentation: Release 1.1 (February 8th, 2017). Retrieved at January 2019 from:

https://media.readthedocs.org/pdf/pentest-standard/latest/pentest-standard.pd