Instituto Tecnológico y de Estudios Superiores de Monterrey
Campus Monterrey

Integración de seguridad informática en redes y sistemas de software
TC2007B.3

# Etapa 3 - Desarrollo

Integrantes:

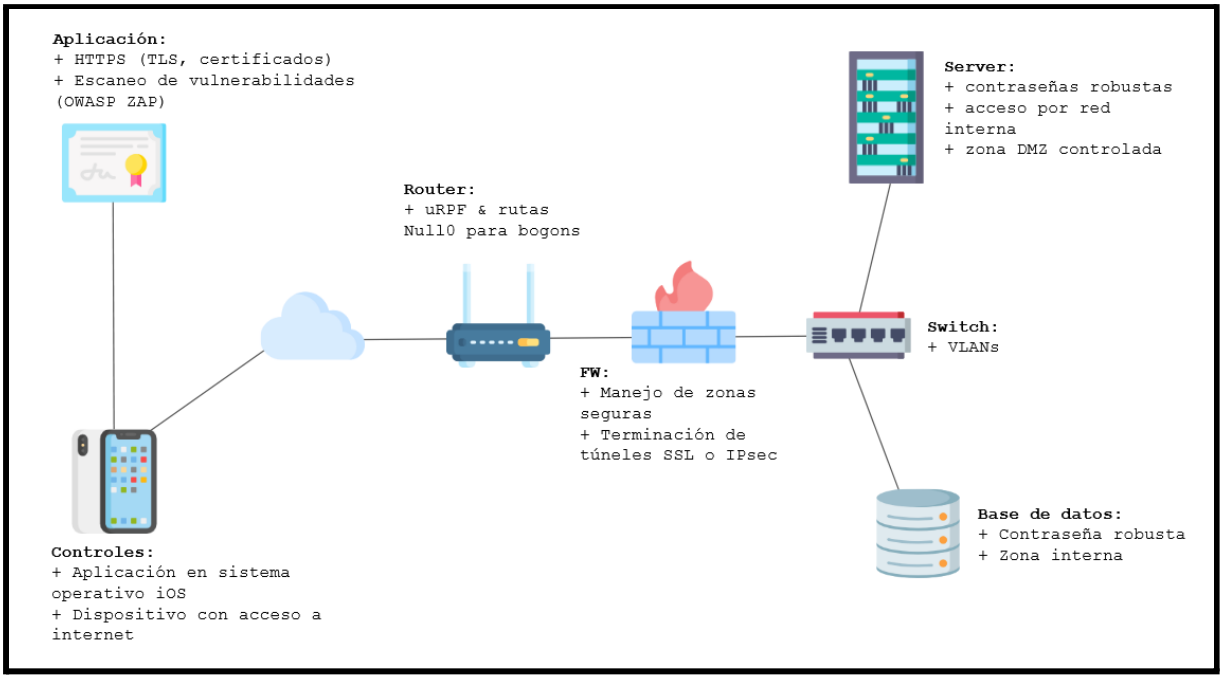

| | |
|---|---|
| Ezequiel Lozano Guerrero | A01734172 |
| Carlos David Toapanta Noroña | A01657439 |
| Abraham Cepeda Oseguera | A00827666 |
| Angel Martín Luna Cantú | A01177358 |


Fecha:
07 de octubre del 2021

## 1. Repositorio de software con el código del servidor, código del cliente

URL: https://github.com/Abrahamcepedao/Marco

## 2. Configuración de la infraestructura necesaria para desarrollar el proyecto.




## 3. Documentación de reuniones con el cliente, desarrolladores y equipo de pruebas

| | |
|---|---|
| **Cliente** | · **Reunión 1:**<br><br>Se mostró el mock-up de la aplicación, el front-end inicial en Xcode, y los SRS (Software Requirements Specification). El cliente aprobó lo presentado y se sugirieron mejoras y funcionalidades para la próxima entrega. Esta fue la última reunión con un representante del Museo Marco. |

| | |
|---|---|
| **Desarrolladores** | El trabajo de desarrollo en Xcode se divide entre los cuatro integrantes del equipo. Cada integrante se encarga de diseñar diferentes pantallas. Se utiliza Github para el control de versiones, y cada integrante sube su trabajo a su branch. Finalmente, se realizan reuniones por Zoom para medir el progreso, y planificar los avances. |

## 4. Identificación de ataques informáticos

**MySQL injection**

Una inyección de MySQL es uno de los ataques más comunes en la red, ya que es sencillo de realizar y si el sistema es vulnerable a este tipo de ataques, pueden tener un impacto catastrófico en la integridad y disponibilidad del sistema. Este ataque se realiza mediante una petición de http, en la cual el atacante incluye código de MySQL para que este se ejecute en la base de datos. De modo que, si el sistema no es capaz de detectar que dentro de la petición existe código malicioso, este se puede hacer realizar cualquier acción en la base de datos, desde modificar un dato, hasta borrar una base de datos entera.

**DDoS**

Los ataques DDoS se conocen como ataques de denegación distribuida de servicio. Su principal objetivo es hacer que se rebasen los límites de cualquier recurso red que habilita la infraestructura web de una empresa para así detener totalmente su capacidad de manejar peticiones y evitar que funcione correctamente.

**Falla de hardware**

El hardware requerido para un proyecto de este tipo es vital, ya que si los servidores, ruteadores, y los demás equipos fallan por alguna razón, toda la infraestructura de la red de la empresa se ve comprometida. Estos fallos pueden ser por incendios, falta de energía eléctrica, razones meteorológicas o falta de mantenimiento.

**Corrupción de base de datos**

La corrupción de la base de datos es algo sumamente peligroso, puesto que pone en riesgo la integridad de los datos al estar incompletos o corruptos. Generalmente, se ocasiona cuando el

proceso de transmisión de datos se interrumpe o se perturba, lo cual se origina por fallos electrónicos, subidas de tensión o problemas mecánicos internos.

**Acceso ilegítimo**

El acceso ilegítimo a la información es una de las principales preocupaciones que se tienen al desarrollar una infraestructura de red, ya que se busca que solamente los usuarios autorizados por el sistema sean capaces de acceder a la información y de realizar distintas actividades sobre la misma. Es por ello que, si el sistema es vulnerable a accesos ilegítimos, toda la infraestructura se encuentra en riesgo.

**Spoofing and Sniffing**

*Spoofing* y *sniffing* son dos tipos de ataques bastante comunes. El primero consiste en obtener las credenciales de un usuario autorizado para acceder a la red y así poder modificar cosas, recaudar información, divulgar *malware,* o modificar los controles de acceso. Por otro lado, *sniffing* se caracteriza por que el atacante falsifica lectores autorizados para monitorear los paquetes que se transmiten a través de la red con el objetivo de encontrar información confidencial valiosa

**Port Scanning**

Esta práctica se utiliza para determinar cuáles puertos de una red se encuentran vulnerables. De modo que, al identificar los puertos vulnerables, los atacantes pueden ya sea recopilar paquetes o enviarlos.

## 5. Métodos de protección de ataques informáticos

**MySQL injection**

Usar captchas en los formularios para validar las peticiones de los usuarios: sirve para impedir que se pueda tener acceso a la función de un script de forma automática. La tendencia actual es usar el método de reCAPTCHA de Google, en la que el lector solo debe marcar una casilla y Google se encarga de comprobar que se trata de un humano y no una máquina.

Crear limitaciones y reglas en los formularios (hablando desde el aspecto de sitios web): se debe utilizar como método en los formularios POST en vez de GET. En las entradas para introducir contraseñas, en vez de <input type="text"> se debe emplear: <input type="password"> En las entradas de texto se puede limitar la cantidad de caracteres usando el atributo "maxlength". En los formularios usados para subir archivos como imágenes, fotos,

etc., puede limitarse el tipo de archivo a subir, basado en su extensión, así como regular su tamaño.

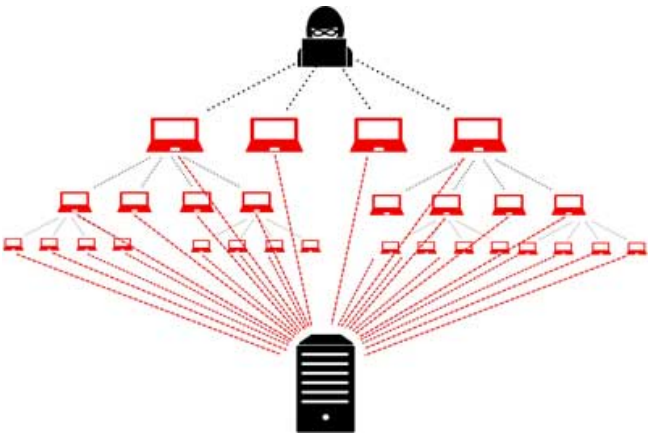
Impedir la entrada de código maligno escapando los caracteres: para evitar las inyecciones SQL y ataques XXS (Cross-site scripting) es necesario *escapar* todo lo que pueda ser introducido en cualquier consulta, reemplazando los caracteres especiales por su equivalente textual, de tal forma que se interprete todo el contenido de la variable como si fuera texto. Se conoce como "sanitizar" las entradas.


**DDoS**

Limitar la tasa de peticiones: limitar el número de peticiones que un servidor aceptará durante un tiempo determinado es una buena manera de mitigar ataques de denegación de servicio. Hay que tener claro que limitar la velocidad de peticiones ralentiza los trabajos de raspadores webs. También reduce los intentos de fuerza bruta para iniciar sesión. Aplicarlo como única solución será insuficiente para prevenir un ataque DDoS.

Implementar un firewall: esta es una herramienta que puede ser útil para mitigar ataques de DDoS en capa 7. Implementando el WAF (Web Application Firewall) entre internet y el servidor de origen, puede servir como un proxi de reversa. Además, se pueden filtrar las peticiones usando como base una serie de reglas para identificar herramientas empleadas en ataques comunes, siendo su principal característica la capacidad para implementar rápidamente reglas *personalizadas* ante cualquier ataque.

Aplicar redes de difusión Anycast: al aplicar una red de difusión Anycast se mitigan ataques de denegación de servicio, ya que, al dispersar el tráfico malicioso, este se puede enviar a través de una red de servidores hasta una red externa; dicho tráfico se vuelve manejable y se puede llevar hasta una desembocadura sin que afecte el entorno. Sin embargo, es importante señalar que la efectividad de una red de difusión Anycast dependerá del tamaño del ataque y la eficiencia de la red interna.



**Falla de hardware**

Control de temperatura y clima: se requiere tener un claro control del clima para mantener una temperatura de funcionamiento constante para los servidores y otro hardware, lo que evita el sobrecalentamiento y reduce la posibilidad de interrupciones del servicio. Los centros de datos deben estar acondicionados para mantener las condiciones atmosféricas en niveles óptimos. Los sistemas de monitoreo y el personal del centro de datos deben garantizar que la temperatura y la humedad estén en los niveles adecuados.

Bases de datos de postgres para clientes: la protección continua mantiene los datos seguros en Heroku Postgres. Cada cambio en sus datos se escribe en registros de escritura anticipada, que se envían a un almacenamiento de alta durabilidad de varios centros de datos. En el improbable caso de una falla irrecuperable del hardware, estos registros se pueden 'reproducir' automáticamente para recuperar la base de datos a unos segundos de su último estado conocido. También es posible realizar una copia de seguridad de las bases de datos para cumplir con una buena retención de datos.

Retención y destrucción de datos de clientes: se debe tener la libertad de definir qué datos se almacenan en las aplicaciones y tener la capacidad de eliminarlos; Si se desaprovisiona la aplicación y la base de datos asociada, el volumen de almacenamiento de la base de datos debe mantenerse durante un periodo de tiempo (por ejemplo una semana), para después destruir archivos automáticamente, lo que hace que los datos sean irrecuperables; esto debe hacerse solo con la información sin utilidad con el fin de liberar espacio y mantener en mejor estado al servidor.

**Corrupción de base de datos y acceso ilegítimo**

Limitar el acceso a datos confidenciales tanto para usuarios como para procedimientos. Es decir, solo deben autorizarse a ciertos usuarios el poder realizar consultas relacionadas con información confidencial.

Además se deben desactivar todos los servicios y procedimientos que no están en uso, para evitar ataques. Aunado a ello, la base de datos debe ubicarse en un servidor al que no se pueda acceder directamente desde internet sin protección, para evitar que la información se exponga a atacantes remotos.

También es importante que los datos confidenciales usen algoritmos de hashing para resguardar bien la información. La mejor manera de proteger una base de datos es hacerla ilegible para cualquier persona que acceda a ella sin autorización.

Sin olvidar que, monitorear, auditar y registrar las acciones y movimientos sobre los datos permite saber quién, qué, cuándo y cómo ha manipulado la información. Tener un historial completo de las transacciones permite comprender patrones en el acceso y modificación de los datos, para así evitar fugas de información, controlar cambios fraudulentos y detectar acciones sospechosas en tiempo real.

**Spoofing**

Es recomendable evitar ingresar a sitios haciendo clic en direcciones o enlaces que se reciban por mail, además de prestar especial atención a las URLs que aparecen en la barra de estado para asegurar que la dirección del sitio sea la correcta, verificando que se navegue con el protocolo HTTPS y que se cuente con certificados SSL.

Observar el aspecto de los sitios web y correos electrónicos, ya que, pueden existir pequeños elementos que indiquen que se trata de un posible ataque. Remitentes desconocidos, tipografías extrañas, tipografías o un estilo y disposición diferente de los textos deben llamar la atención para así detectar posibles fraudes.

No responder a ningún correo electrónico que pida información personal: desconfiar de cualquier entidad o persona que pregunte por sus claves, o cualquier otra información que pueda ser considerada confidencial.

No descargar archivos de procedencia dudosa o de personas desconocidas: hacerlo puede provocar la instalación de virus, malware, etc., que luego son utilizados para sustraer datos personales y privados.


**Sniffing**

Utilizar cifrado: se debe cifrar el correo electrónico, las redes y las comunicaciones, así como los datos en reposo, en uso y en movimiento. De esa manera, incluso si se interceptan los datos, el hacker no podrá descifrarlos sin la clave de cifrado. Para el cifrado inalámbrico se recomienda el acceso protegido Wi-Fi 2 o WPA2. Toda comunicación basada en la web debe usar HTTPS.

Autenticación: autenticar los paquetes entrantes es clave para evitar interceptar paquetes falsificados que se utilizan para perpetrar ataques de suplantación de IP o suplantación de direcciones MAC. Se debe usar protocolos criptográficos, como TLS, extensiones de correo de internet seguras/multipropósito, OpenPGP e IPsec.

Monitoreo de la red: los equipos de seguridad deben monitorear constantemente las redes para detectar actividad anormal mediante el uso de sistemas de detección de intrusos o software de detección y respuesta de punto final.

Mejores prácticas de sensibilización y seguridad: se debe educar a los administradores sobre los riesgos de los ataques de espionaje y las mejores prácticas para protegerse contra ellos. Debido a que muchos ataques de espionaje involucran malware, nunca se debe hacer clic en enlaces o descargar archivos no confiables; además se deben usar contraseñas seguras y estas cambiarse con frecuencia para evitar ataques..

Segmentación de la red: se debe separar la infraestructura crítica de las aplicaciones de la red de invitados, así si un segmento se ve comprometido, el hacker no podrá acceder a los otros segmentos. Aunado a ello se deben ocupar tecnologías de seguridad, como firewalls, VPN y antimalware, a través del filtrado de paquetes, configuración correcta de enrutadores e implementación de firewalls para rechazar cualquier paquete con direcciones falsificadas.

**Port Scanning**

Usar herramientas para comprobar los puertos abiertos: realizar un análisis y comprobar qué puertos se tienen abiertos para encontrar la raíz de cualquier problema.

No abrir más puertos de los necesarios: sería un error abrir una gran cantidad de puertos que en realidad no vamos a necesitar en ningún momento. Así se reduce en gran medida el problema.

Utilizar firewalls permite evitar la entrada de intrusos a la red, ya que actúan como barrera. Esto es muy útil para mantener siempre la seguridad en los equipos y no permitir que se aprovechen de posibles puertos abiertos que hubiera.