**Server-Side Web Scripting Technologies**

Are used for back-end web development technologies that includes the software built by server-side scripts, database/operating system and other server-side languages. The focus for our website mainly covers Java Web Servlets and Java Server Pages (JSP), PHP, Server-Side JavaScript (with Node.JS), and Web Application Security.

**Back-end Overview**

The back-end for a website comprises three parts which are the server, database, APIs, and a back-end web application that is written with server-side languages. The function of a server enables back-end software, while the database stores the website’s data. This would allow the user’s information to be gathered from a networking site with the server-side scripts that the user has input.

**Java Web Servlet**

A servlet is a java programming language class that extends the attributes for the servers to host the applications that is being accessed in a request-response paradigm. In addition, a java servlet allows the web server to be accessed by web developers in a simpler or efficient way in business systems. It serves as a Java platform technology provided in a component-based, platform-independent method in the structure of web-based application.

**Java Server Pages(JSP)**

The technology provides easy and fast development for web developers and web designers in a dynamic web page that has an advantage for business systems. Java Server Pages is platform independent meaning, it could be on any operating system without requiring the Java Virtual Machine(JVM). Moreover, the technology separates the User Interface(UI) from the content and enables web designers to change the layout of the web page without changing the primary dynamic content.

**Java Web Servlet vs. Java Server Pages(JSP)**

Java Server Pages is an extension of Java Servlet technology. The Java Web Servlet is a server-side module perfectly fits in a Web Server framework. Moreover, Java Server Pages(JSP) technology uses XML tags which summarizes the logical content of the webpage. The extension of Java Server Pages is embedded with a Java code into an HTML code while the Java Web Servlet, are Java classes that extends HTTPServlet, GenericServlet and implement Servlet Interface. Java Web Servlet declares a servlet in a web.xml configuration file and modifies the servlet into WebServlet for the web container.

**Java Web Server and Java Server Pages (JSP)**

What are Java Server Pages or JSP for short? These are technologies that helps the software developer create a dynamically generated web page or pages which are based on HTML, XML and other document types. Sun Microsystems released JSP in the year 1999. JSP may be compared to PHP and ASP as they are somewhat identical but what separates JSP is that it uses Java Programming Language.

JSP is viewed as a high-level abstraction of the Java Servlets. Translation of the JSP to Servlets happen during runtime, then each of the translated JSP Servlet is cached and re-used until the modification of the Original JSP is completed. JSP may be used independently or as a view component of a server-side in a model-view-controller design, that is used normally with JavaBeans as the model and Java Servlet. Like any other Java program, JSP is required to be executed within the Java Virtual Machine or JVM that is interacting with the server’s host Operating System in order to provide an abstract, platform-neutral environment. HTML and XML documents are usually associated with JSP but through the use of Output Streams. Several delimiters are used by JSP for the scripting functions.

**Scriplet**

The <% %> is used to contain fragments of the Java code that is a part of the Service() Method. While <%! %> declares the instance variables and functions for the Servlet class. Moreover, <%= %> is an expression Scriplet that is used for printing on page. Lastly, <%@ %> a Directive that gives direction to process a JSP page.

**PHP**

**Overview:**

PHP: Hypertext Preprocessor or PHP for short is an open source general-purpose that is widely-used for scripting language that is especially suited for web development. Ramsus Lerdorf is the creator of this web scripting language in the year 1994 and before becoming PHP: Hypertext Preprocessor, PHP stood for “Personal Home Page”. The PHP code may be embedded into a HTML code, or may be combined with various web template systems, content management, and frameworks. Usually, PHP codes are processed by a PHP interpreter implemented as a module in a web server or as a Common Gateway Interface executable or CGI for short. This is powered by Zend Engines, which is a free software that was released under the PHP License. It was not until the year 2014 where in the language evolved without a written formal specification or standard. This left the canonical PHP interpreter as a real o0r effective standard. PHP hosts a wide range of diverse arrays of web frameworks which require framework-specific knowledge. It is also an "HTML-embedded scripting language" used by developers with a simple and dynamic design for a website or web application. It is an open source scripting language that is being executed in a server mostly Apache, IIS, and many more. It also runs easily in a server side and almost all platforms like Windows, Linux, Unix, Mac OS X, etc. and supports a lot of database. PHP code can only be executed on PHP-enabled computers since the code is running in a plain-text script.

**History Timeline:**

PHP was written by C programming language by Rasmus Lerdorf in 1994, then PHP/FI or PHP 2.0 in June 8, 1995, followed by PHP/FI 2 by Zeev Suraski and Andi Gutmans in 1997, nevertheless, PHP 3 in 1998, and PHP 4-Zend Engine 1.0 in May 2000, lastly, PHP 5-updated Zend Engine 2.0 released in July 2004.

**PHP 3.0**

Developed by Andi Gutmans and Zeev Suraski of Telaviv, Israek in 1997. Since PHP/FI 2.0 is ineffective and lacks features in the applications to be developed, they both redeveloped the project with implementing some configurations on the PHP/FI’s engine and user perspective preference. This was the version that PHP/FI 2.0 has changed to the name – PHP: Hypertext Preprocessor that includes object-oriented programming support with a powerful language syntax.

One of the advantages of PHP 3.0, is that it has flexible features. In addition, it provides end users with an interface that has multiple database, protocols, and APIs. The features have attracted a lot of developers that submitted different kinds of modules.

**PHP 4**

Developed by Andi Gutmans and Zeev Suraski in the year 1998. They both begun the rewrite of PHP with the improvements of the performance of applications and modules in the main PHP’s code base. The applications were made by the features of PHP 3.0 and supports third party database and APIs.

The engine was named ‘Zend Engine’ which was derived from the names of Andi and Zeev, has expectedly captured perfectly the goals of the design they were after and was introduced in year 1999. The features of PHP 4.0 include key features of support for web servers, HTTP sessions, output buffering and more security for user input and others

**PHP 5**

Developed by Andi Gutmans and Zeev Suraski in July 2004. The ‘Zend Engine’ is changed to Zend Engine 2.0 that includes a new object model and new features. The development team already has a lot of developers in PHP projects with support which are PEAR, PECL, and documentation. In addition, the fundamentals of network for infrastructure are distributed over the world in millions of domains.

**PHP Basic Syntax**

The Basic Syntax for PHP is usually developed with an output on the server. The PHP script is placed in a document that uses a tag and starts as “<?php” and ends as “?>:”. The PHP file includes the HTML tags and scripting codes for the PHP. In writing comments in PHP, the line in the code is usually not read by programmers but only used to check if the code is correct. The comments for PHP let’s programmers know what you are doing and helps track down the code you have done before with its function may it be additional things to do or a lack of function. In addition, PHP code with the terms used or keywords like: if, else, while, echo and many other more are NOT case-sensitive.

**PHP Variable**

For declaring variables in PHP, you should start with a “$” sign and next is the variable name. The variable is recommended to place a detailed name like: length, age, total\_height, dogname, and others. In addition, every time you code, the variable name should start with a letter or underscore and the variable name must not start with a number or the code won’t work. Since the terms or keywords in the basic syntax for PHP are NOT case-sensitive, the coding for PHP variable names are CASE-SENSITIVE.

The PHP Variable includes different scopes that is part of the script in PHP that is used for quotations. The scopes are: local, global, and static. For global and local scope, the variable is declared outside in a function and can only gain access outside of a function and the local scope is only accessible within a function. In addition, the global term/keyword is accessed in a global variable inside a function. The global variables are stored in an array called “$GLOBALS[index]” that holds the name of the variable and access inside the functions and could updated directly from the global variable. Lastly, the static term/keyword in PHP lets the functions that are completed, to let all the variable diminish or removed. Whenever the function is called, the variable would then still have the data to be included.

**PHP Data Types**

The PHP data types allow variables to store data in different types. PHP upholds integers, string, Boolean, float, array, null, object, resource. Firstly, the Php data type: Integer contains numbers that are non-decimal and the numbers should be within a range of -2,147,483,648 and 2,147,483,647. The string is an order of symbols that are used inside a quote. The Boolean symbolizes the x and y for True and False and booleans are usually used for conditional testing. The float in PHP data type is used in numbers with an exponent or a number with a decimal point. The array is used to store various variables or a single variable. The PHP Null value is a special data type because it is restricted to only one value called NULL and the data type of variable has no assigned values to it. However, if the variable is invoked without a value, then it is NULL, and the variable can be voided by the condition of value to NULL. The PHP Object data type allows how the data is being processed from the storage of data and information. Lastly, PHP resource is not a data type but it stores quotations to the functions and external resources in PHP.

**Server-Side JavaScript (with Node.JS)**

* Node.js basically is a server-side JavaScript that is built on Google V8 JavaScript engine. Developed in year 2009 by Ryan Dahl, this programming language is an open source that is very fast compared to other server-side programming languages that is written in the C programming language. In addition, JavaScript with Node.js with the server-side language PHP.Node.js, uses a powerful tool to run JavaScript applications frameworks, servers of HTML 5, and messaging middleware. Node.js runs on server-side applications that builds real-time Web APIs. Though Node.js is not a framework, it is a highly modified server engine with libraries like HTTP, SSL, compression, filesystem and many more connectors that builds a simple yet dynamic web server of JavaScript. Moreover, Node.js was sponsored by a software company called Joynet that specializes in high implementation of the infrastructure which can be run on multiple platforms like Windows, Mac OS X, Linux, and many more.

**Node.js**

In the year 2009, the JavaScript-based Node.js platform was introduced by Ryan Dahl for the Linux and Mac OS as an alternative to Apache HTTP Server. The high level Node.js combines the Google V8 JavaScript engine. Node.js is an open source server environment which is free. It runs on various platforms such as Windows, Linux, Unix, Mac OS X, and others. Node.js uses an Asynchronous programming method. Some common tasks for a web server is to open files on the server and return the content to the client. Node.js handles file requests wherein it sends the task to the computer’s file system, then handles the next request. When the file system has opened and read the files, it returns the content to the client. Node.js is a single-threaded, non-blocking, asynchronous program which is very memory efficient and this eliminates waiting and is simply continuous with the next request. Node.js can generate dynamic page content and also open, read, write, delete, and close files in the server. It also collects data which can be added, deleted, or modified in one’s database. A Node.js file contains the tasks that will be executed in certain events for example; someone is accessing a port on the server. The files must be initiated in the server before having its purposed effect. A brief history of JavaScript is that, in the year 1995, a contractor to Netscape named Brendan Eich created the JavaScript Language in order to run web browsers. It was initially intended to have enabled animations and other manipulations of a browser’s document object model or DOM. Shortly afterwards a version of JavaScript for the Netscape Enterprise Server was introduced. The name of JavaScript was chosen for the marketing purposes because of the Sun’s Java language was a widely famous at that time. JavaScript was based primarily on the scheme and self-languages together with superficial Java-like semantics.

**Running JavaScript on a Server**

* JavaScript that runs on a server uses a virtual machine or a JavaScript engine code for hosting with the v8 environment. Node.js runtime system builds a network with other event-based application servers

**Other server-side web scripting technologies:**

**Active Server Pages (ASP/ASP.Net)**

* Developed in the year 2002. Active Server Pages (ASP/ASP.Net) is a server-side web framework with the structure of modern web applications and development of web pages that includes the services of .NET. ASP.NET in the creation of HTML5, CSS, and JavaScript. ASP.net runs on .NET Core or .Net Framework, Cloud, and multiple platforms like Windows, MAC OS X, and Linux.

**ASP.NET Core**

* it is a cross- platform framework with high implementations for the development of cloud-based web applications. The framework supports the creation web applications and services that includes Internet of Things (IoT) applications for mobile backend. In addition, ASP.NET Core utilizes in the development of Web User Interface (UI) and Web Application Interface (API), development of workflows, and could be hosted on IIS, Ngingx, Apache, Docker, and many more.

**ASP.Net**

ASP.Net is a web development platform that provides a programming model which is a comprehensive software infrastructure and some various services required to build up a robust web application on either PC or mobile devices. HTTP protocol work on top of ASP.Net and uses its commands and policies to set a browse-to-server bilateral cooperation and communication. ASP.Net applications are built up of compiled codes, written using extensible and reusable components or objects present in the frameworks. Applications of ASP.net can be written in C#, Visual Basic.Net, Jscript, and J#. ASP.Net is a upgraded version of the Active Server Pages or ASP for sort. This has been designed to work smoothly, with the WYSIWYG HTML editors and some of the programming tools which includes Microsoft Visual Studio.Net. While making web development easy additional functions of ASP.Net provides all of the benefits that the tools have to offer that includes GUI developers that may drop server controls into a web page with a fully integrated support for debugging. Other Developers may use Web Forms or XML web services in the process of creating an ASP.Net application or in other cases combine these in any way the developers see fit. Supported by the same infrastructure that allows the use of authentication schemes, cache the frequently used data, customization of the application’s configuration and many more, which makes ASP.Net an asset to developers who choose to study this tool for an easy web development tool. This Open-source server-side framework for web applications is usually used to produce dynamic web pages. Developed by Microsoft, they allowed programmers build dynamic web sites, applications, and services. It was initially released on the 5th of January in the year 2002 with the version 1.0 of the .Net framework. It is built on a Common Language Runtime or CLR for short, which allows the programmers write ASP.Net code using any of the .Net languages. The Code-behind model places the codes in a separate file or in a special designated script tag. Examples of Code-behind files are in the format “SamplePage.aspx.cs” or “SamplePage.aspx.vb” while in the page is “SamplePage.aspx”. This is an automatic format for Visual Studio and other IDE’s. Directives are special instructions on the processing of the pages in ASP.Net should be. These Directives are the application Directive, Assembly Directive, Control Directive, Implements Directives, Import Directive, Master Directive, MasterType Directive, OutputCache Directive, Page directive, PreviousPageType Directive, Reference Directive, and the Register Directive.

**Ruby on Rails**

Ruby on Rails is a web application development framework. Its main purpose is to make programming web applications easier through making assumptions about the developers need in order to get started. Less code is definitely in the picture when it comes to Ruby on Rails while accomplishing more than any other languages and or frameworks. Developers that are experienced had also testified that web development became fun through this. Model-View-Controller or MVC framework for short provide a default structure for a database, web service, and web pages. This facilitates the web standards such as JSON or XML documents for data transfer together with HTML, CSS, and JavaScript in displaying the user interface. Rails also emphasize the use of other known software engineering patterns together with paradigms, includes Convention Over Configuration (CoC), Don’t Repeat Yourself (DRY), and active record pattern. David Heinmeier Hansson extracted Rails from his own work on the project management tool Basecamp at a web application company which also called Basecamp. The first release on Rails was on July of the year 2004, but the sharing of commit right was not established until the month of February of the following year. A milestone achieved by Rails was when Apple agreed to release the Mac OS X v10.5 “Leopard” together with Rails which happened in the year of 2007 of October.

**Version History:**

* Rails Version 2.3, released on the 15th of March in the year 2009 with new developments in the templates, engines, and with the Rack and nested model forms. Templates are now enabled with the generation of a skeleton application with the custom gems and configurations.
* Rails Version 3, whereas Merb, a web application framework, was launched on the 23rd of December of the year 2008. Merb was merged as part of the Rails Version 3.0 release.
* Rails Version 3.1, released on the 31st of August in the year 2011 with the features of reversible Database Migration, Asset Pipelines, Streaming, jQuery as the default JavaScript library and as a new feature that is CoffeeScript and Sass into the stack.
* Rails Version 3.2, released on the 20th of January in the year 2012 with the faster development mode and routing engine. Rails version 3.2.x is the last of this version that supported Ruby 1.8.7.
* Rails Version 4.0, released on the 25th of June in the year 2013 which introduced Russian Doll Caching, Turbolinks, Live Steaming together with Active Resources, Active Record Observer and other components in splitting it as gems.
* Rails Version 4.1, released on the 8th of April in the year 2014 that introduced Spring, Variants, Enums, Mailer previews and the Sercrets.yml.
* Rails Version 4.2, released on the 19th of December of the year 2014 that introduced Active jobs, Asynchronous emails, Adequate Record, Web Console and Foreign keys.
* Rails Version 5.0, released on the 30th of June in the year 2016 with added functions and introduced Action Cable, API mode, and a new version of TurboLinks which is TurboLinks 5.
* Rails Version 5.0.0.1, released on the 10th of August in the year 2016 with the Exclusive use of Rails CLI.
* Rails Version 5.1, released on the 27th of April in the year 2017 that introduced JavaScript interrogation changes which uses the system test of Capybara, Encrypted secrets, parameterized mailers, and direct resolved routes.

**Common Gateway Interface (CGI)**

The Common Gateway Interface(CGI) is the condition for transmitting information or data between a web server in the World Wide Web and a program of the Common Gateway Interface that determines a paradigm information variable. The program transfers languages like C, Perl, Java, and Visual Basic. CGI programs work in many HTML web pages with forms of data and can be written in any programming language. It is usually executed on a computer to generate web pages dynamically.

In all operating systems, the interface is executed in system variables. For Invocation, the client indicates the URI name of the program to be invoked and the program should be implemented in a specific location at the web server. Lastly the execution, the server distinguishes from the URI by which the request resource could be deployed. Requirements for the execution is that is must meet the set permissions for the web server in allowing the program execution and the extensions for the executable files in the server should be indicated. In addition, for execution, the web server interprets the specification that the client has sent to be able to commence the CGI variables. Then the program from the server is executed in a new method that prints the feedback on the output and builds the feedback from the content that has been eliminated to the output and is sent to the client.

**CGI development**

The client parameters that are to be developed in CGI with Handling request parameters are: HTTP GET method and HTTP POST method. The HTTP GET method are added to the web page URL and the HTTP POST method parameters are instead inserted as an entity for the body of the request HTTP. This requires the use of HTML forms, so that the users could input data in a body of the request.

Since the program can be written in any programming language, then for a compiled programming language the source code should also be compiled normally. As for interpreted scripting language, the files are also deployed. CGI variables comprises of server, request, and headers.

The server variables use a naming convention of SERVER\_SOFTWARE that is to be used for the renaming of name and the change of version in the server software. While SERVER\_NAME allows the hostname or IP of the web server, and the GATEWAY\_INTERFACE is a supported version for the CGI. For the request variables, the variables use the name: SERVER\_PROTOCOL to transfer the protocol name and version, while the SERVER\_PORT links the port to which request it is sent, the REQUEST\_METHOD requests method for HTTP, PATH\_INFO authorizes additional path information, SCRIPT\_NAME invokes the URL with script, and QUERY\_STRING is the query string. Last in the list would be - Environment variables for the headers. The environment is a storage for HTTP headers that contains request. The following are naming conventions used for environment variable headers: HTTP\_USER\_AGENT – it is used for request of browser, HTTP\_ACCEPT\_ENCODING – the client receives the encryption type, HTTP\_ACCEPT\_CHARSET – the client receives a charset, HTTP\_ACCEPT\_LANGUAGE – the client receives the language.

**The Problems with CGI**

The problems with CGI is that whenever a server receives a request, the server creates a new method in order to execute the CGI program that requires a lot of time and a server with substantial resources. The CGI program could not be connected back to the web server. Moreover, the system of the CGI program has ended when the program is finished. This emphasizes the main memory protection of the user’s session. Another problem to be encountered is that a user for example would expose their physical path to an executable program in the web, then it would be compromised.

**Top 10 OWASP Application Security Risks in the Year 2017:**

**The first application is Injection.** The application Injection happens when the suspicious data is being sent to an interpreter in a macro/command or query. It basically makes the hacker attack with a suspicious data and deceives the interpreter in making unintentional commands or accesses the data without permission.

**The second application is Broken Authentication.** The application lets the user accounts compromised by hackers and to exploit usernames, passwords, keys and other personal information. The session management is the foundation of all authentication and access controls, so hackers can identify the application – Broken Authentication with tools that have an index of all password lists and dictionary.

**The third application is Sensitive Data Exposure.** Hackers target protected data in many credit cards, identity theft and many more other crimes. The sensitive data for users could be penetrated without additional security. For example: In a browser, a hacker decides to attack a user in its credentials with retrieved previous passwords in a database using Graphics Processing Units (GPUs).

**The fourth application is XML External Entities(XXE).** The application allows hackers to utilize the vulnerability of XML processors to upload XML that comprises of suspicious content in an XML document. The types of attacks by hackers in this case comprises of internal file sharing, internal port scanning, URI handling and denial of service attacks.

**The fifth application is Broken Access Control.** The application lets the hackers detect the deficiency of access controls without the verification if the function is present. The reason for vulnerability is because the restrictions that provided for authenticated users are not properly implemented. The attacks include exploitations such as the access of unauthorized data, access to user accounts, privilege to view sensitive files, modification of authorized data, and remove the credibility of the user.

**The sixth application is Security Misconfiguration.** The application is a common issue because of the default configuration that hackers could attack easily. The default user accounts that includes passwords and all the configuration without updating regularly all the ad hoc, open cloud storage, HTTP headers, and other sensitive containing information would definitely make an easy target for hackers.

**The seventh application is Cross-Site Scripting (XSS).** The hacker uses suspicious data with a HTML snippet – an automated tool that could exploit all the Cross-Site Scripting that works as a framework, to hack the credentials of authenticated users. The application is the second most common issue in the top 10 OWASP application security risk. In addition, the automated tools could detect automatically the problems of XSS which are PHP, J2EE/JSP, and ASP.NET.

**The eight application is Insecure deserialization.** The application is all about remote code execution which is the most dangerous attacks made by hackers. Moreover, the type of attack includes, replay attacks, injection attacks, and privilege escalation attacks.

**The ninth application is Using Components with Known Vulnerabilities.** The attack can be initiated and can be overpowered if only the components of the applications that includes the libraries, frameworks, and software modules are exploited, then the attack would allow serious data loss or server control. In addition, applications and APIS that are common for hackers to penetrate, would compromise the security for application defense and other various-enabled attacks.

**The tenth application is Insufficient Logging and Monitoring.** Hackers attack through the system with tampering, extraction or collapse of data by the patience in timely for the monitoring and finishing the goal without getting caught. A successful attack by a hacker is determined with vulnerability searching by which it allows searching to continue to raise likelihood of successful exploits.