Centro de Enseñanza Técnica Industrial

Plantel Colomos

Ingeniería en Desarrollo de Software

Nombre Alumno: José Rafael Ruiz Gudiño

Registro: 20110374

Desarrollo Web II

Actividad Integradora

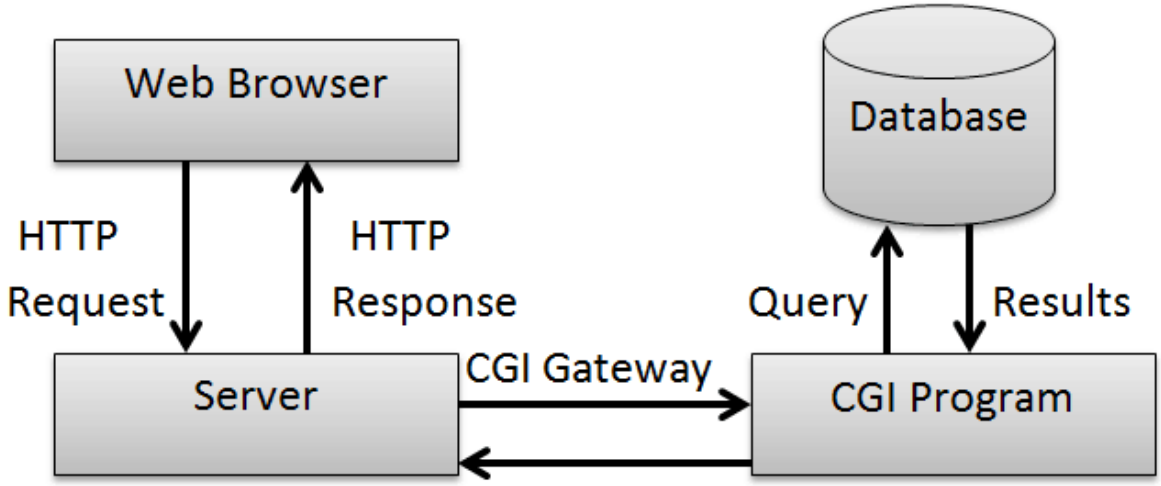
5°P

T/M

22/06/2022

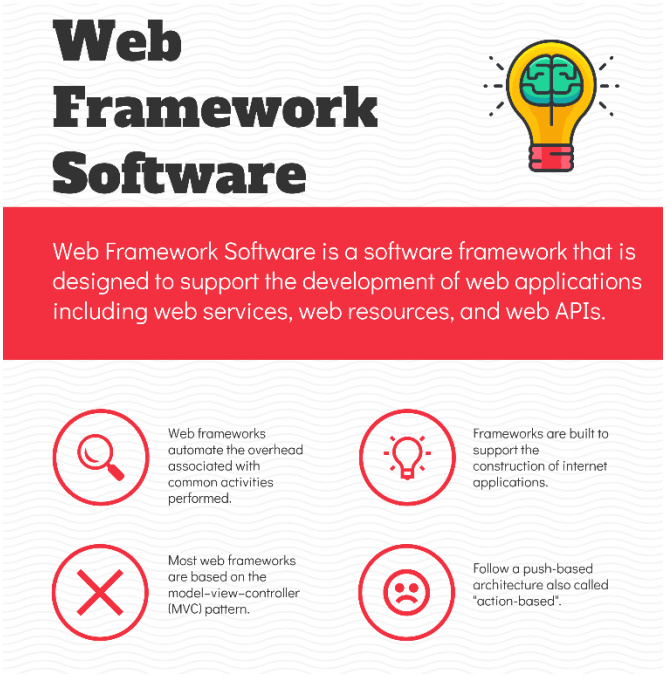
CGI

La interfaz de puerta de enlace común (CGI) proporciona un software intermedio entre el servidor WWW y bases de datos externas y fuentes de información. El Consorcio World Wide Web (W3C) define la interfaz de puerta de enlace común (CGI) y también cómo los programas interactúan con los servidores del Protocolo de transferencia de hipertexto (HTTP). Los servidores web suelen pasar la información del formulario a pequeñas aplicaciones que procesan los datos y posiblemente envían mensajes de confirmación. Este proceso para pasar datos entre un servidor y una aplicación es a lo que se le llama Common Gateway Interface (CGI).



Framework

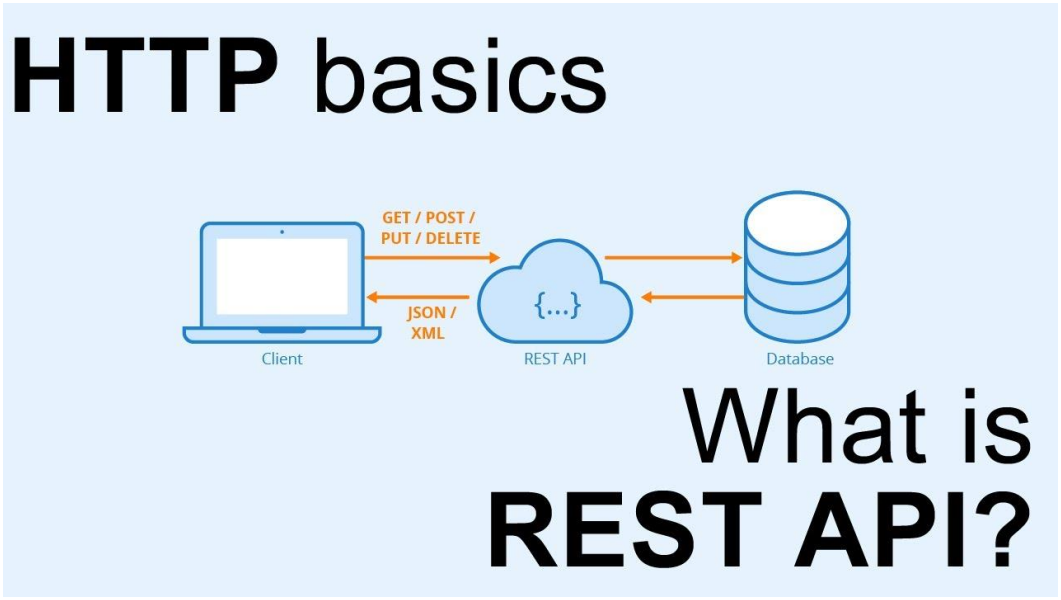
Un framework es el software que proporciona el soporte básico y la guía para la estructura que se está construyendo. Es una herramienta que proporciona componentes o soluciones personalizadas listas para usar para acelerar el desarrollo de software. Los frameworks pueden incluir bibliotecas. Utilizando la programación tradicional, el código personalizado llama a la biblioteca para acceder al código repetitivo. Con IoC, el marco recurre a fragmentos de código personalizados cuando es necesario.



Api REST

Una API o interfaz de programación de aplicaciones es un conjunto de reglas que definen cómo las aplicaciones o dispositivos se conectan y se comunican entre sí. Una API REST es una API que se ajusta a los principios de diseño REST o estilo arquitectónico de transferencia de estado representacional. Por lo que, las API REST a veces se denominan API RESTful.

REST, ofrece a los desarrolladores un grado relativamente alto de flexibilidad y libertad, por lo que las API REST se han convertido en una forma común de conectar componentes y aplicaciones en una arquitectura de microservicios.



Forma de configurar PHP

CGI y configuración de comandos: Por defecto, PHP se construye como un programa CLI y CGI, que puede ser utilizado para el procesamiento de CGI. Si se está ejecutando un servidor web PHP tiene soporte para los módulos, que por lo general debe irse por esta solución por cuestiones de rendimiento. Sin embargo, la versión CGI permite a los usuarios ejecutar diferentes páginas con PHP bajo diferentes identificadores de usuarios.

WinCache: Se recomienda que se use WinCache si se utiliza IIS, especialmente en un entorno de alojamiento web compartido o si se utiliza un NAS.

IIS: En el Administrador de IIS, se debe instalar módulo FastCGI y añadir un manejador para archivos .php.

Bases de datos: Las bases de datos populares proporcionan extensiones de PHP para utilizarlas. Si el sitio web no tiene mucho tráfico, se puede ejecutar el servidor de bases de datos en el mismo servidor web.

Forma de configurar APACHE

ServerRoot: Especifica el directorio en el que está instalado el software del servidor. aquí se encuentra el servidor y todos sus ficheros auxiliares, y también en él se encuentra una serie de subdirectorios como conf, htdoscs, log, etc. En estos subdirectorios se almacena la configuración, los accesos al servidor, programas auxiliares de mantenimiento, etc.

DocumentRoot: Especifica el directorio que se toma como raíz del árbol de directorios servidos por Apache, esto es, el directorio en el que se encuentran los documentos HTML, las imágenes, etc.

El valor por defecto para el parámetro DocumentRoot es ServerRoot/htdocs. Pero es aconsejable separar ambos parámetros en subdirectorios disjuntos para permitir actualizaciones del servidor sin tener que copiar o mover todo el árbol de documentos. Como, por ejemplo, el ServerRoot podría ser /usr/local/apache/ y el DocumentRoot /usr/local/www/docs/.

En el directorio conf, existen varios ficheros relacionados con la configuración del servidor como puede ser access.conf, httpd.conf, magic, mime.types, srm.conf

Ficheros de configuración.
httpd.conf: Las directivas de configuración están agrupadas en tres secciones básicas:
Sección 1: directivas globales de configuración del servidor.

Sección 2: directivas de configuración del servidor principal y valores por defecto para los servidores virtuales. Se establecen los valores empleados por el servidor <<principal>>, que atiende todas aquellas solicitudes que no son atendidas por la definición de un servidor virtual.
Sección 3: directivas de configuración de los servidores virtuales.

Arachni security framework

Arachni es un framework Ruby de código abierto completo, modular y de alto rendimiento diseñado para ayudar a los administradores y testers de penetración a evaluar la seguridad de las aplicaciones web. Es inteligente, se entrena a sí mismo monitoreando y aprendiendo el comportamiento de las aplicaciones web durante el escaneo y es capaz de realizar metanálisis utilizando una variedad de factores para así evaluar adecuadamente la confiabilidad de los resultados e identificar o evitar inteligentemente falsos positivos.

Top 10 de riesgos web según OWASP

A01:2021 - **Pérdida de control de acceso**: Este riesgo sube del quinto a la categoría de mayor riesgo para la seguridad de las aplicaciones web; los datos proporcionados muestran que un promedio del 3,81 % de las aplicaciones probadas tienen una o más enumeraciones de debilidades comunes (CWE), donde hubo más de 318 000 Ocurrencias de CWE en la categoría de riesgo. Los 34 CWE asociados con la pérdida de control de acceso tuvieron más ocurrencias de aplicaciones que cualquier otra categoría.

A02:2021 - **Fallas criptográficas:** Estos riesgos ascienden de un lugar a otro, anteriormente conocido como A3:2017: exposición de datos confidenciales, que es más una característica que una causa raíz. El nuevo nombre se enfoca en fallas relacionadas con el cifrado. Esta categoría a menudo conduce a la exposición de datos confidenciales o al compromiso del sistema.

A03:2021 – **Inyección:** Este riesgo cae al tercer lugar. El 94% de las aplicaciones fueron probadas con algún tipo de inyección y presentaron la mayor incidencia con un 19%, con un promedio de 3,37%, y 33 CWE asociados a esta categoría experimentaron un alto número de recurrencias ocupando el segundo lugar en la aplicación con 274.000 ocurrencias.

A04: 2021 – **Diseño inseguro**: Riegos que se relaciona con las fallas de diseño. Si realmente se quiere madurar como industria, se debe "mover a la izquierda" en las prácticas de seguridad del proceso de desarrollo. Se necesitan más modelos de amenazas, modelos y principios con diseños de seguridad y arquitecturas de referencia. Un diseño inseguro no se puede corregir con una implementación perfecta porque nunca se crean los controles de seguridad necesarios para proteger contra ataques específicos.

A05: 2021 - **Configuración de seguridad incorrecta:** Este riesgo se movió del sexto lugar en la edición anterior; El 90% de las aplicaciones fueron testadas por algún tipo de error de configuración, con una incidencia media del 4,5% y más de 208.000 casos de CWE asociados a este tipo de riesgo. Con el surgimiento de más y más software altamente configurable, no es sorprendente ver crecer esta categoría.

A06: 2021 - **Componentes vulnerables y desactualizados:** Anteriormente conocidos como componentes con vulnerabilidades conocidas ocuparon el segundo lugar entre los diez primeros según la encuesta de la comunidad, pero también tenían suficientes datos para llegar a los diez primeros gracias al análisis de datos. Es un problema conocido por ser difícil de probar y evaluar los riesgos.

A07: 2021 - **Errores de identidad y autenticación**: Anteriormente conocidos como fallas de autenticación, pasaron del segundo lugar y ahora incluyen los CWE más estrechamente asociados con los errores de identidad. Esta categoría todavía se encuentra firmemente entre las diez primeras, pero la mayor disponibilidad de marcos estandarizados parece estar ayudando.

A08:2021 – **Fallas en el software e integridad de datos:** se enfoca en hacer suposiciones sobre actualizaciones de software, datos críticos y CD de canalización de CI/CI sin verificación de seguridad. Corresponde a uno de los efectos más importantes según el Vulnerability Scoring System (CVE/CVSS, abreviatura de Common Vulnerabilities and Vulnerabilities System/Common Vulnerability System).

A09: 2021 - **Fallas en registro y monitoreo:** esta categoría se amplía para incluir más tipos de errores que son difíciles de probar y que no están bien representados en los datos CVE/CVSS. Sin embargo, los errores de esta categoría pueden afectar directamente la visibilidad, las alertas de incidentes y la investigación.

A10: 2021 - **Falsificación de Solicitudes del Lado del Servidor:** se agregó al top 10 en la encuesta de la comunidad (primer lugar). Los datos muestran una prevalencia relativamente baja con una cobertura de prueba superior a la media, así como calificaciones superiores a la media para la explotación y el impacto. Esta categoría representa una situación en la que los miembros de la comunidad de seguridad nos dicen que es importante, aunque no sea visible en los datos en este momento.

Referencias:

Como configurar correctamente Apache. (2022, 11 abril). Programacion webs. Recuperado 21 de junio de 2022, de https://www.programacionwebs.com/apache/como-configurar-correctamente-apache/

GeeksforGeeks. (2019, 9 septiembre). *Common Gateway Interface (CGI)*. Recuperado 20 de junio de 2022, de https://www.geeksforgeeks.org/common-gateway-interface-cgi/

IBM. (2021, 27 mayo). *REST APIs*. Recuperado 21 de junio de 2022, de https://www.ibm.com/cloud/learn/rest-apis

OWASP. (s. f.). *Inicio - OWASP Top 10:2021*. Recuperado 21 de junio de 2022, de https://owasp.org/Top10/es/

PHP: Instalación y configuración - Manual. (s. f.). PHP. Recuperado 21 de junio de 2022, de https://www.php.net/manual/es/install.php

Ranjan, R. (2022, 8 febrero). *What is a Framework in Programming & Why You Should Use One*. Insights - Web and Mobile Development Services and

Solutions. Recuperado 20 de junio de 2022, de https://www.netsolutions.com/insights/what-is-a-framework-in-programming/

Samani, P. (2018, 9 marzo). *Arachni : Web Application Security Scanner Framework*. Linkedin. Recuperado 21 de junio de 2022, de https://www.linkedin.com/pulse/arachni-web-application-security-scanner-framework-prawez