# Analysis of Vulnerabilities in System by Penetration Testing

Sib tul Hassan *

***Abstract*—Internet usage has been increase drastically in past decades or we can say it has become a sensation now days as internet business has built up its strong and vast network so their must need of security of the websites as well which has become a big challenge due rising in the use of internet. Vulnerability assessment and Penetration testing (VAPT) are two different techniques of assessing to analyze the vulnerability if a website these two programs two distinct results with in the same area of application.**

***Index Terms*— Cyber Security, Vulnerability Assessment, Penetration Testing, Ethical Hacking, VAPT.**

## I. INTRODUCTION

ACCORDING Vulnerability Assessment and Penetration Testing (VAPT) are the processes which make sure that arrangements of security system are working properly. The role of artificial intelligence in VAPT it refers to relatively mature industry which are trying to explore new pathways in field of artificial intelligence to cope up with this vulnerabilities of system to be hacked of exploit by the hackers. As organizations find, it hard and challenging to secure their web applications from the cyber threats, as compromise with the protection issues don't seems to be reasonable. Vulnerability assessment and penetration testing helps them to account for the loopholes. These loopholes could also utilize by the attackers to launch attack on technical assets.

Vulnerability is a flaw or loophole in application which allow the attacker to exploit the user by getting system privilege. Attackers get unauthorized excess to user's data and the use it for their advantage. Vulnerability assessment is method in where penetration tester scans a website loophole. In Penetration testing penetration tester actually perform action to exploit those loopholes and create an evidence of the test. Although the majority of web vulnerabilities are easy to understand and paid any attention due to which many web pages and database developers are unfortunately not have much security awareness as a result there exist a large number of vulnerable database pages are on web.

There are two types of methods i.e. manual and automated to perform security assessment of web application. In automatic method there are a lot of penetration testing tools which are available either as open source or as commercial product with different functionalities and applicability. Now it seems quite difficult to choose one of the best vulnerability assessment tool. As none of the tools are entirely complete in nature to identify the security risk in a web application. In manual method testing performed by the professional manually using different security techniques.

Due to rise in the use of electronic gadgets mobile and computers introduce more advance and innovative Windows, Webs and Mobile applications so it is important to ascertain the techniques of security or how to make our web site secure from the hackers or to protect it from being exploit. In present era world organization and institution are trying to overcome these challenges to make their data secure by decreasing the chance of vulnerabilities.

The purpose of this study is to provide comparative and collective analysis of web application vulnerability assessment and penetration testing methods. It may include a brief knowledge about the vulnerability assessment types and methodologies of penetration testing through which we can analyze the system's security and try to keep it protect web applications which are vulnerable to attack like session exploitation, Cross- site scripting and SQL injection etc. We can lower the chance of data loss by using these two techniques.

## II. LITERATURE STUDIES

In 2014 Kushal Singh, Vikas have assisted the technique which detect all session checks and itemized number of analyses to evaluate performances of exploitation detection techniques. They considered session exploitation mechanism in detail along with the prevention tactics and risk factors the risk of web application check point can be low, medium or high depending on how deep to manipulate the parameter of the web application. In the second phase web application security issue analyzed using backtrack. Backtrack is an adaptable function system that derives with number of security assessment and penetration testing tools [1].

In 2015 Insha Altaf, Jawad Ahmed. D studied the possible vulnerabilities for any web page and suggested the removing techniques. Instead of using manual testing, automated techniques of testing were used to get the exactness and correctness of results. In addition to this they also use SQL

Sib tul Hassan is with the Department of Computer Science, Abasyn University Islamabad (correspondence e-mail: sibtul.hasan@abasynisb.edu.pk)

Received: 10-01-2022, Revised: 25-04-2022, Accepted: 01-06-2022

injection method ‘’Acunetix web vulnerability scanner’’ is used to carry all the vulnerabilities. While testing an attempt is made by programmers or hackers to find the vulnerabilities of the system. The vulnerable site is patched by using different injection techniques such as union based injection authentication bypass and blind SQL techniques [2].

In 2016 Tanjila Farah, purposed the black box testing methodology to implement and test XSS and CRSF attack. This methodology gets nearly 30% of the web application are vulnerable to XSS and CRSF attacks while using black box testing approach executing XSS and CRSF attacks take time. This is an ongoing assessment. Their focus would be on XSS and CRSF attacks due to their higher ranking OWASP list [3-5].

In 2016 Prashant S. Shined, Sharikant B, has purposed Vulnerability assessment and penetration testing which help to assess the usefulness and uselessness of security measures of web pages to stay protected from the Cyber threats for any organization proper working for security arrangements has been checked by these two techniques i.e. VAPT. Vulnerability assessments and penetration testing has exploit the number of vulnerabilities such as SQL, Cross Site Scripting attack in web application [6-10].

## III. Types of Vulnerability

Vulnerabilities are system flaws or weaknesses that may lead to security breach. Once an attacker has found a flaw, or application vulnerability, and determined a way to access it, the attacker has the potential to take advantage of the application vulnerability. Thus threat to the confidentiality, integrity, or availability of resources possessed by an application is increased. Attackers typically rely on specific tools or strategies identify application vulnerabilities and compromise the application Before discussing about the VAPT we will first discussed about some of the types of vulnerabilities. Following are the some of the types of vulnerabilities.

### A. Cross-site Scripting (XSS)

Cross site Scripting or XSS vulnerabilities are rumored and exploited since Nineties. XSS got listed top 3rd Vulnerability in the web application Vulnerabilities list. Cross-site scripting (XSS) is a kind of security vulnerability found in web application in which the attacker can inject client side scripts into web pages which are viewed by other users. The injected code is executed at client side. A cross site scripting


FIG. 1: Steps of vulnerability assessment [2]

vulnerabilities are often employed by the attacker to bypass the Same Origin Policy (SOP). Attacker can use vulnerabilities to steal the Identity and Confidential Data, Bypass restrictions in websites, Session Hijack, launch malware Attack, Website Defacement and Denial of Service attacks (DoS), etc. According to persistence capability, there are two types of XSS attacks:

1) Persistent XSS: The Persistent or stored XSS attack happens when the malicious code submitted by attacker is saved by the server within the database, in a message form, visitor log, comment field, etc. So a victim is able to retrieve the stored data from the web application without that information being made safe to render within the browser [3, 11, 12].

2) Non-Persistent XSS: Reflected or Non-Persistent XSS attack happens when user input is instantly returned by a web application in a form of an error message, search result, or any other response that has some or all of the input provided by the user as a part of the request, without that data being made safe for rendering it into the browser, and permanently storing the user provided information [3].This vulnerability frequently occurs in search fields. In case of Non-Persistent XSS attacks, attacker sends the specially crafted URL to target victims and trick them into click the link. When user clicks on the link, the browser will send the injected code to the server, then server reflects the attack back to the victim’s browser and the code is executed by the browser.

### B. Sql Injection (SQLi)

SQL injection is a kind of technique where users can inject SQL commands through input of a web page in an SQL statement. An injected SQL command alters SQL statement and compromises the security of a web application [5]. SQL Injection is a code injection method, used to attack data- driven applications, in which SQL statements are inserted into an entry

field. SQL injection exploits the security vulnerability in an application's software.

With SQL injection exploitation attacker can read sensitive data, modify data, execute administration operations on the database, recover the content of files present on the DBMS file system [3].

## IV. Types of Vulnerability

During this part of the process the tester must aim to gather information about the test target and scanning the target to figure out vulnerabilities. As we have discussed before that vulnerability is the flaw of the system and it might because of the weak password of the systems coding input validation and is configuration of the system. Attacker first account for the vulnerabilities and then use it for vicious purpose.

Vulnerability assessment is the strategy which follows systemic and proactive approach to discover vulnerabilities. It is practiced to look for known and unknown issues in the system.

Vulnerability assessment can be attained with the help of scanners. It is a hybrid solution which is characterized with automated testing and expert analysis.

## V. Advantages of Vulnerability Assessment

a. It is used for the enabling of the automation of the thousands of security checks.
b. It can be done with easily available tools.
c. It serves as the use-full layer one remediation test.
d. It helps in the integrating organization's threat and vulnerability management program.

## VI. Disadvantages of Vulnerability Assessment:

a. Fails to identify logical attack vectors such as application logic flaw and password reuse.
b. It produces remediation recommendations that are generic and based on tool output.
c. It generates incomprehensible and large amount of data along with some false positive results.

## VII. Penetration Testing:

A penetration testing assesses the security posture of a system or network by performing attack. Penetration testing is a proactive and systematic approach for security assessment, in this part the VAPT tester tries to exploit the identified set of vulnerabilities in the same manner as an attacker would do.

## VIII. Types of Penetration Testing Techniques:

A. Functional Testing:

This technique also known as black box testing takes care of the inputs given to a system and the output that is received after processing in the system. It checks the functionality of system that is why it's termed as black box. It is used for system testing under validation which is done by independent software testers. This technique does not require knowledge of programming language. [6]

B. Grey Box Testing:

It is the type of testing in which tester has some or partial information about the network that is to be tester. Grey box testing is the combination of black box testing and white box testing which is performed on domestic or outdoor network. [6]

C. Glass Box Testing:

This technique complements black box testing. In this method system is not black box, every design feature and corresponding code is logically checked with every possible path execution. It takes care of structural paths instead of outputs. It's also known as white box testing technique and is used for unit testing under verification. It's done by software developers. This technique requires knowledge of programming language. [6]

A. Advantages of Penetration Testing:

a. It removes false positive from all layers of the security models.
b. Alleviating controls are taken into account.
c. It allows the chaining together of vulnerabilities to understand the full impact of all the discovered problems.

B. Disadvantages of Penetration Testing:

a. It requires hiring of an outside firm for penetration testing
b. Not every test guaranteed to identify the vulnerability
c. A penetration test is unlikely to provide information about the new vulnerabilities
d. It is more time consuming as that of vulnerability assessment.

## IX. Conclusion:

Due to the advancement of the use of internet threats to the integrity and confidentiality of information and resources are increased. To stay protected from these threats organizations performed vulnerability assessment and penetration testing to check the security posture of the system. As we have gone through the literature survey and we have come to know that there are number of tools for the security checks of the data by VAPT. Attackers finding new ways to overcome the security mechanism so new vulnerabilities are evolving which need to be addressed.

## REFERENCES

[1] Singh, K. (2014). Analysis of Security Issues in Web Applications through Penetration Testing. International Journal of Emerging Research in Management &Technology, 3.
[2] Altaf, I., ul Rashid, F., Dar, J. A., & Rafiq, M. (2015, October). Vulnerability assessment and patching management. In 2015 International

Conference on Soft Computing Techniques and Implementations (ICSCTI) (pp. 16-21). IEEE.

[3] Muhammad Nasir Khan, Syed K. Hasnain, Mohsin Jamil, Sameeh Ullah, "Electronic Signals and Systems Analysis, Design and Applications International Edition," in Electronic Signals and Systems Analysis, Design and Applications: International Edition , River Publishers, 2020

[4] Khan, Muhammad Nasir, Hasnain Kashif, and Abdul Rafay. "Performance and optimization of hybrid FSO/RF communication system in varying weather." Photonic Network Communications vol. 41, no. 1, pp. 47- 56, 2021.

[5] Jamil, Mohsin, Muhammad Nasir Khan, Saqib Jamshed Rind, Qasim Awais, and Muhammad Uzair. "Neural network predictive control of vibrations in tall structure: An experimental controlled vision." Computers & Electrical Engineering, vol. 89, pp. 106940, 2021.

[6] Khan, Muhammad Nasir, Mohsin Jamil, Syed Omer Gilani, Ishtiaq Ahmad, Muhammad Uzair, and H. Omer. "Photo detector-based indoor positioning systems variants: A new look." Computers & Electrical Engineering, vol. 83, pp. 106607, 2020.

[7] Kashif, Hasnain, Muhammad Nasir Khan, and Ali Altalbe. "Hybrid optical-radio transmission system link quality: link budget analysis." IEEE Access, vol. 8, pp. 65983-65992, 2020.

[8] Khan, Muhammad Nasir, and Fawad Naseer. "IoT based university garbage monitoring system for healthy environment for students." In 2020 IEEE 14th International Conference on Semantic Computing (ICSC), pp. 354-358. IEEE, 2020.

[9] OWASP, T. I. V. (2016). [Online] https://www. owasp. org/index. php.

[10] Shinde, P. S., & Ardhapurkar, S. B. (2016, February). Cyber security analysis using vulnerability assessment and penetration testing. In 2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave) (pp. 1-5). IEEE.

[11] Shah, S., & Mehtre, B. M. (2013). A modern approach to cyber security analysis using vulnerability assessment and penetration testing. Int J Electron Commun Comput Eng, 4(6), 47-52.

[12] Vibhandik, R., & Bose, A. K. (2015, September). Vulnerability assessment of web applications-a testing approach. In 2015 Forth International Conference on e- Technologies and Networks for Development (ICeND) (pp. 1-6). IEEE.