TALENTO TECH

TIC

REGIÓN 3

CAUCA – NARIÑO

LECCIÓN 2 – UNIDAD 1

Universidad Tecnológica de Pereira

faceIT

Lección2: Fallas de Seguridad en el protocolo HTTP

El protocolo HTTP, a pesar de ser fundamental para la comunicación en la web, presenta vulnerabilidades. Una de las principales debilidades radica en la transmisión de datos en texto plano, lo que significa que cualquier información enviada entre el cliente y el servidor, incluyendo contraseñas, números de tarjetas de crédito y otros datos sensibles, puede ser interceptada y leída por terceros malintencionados. Esta vulnerabilidad hace que en redes públicas como las de cafeterías o aeropuertos los atacantes puedan interceptar el tráfico de red y leer la información privada. Además, el protocolo HTTP no proporciona ninguna garantía de autenticidad, lo que permite a los atacantes suplantar la identidad de servidores legítimos y llevar a cabo ataques de phishing.

Como se vio en la lección anterior una trama de datos HTTP puede ser llenada por un atacante con información de su conveniencia y así robar la información de los usuarios sin que se den cuenta que están sufriendo ataques del tipo Man in The middle.

HTTPS:

Para abordar las deficiencias de seguridad del HTTP, surgió el protocolo HTTPS (Hypertext Transfer Protocol Secure). HTTPS es una extensión del HTTP que utiliza el protocolo SSL/TLS (Secure Sockets Layer/Transport Layer Security) para cifrar la comunicación entre el cliente y el servidor. Este cifrado garantiza que los datos transmitidos estén protegidos contra la interceptación y la modificación por parte de terceros no autorizados. Funciona codificando los paquetes de datos del payload en HTTP evitando que terceros malintencionados puedan leer el contenido de los paquetes. Además, HTTPS proporciona mecanismos de autenticación que permiten verificar la identidad del servidor y proteger contra ataques de phishing.

La adopción de HTTPS ha mejorado la seguridad en la web, ofreciendo numerosos beneficios. En primer lugar, HTTPS protege la privacidad de los usuarios algarantizar que sus datos personales y financieros estén cifrados y sean inaccesibles para los atacantes. En segundo lugar, HTTPS mejora la confianza de los usuarios en los sitios web. Una forma fácil para que un usuario sepa que un sitio es seguro, es revisando el certificado de los sitios web, disponible en la barra de direcciones de los navegadores.

Generalmente se muestra como un ícono de un candado verde e indica que la conexión es segura. Otras mejoras consisten en adiciones de seguridad en servicios ampliamente utilizados. Por ejemplo, los motores de búsqueda como Google hacen que los sitios web que utilizan HTTPS aparezcan de primero por encima de aquellos sitios que no tienen cifrado. De esta forma ayudan a los usuarios a no dirigirse a sitios web inseguros.

Implementar HTTPS en un sitio web requiere la obtención de un certificado SSL/TLS de una autoridad de certificación de confianza. Este certificado se utiliza para cifrar la comunicación y verificar la identidad del servidor. Sin embargo, la implementación de HTTPS no garantiza la seguridad completa de un sitio web. Es fundamental combinar HTTPS con otras medidas de seguridad, como firewalls, sistemas de detección de intrusiones y prácticas de desarrollo seguro, para protegerse contra una amplia gama de amenazas cibernéticas. Además, es importante mantener los certificados SSL/TLS actualizados y revocarlos en caso de compromiso.

Servidores de nombres

Así como todos los equipos necesitan una dirección IP única, los sitios web requieren direcciones IP únicas. Cada portal como la página de un banco, la web de una tienda en línea, la dirección de un servicio de streaming, requieren de una dirección IP. Para los usuarios sería muy complicado aprenderse todas las direcciones IP de las páginas y servicios que requieren. Ejemplo en clase: Pida a los estudiantes que entren a un navegador y accedan a la dirección: 142.250.78.46

Así como en el ejemplo la dirección 142.250.78.46 nos lleva al buscador Google, sería muy difícil aprenderse tantos números como direcciones un usuario requiera. Por ese motivo se crearon los servidores de nombres de dominio.

Un servidor de nombres o DNS es un computador que recibe solicitudes en formato de texto legible por humanos, busca el registro de interés en una tabla que contiene el texto de un portal (nombre) y su correspondiente dirección IP y entrega como resultado la dirección IP en el formato visto.

Por ejemplo, un servidor de nombres se encarga de convertir la dirección www.google.com en el número 142.250.78.46. De esta forma, los usuarios no deben recordar direcciones IP sino nombres de dominio. Cuando en un navegador se escribe un nombre de dominio (Google.com, nmicrosoft.com, mintic.gov.co) la solicitud viaja a un servidor de nombres que encuentra la dirección IP y direcciona los paquetes desde esa dirección hacia el computador que hace la solicitud.

En internet hay muchos computadores cuya función es traducir nombres. Si una solicitud llega a un equipo que no conoce el nombre, esta viaja hacia el siguiente equipo e intenta buscar la dirección IP correspondiente. En caso de que el sitio no se encuentre en ningún servidor o se tarde más de lo esperado, el equipo que inició la solicitud mostrará un error llamado: “el servidor DNS no responde”. Ejercicio: escribir un dominio inexistente en el navegador y validar el mensaje, puede ser sitioficticiodepruebas.com

Enrutamiento

Cuando se han agregado las direcciones IP al paquete mediante el protocolo HTTP, ya se puede transmitir a través de la red. Si la dirección IP existe en la red, el paquete se envía directamente al dispositivo. Sin embargo, si la dirección IP está fuera de la red, debe pasar a través de un enrutador. Un enrutador es un dispositivo físico que conecta una red a otra. Por ejemplo, si se quiere llevar una carta a una persona que vive a unas casas, se podría ir a llevar directamente. Pero si vive en otra ciudad el destinatario, es necesario entregar la carta a un servicio de correos que lee la dirección de destino y se encarga de direccionarla hacia esa ciudad. En la ciudad será direccionada al sector en donde está el destinatario. En este ejemplo, el servicio postal es el enrutador y se encarga de buscar la mejor ruta para que el mensaje llegue al destinatario.

En internet el enrutamiento es similar. Si se quieren enviar o recibir datos de un equipo remoto, hay muchos dispositivos que enrutan la información para que lleguen los paquetes desde el origen hasta el destinatario.