Rapport Pentest sur Application Web Médicale

# Introduction

Dans un environnement où la santé et la confidentialité des données patients sont primordiales, la sécurité des applications web dans le domaine médical revêt une importance stratégique. Ce document présente un processus complet de pentesting légal, adapté aux spécificités d’une application web médicale. Il aborde l’ensemble des phases du test d’intrusion (reconnaissance, scanning, exploitation, post-exploitation et reporting) en détaillant les objectifs, outils et précautions à prendre pour respecter les exigences légales et sécuritaires (ex. RGPD, normes HDS).

# 1. Phase de Reconnaissance et Collecte d'Informations

## Objectifs

- Identification de la surface d’attaque  
- Compréhension de l’environnement réglementaire

## Méthodologie et Outils Spécifiques

- OSINT adapté aux applications de santé : Maltego, theHarvester, Google Dorks, Shodan  
- Analyse DNS, WHOIS et Réseaux : Recon-ng, dnsenum, vérification SSL/TLS et conformité HDS

## Recommandations Spécifiques

- Réaliser une veille sur la réglementation  
- Documenter toutes les sources

# 2. Phase de Scanning et Énumération

## Objectifs

- Identifier les services et ports ouverts  
- Localiser les vulnérabilités

## Méthodologie et Outils Spécifiques

- Analyse des ports et services : Nmap, Masscan, Netcat  
- Scan de vulnérabilités : Nikto, OWASP ZAP, Burp Suite, OpenVAS, Nessus

## Recommandations Spécifiques

- Planifier des scans non-destructifs  
- Segmenter le réseau

# 3. Phase d’Exploitation

## Objectifs

- Valider les vulnérabilités  
- Mesurer le niveau d’accès

## Méthodologie et Outils Spécifiques

- Exploitation : Metasploit, SQLmap, Burp Suite  
- Configurations faibles : erreurs SSL, redirections, MFA

## Recommandations Spécifiques

- Procéder sous surveillance  
- Utiliser des environnements de test

# 4. Phase de Post-Exploitation et Maintien de l’Accès

## Objectifs

- Analyser l’impact  
- Maintenir un accès contrôlé

## Méthodologie et Outils Spécifiques

- Élévation de privilèges : LinPEAS, WinPEAS, Mimikatz  
- Maintien d’accès : Empire, ProxyChains, Chisel

## Recommandations Spécifiques

- Éviter le maintien d’accès en production  
- Documenter chaque action

# 5. Phase de Reporting et Rétro-ingénierie

## Objectifs

- Documenter les vulnérabilités  
- Proposer des recommandations

## Méthodologie et Outils Spécifiques

- Rédaction : Dradis, Faraday  
- Rétro-ingénierie : Ghidra, IDA Pro, Radare2  
- Rapport conformité et impact  
- Plan de remédiation

## Recommandations Spécifiques

- Assurer la clarté du rapport  
- Prévoir une session de restitution

# Conclusion

La réalisation d’un pentest sur une application web médicale nécessite une approche méthodique et rigoureuse. Chaque étape doit être adaptée pour respecter les contraintes légales, les exigences de confidentialité et la criticité des données de santé. En suivant la démarche présentée et en appliquant les outils et recommandations spécifiques, il est possible de renforcer significativement la sécurité de l’application, minimisant ainsi les risques d’attaques et d’incidents de sécurité.  
  
La collaboration étroite entre les équipes techniques, la direction de la sécurité et les responsables réglementaires est cruciale pour assurer la protection des systèmes et des données sensibles dans le secteur médical.