DuocUC® INFORMÁTICA Y TELECOMUNICACIONES

Introducción a las pruebas de seguridad

Calidad de Software - CSY4111

CONTENIDO

DuocUC®

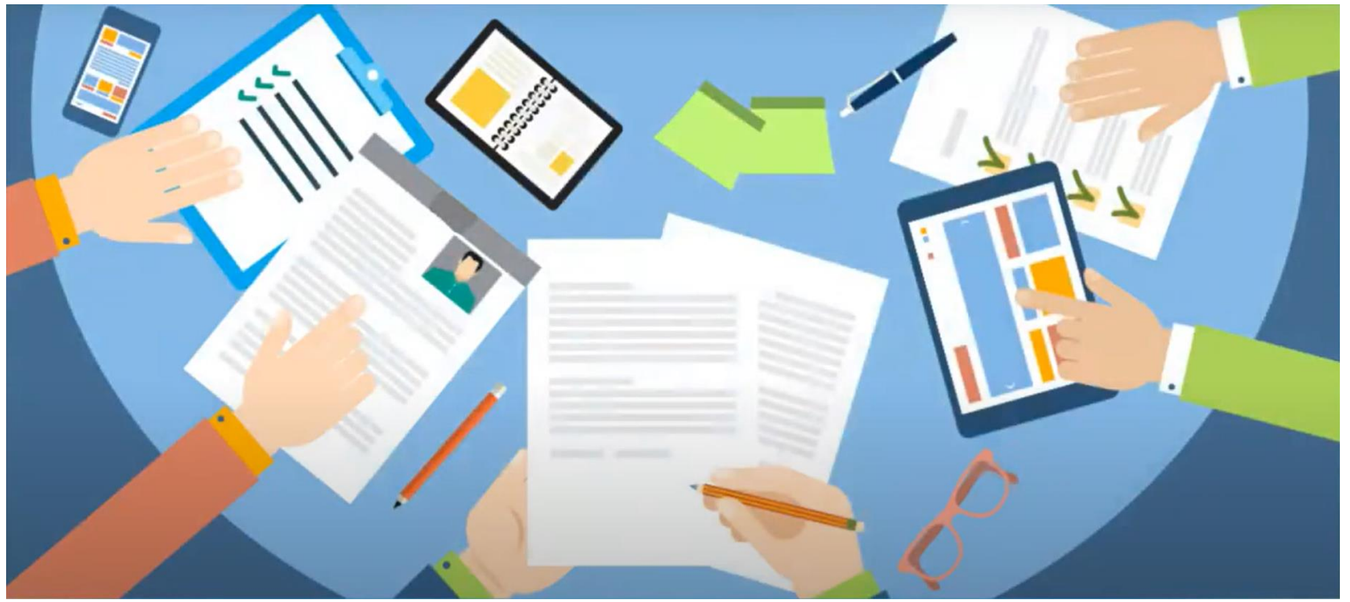
Refrescando conocimiento

DuocUC®

REFRESCANDO CONOCIMIENTOS

El cierre del proceso de pruebas es una etapa crítica que marca el final de las actividades de pruebas y es fundamental para proporcionar una evaluación integral de la calidad del software.

A continuación, se detalla el proceso de cierre de pruebas con sus respectivos roles y responsabilidades.



REFRESCANDO CONOCIMIENTOS

Es un documento crucial que resume los resultados y las conclusiones del proceso de pruebas realizado.

A continuación, se detallan los elementos clave que debe contener un informe de certificación de pruebas

1.- Información general:

- Nombre del proyecto.
- Fecha del informe.
- Equipo de pruebas y sus roles.

DuocUC®

01

INTRODUCCIÓN A LAS PRUEBAS DE SEGURIDAD

DuocUC®

INTRODUCCIÓN A LAS PRUEBAS DE SEGURIDAD

La seguridad es un conjunto de medidas implementadas para proteger una aplicación de acciones imprevistas que pueden detener su funcionamiento, estas acciones pueden ser intencional o no intencional.

Las pruebas de seguridad son una parte fundamental del proceso de aseguramiento de la calidad del software.

Estas pruebas tienen como objetivo identificar vulnerabilidades, debilidades y riesgos de seguridad en una aplicación o sistema de software, y evaluar su capacidad para resistir ataques maliciosos.

DuocUC®

INTRODUCCIÓN A LAS PRUEBAS DE SEGURIDAD

El propósito principal de las pruebas de seguridad es detectar vulnerabilidades y luego repararlas.

Ayuda a impulsar el sistema actual y asegurarse de que el sistema pueda funcionar durante un tiempo prolongado. Para notar lagunas que provocarán la pérdida de información vital.

Es importante mencionar que estas pruebas se deben realizar siempre con el consentimiento del cliente.

INTRODUCCIÓN A LAS PRUEBAS DE SEGURIDAD

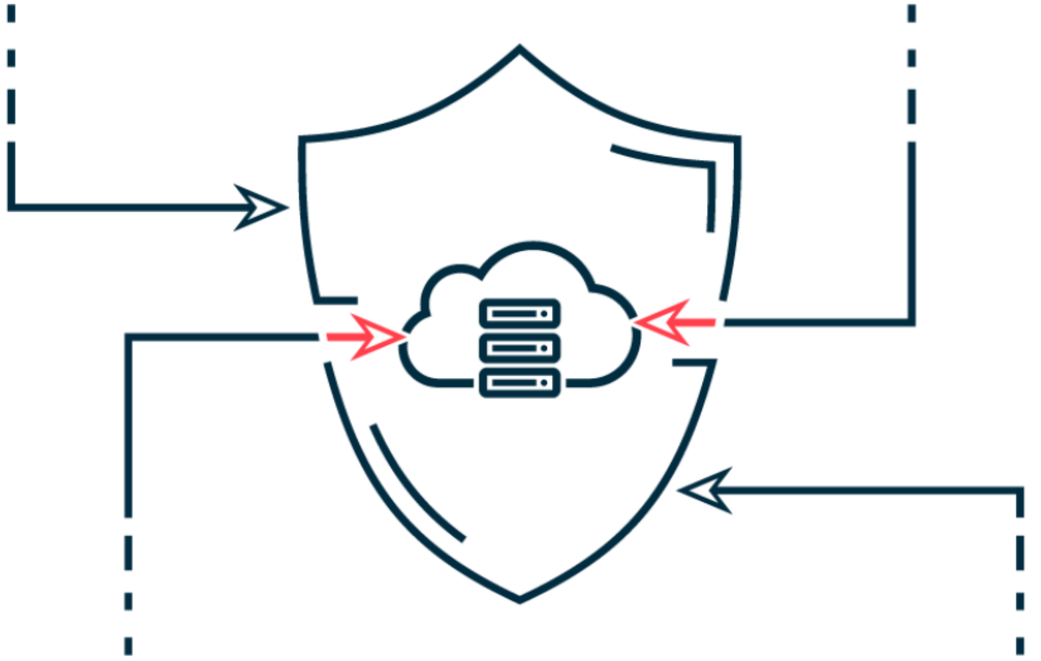
A continuación, se presentan los pasos comunes para realizar pruebas de seguridad de sistemas o pentesting

1.- Reconocimiento:

Se recopila información sobre el sistema objetivo y su infraestructura.

Esto implica buscar información pública, identificar hosts, servicios, puertos abiertos y posibles vulnerabilidades.

El objetivo es obtener una comprensión general del sistema y determinar posibles puntos de entrada.



DuocUC

INTRODUCCIÓN A LAS PRUEBAS DE SEGURIDAD

2.- Análisis de vulnerabilidades:

En esta etapa, se realiza un escaneo exhaustivo del sistema para identificar vulnerabilidades conocidas.

Esto puede incluir el uso de herramientas automatizadas de escaneo de seguridad, así como la **revisión manual de configuraciones y sistemas.**

El objetivo es identificar debilidades que podrían ser explotadas posteriormente.

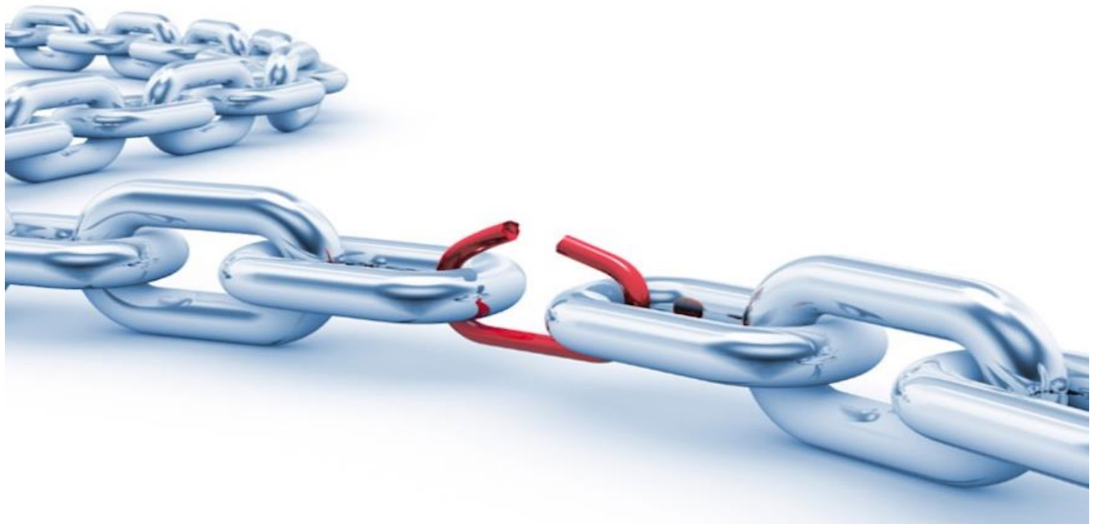
En ocasiones el cliente solo espera que el pentesting llegue hasta aquí, sin la necesidad de explotar las vulnerabilidades encontradas.

INTRODUCCIÓN A LAS PRUEBAS DE SEGURIDAD

3.- Explotación:

En esta etapa, se intenta aprovechar las vulnerabilidades identificadas en la etapa anterior para obtener acceso no autorizado al sistema.

Esto puede implicar el uso de técnicas de explotación, como la ejecución de comandos remotos, inyecciones de código, escalada de privilegios u otras tácticas.



El objetivo es demostrar la viabilidad y el impacto de las vulnerabilidades encontradas.

DuocUC®

INTRODUCCIÓN A LAS PRUEBAS DE SEGURIDAD

4.- Post-explotación:

Una vez que se ha logrado el acceso al sistema objetivo, se realiza una exploración adicional para recopilar información adicional, buscar datos sensibles o buscar posibles movimientos laterales dentro de la red.

También se busca mantener el acceso al sistema comprometido para demostrar la persistencia del ataque.

El objetivo es evaluar la amplitud del compromiso y evaluar los posibles daños que podrían ocurrir en un escenario real.

DuocUC®

INTRODUCCIÓN A LAS PRUEBAS DE SEGURIDAD

5.- Informe de hallazgos:

Al finalizar el proceso de pentesting, se elabora un informe detallado que resume todos los hallazgos, vulnerabilidades explotadas y recomendaciones para mejorar la seguridad del sistema.

Este informe se entrega al cliente y suele incluir descripciones de los problemas encontrados, evidencia de las explotaciones exitosas, impacto potencial y **medidas recomendadas para mitigar** los riesgos identificados.

DuocUC®

02

JUSTIFICACIÓN

DuocUC®

JUSTIFICACIÓN

Las pruebas de seguridad son fundamentales para garantizar la protección de los datos sensibles y la integridad del sistema.

Algunos de los beneficios clave de realizar pruebas de seguridad son:

1.- Identificación de vulnerabilidades:

Las pruebas de seguridad ayudan a identificar y corregir vulnerabilidades en el software antes de que sean explotadas por atacantes.

Esto reduce el riesgo de brechas de seguridad y la exposición de datos sensibles.

JUSTIFICACIÓN

2.- Protección de la reputación:

- Un fallo de seguridad puede tener un impacto negativo en la reputación de una organización.
- Las pruebas de seguridad permiten detectar y solucionar vulnerabilidades antes de que se conviertan en incidentes graves que afecten la imagen de la empresa.

Estas pruebas de seguridad son clave para la imagen de la empresa

DuocUC®

JUSTIFICACIÓN

3.- Cumplimiento normativo:

En muchos sectores, existen regulaciones y estándares que exigen la implementación de medidas de seguridad adecuadas.

Las pruebas de seguridad ayudan a demostrar el cumplimiento de estas normativas y garantizan la protección de la información confidencial.

La seguridad de la información y la privacidad de los datos, garantizan el cumplimiento de las regulaciones y estándares establecidos.

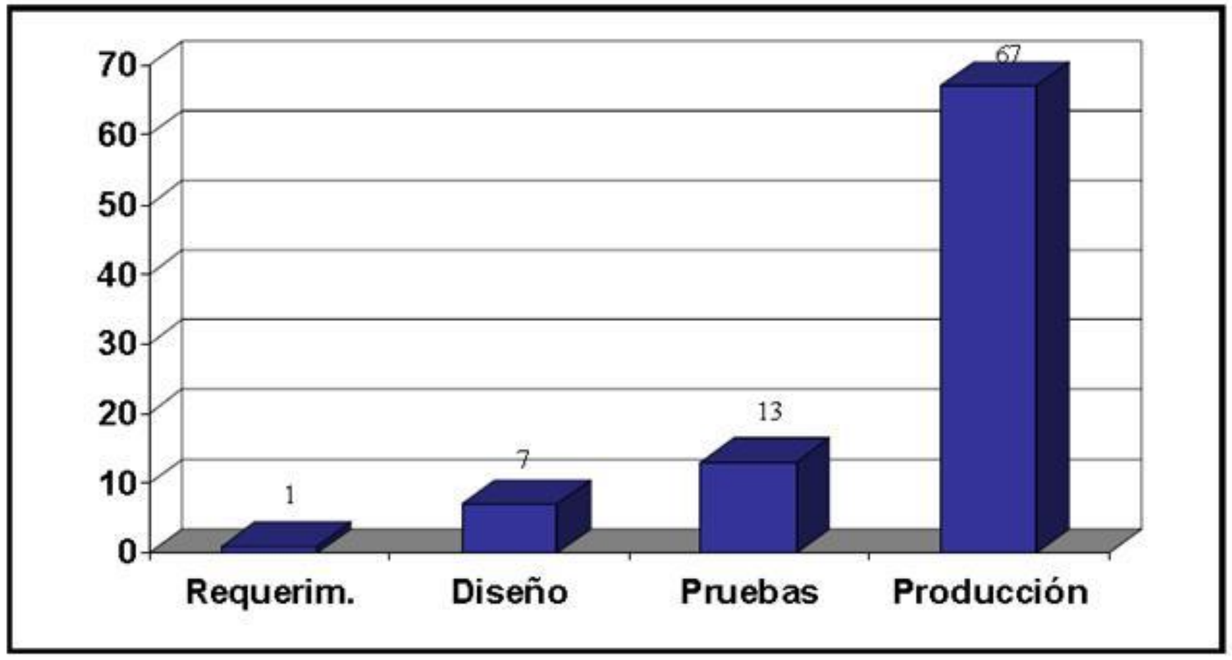
DuocUC®

JUSTIFICACIÓN

Ahorro de costos a largo plazo:

Detectar y solucionar vulnerabilidades de seguridad en etapas tempranas del desarrollo de software es más económico que corregirlas en etapas avanzadas o después de que se hayan producido ataques.

Costo de detectar y corregir errores según su etapa en el desarrollo del proyecto



DuocUC®

03
HERRAMIENTAS

DuocUC®

HERRAMIENTAS

Existen numerosas herramientas disponibles para realizar pruebas de seguridad de software. Estas herramientas pueden automatizar parte del proceso de evaluación de la seguridad y ayudar a identificar vulnerabilidades comunes.

Algunas de las herramientas populares para las pruebas de seguridad incluyen:

Burp Suite: Una suite de herramientas que se utiliza para realizar pruebas de seguridad en aplicaciones web. Permite identificar vulnerabilidades como inyección de SQL, cross-site scripting (XSS) y secuencias de comandos entre sitios (CSRF).

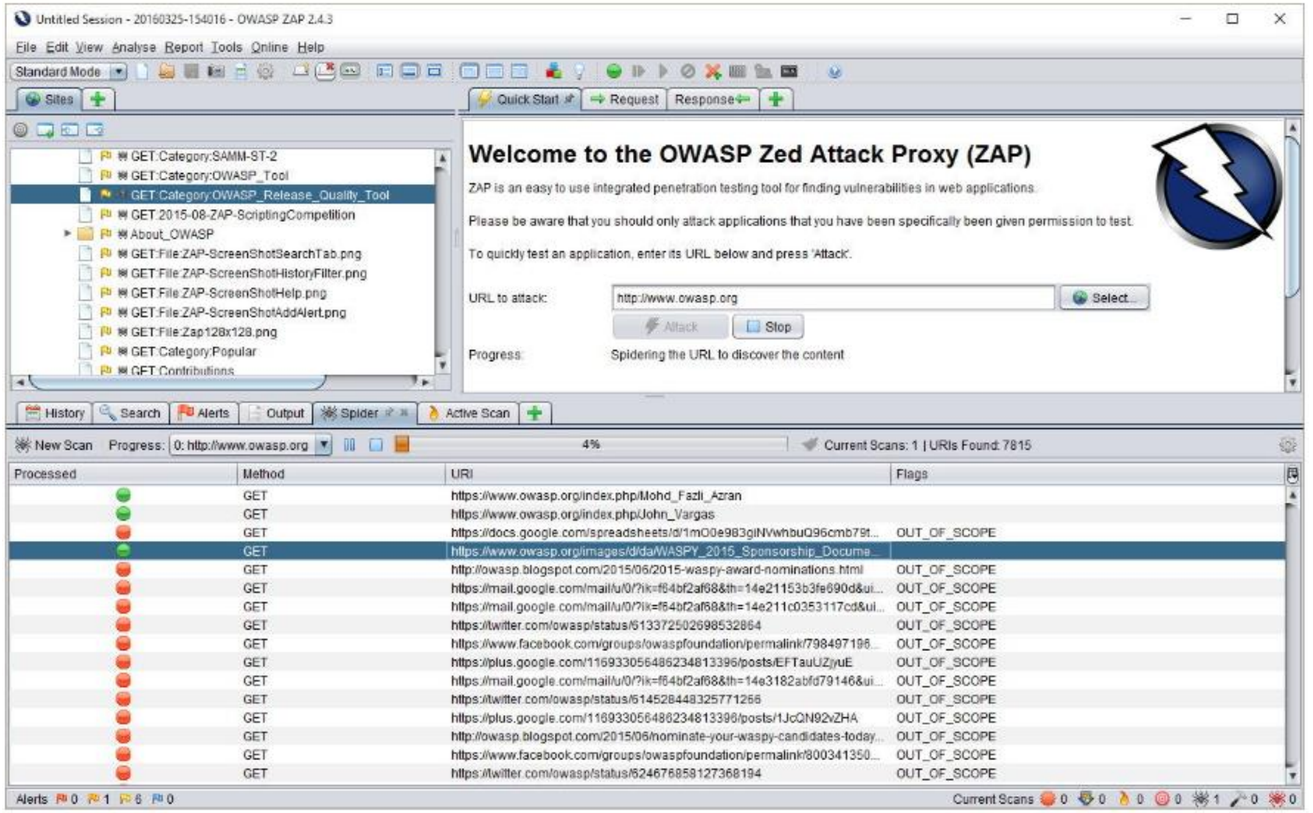
HERRAMIENTAS

OWASP ZAP: Es una herramienta de seguridad de aplicaciones web de código abierto que permite identificar y explotar vulnerabilidades en aplicaciones web.

Proporciona una amplia gama de funcionalidades, como escaneo de vulnerabilidades, análisis de seguridad y generación de informes.

https://devopedia.org/owasp-zap

Open Web Application Security Project (OWASP)



HERRAMIENTAS

Metasploit: Es un framework de prueba de penetración que permite simular ataques reales para evaluar la seguridad de un sistema.

Proporciona una amplia gama de módulos y exploits que pueden ser utilizados para probar la resistencia de un sistema ante ataques conocidos.

https://www.metasploit.com/

DuocUC®

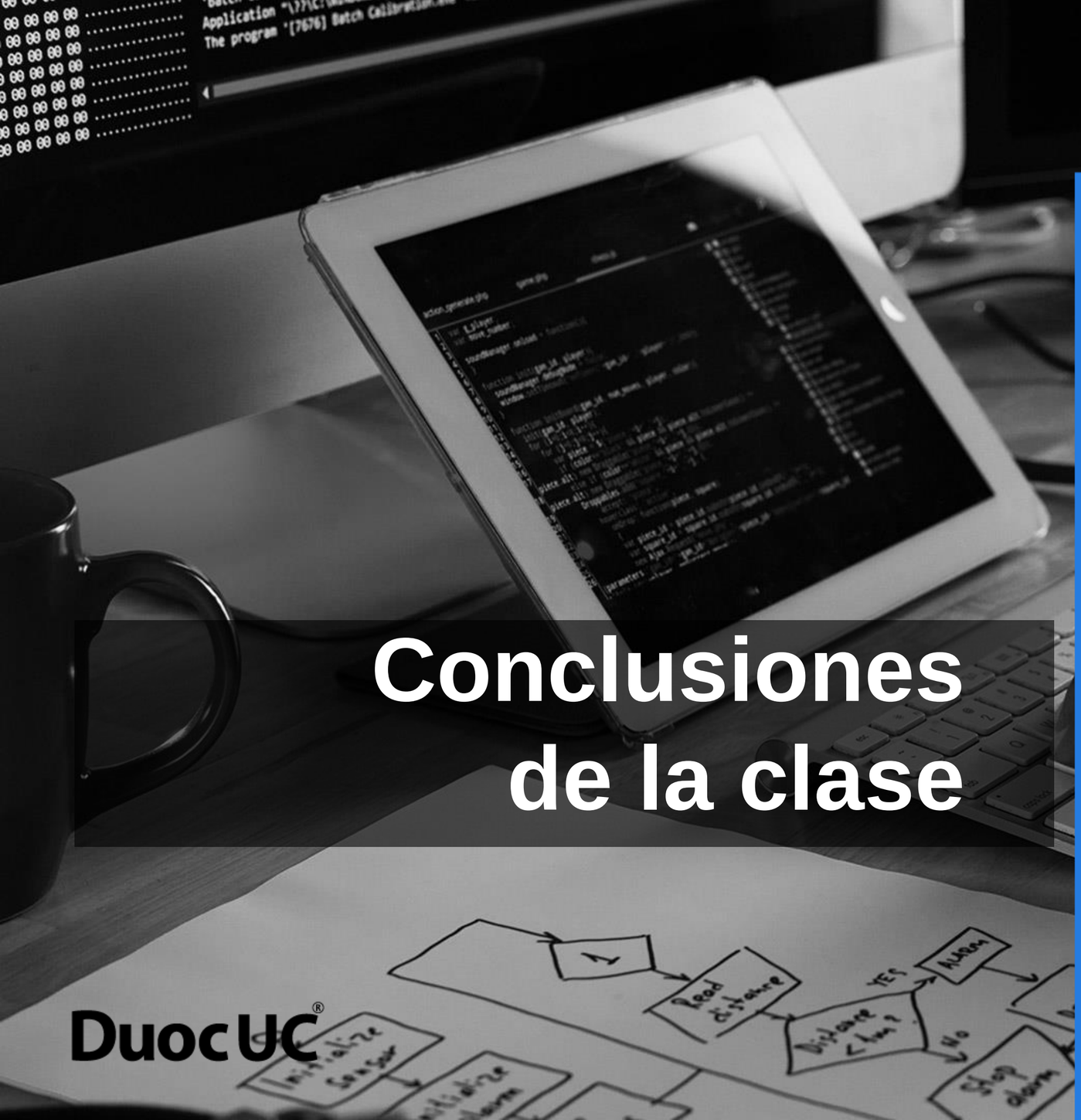
HERRAMIENTAS

Nmap: (Network Mapper) es una herramienta de escaneo de red de código abierto que se utiliza para descubrir hosts y servicios en una red, así como para identificar puertos abiertos, sistemas operativos y realizar evaluaciones de seguridad.

Nmap utiliza paquetes IP para determinar la disponibilidad de hosts y servicios en una red.

DuocUC®

Conclusiones de la clase



DuocUC®

Conclusiones

- ✓ Las pruebas de seguridad son un conjunto de medidas implementadas para proteger una aplicación de acciones imprevistas que pueden detener su funcionamiento.

- ✓ Costo de detectar y corregir errores según su etapa en el desarrollo del proyecto.

- ✓ Importante que estas pruebas se realicen siempre en conocimiento del cliente.

Bibliografía

- ✓ Tokio School. (27/10/2022). ¿Qué es y en qué consiste el pentesting?. https://www.tokioschool.com Recuperado de https://www.tokioschool.com/noticias/pentesting/#:~:text=El%20pentesting%20es%20un%20ataque,las%20aplicaciones%20y%20p%C3%A1ginas%20web.

DuocUC®

DuocUC® INFORMÁTICA Y TELECOMUNICACIONES

Introducción a las pruebas de seguridad

Calidad de Software - CSY4111