Tarea online PPS02.

Título de la tarea: Pruebas de SQL Injection

Unidad: 2

Ciclo formativo y módulo: Curso de especialización en ciberseguridad en entornos de las tecnologías de la información - Puesta en Producción Segura.

Curso académico: 2023-2024

¿Qué contenidos o resultados de aprendizaje trabajaremos?

Resultados de aprendizaje

- **RA2.** Determina el nivel de seguridad requerido por aplicaciones identificando los vectores de ataque habituales y sus riesgos asociados.

Contenidos

1.- Determinación del nivel de seguridad requerido por aplicaciones.
    1.1.- Fuentes abiertas para el desarrollo seguro.
    1.2.- Lista de riesgos de seguridad habituales.
    1.3.- Comprobaciones de seguridad.
    1.4.- Requisitos de verificación necesarios.

Creado con eXeLearning (Ventana nueva)

1.- Descripción de la tarea.

Caso práctico

Pixabay (Dominio público)

Julián está preocupado porque necesita crear un aplicativo web que interactuara con una base de datos y sabe que uno de los principales riesgos es la entrada de datos de usuarios ya que podrían provocar acceso a información que no debiera de la base de datos. Ha buscado información sobre vulnerabilidades de este tipo y ha decidido que debe aprender como desarrollar de forma más segura

Para ello crea el entorno de pruebas Damn Vulnerable Web Application (https://github.com/digininja/DVWA) donde podrá configurar distintos niveles de seguridad, ver cómo se refleja en el código y probar distintos tipos de ataque y ver de qué manera se comporta el aplicativo y sobre todo ver que recibe la base de datos.

Va a probar ataques de tipo Injection o inyección que es uno de los principales riesgos identificados en OWASP.

¿Qué te pedimos que hagas?

- **Apartado 1: Responde a las siguientes cuestiones**

  Buscar información sobre la vulnerabilidad **CVE-2023-39417** y rellenar la siguiente tabla

Breve descripción	
Impacto	
Productos y versiones vulnerables	
Posibles soluciones	

Buscar información del requisito **ASVS v4.0.3-5.3.4** (**ASVS versión 4.0.3 capítulo 5, apartado 3, requisito 4)** y rellena la siguiente tabla

Breve descripción	
Niveles a los que debe aplicarse	
Categoría CWE	

- **Apartado 2: Crea el entorno de pruebas**

Hoy en día la mayoría de los equipos de desarrollo utilizan contenedores para montar los entornos de desarrollo. En la página web del proyecto de DVWA (https://github.com/digininja/DVWA) explican como instalar la aplicación con Docker, que es una de las herramientas más habituales para trabajar con contenedores.
Sigue las siguientes instrucciones:

- Instalar Docker y si es necesario docker compose (en algunas versiones ya viene con docker). En la página oficial de Docker explican cómo instalarlo
- Descargar el proyecto DVWA y descomprimirlo
- Abrir una terminal y cambiar al directorio donde se ha descomprimido.
- Ejecutar la línea de comandos: **docker compose up -d**

Una vez instalado, para acceder a DVWA:
Abrir un navegador con la dirección **http://localhost:4280 El usuario es admin y la clave es admin**
La primera vez que se abre la aplicación es necesario pulsar en el botón Create/Reset Database
A partir de ese momento el usuario es **admin** y la clave es **password**
Para cambiar el nivel de seguridad debes ir a **DVWA Security**

- **Apartado 3: Pruebas de vulnerabilidades.**

Procederemos a realizar distintas pruebas de SQL Injection

- Accederemos en modo **Low**
- Pulsar en el menú lateral **SQL Injection**
- Primero comprobaremos como se comporta nuestro aplicativo cuando le damos IDs de usuarios (puedes probar con 1, 2, 3..)
- Trataremos de ver qué sucede cuando le damos resultados no esperados, por ejemplo tres comillas simples '''
- Revisaremos el código del aplicativo web para entender qué ha sucedido y que consulta (query) se ha intentado realizar. Para ver el código pulsar el **botón View Source** que hay al final de la página.
- Probaremos con otros IDs como: **' OR '1'='1** (muy importante poner bien las comillas)
- Revisaremos el código del aplicativo web para entender qué ha sucedido y que consulta (query) se ha realizado. Para ver el código pulsar el **botón View Source** que hay al final de la página.
- Probaremos a cambiar el modo de seguridad de DVWA a **Impossible** (dónde no debería haber vulnerabilidades) y volveremos a realizar todos los pasos de este apartado: probar con un id de usuario, probar con tres comillas, probar con ' OR '1'='1 y revisar el código del aplicativo.

- **Apartado 4: Preguntas finales**

- ¿Cómo se ha comportado el aplicativo web cuando ha recibido 3 comillas simples en el modo **Low**?¿Qué consulta crees que se ha intentado lanzar en la base de datos?
- ¿Cómo se ha comportado el aplicativo web cuando ha recibido 3 comillas simples en el modo **Impossible**?¿Qué consulta crees que se ha intentado lanzar en la base de datos ?
- ¿Cómo se ha comportado el aplicativo web cuando ha recibido ' OR '1'='1 en el modo **Low**? ¿Qué consulta crees que se ha lanzado en la base de datos?
- ¿Cómo se ha comportado el aplicativo web cuando ha recibido ' OR '1'='1 en el modo **Impossible**? ¿Qué consulta crees que se ha lanzado en la base de datos?

- ¿Qué diferencia ves en el código PHP cuando esta en modo **Low** y cuándo está en modo **Impossible**? ¿Cómo crees que afecta ese código a las vulnerabilidades que estábamos explotando?

NOTA IMPORTANTE

Para todos los apartados es necesario entregar las capturas de pantalla de los principales pasos realizados, explicando el proceso seguido en cada uno de ellos. Las capturas de pantalla realizadas deben tener como fondo de pantalla la plataforma con tu usuario mostrando claramente la foto de tu perfil. Aquellos apartados/subapartados que no cumplan esta condición no serán corregidos.

2.- Información de interés.

Recursos necesarios y recomendaciones

Recursos necesarios

- Ordenador personal con, al menos, 4 Gigabytes de memoria RAM.
- Conexión a Internet.
- Sistemas Operativos Windows 10 o superior, Ubuntu 20.04 o superior
- Navegador web.
- Docker

Recomendaciones

- Antes de abordar la tarea:
- Lee con detenimiento la unidad, consulta los enlaces para saber más, examina el material proporcionado por el profesor y aclara las dudas que te surjan con él.
- Realiza el examen online de la unidad, y consulta nuevamente las dudas que te surjan. Solo cuando lo tengas todo claro, debes abordar la realización de la tarea.
- No olvides elaborar el documento explicativo.
- Puedes descargar Docker de la página oficial donde explican cómo instalarlo en el sistema operativo que quieras (ver enlace)
- El archivo **docker-compose.yml** que tiene el proyecto DVWA contiene la configuración de los contenedores que se van a levantar.

Indicaciones de entrega

Una vez realizada la tarea, el envío se realizará a través de la plataforma. El archivo se nombrará siguiendo las siguientes pautas:

Apellido1_Apellido2_Nombre_PPS_Tarea02

3.- Evaluación de la tarea.

Criterios de evaluación implicados

Criterios de evaluación RA2

- a) Se han caracterizado los niveles de verificación de seguridad en aplicaciones establecidos por los estándares internacionales (ASVS, “Application Security Verification Standard”).
- b) Se ha identificado el nivel de verificación de seguridad requerido por las aplicaciones en función de sus riesgos de acuerdo a estándares reconocidos.
- c) Se han enumerado los requisitos de verificación necesarios asociados al nivel de seguridad establecido.
- d) Se han reconocido los principales riesgos de las aplicaciones desarrolladas, en función de sus características.

¿Cómo valoramos y puntuamos tu tarea?

Rúbrica de la tarea	
Apartado 1: Responde a la pregunta del CVE rellenando la tabla	1 punto
Apartado 1: Responde a la pregunta del requisito ASVS rellenando la tabla	1 punto
Apartado 2: Instala y configura el entorno DVWA	2 puntos
Apartado 3: Realiza las pruebas y determina que sucede cuando introducimos tres comillas simples como input u otros parámetros mal formados	1 punto
Apartado 4: Determina por qué ha devuelto esos datos la base de datos	1,5 puntos
Apartado 4: Determina cómo ha procesado el aplicativo las consultas que hemos hecho. Que consultas exactas ha realizado en nuestras pruebas.	1,5 puntos
Apartado 4: ¿Qué ha cambiado en el código cuando cambiamos el modo de seguridad del aplicativo?	1 punto
Apartado 4: ¿En qué crees que afecta a la seguridad y a las pruebas que hemos hecho los cambios en el código?	1 puntos

NOTA IMPORTANTE

Aquellos apartados/subapartados en los que las capturas de pantalla no sean claras o no tengan como fondo de pantalla la plataforma con tu usuario mostrando claramente la foto de tu perfil, no serán corregidos.