International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

Vulnerability Assessment and Penetration Testing of Web Application

Vrunda Dhameliya[1], Prof. Apexa Patel[2]

[1,2] Department of cyber security, GIT Gandhinagar University

Abstract

As Internet usage is rising day by day security has become a vital facet to the Internet world. Security of the website in today's world is very important. Vulnerability assessment and the penetration test are two different vulnerability tests. This testing hasmuch strength and is often combined to gaina more complete analysis of vulnerabilities. Penetration Testing andVulnerability Assessments execute two different tasks, usuallywith distinctive outcomes, within the same area of application.For any organization, proper working of security arrangement ischecked by Vulnerability Assessment and Penetration Testing. Web applications are vulnerable to attacks, such as the operation of sessions,Scenarios of the transverse site, SQL injection, making the length of the cross -demand,boofer above flows and poor safety configuration, etc.Described in Open Web Application Security Project Top 10. A Can be manually penetrated or automatically tested depends on the vulnerability. A comparison will be madebetween these two tests.

Keywords: VulnerabilityAssessment and Penetration testing, Cross-Site Scripting, SQL Injection, Cross Site Request Forgery, Open Web Application Security Project.

1. Introduction

For enterprises, security is a crucial topic. Attackers targeted numerous websites in a short period of time. Over the past few years, hacking has rapidly increased. Since the majority of work-related activities, including bill payment, chat, e-commerce, e-government, and online banking, take place online, security is crucial [1].The availability of web applications may be impacted and private information may bestolen if a website is compromised. Consequently, protecting web apps is vital. Web application flaws are found through vulnerability assessment and penetration testing, whereas penetration testers look for website flaws[2].

The system can be compromised because of existing vulnerabilities. The network, application or systems consisting of these vulnerabilities are termed as a vulnerable application or network. Therefore, it is important to perform the Vulnerability Assessment and Penetration Testing (VAPT) of the web applications before releasing to the market. Websites in the real world are intricate systems that communicate can store and analyze data in numerous locations, as well as combine data with other systems. Stated differently, they are made up of various amounts of parts and technologies, such as web servers and server-side application development tools, as well as web browsers and client-side tools (such JavaScript and Flash).

Web application security threats are identified, examined, and reduced through the use of vulnerability assessment and penetration testing, or VAPT. Security risks have increased due to the growing dependence on web applications, which calls for sophisticated techniques and tools for efficient vulnerability evaluation and penetration testing. The current research, instruments, strategies, and practices utilized in web application security testing are examined in this review of the literature.

Literature Review

1. Web Application Security and Common Vulnerabilities -Owasp Top 10, the widely recognized list of the most important security risk helps developers and organizations to understand and reduce these dangers. Some of the most common weaknesses below are [OWASP (2023)]:

i. SQL Injection (SQLI):-

Attackers utilize inappropriate hygiene input areas to manipulate SQL issues.

This can lead to unauthorized access, data leakage, modification or deletion.

Limit: Use parameters, prepared statements and entry confirmation.

ii. Cross-Site Scripting (XSS):-

The malicious script is injected on web pages, which is then performed in users' browsers.

Increased can lead to kidnapping, identification theft and rejuvenation in malicious places.

Limit: Use material safety policies (CSPS), users avoid input and use frames that automatically handle hygiene.

iii. Cross-Site Request defeated (CSRF):-

An attacker lurks a login user to take unexpected actions on a website.

This can lead to unauthorized transactions, password changes or privilege.

Limit: Use CSRF symbols, use cookies for uniform location, and sensitive tasks require the user's authentication re-autoization.

2.Vulnerability Assessment Techniques -

Vulnerability assessment is an critical cybersecurity approach that facilitates discover safety flaws in web packages before attackers can take advantage of them. Vulnerabilities are diagnosed, investigated, and mitigated using loads of strategies. Here are some vital techniques:

i. Automated Scanners:-

Automated tools help find security weaknesses by scanning applications for known problems. Some popular scanners include:

Nessus – Detects community and application vulnerabilities, which includes misconfigurations and outdated software program.

OpenVAS – An open-supply device that gives enormous vulnerability scanning for programs and networks.

Burp Suite – Widely used for web safety checking out, which includes guide and automated assessments.

ii.Static and Dynamic Analysis: -

a) static application security testing (SAST):-

The source codes, bite code or books without performing the program.

SQL identifies weaknesses such as injection, buffer overflow and hard -coded identification.

Equipment: Sonarakwe, Fortify, Czechmax[4].

B) Dynamic Application Security Testing (Dast):-

Search during driving time by following the attacks.

The authentication detects security errors such as bypass and increased kidnapping.

Equipment: Burp Suite, Owasp Zap, Appscan.

3. Penetration Testing Method-

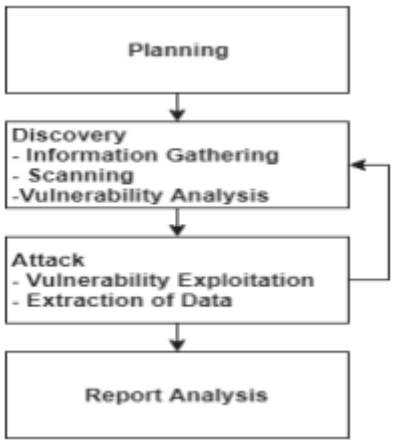

Fig. 1. Penetration Testing Method

i. Planning:-.

This stage involves defining the scope, objectives, and methodologies for the assessment.

ii. Discovery

InformationGathering: Collecting data about the target system.

Scanning: Using automated tools to detect security weaknesses.

Vulnerability Analysis:

Evaluatingdiscoveredvulnerabilities and their potential risks.

ii. Attack

Vulnerability Exploitation: Simulating real-world attacks to exploit security flaws.

Extraction of Data: Gathering and analyzing compromised data.

iii.Report Analysis

Documenting findings, assessing impact, and providing recommendations for mitigation[5].

4.Popular Web Application Security Tools-

i.Acunetix Web Vulnerability Scanner:-

Each online application must be secured. His highest priority is in any organization that depends on technology. Acunetix is responsible for identifying all weaknesses of web applications. Any program must be extremely safe to function properly. Thus, Acunetix contributes to the safety of any web application. One of the safest test units that can identify all vulnerabilities for the system is the "Acunetix web vulnerable scanner." There are many types of weaknesses that can occur in a system, including SQL injections and scripting across the site.

Steps for "Acunetix Web Vulnerable Scanner" is as follows:

• Website Analysis: After scanning a website, Acunetix Deep Scan Scanner Pages and Links related to the site shows. Each information about the web application is acquired.

• Turn on Acunetix ACU sensor in scanner

The web contains folders and files in the application.

• Displays the potential weaknesses in the web application.

• After the scan is completed, the conclusions Protected in a document. The reporter allows the scan results to create a printable report on the results[6].

ii. OWASP Zed Attack Proxy (ZAP):

The OWASP Zed Attack Proxy Tool (or ZAP) is a pen checking out and proxy tool. ZAP needs to setup the browser's proxy manually. The motive of this tool is to permit builders to check the steadiness and protection in their internet site or utility. ZAP has a capability to speedy assault a internet site with only a click on of a button. Once the URL is entered and the consumer clicks on "Attack" button, this system will actively attack the website and document a listing of problems that the internet site has. OWASP ZAP permits generating the reports of scan results in a HTML, XML format. ZAP uses the deal with "local host" and port "8080" by way of default, however this can be changed via the "Options Local Proxy" display screen within the program. Check the browser's proxy settings, and ZAP's proxy settings[7].

iii. Burp Suit:

Burp Suite is a group of different devices that are place In order to work in passive/active mode, it supports Input exams in the entire test process, from Plan phase to identify and utilize weaknesses.These weaknesses [8]. A Barp-Proxy man can act as a mid-attack vector due to traffic obstacle Between the browser and the target application. Burp-out is required Manually set up as a power of attorney in the browser. Using Burp suit Standard as standard "local host" and port "8080" but it can be Better through the "option" screen in the program. Secondly, configure the browser to use Burp Proxy listens It's http like a proxy server. To use Burp Proxy, Change Browser proxy settings using proxy host address (off) Standard, 127.0.0.1) and port (as standard, 8080) for both http And https protocol, without exception.

Burp scanner is used to find security weaknesses Automatically in the web application. Passive scan mode Analyze the content of existing requests and reactions, and Reduces weaknesses from these people. In active scan mode, Burpsuit sends various requests made for application, and

Analysis analyzes reactions to gather evidence of weaknesses [8].

Conclusion

VAPT plays a critical role in securing web applications against cyber threats. While existing methodologies and tools provide substantial protection, continuous advancements in AI, automation, and threat intelligence are necessary to combat evolving security challenges. Future research should focus on improving accuracy, reducing false positives, and integrating security practices into development workflows.

References

1. Khushal Singh, Vikas, “Analysis of Security Issues in Web Applications through Penetration Testing”, International Journal of Emerging Research in Management &Technology, Volume 3, March 2014.2.
2. Prashant S. Shinde, Shrikant B. Ardhapurkar, “Cyber security analysis using vulnerability assessment and penetration testing”, IEEE 2016.
3. OWASP (2023). "OWASP Top 10: The Ten Most Critical Web Application Security Risks."
4. J. Yang, L. Tan, J. Peyton and K. A Duer, "Towards Better Utilizing Static Application Security Testing," *2019 IEEE*
5. Arvind Goutam and Vijay Tiwari “Vulnerability Assessment and Penetration Testing to Enhance the Security of Web Application” 4th International Conference Nov 21-22 2019
6. Insha Altaf, Jawad Ahmad Dar, “Vulnerability Assessment and Patching Management”, International Conference on Soft Computing Techniques and Implementations, IEEE 2015
7. Russ McRee, “OWASP ZAP Zed Attack”, ISSA member, Puget Sound (Seattle), USA, November 2011
8. Zoltan Panczel, “Burp Suite(up) with fancy scanning mechanisms”, SANS Institute InfoSec, December 20th, 2015.