International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 6 | ISSN : 2456-3307

Vulnerability Assessment and Penetration Testing in Web Application and Its Prevention

Nidhi Vora*1, Chandresh Parekh2

*1 Research Scholar, IT and Telecommunication Department, Raksha Shakti University, Gujarat, India
2 Assistant Professor, IT and Telecommunication Department, Raksha Shakti University, Gujarat, India

ABSTRACT

Utilization of PCs are expanding step by step, System's intricacy is expanding, most of the frameworks are associated with the web. As the Use of more web t like online networking sites, distributed computing we have to secure web application. Utilization of more web that prompts an ever-increasing number of vulnerabilities in framework. Assailants, use their vulnerabilities to misuse the casualty's framework. As a security reason we need to discover these vulnerabilities ahead of time before aggressor do. To keep this issue one arrangement was recommended named weakness evaluation and infiltration testing for security of web application. Powerlessness evaluation is the source by which we can discover blame in the framework. The capacity of infiltration testing is the recognize the vulnerabilities and we can get access into site and system as unapproved client and discovering escape clauses. Because of these vulnerabilities quantities of frameworks are misuse each year. Helpless sites, system or framework might be bargained by different assaults, for example, DDos(Distributed Denial of service)attack, DNS(Domain name server)Spoofing, DHCP(Dynamic Host Configuration Protocol)snooping, ARP(Address Resolution Protocol)Poisoning, Smurf assaults, Man-in-the-Middle, Buffer flood, SQL infusion and numerous other digital assaults alongside various noxious digital assaults containing numerous malware, for example, infections, Trojan Horse, Worms, Rootkits, spyware and adware, botnet and so forth. These vulnerabilities principle explanation for this is week passwords, programming bugs, don't utilize refreshed frameworks, non-fixing of working frameworks. Content code infusion spaces and so on. The primary goals of this paper are discovering vulnerabilities from sites and give aversion remediation.

Keywords : Cyber security, Vulnerability assessment, penetration testing, web attacks.

I. INTRODUCTION

Vulnerability Assessment and Penetration Testing (VAPT) is a Systematic analysis of security status of Information systems [1]. The growing connectivity of computers through the Internet, the increasing extensibility of systems, and the unbridled growth of the size and complexity of the systems have made Cyber security a bigger problem now, than in the past. Furthermore, it is a Business Imperative to adequately protect an Organization's Information assets by following a comprehensive and structured approach to provide protection from the risks an organization might face. In an attempt to resolve the Cyber threats, and comply with the mandated security regulations, Vulnerability Assessment and Penetration Testing (VAPT) proves to be an assured assessment tool to ensure the Cyber Security arrangements of an Organization [5].

In an attempt to resolve the Cyber threats, and comply with the mandated security regulations, Vulnerability Assessment and Penetration Testing (VAPT) proves to be an assured assessment tool to ensure the Cyber Security arrangements of an Organization. The Technique has become a widely used and integral part of Quality Assurance Techniques for the systems used by various financial organizations particularly Banks. Vulnerability Assessment, as the name suggests, aims at discovering the possible threats and subset of input space with which a malicious user can exploit logical errors in a system to gain profit or drive the system into an insecure state. Vulnerability Assessment, as the name suggests, aims at discovering the possible threats and subset of input space with which a malicious user can exploit logical errors in a system to gain profit or drive the system into an insecure state. While, Penetration testing, aims at assessing the difficulty level for someone (basically an attacker/hacker) to penetrate an Organization's Cyber security controls against unauthorized access to its information and information systems. VAPT is done by simulating an unauthorized user (attacker) attacking the system using either Automated Tools or Manual Excellence or a combination of both. Hence the process of VAPT is sometimes also referred as Ethical Hacking. VAPT helps in identifying Cyber Threats and vulnerabilities under controlled circumstances, so that they can be eliminated before actual hackers/attackers aim to exploit them [2].

II. OVERVIEW OF VAPT

The complete process of VAPT is conducted in two major parts. The first part deals with the Analysis and Discovery of existing Vulnerabilities, which may lead to various Cyber threat. The second part deals with the Exploitation of the detected set of Vulnerabilities, to judge their Severity and Impact over the Target system

A. Vulnerability assessment

Powerlessness Assessment (VA) or Vulnerability Analysis (VA) or Vulnerabilities the way toward examining the framework or programming or a system to discover the defects and shortcoming in that. This likewise incorporates arrangement of methodical measures used to audit and organize security vulnerabilities in a system or correspondence framework or any application benefit. Helplessness Assessment enables organizations in the assurance of security to stance of the earth and the level of presentation to dangers. Helplessness Assessment assume a key part in each sort of PC applications, framework and foundation. Any framework which is giving any sort of figuring administrations may contain vulnerabilities so VA test plays a key for each sort of PC application. In PC systems and interchanges, our data use to go out of PCs so nearness of vulnerabilities may trade off our entire systems to abused [4].

B. Need of vulnerability assessment

The fundamental target of any association to make benefits towards its vision and objectives. So, associations have chance to convey Information Technology infrastructures. After sending of the data innovation framework, the fundamental point of any association is to keep their correspondence arrange and secure their secret data from unapproved get to.

In this manner helplessness evaluation performs to look at shortcoming and imperfections in a framework. Goal of Vulnerability Assessment may incorporate System Accreditation, Risk Assessment, Network Auditing, Compliance Checking and Continuous Monitoring. Real reason for vulnerabilities are because of frail passwords, defects in frameworks, broken and wrong setup and human mistakes like, improper authorizations appointed to clients, unseemly system outline and gadgets and like this and so forth. Some business gauges foundations like PCI-DSS expect associations to perform powerlessness appraisal on their system or frameworks [4].

C. Penetration testing (Pen-testing)

Infiltration Testing or just Pen-Testing or Security Testing otherwise called moral hacking the strategy used to find vulnerabilities in arrange framework before an assailant misuses. This is the demonstration of accessing systems or frameworks assets without the information of client qualifications like usernames and passwords. Infiltration testing report imagine the proof that vulnerabilities are available in your system or framework from that point entrance is conceivable in. besides an entrance test report is proficient to picture the proactive and medicinal measures to ensure your system and improve exhaustive protective technique. The infiltration test report likewise portrays the palatable security approaches embraced by our security mindful experts. These test report are likewise regularly required by security organizations, peace offices, data frameworks evaluators and different investors.

It is noteworthy to talk about that it is not at all like that a pen-analyser will reveal all vulnerabilities in a single pen-test report. For instance, if a pen-analyser has created a report today clearly it might never again be substantial following one month. It is on account of after the endorsement of pen-test report by proprietor, framework may have get fixed with new updates which may last a helplessness in some web server which may considered secure in last pen-test report. So, keep up a protected foundation, consistent watchfulness is considered necessary [4].

D. Need of penetration testing(Pen-testing)

Entrance tests are imperative for various reasons like:

- Determining the likelihood of specific assaults to occur.
- Discover high hazard vulnerabilities coming about because of okay vulnerabilities.
- Identifying vulnerabilities that might be troublesome or difficult to recognize with general checking programming.
- Identifying greatness of an effective assault to a powerless system.
- Testing capacities of system protectors to recognize and reaction to arrange assaults.
- Provide confirmation to build assignments in security spending plans.

Before propelling another framework, it is exceedingly prescribed that it ought to be tried first so that to check any defencelessness in the framework [4]. By this training heaps of vulnerabilities are distinguished before the framework propelling to maintain a strategic distance from genuine adventures. The Payment Card Industry (PCI) Data Security Standard (DSS) characterize Penetration Testing Standards. At any rate these guidelines are required to get meet for agreeable pen-testing approach.

III. VULNERABILITY OF WEB APPLICATION

a) **SQL- Injection:** SQL Injection is the hacking method which endeavors to pass SQL summons(articulations) through a web application for execution by the backend database. If not cleaned appropriately, web applications may result in SQL Infusion assault that permit programmers to see data from the database as well as even wipe database as well as even wipe database as well as even wipe database as well as even wipe it out. In SQL Injection, the programmer utilizes SQL inquiries and inventiveness to get to the database of touchy corporate information through the web application [1].

b) **Cross-Site Scripting**: If the web site allows uncontrolled content to be supplied by users. User can introduce malicious code in the content for example: Modification of the Document Object Model-DOM (change some links, add some buttons), Send personal information to third party (JavaScript can send cookies to other sites) [1]. XSS attacks involve three parties:

- The attacker
- The victim
- The vulnerable web site that the attacker exploits to take action on the victim.

XSS vulnerabilities exist when a web application accepts user input through HTTP requests such as a GET or a POST and then redisplays the input somewhere in the output HTML code

c) **Broken Authentication and Session Management**: Application capacities identified with validation what's more, session administration is regularly not actualized correctly, allowing assailants to bargain passwords, keys, session tokens, or adventure other execution blemishes to expect different client's personalities [1]. Record accreditations and sessions tokens are regularly not legitimately secured, outsider can access to one's record. Technique for assault utilize shortcoming in verification instrument:
   - Logout
   - Secret word Management Timeout
   - Remember me

d) **Insecure Direct Object References**: Occurs when designer employments HTTP parameter to allude to inner protest. An immediate protest reference happens at the point when a designer opens a reference to an interior execution question, for example, a record, registry, database record or then again key, as a URL or, then again shape parameter. An assailant can control coordinate protest references to get to different items without approval, unless an entrance control check is input. For illustration, in Web Keeping money applications, it is regular to utilize the record number as the essential key. Consequently, it is enticing to utilize the record number straightforwardly in the web interface. Regardless of whether the engineers have utilized parameterized SQL questions to forestall SQL infusion, if there is no additional watch that the client is the account holder and approved to see the account, an assailant altering the record number parameter can see or change all records [1].

e) Failure to Restrict URL: Many web applications check URL get to rights before rendering ensured connections and catch. In any case, applications need to perform comparable access control checks each time at the point when pages are gotten to, or assailants will have the capacity to fashion URLs to get to these concealed pages at any rate. Some site simply keeps the show connections or URL's to unapproved clients, aggressors can get to straightforwardly the URL's by accessing secured territories. Code that assesses benefits on the customer rather than on the server. Benefits tried in JavaScript and access to a shrouded address. However, aggressor can see the code the address [1].

f) Remote Code Execution: This powerlessness permits an assailant to run self-assertive, framework level code on the powerless server what's more, recover any wanted data contained in that. Shameful coding mistakes prompt this defenselessness. It is hard to find this weakness amid entrance testing assignments be that as it may, such issues are regularly uncovered while doing a source code survey. Nonetheless, when testing web applications is vital to keep in mind that abuse of this powerlessness can prompt aggregate framework bargain with an in distinguishable rights from the web server itself [1].

IV. BENEFITS OF VAPT

VAPT is led in three noteworthy ranges Physical Structure of the framework, Logical Structure of the framework what's more, the Response/Work stream of the concerned framework. These three zones are nearly most inclined to digital assaults consequently evaluating these three zones gives an entire thought of the level of Cyber Security courses of action in the target framework. A. Extent of Vulnerability Assessment and Penetration Testing The above expressed three zones of concern, finish up and characterize the general extent of weakness evaluation and infiltration testing process [2].

- System Testing: In this part, the VAPT analyzer points at distinguishing the security imperfections related with the Outline, Implementation and Operation of the objective association's system. The analyzer investigations and checks different segments like Modems, Remote Access Gadgets also, other associations for conceivable mis-arrangements, which may go about as a passage point for an aggressor to hack into the objective's system.

- Application Testing: The VAPT analyzer here, goes for testing the applications controlled by the test target fundamentally the web applications as they remain relatively more powerless against assaults. The analyzer uncovered the adequacy of an application's security controls by featuring the dangers postured by real exploitable vulnerabilities.

- Social Engineering: In this piece of VAPT the analyzer points at inspecting the Work stream of the target Association, by focusing on the human collaborations to accumulate private data with respect to the objective or any of its segment frameworks, which generally is expected to be kept classified.

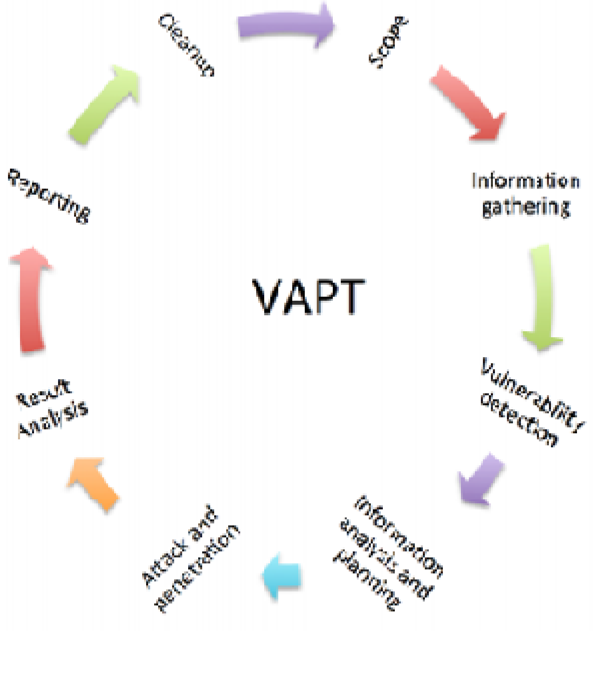

Figure 1. Process Of VAPT

VAPT is an esteemed confirmation evaluation instrument that advantages both business and its operations. For an Organization to stay guaranteed of its Security Infrastructure, it must lead VAPT occasionally, it not just guarantees the Security level of its part frameworks and assets, yet in addition educates about new vulnerabilities and adventures conceivable, which may prompt budgetary and information misfortunes.

- Business Point of View: For any budgetary Association, its Corporate Image remains a major concern, VAPT causes an Organization to shield against any conceivable Failure by anticipating Financial misfortunes, demonstrating due persistence what's more, consistence to industry controllers, clients what's more, investors, in this manner safeguarding Corporate Image and think Data Security ventures. Associations burn through a huge number of dollars to recuperate from a security break because of notice costs, remediation endeavors, diminished efficiency and lost income. The PC Society of India (CSI) think about assessments recuperation endeavors of around $167,713.00 per occurrence.
- VAPT being a Proactive Administration can effectively Distinguish and address security chances before real security breaks happen, subsequently keeping any Unauthorized Access, Information Corruption and budgetary misfortune caused by security breaks. VAPT gives a Proof of Issue and a strong case for proposition of venture to senior administration, along these lines making high attention to Security's significance by any stretch of the imagination levels of an Organization [2].
- Operational Point of View: Conducting VAPT makes a difference an Association in molding Data Security Procedures through speedy and exact recognizable proof of vulnerabilities, Proactive disposal of recognized dangers, execution of remedial measures what's more, improvement of IT information. VAPT gives itemized data on real, exploitable security dangers on the off chance that it is incorporated into an Organization's security Doctrine and Processes. By giving the Information required to viably and proficiently Isolate and Prioritize vulnerabilities, VAPT can help the Organizations to Fine-tune the test setup changes or Patches to star effectively dispose of distinguished dangers.

V. RISKS OF VAPT

Security Testing makes hazards the objective by its extremely nature. Like an Attacker the VAPT Tester purposely clears out the moderately safe ground of planned utilize and expected exercises. Security Testing is inalienably intrusive where it utilizes methods like those utilized as a part of an assault [5].

A. The Specific Risks of VAPT can be ordered as takes after:

- Specialized Risks: These are the dangers caused specifically by the Testing Activities or by the System being tried. Some of the real specialized dangers are Failure of the objective or associated frameworks, Disruption of administration, Reduced Performance, Adjustment or Contamination of information and Disclosure of information.
- Hierarchical Risks: The VAPT testing likewise includes some Organizational symptoms like Unnecessary activating of episode taking care of procedures, Disruption of business procedures, and Loss of Reputation if outsiders are influenced.
- Legitimate Risks: These sorts of dangers are experienced because of lawful commitments and conceivable reactions of outsiders like Infringement of Legal Obligations and incidentally submitting culpable acts.

B. General Precautions for VAPT: In light of the hazard factors engaged with VAPT, the analyzers need to concentrate on a few safety measures keeping in mind the end goal to keep any startling mischief to the objective framework. The analyzers by and large embrace the accompanying real methodologies to do as such:

- Circuitous Testing: The analyzers as opposed to testing the genuine imperfections expect to gather adequate confirmations to reason that weakness is probably going to be available. The system is valuable when managing known vulnerabilities.
- Restricted Exploitation: The analyzers endeavor to lean toward Test Cases that show the defenselessness and its adventure, and attempt to decrease the genuine measure of misuse. The analyzers utilize certain Payloads that show quantifiable impacts without causing any extreme reactions.

- Postponed Effects: Sometimes, if conceivable, analyzers configuration tests for deferred impacts. The analyzers at that point assess the test comes about inside the framework and drop or hinder any further handling before it would happen. The methodology is compelling in situations where the tests have certifiable impacts.
- Interruptible Testing: In Some testing scenarios, analyzers need to guarantee that they can interfere with their testing whenever, so they can quickly respond if any unintended outcomes are watched [5].
- Testing Tests: Exploratory testing approaches, where the analyzers grow new tests in light of their powerlessness speculations, are characteristically more hazardous than executing all around arranged tests. Thus, analyzers must utilize a lab situation to create and attempt tests before sending them against genuine targets.

VI. CONCLUSION

Risks to honesty and mystery of information and resources are extended. To remain secured, affiliations perform VAPT to check the security position of the system. As we have encountered the composing review about VAPT systems, it is discovered that there are diverse mechanical assemblies available for performing VAPT. Aggressors are finding better approaches to evade security instruments so new vulnerabilities are propelling which ought to be tended to. In this way existing apparatuses ought to be included with component to perceive and overview the as of late propelled vulnerabilities. This issue can be had a tendency to by making instruments so versatile that new ambush imprints can be included for sorts of vulnerabilities. In Vulnerability Assessment and Penetration Testing utilized for Cyber Security Analysis we begin with contrasting and pointing out similitudes of Vulnerability Evaluation with Entrance Testing with their focal points furthermore, disservices [3]. We have clarified how Vulnerability Evaluation furthermore; Penetration Testing can be utilized as a powerful digital resistance innovation. In future I am planning to find maximum vulnerabilities on websites and then find loopholes and show its prevention will occur.

VII. ACKNOWLEDGEMENT

I am happy to offer my thanks to all who rendered their significant offer assistance for the fruitful finish of the task. I am grateful to my guide Mr. Chandhresh Parekh for his direction and consolation in this work. I might likewise want to express my gratefulness and on account of all my associates and relatives who purposely or accidentally have helped what's more, supported me all through my work.

VIII. REFERENCES

[1]. Ankita Gupta, Kavita, Kirandeep Kaur. "Vulnerability Assessment and Penetration Testing". International Journal of Engineering Trends and Technology (IJETT). V4(3):328-333 Mar 2013.

[2]. A Modern Approach to Cyber Security Analysis Using. Vulnerability Assessment and Penetration Testing. Sugandh Shah SEP-2013

[3]. Vulnerability Assessment and Penetration Testing used for Cyber Security. Authors: Shreeyash Bothare, Parth Sagar,Vol 2, No 1 (2017)

[4]. Penetration Testing and vulnerability assessment, Irfan Yaqoob, Syed Adil Hussain, Saqib Mamoon, Nouman Naseer, Jazeb Akram, Anees ur Rehman University of the Punjab, Jhelum Campus, Pakistan 6 University of Engineering and Technology, Lahore, Pakistan

[5]. Kumar, K. Srinivasa Rao, A. Latest Approach to Cyber Security. Analysis using. Vulnerability. Assessment and Penetration Testing, International Journal of Emerging.