**CHAPTER 1**

**INTRODUCTION**

**Company Overview:**

Andhra Pradesh Technology Services Limited (APTS) is an Andhra Pradesh State Government undertaking company incorporated under the Companies Act, 1956 focusing on e-Governance. It provides consultancy, procurement services, and implementation support to the government entities for their IT/ ICT related initiatives.

APTS is a pioneer in consultancy services to all State Government Departments of Andhra Pradesh. In the year 1983, Andhra Pradesh State Government approved a policy framework to introduce computers in government departments and constituted a study group for identifying areas of application. The Study Group recommended setting up an organization to provide system development including research, maintenance (AMC), training and computer operations including data preparation services.

The Government accepted recommendations of the study group and constituted an organization named 'Andhra Pradesh Technology Services Limited' and registered it under the Companies Act 1956 in the year 1986. While APTS was kept under the administrative control of the Finance & Planning (Planning Wing) Department vide G.O Ms.No.71 Finance & Planning Department dated 30th December 1985, it was brought under the administrative control of IT & C department on creation of a separate department for Information Technology.

The different services providing by the APTS are hardware and software procurement, Networking, office automation, communication, software development, training, customer support service, IT Security & IS Auditing.

Audit Team:

For providing the IT Security & IS Auditing consulting services APTS has deployed a team that will perform the VAPT of different applications and infrastructures of the Andhra Pradesh government.

The team will provide services in these security domains:

* Infrastructures and networks
* Web applications
* Mobile applications

**OUTLINE:**

The majority of IT companies and many organizations are using web applications for their business use or information sharing. Due to the increase, the usage of internet the accessing on web applications from anywhere made easy and has become essential in the daily lives of people, business and all organizations.

A web application will commonly use the web application servers and database servers as a backend to work a web application smoothly. These backend servers are very crucial for running applications and storing highly valuable data. So, a web application is becoming an important target for cyber attackers. In order to protect the confidential data stored by web application the security mechanism must be implemented and nowadays providing security for web applications has become one of the big concerns.

Different vulnerabilities will be available in the web application and these vulnerabilities will change based on the front end and backend technologies used by a web application. vulnerability is a security weakness or a loophole that will take advantage of the attacker or malicious users to gain unauthorized access. Day by day the web application usage has increased, and the new vulnerabilities are also increasing.

The vulnerabilities in web applications will incur due to the security misconfigurations, programming mistakes, improper usage of security measures, etc. So, vulnerability assessment and pen testing will help to figure out the different vulnerabilities present in web applications. The websites are also using to deliver the critical services to its customers so it must run each and every time without any interception, in order to do this VAPT will play a crucial role.

The web application will be developed and deployed on the complex infrastructure and different development technologies so there will be an inconsistency due to a huge range of technologies and secure development can also be error-prone and can lead to vulnerabilities so VAPT can be the important factor in finding the vulnerabilities.

Web Application Security Consortium, about 49% of the web applications being reviewed contain vulnerabilities of high-risk level and more than 13% of the websites can be compromised completely automatically [2]. A recent report [3] reveals that over 80% of the websites on the Internet have had at least one serious vulnerability.

**Report contents**

This report is organized as follow chapter 2

**Chapter 2**

**Introduction to Web Applications**

The Web Application Security Consortium (WASC) defines a web application as “a software application, executed by a web server, which response to dynamic (or) static web page requests over HTTP.”A web application will commonly consist of different components in order to render the specific page requested by the user from the server. The different components available are the client(browser) in order to request the resource, internet in order to pass the request and response, server in order to process the request, store the web application pages, database in order to store the data.

A web application consists of a series of scripts, style sheets, Html pages, images, etc. that reside on a web server and communicate with dynamic content repositories or other sources. Using Internet infrastructure, web applications enable service providers and consumers to exchange and manipulate information.

In web application development, front-end development and backend development technologies will be used. The front-end development technologies will use for building the user interface and look and feel. The different programming languages that will be used are HTML, CSS, JavaScript, Angular JS, etc. The back-end development technologies will use for building the functionalities, working, and behavior of web applications. The back-end technologies will include server-side scripting languages like PHP, Java, Python, etc., Databases like MySQL, MsSql, oracle, etc., frameworks. The different technologies that are being used in a web application are shown in the below image.

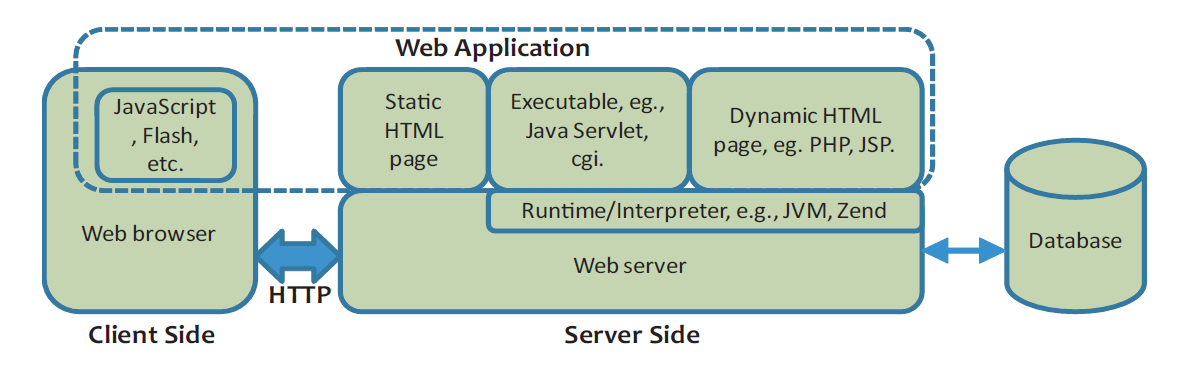


Figure 1. Web Application Environment

There are two kinds of a web application that is static and dynamic. In a static web application, the content will not be change based on users’ roles it primarily used to provide or share the information. The example of static application is Wikipedia.in dynamic web application the content will change based on the user role.

Basically, HTML (Hypertext Markup Language) will be used in order to design the basic skeleton of a web application. By HTTP (Hypertext Transfer Protocol) the communication between the client and server will happen in form of request and response. The HTTP request will request the resource from the server and the HTTP response will help to get data from the server that is being processed by the server.in order to request the resource from the server. The HTTP request will have methods like GET, POST, PUT, DELETE, TRACE, HEAD, OPTION, CONNECT. Based on the required information the methods

will be used. The HTTP request and response will also contain request and response headers and will be discussed in detail in VECHAPER.

A web application has a distributed n-tiered architecture. Typically, there is a client (web browser), a web server, an application server (or several application servers), and a backend (database). Figure 1 represents the communication flow of web application request and response. and There may be a firewall, proxy servers, WAF’s in between web client and web server for additional security.



Figure 1. Web Application Environment

Basically, the web application will contain the client, server, database. The client is a browser which maybe Firefox, chrome, etc. The server will help to process the request and helps to store the resource also. There will be different servers but will be used based on programming languages, basically used servers for web application is apache, Nginx​, Internet Information Services​, Tomcat​,Lighttpd​.database will help to store and manage the huge amount of data in an organized manner. The basically used databases are Oracle ​, MySQL​, Microsoft SQL Server​, PostgreSQL​, MongoDB​, MariaDB​, Amazon EC2​.