CYBER DEFENCE: A HYBRID APPROACH FOR INFORMATION GATHERING AND VULNERABILITY ASSESSMENT OF WEB APPLICATION.

Deepak Upadhyay
Assistant Professor
School of Engineering and Technology
Gujarat Technological University
Ahmedabad, India
ap_deepak@gtu.edu.in

Dixit Kumar. V. Prajapati
Master of Engineering (Cyber security)
School of Engineering and Technology
Gujarat Technological University
Ahmedabad, India
dixitprajapati99@gmail.com

ABSTRACT

Vulnerability assessment and penetration testing (VAPT) is an important step for protect cyber defense of systems or networks and live web application. Day by day growing internet connection, everywhere remains connected to each other in the world. Web application security major captative of all cyber space in information gathering. So there is various kind of tool available in the world for website information gathering and VAPT. All VAPT and web application information gathering tools have own format and functionality. Mostly information gathering and VAPT tools are too much costly and also some tool is open source. There are many best VAPT tools are available but they are not able to give 100 % accuracy and solution to find out particular vulnerability. And our approach to combine multiple VAPT tools (open source). The tool will approach to provide good accuracy and efficiency also more security open source effective solution for information gathering and VAPT. The approach is to make a tool for web application on information gathering and VAPT and also the result send to pdf report via user's mail-id or download pdf report on same.

Keywords: Cyber security, web application, information gathering, Vulnerability assessment and penetration testing (VAPT).

1. INTRODUCTION

Now days various kind of web application are launched on World Wide Web. There are different categories of web application. The volume of WWW (the internet) the web contains indexed at least 4.45 billion pages and the web contains Dutch indexed at least 145.64 million pages up to (Sunday, 28 October, 2018)[9]. Recent attackers are very smart to hack the web application. Mostly attacker targeted government web application and high profile Company where they are finding some important database or some financial things. Attacker will apply various techniques to take over particular web application. On web application have some important data, e-governing, e-commerce, online banking, live web applications, social networking, quality information, communication, sharing the resources, payment of utilities bills etc. In web applications, security vulnerabilities may result in breach of data integrity; affect web application availability or stealing of confidential data. Web applications are one of the most critical jobs of securing. In mobile computer sector and Web application are sometimes related with local applications, mostly all applications that are made particularly for individual platform or gadget and put and also install and verify on that particular device. Programmes for combine approaches are sometimes referred to as hybrid approach applications.

2. WEB APPLICATION

A Web application (Web app) is one kind of application Programme are stored on remote server and also delivered over the medium of internet a browser interface. Mostly web application design by user requirements. Web applications have content, function, security, database etc...

2.1 Web Application Types: Static Web Page to a Progressive Web App [13]

2.1.1 STATIC WEB APPS

The term ‘static’ comes from these web apps’ lack of flexibility. Static web apps have their pages generated by a server and offer little to none (with no JavaScript code used) interactivity. Static web pages are often difficult to maintain and the excessive amount of data they send and receive creates risks of poor performance.

2.1.2 Dynamic Web Apps

Any dynamic web app is based on a *framework* – web app software that controls web page construction and facilitates maintenance. The way such web apps are displayed on a user’s screen is not predetermined but rather implemented on server side or client side as shaped by logic dynamic applications. Different way in how they work of this kind of applications, and their use cases determine their development approach and the architecture.

2.1.3 Multi-Page Apps (MPA)

In multi-page web apps, the logic is almost fully on the backend. This means that for any change to take effect, all the requests from the client-side go to the server and back. Aside from the use of a framework, this principle was almost identical to that of static web apps in the past. MPAs take advantage of AJAX technology that enables instant changes without a full page reload. If designed as responsive, such web apps can even adapt to mobile environment. Also, MPAs are highly secure.

2.1.4 Rich Internet Apps (RIA)

RIAs tried to overcome browser limitations and heavily relied on client-side plugins, such as Flash, Shockwave, and Silverlight. Installed and regularly maintained by the users, these plugins were supposed to interpret either some highly interactive parts of a web app page or, at times, the web app’s very core. The problem was in the plugins’ vulnerability as well as some inconveniences they created: if a plugin was just a little outdated, some parts of a web app, or sometimes the whole app, had no chance to function properly.

2.1.5 JavaScript-Powered Web Apps

With the appearance of such front-end JavaScript frameworks as Angular, React, Meteor, and Ember, the logic of web apps has started its shift to the client-side, allowing for even better flexibility than occasionally embedded AJAX. Client-side logic has begun to take over the server-side’s responsibility of processing user requests and rendering the responses.

2.1.6 Single Page Apps (SPA)

SPAs managed to fulfil the promise of their name: they indeed let users freely interact with a web app from a single page. What’s more, the interaction is much swifter, as requests and responses communicate in small amounts of data and occur almost instantly.

2.1.7 Progressive Web Apps (PWA)

The catch is that progressive web apps aren’t about new principles in architecture, but rather features that improve performance and mobile adaptability of any web app. Cashing, home screen installation, and better data transfer over HTTP/2 are the key enhancements. One of the PWA ideals is improving mobile web experience and making it available for users with slow or bad Internet connection

3. INFORMATION GATHERING AND AVAILABLE TOOL LIST & TECHNIQUES

First we have to understand why information gathering is required, an Information gathering is helps the target of individual or an organization to carry out difficult steps that very hard to achieve, if it is doesn't benefit so its not worth fully. As we know information gathering is the art and act of collecting meaningful data from various place or sources. Information gathering is also part of foot printing [8]

TABLE 1- INFORMATION GATHERING TOOL AND TECHNIQUES. [8]

Information gathering techniques	Tool name	Purpose of tool
1.Information gathering through Search Engine[8]	1)www.netcraft.com	server OS, version details, particular server IP address ,name_server, DNS details.
	2)www.shodan.io	find out targeted computers,servers,IP address camera with country, region.
	3)Google-Maps	physical location of aorganisation or target
	4)Social Media Sites	information about people
	5)Google Finance	financial related information of target
	6)Google Alert	Latest alerts and news for your choice
2.Information gathering for Website[8]	7)Web Data Extractor	find out sensitive information to Website crawl using scripts.
	8)HTTrack Website Mirroring	Same copy entire target website on your local machine/computer.
	9)Web Archive	the target website older version watch
	10)Website Watcher	Each and every watch on targeted website
	11)Website Traffic Analysis	know traffic of the website
3.Advanced Information gathering[8]	12)Email Tracker Pro	geographical location of email sender…
	13)Polite Mail	advanced and critical information, mail open or not all.
	14)Hoovers	business information of competitors and target organization, economical information, employees, business related information.
	15)Business Wire	Analysis, photos,news,trending of the organization
4.Lookup Information Gathering[8]	16)WHOIS LOOKUP	Find out details of owner and admin and name and name server and server and registration record, expiry details of domain.
	17)DNS LOOKUP	Gather information targeted website of domain name server
5.Network Information Gathering[8]	18)Path Analyzer Pro	route of the target IP
	19)Windows Command Promt	route of the IP address
6.Network Information with social engineering[8]	20)Shoulder Surfing:	keep watching on attackers movements and actions.
	21)Eavesdropping:	Phone call, video, conference intercepting or listen of target.
	22)Dumpster Diving	Collecting garbage data of old documents, bills, sensitive papers etc.

4. AN OVERVIEW OF VAPT

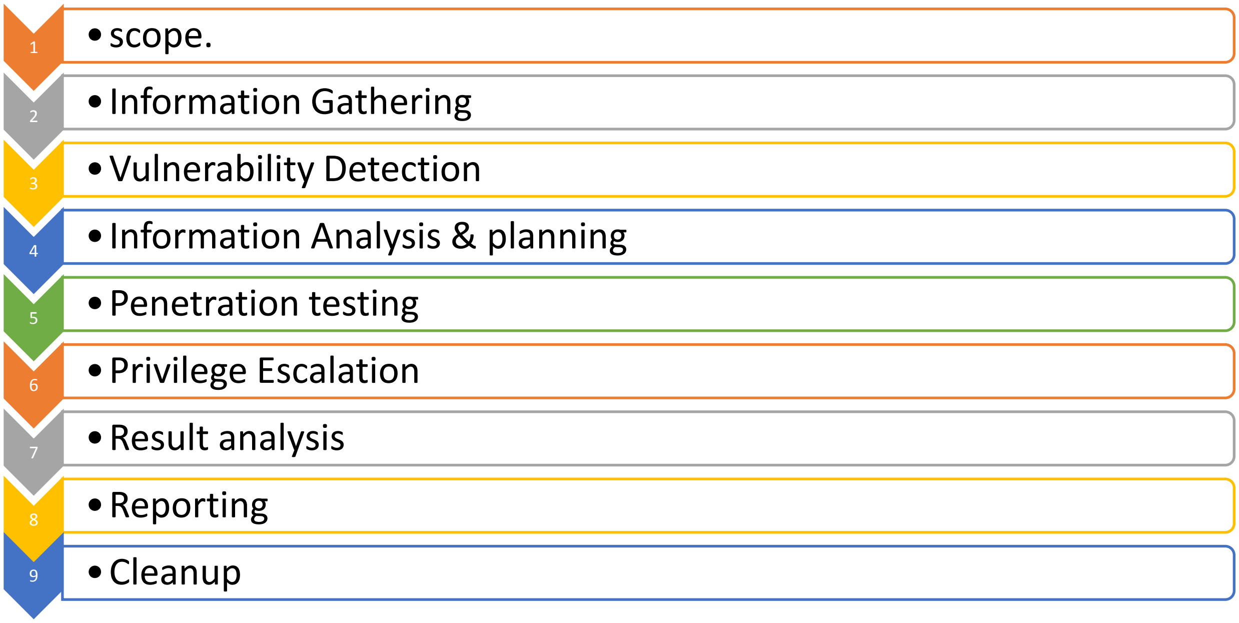
What is vapt? VAPT is show the honest and sure assessment technique to monitor the effect of the information security infrastructure of organization. The process of VAPT is occasionally doing as ethical Hacking effects.VAPT is various ways to approach to trying the scripter and tester and hacker was performing and utilizes the information of corrupt network or system of target, and there are continue planning of cyber defense world to protect. And many organization was perform same self VAPT on own environment to cyber space. VAPT is useful to measure the present arrangement of security and making solution parches to protect up coming risk. Some organization was outsider agency hired to auditing. That external auditing company procedure of provide trust and information discloser and risk assessment itself. As per survey VAPT is most popular thing to perform on the ourequipments like website or application or network or system. There are many capable open source and free and chargeable tool here below we discuss to conduct VAPT (Hacker/Attacker) attacking the system.

5. LIFECYCLE OF VAPT

Here we are discuss the lifecycle of VAPT. Here below we seen diagram no-1 there are mention total 9 no of steps.

Each and every steps have own functionality, all tester will perform same. First step find out scope of taget. Then collect the information of particular scope of target IP, OS, network. Also doing some investigation on all details. After perform vulnerability assessment (VA) for finding vulnerabilities. Then analysis the information and also planning to perform penetration testing (PT). PT is got the vulnerabilities and doing attach on same and also prove a risk of targeted system or network or web application. Then secure tester was developing the resolve the vulnerabilities from victim system result analysis. Then done reporting process and cleaning up and repair the system.

Diagram 1- VAPT lifecycle process



1 • scope.

2 • Information Gathering

3 • Vulnerability Detection

4 • Information Analysis & planning

5 • Penetration testing

6 • Privilege Escalation

7 • Result analysis

8 • Reporting

9 • Cleanup

6. VULNERABILITY SEVERITY AND IMPACT ANALYSIS

OWASP and SANS provide the list of standard most popular common and dangerous security vulnerabilities. Based on the list of vulnerabilities they are provide rank of security level and there impact. An organization MITRE corporation also standardized the general language of all types of vulnerabilities. Here we define the language of CWE- common weakness enumeration. Every vulnerabilities have own CWE code to diagonally the over the globe. Table no-1 was shows the owasp foundation maintained top ten vulnerabilities list and also rank and CWE code. All vulnerability mostly based on web applications. Table no-2 describe about the CWE/SANS foundation top 2 vulnerabilities. List of 2 vulnerabilities was mentioning all types of applications. These all are maintained by sans and mire corporation team. They are establishing the severity vulnerability and class. The vulnerability provides the compromise the most critical security fundamentals and flows. After the vulnerability assessment measurement also before we are planning for penetration testing. And also these are map of vulnerabilities list and better approach of security and identify the issue.

Table 2. OWASP Top 10 vulnerability list CWE [11]

Rank	CWE	VULNERABILITY NAME.
A1	1027	Injections.
A2	1028	Broken Authentications.
A3	1029	Sensitive Data Exposures.
A4	1030	XML External Entities (XXE).
A5	1031	Broken Access Controls.
A6	1032	Security Misconfigurations.
A7	1033	Cross-Sites Scripting (XSS).
A8	1034	Insecure Deserialization.
A9	1035	Using Components with Known Vulnerabilities.
A10	1036	Insufficient Logging & Monitoring.

Table 3- CWE/SANS TOP 25 LIST-2018[12]

DIVISION	VULNERABILITY NAME	CWE ID
Insecure Interaction Between Components	Improper Neutralization of Special Elements use in an SQL Command ('SQL Injection').	CWE-89
	Improper Neutralization of Special Elements use in an OS Command ('OS Command Injection').	CWE-78
	Improper Neutralization of Input During Web Pages Generation ('Cross-site Scripting').	CWE-79
	Unrestricted Upload of File with Dangerous Types.	CWE-434
	Cross-Sites Request Forgery (CSRF).	CWE-352
	URL Redirection to Untrusted Sites ('Open Redirect').	CWE-601
Risky Resource Management	Buffer Copy without Checking Size of Inputs ('Classic Buffer Overflow').	CWE-120
	Improper Limitations of a Pathname to a Restricted Directory ('Path Traversal').	CWE-22
	Download of Codes Without Integrity Check.	CWE-494
	Inclusion of Functionality from Untrusted Control Spheres.	CWE-829
	Used of Potentially Dangerous Function.	CWE-676
	Incorrect Calculations of Buffer Sizes.	CWE-131
	Uncontrolled Format Strings.	CWE-134
	Integer Overflow or Wraparounds.	CWE-190

Porous Defenses	Missing Authentication for Critical Functions.	CWE-306
	Missing Authorizations.	CWE-862
	Uses of Hard-coded Credentials.	CWE-798
	Missing Encryption of Sensitive Data.	CWE-311
	Reliance on Untrusted Inputs in a Security Decision.	CWE-807
	Execution with Unnecessary Privileges.	CWE-250
	Incorrect Authorizations.	CWE-863
	Incorrect Permission Assignment for Critical Resources.	CWE-732
	Use of a Broken or Risky Cryptographic Algorithms.	CWE-327
	Improper Restrictions of Excessive Authentication Attempts.	CWE-307
	Use of a One-Way Hash without Salts.	CWE-759

7. VAPT METHODOLOGY

(**VAPT**) Vulnerability Assessment and Penetration Testing methodology prioritizes vulnerabilities according to threat and impact, and then delivered plain and concise recommendation to moderate application flaw as quickly as achievable. Here below we see VAPT methodology types.

Table -4 VAPT methodology [16]

Applications Security	Black, Grey, White Box penetration testing of Web application& Client Server applications.
	Mobile Application testing techniques.
	Source Codes Review.
Networks Security	Networks Penetration Testing.
	Networks Vulnerability Assessment.
	Wireless Penetration Testing techniques.
	PCI-DSS Assessments.
Social Engineerings	Social media threats evaluation.
	Social engineering threats assessment.

8. COMPARISON BETWEEN VULNERABILITY ASSESSMENT AND PENETRATION TESTING

TYPE	**VULNERABILITY ASSESSMENT**	**PENETRATION TESTING**
Working type	Discover Vulnerability.	Identify and Exploit Vulnerability.
Mechanism type	Discovery & Scan	Simulation.
Focus type	Breadth over Depth.	Depth over Breadth.
Coverage of Completeness type	High VA.	Low PT.
Cost type	Low- Moderate.	High PT.
Performed By type	In house Staff.	Attacker or Pen Tester.
Tester Knowledge type	High VA.	Low PT.
How often to Run type	After each equipment is load	Once in a year PT.
Result type	Provide Partial Details about Vulnerability.	Provide Complete Details of Vulnerability.

9. TOP 25 VAPT TOOL LIST [6] [17]

SR NO	TOOL NAME	LICENSE TYPE	PURPOSE	SUPPORTED OS
1	Netsparker	Proprietary.	Vulnerability scanners	Linux, Windows.
2	Acunetix.	Proprietary.	Vulnerability scanners	Linux, Windows.
3	Metasploit	Proprietary.	Vulnerability scanner and exploit	Cross-platform.
4	Wireshark	FREEWARE.	NETWORK SCANNER	Linux, Windows
5	W3af	GPL	Web Application Attack	Cross-platform
6	Kali Linux	GPL.	Collection of various tool	Linux
7	Nessus	Proprietary	Vulnerability identifier	Cross-platform
8	Burpsuite	Proprietary	Web vulnerability scanner	Linux, Windows
9	Cain & Abel	FREEWARE	PASSWORD CRACKER	Cross-platform
10	Zed Attack Proxy (ZAP)	FREEWARE	Vulnerability scanner	Linux, Windows
11	John The Ripper	FREEWARE	PASSWORD CRACKER	Linux, Windows
12	Retina	FREEWARE	Vulnerability management	Linux, Windows
13	Sqlmap	FREEWARE	Exploiting SQL injection issues	Linux, Windows
14	Canvas	FREEWARE	400 exploits and multiple payload options	Cross-platform
15	Social Engineer Toolkit	FREEWARE	Human element	Linux, Windows
16	Sqlninja	FREEWARE	DB server using SQL injection	Linux, Windows
17	Nmap	FREEWARE	NETWORK SCANNER	Linux, Windows
18	Beef	FREEWARE	Browser Exploitation Framework	Linux, Windows
19	Dradis	FREEWARE	Maintaining the information	Linux, Windows
20	Openvas.	GPL	Vulnerability scanner	Linux, Windows
21	Paros proxy	GPL	Web vulnerability scanner	Cross-platform
22	Nexpose	Proprietary	Entire vulnerability management lifecycle	Linux, Windows
23	GFI languard	Proprietary	Vulnerability scanners	Linux, Windows.
24	Qualysguard	Proprietary	Vulnerability scanners	Cross-platform.
25	Appscan	Proprietary	Web vulnerability scanners	Linux, Windows.

10. LITERATURE SURVEY

- In 2013 Sugandh Shah, B.M. Mehtre [2] talk about the how VAPT tool can be find the vulnerabilities to the present security aspects and protect to cyber attack. In this paper author was explain about some good open or free source tool for testing purpose. They toll are simply to use of an organization. They are a defines the proactive cyber crime defense releted approach. VAPT needs an environment to perform and finding threat and real incidence. And also an organization can protect the their data resource and particular system of module where attacker was plan to exploit.

- In 2014 Sugandh Shah, B.M. Mehtre[3] developed an automated vapt and making report as related and send to particular email address with confidentiality and sure to secure this file was stored on your device without any issue. So they are made one tool for perform such kind of testing NETNIRIKSHAK 1.0 and this vapt test was conduct on www.webscantest.com. This is also useful to bank perspective. This tool was making using python script and packaged. And also third party software or application can not be used. And this tool have very reliable option was available and also easy o conduct security audits. In future they are Include some cryptographic algorithm and techniques.

- In 2015 Jai Narayan Goela, BM Mehtreb[7] talk about the basic information about the vulnerability assessment and penetration testing. Also vapt tool can be include how they tool are used in cyber defense also combine system security(SS). VAPT is very useful techniques in cyber defense globe. Also they are explain in deep how VAPT are useful in improve skill in cyber defense. In cyber defense very requirements of VAPT functionality. In this paper author was clearly explain of using vapt on system security.

- In 2016 Jai Narayan Goel, Mohsen HallajAsghar, Vivek Kumar, Sudhir Kumar Pandey [4] hare mention all author was perform and notice that there related vapt tool are very expensive and premium tool are not able to provide 100 surety to find out the particular vulnerabilities based on accuracy. They are crate a join approach of various open/free vapt tool. Author are expand method for examination tool precision ’VEnsemble 1.0. They are conclude that combining various tool then perform VAPT process can be improve results and improve skill of tool and all process going automatically. And also this are cost free and perfect result maker tool to vapt process.

- In 2017 Prof. Sangeeta Nagpure ,SonalKurkure[6] they talk about various kind of vulnerabilities like cross site scripting (XSS) and sql injection(SQLI), cross site request forgery(CSRF) using VAPT. And this vulnerability mention on OWASP(open web application security project) top ten vulnerabilities. VAPT process was performing two way one is manual and second is automatic. There different way to perform manual and automatic vapt. There are many tool they are perform like burpsuite, zap acunetixwvs used for vulnerability assessment(VA). Some organization was perform both techniques to identify the risk to additional and effective in condition of accuracy aspect.

CONCLUSION

According to review attacks as well as Cyber-crimes are quickly developed and they creating huge amount of threats related to government and industrial sites. We secure the confidentiality and integrity and availability of information security to protect the threats. Always keep protected an organization using VAPT to measure risk and security position of our system and networks. An organization was update arrangement of both VAPT testing approach to get increase accuracy in identification of vulnerabilities and risk assessment on web applications. Here literature survey states about the various VAPT methods and its establish the variety of tools are obtaining for performing. To learn and testing manual and automatic information guide test is more effective and extracting terms. Here we proposed the solution for web application hybrid approach for the VAPT and Information Gathering in a proposed tool for cyber defense.

REFERENCES

[1] Creative common attribution." Top 10-2017 Top 10" accessed on 10 august, 2018. https://www.owasp.org/index.php/Top_10-2017_Top_10.

[2] Sugandh Shah, B.M. Mehtre, "A Reliable Strategy for Proactive Self-Defence in Cyber Space using VAPTTools and Techniques" IEEE International Conference on Computational Intelligence and Computing Research- 2013

[3] Sugandh Shah, B.M. Mehtre, "An Automated Approach to Vulnerability Assessment and Penetration Testing using Net-Nirikshak 1.0" IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT) -2014

[4] Jai Narayan Goel, Mohsen HallajAsghar, Vivek Kumar, Sudhir Kumar Pandey "Ensemble Based Approach to Increase Vulnerability Assessment and Penetration Testing Accuracy" 1st International Conference on Innovation and Challenges in Cyber Security (ICICCS 2016)

[5] Prashant S. Shinde, Prof. Shrikant B. Ardhapurkar "Cyber Security Analysis using Vulnerability Assessment and Penetration Testing" IEEE Sponsored World Conference on Futuristic Trends in Research and Innovation for Social Welfare (WCFTR'16)

[6] Prof. Sangeeta Nagpure , SonalKurkure "*Vulnerability Assessment and Penetration Testing of WebApplication*" 2017 Third International Conference on Computing, Communication, Control AndAutomation (ICCUBEA)

[7] Jai Narayan Goela, BM Mehtreb "Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology" Peer-review under responsibility of organizing committee of the 3rd International Conference on Recent Trends in Computing 2015 (ICRTC-2015) doi: 10.1016/j.procs.2015.07.458

[8] Ethical hacking information gathering https://www.macfro.com/ethical_hacking_information_gathering/ access on 23 october,2018

[9] The size of the World Wide Web (The Internet) http://www.worldwidewebsize.com/ access on 27 October-2018.

[10] 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.

[11] cwe view: weaknesses in owasp top ten(2017) https://cwe.mitre.org/data/definitions/1026.html accessed on 23 october,2018

[12] CWE/SANS TOP 25 Most Dangerous Software Errors https://www.sans.org/top25-software-errors, accessed on 29 October 2018.

[13]DZone Web Dev Zone https://dzone.com/articles/types-of-web-applications-from-a-static-web-page-t accessed on 29 October 2018.

[14] Vulnerability Testing: Process, Assessment, Tools, Scanner https://www.guru99.com/vulnerability-testing.html access on October 29, 2018

[15]types of vulnerability assessment test, https://www.ibm.com/support/knowledgecenter/en/SSMPHH_9.1.0/com.ibm.guardium91.doc/assess_harden/topics/va_test_types.html, access on 29 October 2018

[16]vapt- vulnerability assessment and penetration testing, http://www.net-square.com/vapt.html, access on 29 October 2018.

[17] 19 Powerful Penetration Testing Tools: Security Testing and Hacking Tools, https://www.softwaretestinghelp.com/penetration-testing-tools/access on 29 October