Laboratorio 2

Detección de Vulnerabilidades

Profesores: Alejandro Hevia y Eduardo Riveros
Auxiliares: Sergio Rojas
Ayudantes: Darlene Sobarzo y Tomás Alvarado

- Trabajo personal o en parejas
- Entrega: lunes 12 de mayo a las 23:59 hrs.

En este laboratorio realizaremos un proceso de **pentesting** a un servicio web de juguete, intentado simular el proceso legal que se realizaría en la realidad para detectar vulnerabilidades.

El equipo docente del curso está lanzando un nuevo servicio web y contrató a sus estudiantes para realizar **pentesting** (gratis). El equipo docente les entregó todos los permisos legales para que puedan explotar este servicio de cualquier forma (en la realidad esto es súper importante, siempre necesitan la autorización legal de los dueños del servicio para no considerar el trabajo como un crimen).

Para poder terminar el trabajo solicitado, les tendrás que entregar todas las vulnerabilidades que hayas encontrado en un reporte.

1. Página web

El servicio web en la que tendrán que buscar vulnerabilidades es lab2.cc5327.hackerlab.cl/DVWA. Podrán conectarse al servidor solamente si están conectados a las redes *fcfm* o *DCCAIR*. Si están trabajando fuera de la universidad, tendrán que acceder mediante la *VPN* del CEC. Se tendrán que loggear con:

- username: admin
- password: password

2. Reporte de la vulnerabilidad

En la sección enlaces de U-Cursos encontrarán una plantilla de un reporte. Cuando encuentren una vulnerabilidad, deberán ingresar esta en un reporte a partir de esa plantilla, el cual deberá tener **todos** sus campos rellenados.

Al momento de asignar un nivel de criticidad a la vulnerabilidad, les solicitamos revisar el puntaje CVSS asignado a ella:

- Si el puntaje es mayor o igual a 9, se considera CRÍTICA
- Si el puntaje es mayor o igual a 7, se considera ALTA
- Si el puntaje es mayor o igual a 5, se considera MEDIA

En cualquier otro caso, se considera BAJA

3. Recursos importantes

- Common Vulnerabilities and Exposures: link cve
- Common Weakness Enumeration: link cwe
- Common Vulnerability Score System: link cvss

4. Entregables

Por U-Cursos tendrán que subir un reporte que contenga:

- **(2.0 pts)** Una vulnerabilidad relacionada con inyecciones SQL.
- **(2.0 pts)** Una vulnerabilidad relacionada con XSS.
- **(2.0 pts)** Una vulnerabilidad extra, relacionada a cualquier tipo de ataque.