Web Application Safety by Penetration Testing

Ashikali Hasan[a], Dr. Divyakant Meva[b]

[a]*Reserach Scholar, Marwadi University, Gujarat, India*
[b]*Associate Professor, Marwadi University, Gujarat, India*

Abstract: By taking advantage of vulnerability, Cyber criminals is easily able to steal confidential data of the ICT, results in heavy loss. Vulnerability Assessment and penetration testing is a special approach to eliminate various security threats from the web application. By focusing high risk vulnerability such as SQL Injection, Cross Site Scripting, Local File Inclusion and Remote File Inclusion, in this paper, we have surveyed literatures to study the general mechanics of VAPT process and gather tools which can be useful during VAPT process.

Keywords—component; Vulnerability Assessment and Penetration Testing, Web Application Security Testing, SQL Injection, Cross Site Scripting, Local File Inclusion, Remote File Inclusion.

1. Introduction

The web application can be affected by various logical and technical vulnerabilities. SQL injection, cross site scripting, remote file inclusion and local inclusion are the examples of technical vulnerability (Ashikali M. Hasan; Divyakant T. Meva; Anil K. Roy; Jignesh Doshi, Dec 2017). These vulnerabilities affect the security of web application. Vulnerability can be occurred due to various reasons such as due to poor programing or due to an outdated system (Hossain Shahriar, Mohammad Zulkernine, June 2012).

Although web application can be secure by various ways wherein Vulnerability Assessment and Penetration Testing (VAPT) process is a special approach to secure web application from both logical and wide range of technical vulnerability. This approach audit web application security and also can be used to secure associated layers. VAPT includes to audit system for finding vulnerabilities, which may be existing in the system, exploit vulnerability same as an attacker exploit and produce data which represent the risk level of the system (Ashikali M. Hasan; Divyakant T. Meva; Anil K. Roy; Jignesh Doshi, Dec 2017).

In purpose of dive little deeper in the area of vulnerability assessment and penetration in this paper we have analyzed overview of the penetration testing process and its limitations and includes various tools which are helpful to conduct VAPT process of these high-risk vulnerabilities.

The paper is presented as follows: section 2 provides background information on our study, section 3 describe literature survey, section V present the general mechanism of VAPT, section VI presents the tools used in VAPT section VII summarizes the contributions of our research and proposes the future work.

2. Background

Researcher considers that SQL Injection, Cross Site Scripting, Remote File Inclusion and Local file inclusion are the high-risk vulnerabilities (Dimitris Mitropoulos; Panagiotis Louridas; Michalis Polychronakis; Angelos D. Keromytis, 2017,). OWASP also included these threats in Top 10 High Risk of web application. These technical vulnerabilities occurred when the web application processes data without proper filtration or validation.

2.1. SQL Injection

SQL Injection vulnerability may affect to dynamic web application which stored data in the associated database. Through SQL Injection, attacker passes malicious code to SQL Server through inserting it in the strings. This malicious code is commonly known as payloads that instruct the database server to retrieve specific information from database (Rahul Johari; Pankaj Sharma, 2012).

By taking advantage of an SQL injection vulnerability attacker can download the entire database on his computer machine and enumerate important information such as database version, database user name, table information and sensitive data available in database column such as password, username etc.

In several cases, attackers can perform various operations such as add, modify and delete records in a database or attacker may able to execute system-level commands and can be successful to launch additional attacks such as denial of service. These additional attacks are depended on the role and privilege set in SQL server of target machine (OWASP, 2016).

2.2. Cross Site Scripting

Cross site scripting also known as XSS is scripting attack in which attacker injects or execute code through the browser at user side for the purpose to steal information of the user's credential. Attacker attempt to steal the user's credential through the vulnerable web application by executing the payloads at client side. The typical example scenario is attacker may inject the payload to the vulnerable field of web application and when the user visits the page at the time payload placed in the page steal other user's cookie and send it to the attacker or may redirect users to phishing sites (M. Ridwan Zalbina; Tri Wanda Septian; Deris Stiawan; Moh. Yazid Idris; Ahmad Heryanto; Rahmat Budiarto, 2017). There are three types of XSS attack known which are persistent, not persistent and DOM based cross site scripting (OWASP Testing Guide v2, n.d.).

In non-persistent XSS also refer as reflected XSS, in which attacker craft malicious URL and then tries to execute in the user's browser to steal the data or may redirect users to a phishing page.

Persistent XSS is more powerful attack in which code injected by attacker stored in secondary storage such as databases.

DOM based XSS occurred when application access the user's information and write it in html format. This type of vulnerability commonly seen in RSS feed.

2.3. Local File Inclusion

Local File Inclusion (also known as LFI) is the high-risk web application vulnerability as it affects widely to application (Mir Saman Tajbakhsh; Jamshid Bagherzadeh, 2015). Generally, this vulnerability occurs when inputs are not properly sanitized. An attacker may perform LFI attack to gather confidential information by accessing different files and thus Harvest useful information. LFI vulnerability also leveraging an attacker to place a backdoor (A Shell) in the target server through vulnerable web application. In addition, an attacker may remotely execute commands by combining this vulnerability with some other attack vectors, such as file upload vulnerability or log injection.

2.4. Remote File Inclusion

Remote file inclusion also known as RFI is very critical vulnerability. By leveraging this vulnerability attacker can execute backdoor programs on the server through vulnerable web application. Thus, an attacker can retrieve confidential information through the backdoor. RFI and LFI vulnerability are very similar, however the only difference is that LFI provides an opportunity for an attacker to directly place a backdoor in target server while in RFI attacker use remote location to execute and retrieve backdoor (Hugo F. González Robledo, 2008).

2.5. Web Application Security

There are various approaches available to resolve the vulnerability, which may be available in the web application such as code review, secure coding practices, web application firewall. All these techniques are providing an option to secure the web application at each phrase since the development to deployment of web application. Now days due to these multiple security options these technical vulnerabilities can be eliminated from the web application. However, each security approach has its own advantage and limitations. For instance, secure coding approach required additional knowledge of secure programing (Ashikali M. Hasan; Divyakant T. Meva; Anil K. Roy; Jignesh Doshi, Dec 2017).

In addition to another approach, VAPT can also be used as a specialized approach to secure web application. VAPT is a single test process provides a more detail test of the entire system and all its associated layers. This test provides more detail information about the risk level of a web application. VAPT process includes scanning of all parts of ICT infrastructure, thus enabling to protect the digital infrastructure of an organization. As an on-demand solution VAPT can be carried out from anywhere through the internet any of the time. VAPT considered as a hybrid solution because this process is performed by the external security expert who use automated tools and techniques to test the system. Thus, VAPT is convenient approach which can be used to secure a web application because this approach is possible to implement at any of the time (Ashikali M. Hasan; Divyakant T. Meva; Anil K. Roy; Jignesh Doshi, Dec 2017).

In the area of web application security through VAPT, there has been various research going on in the both academic institutes as well as industries since couple of years. We have surveyed some papers of researchers which gives overview of VAPT process in the area of web application to identify the general mechanism of VAPT process and extracted some useful open source, free tools and methods which can be used in VAPT process to eliminate SQLI, XSS, RFI and LFI vulnerabilities.

3. Literature Survey

Various models, techniques and tools available to perform penetration testing to check the SQL Injection, Cross Site Scripting, Local File Inclusion and Remote File Inclusion vulnerability of websites. The section below describes the related work through such models, techniques and tools:

In 2014, Sugandh Shah[1] et al, B. M. Mhetre[2] et al proposed an automated VAPT Testing Tool named NetNirikshak 1.0 developed at IDRBT. The tool has been built up in 8 different modules. It is helpful to conduct the VAPT process by assessing Services and analyses Security Posture. It works based on services running in the target system and identify the vulnerabilities. The tool is capable to detect SQL injection vulnerability and it report all the identified vulnerable links. The tool also contains exploitation process which exploits the vulnerability automatically and steal confidential data from target system by exploiting SQL injection vulnerability. This tool also smartly sends all the findings through a write-protected pdf report to a specified email and remove the copies from hard disk for purpose to maintain confidentiality in VAPT process (Sugandh Shah; B. M. Mehtre, 2014).

In 2015, Insha Altaf[1] et al Firdous ul Rashid[2] et al, Jawad Ahmad Dar[3] et al Mohd. Rafiq[4] et al discussed various SQL injection methods with the use of automated testing approaches and main principles of automated testing approach. they have explained various reasons for conducting VAPT process and explained Authentication by pass, Union based SQL Injection, Firewall Bypassing attacks mechanics and its patching techniques. A part of their research study they have explained the Working Procedure of Acunetix Vulnerability Scanner (Insha Altaf; Firdous ul Rashid; Jawad Ahmad Dar; Mohd. Rafiq, 2015).

In the same year, Jai Narayan Goel[1] et al, BM Mehtre[2] et al described complete process to use VAPT process and proved that how can be used as a cyber defense technology. They have described complete life cycle of VAPT process. They have included top 15 VAPT tools both open sources and commercial available in the markets with their usage and the operating system compatibility which can be useful in assessment and exploitation

during VAPT process. They have concluded, necessity to increase use of VAPT (Jai Narayan Goel, B.M. Mehtre, 2015).

In 2016, Kamran Shaukat[1] et al, Amber Faisal[2] et al, Rabia Masood[3] et al, Ayesha Usman[4] et al, Usman Shaukat[5] et al surveyed different frameworks which can be secure during testing level. They have proposed an entrance testing technique to secure the databases, networks, web applications and Android. In context of entrance testing during their technical review, identified that studied approaches useful to particular frameworks and not each strategy can be applied to single framework and critics as neglect able. To defeat these issues, they have attempted and proposed another methodology and explained all the components. (Kamran Shaukat; Amber Faisal; Rabia Masood; Ayesha Usman; Usman Shaukat, 2016).

During this year, Jai Narayan Goel[1] et al, Mohsen Hallaj[2] Asghar et al[3], Vivek Kumar[4] et al, Sudhir Kumar Pandey[5] et al propose an Ensemble approach with various VAPT tools which reliable in prediction of vulnerability for the purpose of decrease false positive. They have also implemented their study and made a software based on their approach called "VEnsemble 1.0" which is capable to use with number of other both open source and commercial tools and included the results (Jai Narayan Goel, Mohsen Hallaj Asghar, Vivek Kumar, Sudhir Kumar Pandey, 2016).

In the same year, Prashant S. Shinde[1] et al, Shrikant B. Ardhapurkar[2] et al explained clearly of various techniques used in vulnerability assessment and penetration testing (VAPT). Also pay attention to cyber security awareness and importance in organization to stay safe. they conclude that there are various tools available for VAPT, with new vulnerability evolution existing tools should be updated to identify new vulnerabilities and makes them flexible so that new attack signature can be added (Prashant S. Shinde; Shrikant B. Ardhapurkar, 2016).

In 2017, S. Sandhya[1] et al, Sohini Purkayastha[2] et al, Emil Joshua[3] et al, Akash Deep[4] et al discussed the utilization of penetration testing approach using Wireshark tool and demonstrated a method. They have also survived several tools for penetration testing to solve security issues (S Sandhya, Sohini Purkayastha, Emil Joshua, Akash Deep, 6-7 Jan. 2017).

4. Overview Of VAPT

Vulnerability assessment and penetration testing both contain execution of different process aim to secure a web application, however both are closely related to each other. The vulnerability assessment process provides information of possible vulnerability while penetration testing process includes exploiting the vulnerability to assume risk level. The overall mechanism of VAPT is illustrated in figure 1. as under.

Fig. 1 - General VAPT process model (Ashikali M. Hasan; Divyakant T. Meva; Anil K. Roy; Jignesh Doshi, Dec 2017).

VAPT is beneficial approach which can be used to secure a web application, however there are certain limitation associated with it. Herein we have discussed several key points in this regard.

- Testing is not a time bound process. A limitation in time may reduce efficiency levels of penetration testing process.
- The success is depending on the testers skill and efforts so test does not guarantee to identify a vulnerability.
- Generally, VAPT carried out by external person or outside firm due to these factors raised the overall budget of the system.
- VAPT is a repetitive process. Upon change or modification in the system again penetration testing is required.
- VAPT process may damage to system for example, during the process tester use various tools and techniques to scan the application which may affect to bandwidth.
- VAPT process also contains legal limitations, for example a web application hosted on shared server cannot be penetrated without permission of the web server provider because testing may affect the performance of overall sever and cause damage of another web application which are hosted on the same sever.

In spite of several limitation VAPT is far beneficial approach to secure a web application. Various tools and techniques can be use during the penetration testing process.

5. VAPT Tools

To support VAPT process, there are a number of tools, both commercial and open source are available to find SQLI, XSS, LFI and RFI vulnerabilities. In this section, we have discussed some selective tools which are helpful in VAPT process.

5.1. W3af

W3af is a free and open source automated Black-box web application scanning tool contain various plugins. This tool is available in both GUI and command line use interface, capable to asses a web application for a range of vulnerabilities and able to exploited it. Plugins are interlay connected which share information to each other (Kamran Shaukat; Amber Faisal; Rabia Masood; Ayesha Usman; Usman Shaukat, 2016).

5.2. Havij

Havij 1.16 pro is a free tool designed with very easy graphical user interface. This tool includes number of different exploitation techniques of SQL Injection vulnerabilities and support many different database types. It supports HTTPS protocol and also contain post exploitation task such as hash cracking. This tool is very handy and easy to install and use (Bharti Nagpal; Nanhay Singh; Naresh Chauhan; Angel Panesar, 2015).

5.3. Fimap

Fimap is a written in python language and a command line security tool helpful to find and exploit LFI and RFI vulnerability from a web application. (Joe Beauchamp, 2016).

5.4. Metasploit

Metasploit is available in both commercial and opensource platform. This tool includes large database of various exploits and methods which provides smart testing platform to penetration tester. The tool support in extensive security auditing of a web application.

5.5. Kali Linux

Kali Linux is an open source security distribution built with Linux operating system. this distribution contains large repository of auditing and exploitation tools. The distribution specifically designed for forensics and penetration testing. the distribution is available in various medium i.e. Live CD, installable source, Virtual image etc.

5.6. Acunetix

Acunetix is commercial web vulnerability scanner capable to scan a web application with black box approach. It is automated tools GUI tool which scan a web application for number of different vulnerabilities. The tool is produce user-friendly and professional report of scanning.

5.7. Nexpose

Nexpose is GUI and automated vulnerability assessment tool available in both commercial and free version where nexpose community version is available for a year with limited functionality while commercial version of nexpose is equipped with full functionality.

5. Conclusion and Future Work

VAPT is a very compressive process. Various research and methods are introduced by researchers to support VAPT process, we have gone through a literature survey and analyzed overview of VAPT process and identify several limitations associated with the process. We have also discussed several tools which can be helpful conduct VAPT process to find SQLI, XSS, LFI and RFI vulnerabilities. We conclude that VAPT is very important process helps in identifying security defects. Many repositories inform of tools, methods and mechanics available to support VAPT. In the future, we will more closely look for various problems associated with the VAPT process such as identify the factors which slow down businesses to adopt VAPT process and continue our research and study in this area.

REFERENCES

References

Ashikali M. Hasan; Divyakant T. Meva; Anil K. Roy; Jignesh Doshi. (Dec 2017). Perusal of web application security approach. *Intelligent Communication and Computational Techniques (ICCT), 2017 International Conference on*. doi:10.1109/INTELCCT.2017.8324026

Bharti Nagpal; Nanhay Singh; Naresh Chauhan; Angel Panesar. (2015). Tool based implementation of SQL injection for penetration testing . *International Conference on Computing, Communication & Automation*(IEEE Conference Publications), 746 - 749, DOI: 10.1109/CCAA.2015.7148509.

Dimitris Mitropoulos; Panagiotis Louridas; Michalis Polychronakis; Angelos D. Keromytis. (2017,). Defending Against Web Application Attacks: Approaches, Challenges and Implications. *IEEE Transactions on Dependable and Secure Computing (IEEE Early Access Articles), Volume: PP*(Issue: 99), 1 - 1, DOI: 10.1109/TDSC.2017.2665620.

Insha Altaf; Firdous ul Rashid; Jawad Ahmad Dar; Mohd. Rafiq. (2015). Vulnerability assessment and patching management. *IEEE Conference Publications, International Conference on Soft Computing Techniques and Implementations (ICSCTI), 2015, Pages: 16 - 21*. Faridabad, India .

Kamran Shaukat; Amber Faisal; Rabia Masood; Ayesha Usman; Usman Shaukat. (2016). Security quality assurance through penetration testing. *2016 19th International Multi-Topic Conference (INMIC)*(IEEE Conference Publications), 1 - 6, DOI: 10.1109/INMIC.2016.7840115.

M. Ridwan Zalbina; Tri Wanda Septian; Deris Stiawan; Moh. Yazid Idris; Ahmad Heryanto; Rahmat Budiarto. (2017). Payload recognition and detection of Cross Site Scripting attack. *2017 2nd International Conference on Anti-Cyber Crimes (ICACC)*(IEEE Conference Publications), 172 - 176, DOI: 10.1109/Anti-Cybercrime.2017.7905285.

Mir Saman Tajbakhsh; Jamshid Bagherzadeh. (2015). A sound framework for dynamic prevention of Local File Inclusion. *2015 7th Conference on Information and Knowledge Technology (IKT)*(IEEE Conference Publications), 1 - 6, DOI: 10.1109/IKT.2015.7288798.

Rahul Johari; Pankaj Sharma. (2012). A Survey on Web Application Vulnerabilities (SQLIA, XSS) Exploitation and Security Engine for SQL Injection. *2012 International Conference on*

Communication Systems and Network Technologies(IEEE Conference Publications), 453 - 458, DOI: 10.1109/CSNT.2012.104.

Sugandh Shah; B. M. Mehtre. (2014). An automated approach to Vulnerability Assessment and Penetration Testing using Net-Nirikshak 1.0. *2014 IEEE International Conference on Advanced Communications, Control and Computing Technologies*(IEEE Conference Publications), 707 - 712, DOI: 10.1109/ICACCCT.2014.7019182.

Hossain Shahriar, Mohammad Zulkernine. (June 2012). Mitigating program security vulnerabilities: Approaches and challenges. *ACM Computing Surveys (CSUR), Volume 44*(Issue 3), Article No. 11. doi:10.1145/2187671.2187673

Hugo F. González Robledo. (2008). Types of Hosts on a Remote File Inclusion (RFI) Botnet. *Electronics, Robotics and Automotive Mechanics Conference, 2008. CERMA '08*(IEEE Conference Publications), 105 - 109, DOI: 10.1109/CERMA.2008.60.

Jai Narayan Goel, B.M. Mehtre. (2015). Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology. *Procedia Computer Science, 57*(http://www.sciencedirect.com/science/article/pii/S1877050915019870), 710-715, ISSN 1877-0509, http://dx.doi.org/10.1016/j.procs.2015.07.458.

Jai Narayan Goel, Mohsen Hallaj Asghar, Vivek Kumar, Sudhir Kumar Pandey. (2016). Ensemble Based Approach to Increase Vulnerability. *Innovation and Challenges in Cyber Security (ICICCS-INBUSH), 2016 International Conference on*. doi:10.1109/ICICCS.2016.7542303

Joe Beauchamp. (2016). *VisualFI: File Inclusion Identification, Exploitation and Reporting Tool.* England: University of the West of England. Retrieved from http://www.cems.uwe.ac.uk/~pa-legg/teaching/fyp/projects/2016beauchamp.pdf

OWASP. (2016, April 26). *Testing for SQL Injection (OTG-INPVAL-005)*. (OWASP Foundation Inc) Retrieved Jun 6, 2017, from https://www.owasp.org/index.php/Testing_for_SQL_Injection_(OTG-INPVAL-005)

OWASP Testing Guide v2. (n.d.). *Testing for Cross site scripting*. Retrieved May 5, 2017, from https://www.owasp.org/index.php/Testing_for_Cross_site_scripting

Prashant S. Shinde; Shrikant B. Ardhapurkar. (2016). Cyber security analysis using vulnerability assessment and penetration testing. *2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave)*(IEEE Conference Publications), 1 - 5, DOI: 10.1109/STARTUP.2016.7583912.

S Sandhya, Sohini Purkayastha, Emil Joshua, Akash Deep. (6-7 Jan. 2017). Assessment of Website Security by Penetration. *Advanced Computing and Communication Systems (ICACCS), 2017 4th International Conference on*. doi: DOI: 10.1109/ICACCS.2017.8014711

.