Informe Laboratorio 2

Sección x

Alumno x
e-mail: alumno.contacto@mail.udp.cl

Septiembre de 2025

Índice

1. Descripción de actividades

Utilizando la aplicación web vulnerable DVWA
(Damn Vulnerable Web App - https://github.com/digininja/DVWA (Enlaces a un sitio externo.)) realice las siguientes actividades:

- Despliegue la aplicación en su equipo utilizando docker. Detalle el procedimiento y explique los parámetros que utilizó.
- Utilice Burpsuite (https://portswigger.net/burp/communitydownload (Enlaces a un sitio externo.)) para realizar un ataque de fuerza bruta contra formulario ubicado en vulnerabilities/brute. Explique el proceso y obtenga al menos 2 pares de usuario/contraseña válidos. Muestre las diferencias observadas en burpsuite.
- Utilice la herramienta cURL, a partir del código obtenido de inspect elements de su navegador, para realizar un acceso válido y uno inválido al formulario ubicado en vulnerabilities/brute. Indique 4 diferencias entre la página que retorna el acceso válido y la página que retorna un acceso inválido.
- Utilice la herramienta Hydra para realizar un ataque de fuerza bruta contra formulario ubicado en vulnerabilities/brute. Explique el proceso y obtenga al menos 2 pares de usuario/contraseña válidos.
- Compare los paquetes generados por hydra, burpsuite y cURL. ¿Qué diferencias encontró? ¿Hay forma de detectar a qué herramienta corresponde cada paquete?
- Desarrolle un script en Python para realizar un ataque de fuerza bruta:
  - Utilice la librería requests para interactuar con el formulario ubicado en vulnerabilities/brute y desarrollar su propio script de fuerza bruta en Python. El script debe realizar intentos de inicio de sesión probando una lista de combinaciones de usuario/contraseña.
  - Identifique y explique la cabecera HTTP que empleará para realizar el ataque de fuerza bruta.
  - Muestre el código y los resultados obtenidos (al menos 2 combinaciones válidas de usuario/contraseña).
  - Compare el rendimiento de este script en Python con las herramientas Hydra, Burpsuite, y cURL en términos de velocidad y detección.
- Investigue y describa 4 métodos comunes para prevenir o mitigar ataques de fuerza bruta en aplicaciones web:
  - Para cada método, explique su funcionamiento, destacando en qué escenarios es más eficaz.

2. Desarrollo de actividades según criterio de rúbrica

2.1. Levantamiento de docker para correr DVWA (dvwa)

2.2. Redirección de puertos en docker (dvwa)

2.3. Obtención de consulta a replicar (burp)

2.4. Identificación de campos a modificar (burp)

2.5. Obtención de diccionarios para el ataque (burp)

2.6. Obtención de al menos 2 pares (burp)

2.7. Obtención de código de inspect element (curl)

2.8. Utilización de curl por terminal (curl)

2.9. Demuestra 4 diferencias (curl)

2.10. Instalación y versión a utilizar (hydra)

2.11. Explicación de comando a utilizar (hydra)

2.12. Obtención de al menos 2 pares (hydra)

2.13. Explicación paquete curl (tráfico)

2.14. Explicación paquete burp (tráfico)

2.15. Explicación paquete hydra (tráfico)

2.16. Mención de las diferencias (tráfico)

2.17. Detección de SW (tráfico)

2.18. Interacción con el formulario (python)

2.19. Cabeceras HTTP (python)

2.20. Obtención de al menos 2 pares (python)

2.21. Comparación de rendimiento con Hydra, Burpsuite, y cURL (python)

2.22. Demuestra 4 métodos de mitigación (investigación)

Conclusiones y comentarios