Seguridad Informática – Seguridad Web
4^o Grado en Ingeniería en Informática, curso 2020/21

Práctica 6: Pentesting de aplicaciones Web

En esta práctica se van a aplicar los conocimientos adquiridos en clase sobre las técnicas de explotación de las vulnerabilidades de aplicaciones Web. Se proporciona una máquina virtual con diferentes aplicaciones Web deliberadamente vulnerables y herramientas de soporte para automatizar las pruebas de penetración.

1. Entorno de la práctica

La práctica se realiza con la máquina virtual *Dojo* (confeccionada y proporcionada por la empresa *Maven Security Consulting*) en la que se encuentran instaladas varias aplicaciones Web, todas ellas instaladas en local, y herramientas útiles para automatizar las pruebas de penetración.

La máquina virtual (formato OVA) ejecuta una versión de Linux Ubuntu v16.04 a 64-bits. Las credenciales de acceso a la máquina virtual son:

usuario: dojo
contraseña: dojo

2. Aplicación Web DVWA

La aplicación *Damn Vulnerable Web Application (DVWA)* es una de las aplicaciones vulnerables disponibles para las pruebas de penetración y trabajaremos principalmente con ella. DVWA ha sido desarrollada en PHP – el servidor Web es Apache2 y el servidor DBMS es MySQL – y podemos acceder con el navegador a la página principal de autenticación:

URL: `dvwa.local/dvwa`

con el navegador.

Utilizamos el usuario `admin` (cuya contraseña es `password`) para la autenticación: la aplicación presenta la página de bienvenida donde podemos encontrar las instrucciones generales (ver Figura 2.1). La aplicación ofrece cuatro niveles de seguridad (menú a la izquierda – opción *DVWA Security*):

- El nivel *bajo* corresponde a la ausencia de mecanismos de protección, es decir, la aplicación es vulnerable a todos los ataques (incluso a los más conocidos y sencillos).

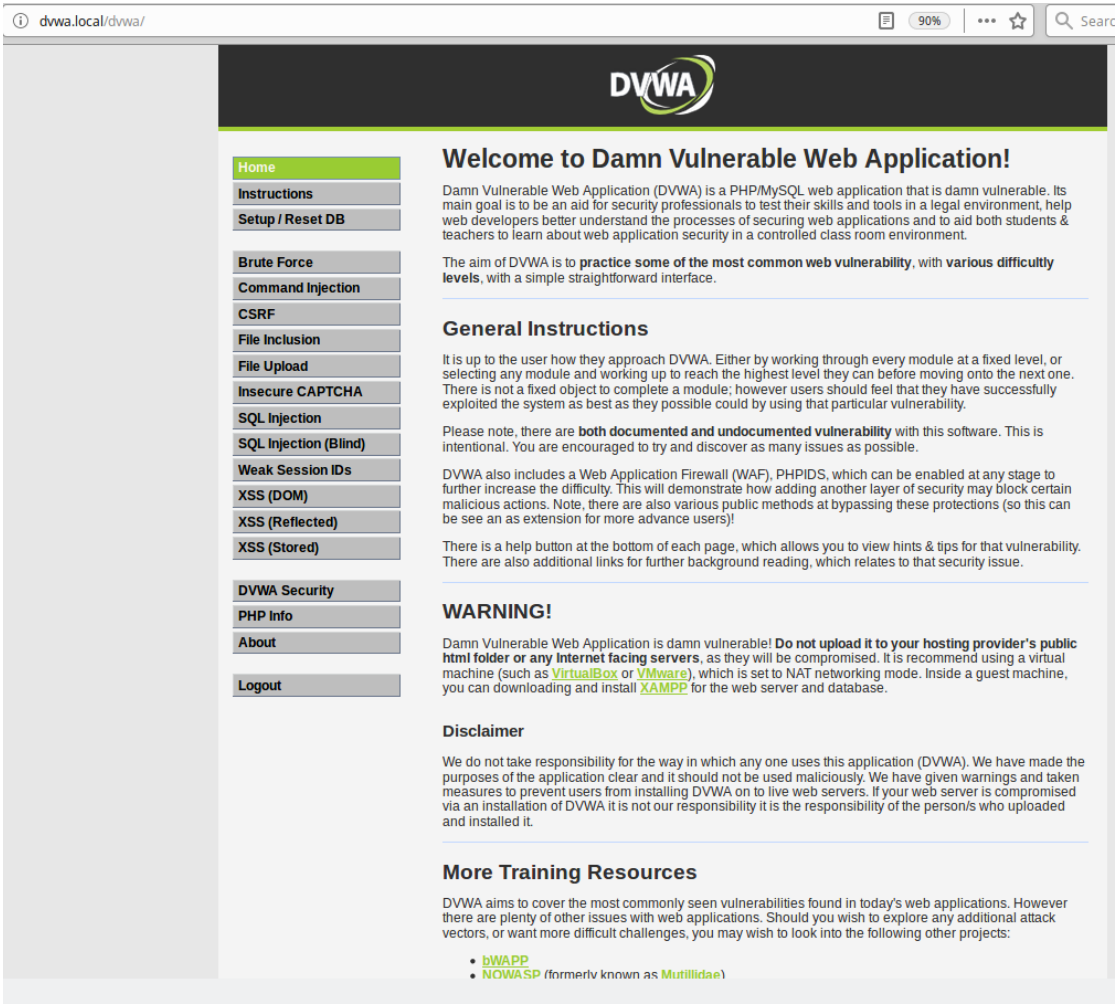

Figura 2.1: Página de bienvenida de la aplicación DVWA.

- El nivel *intermedio* proporciona una versión que sigue siendo vulnerable, pero las técnicas de ataques se tienen que refinar.
- El nivel *alto* corresponde a una versión "segura"de la aplicación, para explotar las vulnerabilidades hace falta más destreza.
- El último nivel *imposible* corresponde a una versión "super-segura" de la aplicación y no debería ser vulnerable a los tipos de ataque conocidos. El código de este nivel puede usarse como referencia. Se recomienda comparar el código de este nivel con el código empleado para implementar las versiones de la aplicación DVWA correspondientes a los niveles anteriores.

Se pueden considerar diferentes tipos de vulnerabilidades Web (ver Figura 2.1, menú a la izquierda). Para cada tipo de vulnerabilidad, se plantea un objetivo de ataque y sugerencias sobre como explotar la vulnerabilidad para cada uno de los niveles de seguridad de la aplicación.

La Figura 2.2 muestra un ejemplo de vulnerabilidad de inyección SQL (página Web a la izquierda), la página de ayuda en la que se encuentran el objetivo de ataque y las

sugerencias (a la derecha) y el código PHP del módulo que gestiona la petición generada en la página Web correspondiente (al fondo). La documentación sobre la aplicación

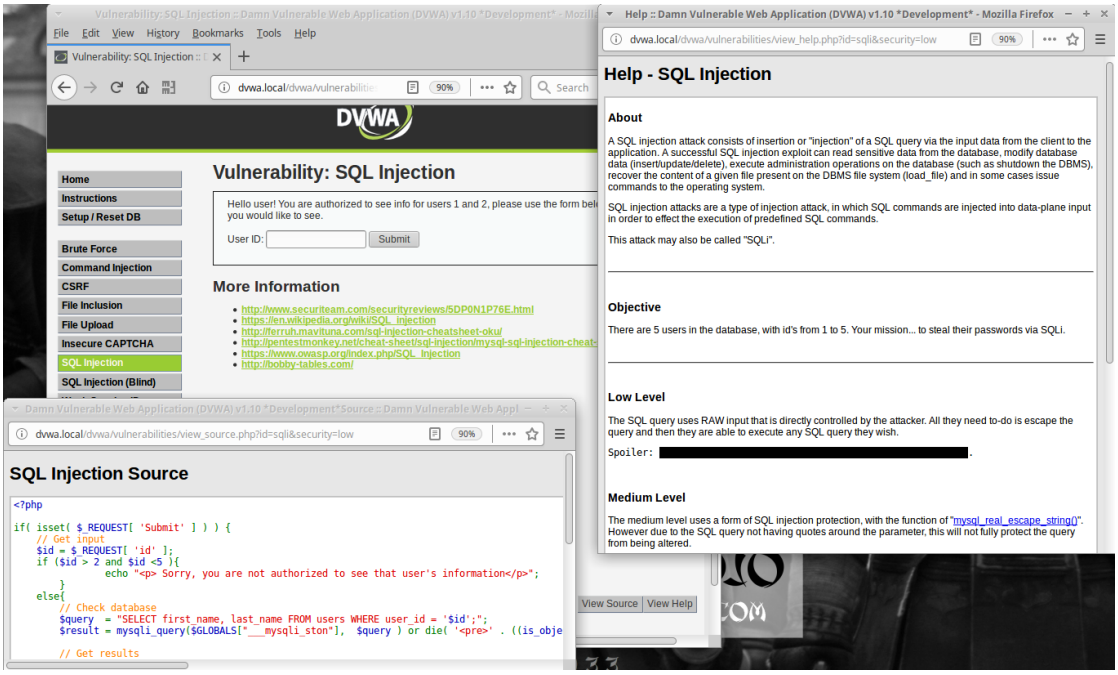

Figura 2.2: Vulnerabilidad de inyección SQL.

DVWA se encuentra en el siguiente directorio:

`/var/www/dvwa/docs/`

y en las páginas Web de la propia aplicación.

3. Pruebas de penetración

Se pide realizar pruebas de penetración considerando los siguientes tipos de vulnerabilidades:

SQLi. El objetivo es robar las contraseñas de los 5 usuarios del sistema.

SQLi blind. El objetivo es encontrar la versión del servidor DBMS.

CSRF. El objetivo es cambiar la contraseña del usuario `admin` sin su consentimiento. El atacante explota exclusivamente la vulnerabilidad CSRF para conseguir su objetivo.

XSS (reflected). El objetivo es robar las cookies de sesión de un usuario.

XSS (persistent). El objetivo es redireccionar cualquier usuario que visite la página web a otra página elegida por el atacante.

Las pruebas de penetración se pueden realizar de forma manual o con el uso de herramientas de explotación. En la evaluación de esta práctica se considerará **positivamente** el uso de algunas herramientas que se encuentran instaladas en el directorio `$HOME/tools`.

Se pide hacer las pruebas de penetración siguiendo las pautas indicadas en la páginas de ayuda de cada tipo de vulnerabilidad mencionada anteriormente (de 1 a 5). Es necesario realizar las pruebas configurando la aplicación con los siguientes niveles de seguridad:

- Bajo
- Medio

La configuración por defecto es "nivel Bajo". No obstante, se puede cambiar la configuración del nivel accediendo a la página inicial de la aplicación Web y seleccionando la opción *DVWA Security* (Figura 2.1, menú a la izquierda)

4. Bola extra (opcional)

Se propone realizar pruebas de penetración en la misma aplicación DVWA considerando otros 3 tipos diferentes de vulnerabilidades con los niveles de seguridad *bajo*, *medio* y *alto*.

5. Puntuación

La valoración máxima de esta práctica es **10 puntos** así repartidos:

- Parte obligatoria (Sección 3): **8 puntos**
- Bola extra (Sección 4): **2 puntos**

6. Entrega

Se pide entregar el siguiente material en Moodle:

- Nombre, apellidos y NIA de cada miembro del grupo de práctica, así como el correspondiente grupo de prácticas (*inf1* ... *inf4*).
- Un informe donde se explique el procedimiento seguido para la explotación de cada tipo de vulnerabilidad Web considerada. En particular:
  - Indicar si se han utilizado herramientas de *pentesting* y si han sido útiles o no.
  - Añadir observaciones sobre los resultados obtenidos para el tipo de ataque realizado, explicando por qué el ataque tiene éxito para un nivel de seguridad de la aplicación y por qué no para niveles superiores. En estos casos, ¿cuáles son las contramedidas implementadas que derrotan el ataque?

La fecha límite de entrega de esta práctica es **tres semanas desde la realización de la práctica**.