IT/Dev Internship : Automate Security test for Telemis installation

Telemis is a medical equipment company specializing in PACS/MACS solutions, digital pathology, and Business Intelligence for healthcare. Its products help healthcare facilities, private practices, and so on, to efficiently manage medical imaging and healthcare data. At Telemis, we cultivate a close-knit atmosphere where mutual support and spontaneous collaboration are the norm.

Project Objective

The primary goal of this internship is to design, develop, and implement an automated security testing framework. This framework will continuously assess the security posture of our web applications and portals deployed at customer sites (hospitals), ensuring they are securely configured and hardened against common vulnerabilities.

Context

Telemis provides critical software solutions to the healthcare industry. Our applications are installed in complex IT environments within numerous hospitals. Manually verifying the security of each unique installation is time-consuming and doesn't scale effectively.

To proactively manage our security landscape, we need to transition from manual spot-checks to a continuous and automated validation process. The intern will build a solution that can regularly scan a list of customer URLs for security misconfigurations and vulnerabilities like those identified in our internal penetration tests.

Internship Objectives *(adapted depending on duration and skill level)*

- Familiarize yourself with our existing security test reports and documentation.
- Automate specific security checks. Examples include:
    - Verifying TLS/SSL certificate validity and cipher strength.
    - Detecting exposed administration portals or services.
    - Checking for information leakage from error pages, headers (e.g., Server version), and stack traces.
    - Probing for default credentials on known endpoints.
- Build a core engine that takes a list of target URLs and systematically runs the suite of test scripts against each one.
- Document the framework, the individual test scripts, and the procedure for running the scans and interpreting the results.

What the intern will gain from this experience

- **Practical Cybersecurity Skills:** Gain hands-on experience in identifying and testing for real-world security vulnerabilities in a corporate environment.
- **Automation & DevSecOps:** Learn how to build security automation tools from scratch, a highly sought-after skill in the field of DevSecOps (Development, Security, and Operations).
- **Web Application Security:** Deepen your understanding of how web applications are attacked and, more importantly, how they are secured and hardened.
- **Healthcare IT Insight:** Gain valuable experience working on security challenges within the critical and highly regulated healthcare technology sector.

Profile

- Currently pursuing a degree in Computer Science, Cybersecurity, Information Technology, or a related field.
- Strong scripting skills, preferably in Python.
- A good understanding of web technologies and protocols (HTTP/HTTPS, APIs, Cookies, Headers)

Stage IT/Dev : Automatiser les tests de sécurité pour l'installation Telemis

Telemis est une entreprise d'équipement médical spécialisée dans les solutions PACS/MACS, la pathologie numérique et la Business Intelligence pour la santé. Ses produits aident les établissements de santé, les cabinets privés, etc., à gérer efficacement l'imagerie médicale et les données de santé. Chez Telemis, nous cultivons une ambiance de soutien mutuel et de collaboration spontanée.

Objectif du projet

L'objectif principal de ce stage est de concevoir, développer et mettre en œuvre un cadre de test de sécurité automatisé. Ce cadre évaluera en permanence la posture de sécurité de nos applications et portails web déployés chez nos clients (hôpitaux), en veillant à ce qu'ils soient configurés de manière sécurisée et renforcés contre les vulnérabilités courantes.

Contexte

Telemis fournit des solutions logicielles critiques au secteur de la santé. Nos applications sont installées dans des environnements informatiques complexes au sein de nombreux hôpitaux. La vérification manuelle de la sécurité de chaque installation unique prend beaucoup de temps et n'est pas efficace à grande échelle.

Pour gérer de manière proactive notre paysage de sécurité, nous devons passer de vérifications ponctuelles manuelles à un processus de validation continu et automatisé. Le stagiaire construira une solution capable d'analyser régulièrement une liste d'URL clients à la recherche de mauvaises configurations de sécurité et de vulnérabilités telles que celles identifiées lors de nos tests d'intrusion internes.

Objectifs du stage *(adaptés en fonction de la durée et du niveau de compétence)*

- Se familiariser avec nos rapports et documentations de tests de sécurité existants.
- Automatiser des vérifications de sécurité spécifiques. Exemples :
    - Vérifier la validité des certificats TLS/SSL et la force des chiffrements.
    - Détecter les portails ou services d'administration exposés.
    - Vérifier les fuites d'informations provenant des pages d'erreur, des en-têtes (par exemple, version du serveur) et des traces de pile.
    - Rechercher les identifiants par défaut sur les points d'accès connus.
- Construire un moteur central qui prend une liste d'URL cibles et exécute systématiquement la suite de scripts de test sur chacune d'elles.
- Documenter le cadre, les scripts de test individuels et la procédure d'exécution des analyses et d'interprétation des résultats.

Ce que le stagiaire retirera de cette expérience

- Compétences pratiques en cybersécurité : Acquérir une expérience pratique dans l'identification et le test de vulnérabilités de sécurité réelles dans un environnement d'entreprise.
- Automatisation et DevSecOps : Apprendre à construire des outils d'automatisation de la sécurité à partir de zéro, une compétence très recherchée dans le domaine du DevSecOps (Développement, Sécurité et Opérations).
- Sécurité des applications web : Approfondir la compréhension des attaques contre les applications web et, plus important encore, de la manière dont elles sont sécurisées et renforcées.
- Connaissance de l'informatique de la santé : Acquérir une expérience précieuse en travaillant sur les défis de sécurité au sein du secteur critique et hautement réglementé des technologies de la santé.

Profil

- Actuellement en cursus en informatique, cybersécurité, technologies de l'information ou un domaine connexe.
- Solides compétences en scripting, de préférence en Python.
- Une bonne compréhension des technologies et protocoles web (HTTP/HTTPS, API, Cookies, En-têtes).