Año 2025

Desarrollo Seguro de Aplicaciones
Práctica 2
Pérdida de Control de Acceso

Fecha de entrega: 08/05/2024 a las 17:59

Términos relacionados:

- OWASP top 10 (**2021**): **A01 (pérdida de control de acceso)**
- OWASP top 10 (2013): A04 (referencia directa insegura a objetos)
- OWASP top 10 (2013): A07 (ausencia de control de acceso a las funciones)

Aviso: para la realización de esta práctica, cada grupo tendrá un repositorio de código en GitHub, el cual podrán clonar con “git clone <URL git del repositorio del grupo>”.

Instalación

Instalar docker/Docker Desktop.
Instalar docker-compose

```
git clone <URL git del repositorio del grupo>
cd practica2/
docker-compose up
```

Ejercicio 1 - Broken Access Control

Reto **ejercicio1** (https://tp2-ejercicio1.dsa.linti.unlp.edu.ar/)

Loguearse con:

Usuario: *user* **Password**: *pass*

Objetivo: Obtener las tarjetas de crédito de otros usuarios. En el CTF la flag estará en la tarjeta de crédito del usuario “admin”

Ejercicio 2 - Insecure DOR (Order Tickets)

Para los ejercicios 2, 3, 4 y 5 se utilizará la aplicación **bWAPP** (“an extremely buggy web app” https://sourceforge.net/projects/bwapp/files/bWAPP/, http://www.itsecgames.com/index.htm).

Utilizando el navegador ingresar a http://localhost:12000/**install.php** (por defecto los lleva a /login.php y tira un error porque todavía no está creada la DB y seteada la config de la aplicación).

Clic en el enlace “Click **here** to install”.

Login con user/pass: **bee**/**bug**

Luego ingresar a http://localhost:12000/security_level_set.php y configurar el nivel de seguridad en “**low**”.

En el menú “Bugs” (Portal) buscar en la lista los retos de la categoría “A4 - Insecure Direct Object References” y “A7 - Missing Functional Level Access Control”.

Reto **bWAPP** (http://localhost:12000/insecure_direct_object_ref_2.php)

Esta página simula un sitio para comprar/encargar entradas de cine por un valor de “15 EUR”.

Objetivo a cumplir: encargar tickets gratis o por un valor distinto.

Ejercicio 3 - Insecure DOR (Change Secret)

Reto **bWAPP** (http://localhost:12000/insecure_direct_object_ref_1.php)

Esta página permite cambiar el “Secret” de tu usuario (ver http://localhost:12000/user_extra.php).

Objetivo a cumplir: cambiar el “Secret” de otro usuario que no sea el logueado. Verificar que se cambió correctamente el secret logueando con el usuario víctima, accediendo a http://localhost:12000/insecure_crypt_storage_1.php y viendo el localStorage

Ejercicio 4 - Directory Traversal

Reto **bWAPP** (http://localhost:12000/directory_traversal_2.php?directory=documents)
Reto **bWAPP** (http://localhost:12000/directory_traversal_1.php?page=message.txt)

Objetivo a cumplir: listar los usuarios del sistema operativo subyacente (sistema del contenedor docker).

Ejercicio 5 - Restrict Device Access

Reto **bWAPP** (http://localhost:12000/restrict_device_access.php)

Esta página solo muestra su contenido cuando se la accede con un dispositivo móvil.

Objetivo a cumplir: acceder sin usar un dispositivo móvil. (Ayuda: pueden utilizar Mozilla Firefox y ver la “respuesta”)

Ejercicio 6 - Subir un fix

Cree un branch llamado “fix-practica2”

Modifique el código del ejercicio 1 para que no sea posible obtener los datos personales ni las tarjetas de crédito de otros usuarios. Solamente que se pueda acceder a los datos del usuario logueado.

Ejercicio 7 - Entrega de Informe

Desarrolle un informe que incluya una breve explicación de:

- Cómo explotó las vulnerabilidades de los ejercicios 1, 2, 3, 4 y 5 (con capturas de pantalla)
- Qué soluciones aplicaría para evitar este tipo de vulnerabilidades

Entregue el informe a través de la tarea correspondiente en https://catedras.linti.unlp.edu.ar en **formato PDF**.