# Índice:

Ejercicio 1 ..... 2
a) Descriptores ..... 2
b) XSS y SQL Injection ..... 2
c) mitos HTTPS y SSL Trip ..... 3
d) Hosting web ..... 4
e) cookies y tipos MIME ..... 4

# Ejercicio 1

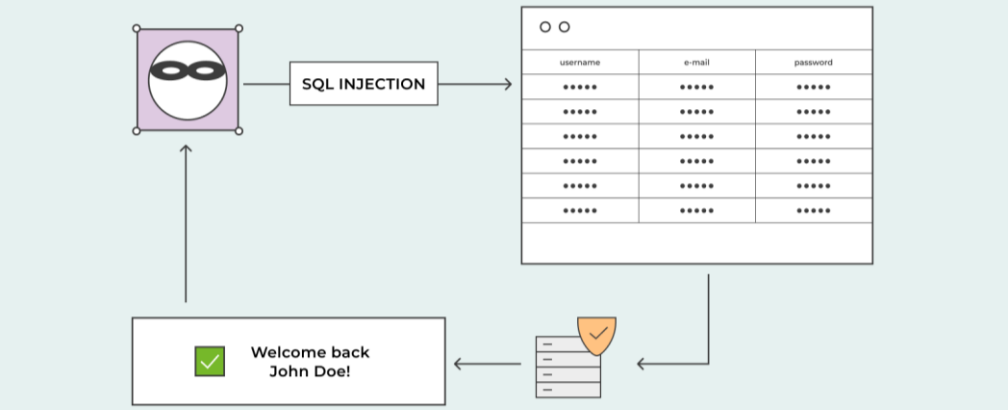
## a) Descriptores

Solución:

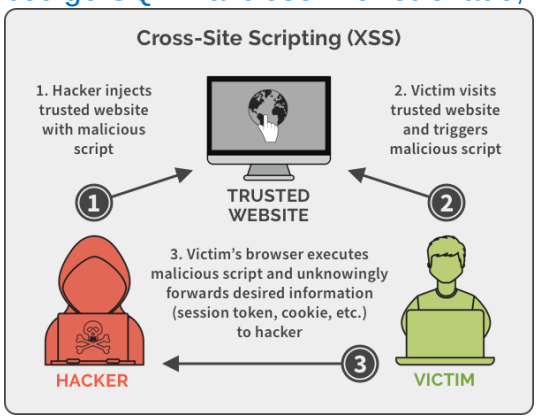
Un descriptor de despliegue de una aplicación web es un fichero que contiene información crucial para el despliegue de la aplicación. Este incluye parámetros de inicialización, configuración de sesión, definiciones de Servlets/JavaServer Pages, y el mapeado de tipos MIME. En el contexto de las aplicaciones J2EE, el descriptor de despliegue guía una herramienta de despliegue para implantar la aplicación con opciones específicas y proporciona detalles de configuración que un desplegador puede abordar. Además, el término "descriptor de despliegue" se utiliza de manera más general para referirse a un archivo de configuración para cualquier artefacto desplegado en algún contenedor.

## b) XSS y SQL Injection

Solución:




Los ataques SQL Injection buscan aprovechar debilidades en la validación de las entradas a la base de datos de una aplicación, permitiendo la inserción de código SQL malicioso. Por otro lado,



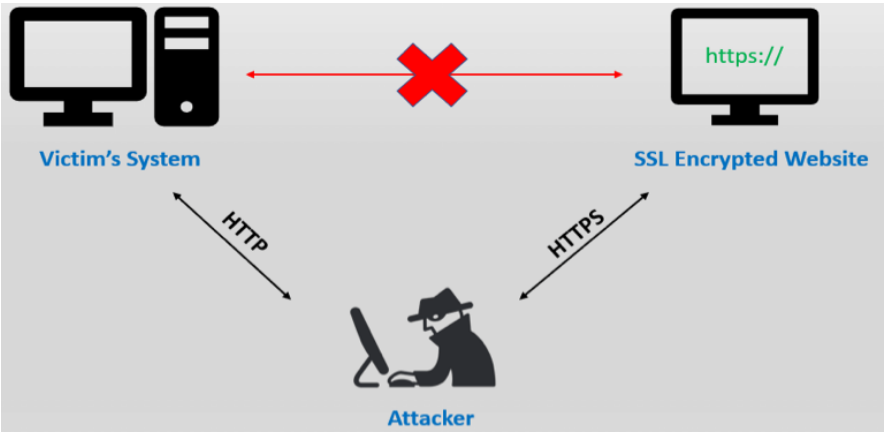

XSS (Cross-Site Scripting) es una vulnerabilidad en aplicaciones web que permite la inyección de código JavaScript o similar en las páginas visitadas por el usuario, comprometiendo la seguridad al robar información o secuestrar sesiones. Existen dos tipos de XSS: persistente/directo, que inyecta código HTML de forma permanente, y reflejado/indirecto, que altera los valores transmitidos por URL o en las cabeceras HTTP.

Ambos tipos de ataques representan amenazas a la seguridad en el entorno web, buscando explotar fallos en la validación y ejecución de código para realizar acciones maliciosas como robo de datos, phishing y desestabilización de foros. Es importante comprender y mitigar estas vulnerabilidades para garantizar la integridad y seguridad de las aplicaciones web.

## c) mitos HTTPS y SSL Trip

Solución:

En cuanto a los Mitos HTTPS, se destaca la importancia de validar el protocolo HTTPS al acceder a sitios web para garantizar la seguridad de la información transmitida. Sin embargo, se señala que aunque HTTPS cifra la información durante la transmisión, al llegar al servidor web, la información deja de estar cifrada, permitiendo a un atacante malintencionado visualizarla. Además, se aborda el mito de que un certificado SSL es necesario para cada dirección IP, dominio o subdominio, aclarando que existen opciones versátiles como los certificados wildcard.




En relación con SSL Trip, se describe que este ataque hace creer al usuario que está bajo una conexión segura, manipulando la visualización del candado de seguridad. Cuando se lanza SSL Strip sobre una víctima, el usuario puede no darse cuenta de que la conexión segura ha desaparecido al acceder a páginas HTTPS, lo que puede resultar en la exposición de credenciales en texto plano. También se mencionan algunos mitos sobre SSL Strip, como la necesidad de un certificado SSL para cada IP, dominio o subdominio, así como la percepción de que HTTPS es muy lento.

## d) Hosting web

Solución:

Los Servicios de alojamiento web (Hosting web) ofrecen a los usuarios un espacio en Internet para almacenar información, imágenes y otros contenidos accesibles a través de la web. Empresas denominadas web hosts proporcionan este servicio, ya sea mediante contratos con proveedores de internet o a través de empresas independientes. Se distinguen servicios de pago, como 1and1 y e-Hosting, y gratuitos, como Miarroba y 000webhost. Los gratuitos a menudo incluyen publicidad para financiarse y tienen limitaciones, como espacio reducido y restricciones en el tipo de contenido permitido.

En cuanto a la comparativa de Hosting Web, se presentan distintos proveedores con sus respectivos planes, costos, espacio y transferencia. Se destacan las ventajas del alojamiento web dedicado, como mayor flexibilidad, control total sobre el servidor y mayor seguridad, pero también se mencionan desventajas como el mayor costo y la recomendación para negocios con planes a largo plazo.

## e) cookies y tipos MIME

Solución:

Cookies y Tipos MIME son elementos esenciales en el ámbito web.

Cookies:

- Son archivos creados por sitios web para almacenar pequeñas cantidades de datos.
- Identifican al usuario y registran su historial de actividad en un sitio web.
- Permiten personalizar la experiencia del usuario al ofrecer contenido adaptado a sus hábitos de navegación.
- Pueden inyectarse en dominios cruzados mediante atributos como "domain".
- Las cookies pueden presentar riesgos de seguridad, como la inyección de cookies con cruce de límites de seguridad.

MIME (Multipurpose Internet Mail Extensions) establece convenciones para el intercambio de archivos en Internet.

Se utiliza para enviar diversos tipos de archivos (texto, audio, vídeo, etc.) de forma transparente.

Define tipos de contenido como "texto/html" para páginas web, "texto/plano" para texto común, "Aplicacion/de fuente octeto" para descargas de archivos, etc.

Algunos tipos MIME, como los programas ejecutables, son restringidos por motivos de seguridad.

La suposición incorrecta de tipos MIME puede llevar a vulnerabilidades, como en el caso de Internet Explorer.