Cahier des charges: ThreatXplore

Scanner de vulnérabilités web réalisé dans le cadre d'un projet annuel par :

Daniela Ceraku & Salla Diop

Table de matières

Introduction

ThreatXplore est un projet annuel visant à développer et perfectionner un scanner de vulnérabilités web capable de détecter jusqu'à 30 types de vulnérabilités sur un site web donné. Le scanner est conçu pour fonctionner dans trois modes distincts : page web, application et en ligne de commande (CLI). Chaque vulnérabilité identifiée par ThreatXplore vient avec des recommandations détaillées sur les moyens de défense et des explications sur les méthodes d'exploitation potentielles.

Contexte et Motivation du Projet

Dans un monde de plus en plus connecté, la sécurité des applications web est devenue un enjeu majeur pour les entreprises et les développeurs. Les cyberattaques sont de plus en plus sophistiquées, et les vulnérabilités web représentent une porte d'entrée courante pour les attaquants. C'est dans ce contexte que nous avons choisi de développer ThreatXplore.

Notre objectif principal est de fournir un outil accessible et polyvalent pour aider les développeurs et les entreprises à identifier et corriger rapidement les failles de sécurité dans leurs applications web. En offrant des modes de fonctionnement variés (web, application, CLI), nous souhaitons répondre aux besoins diversifiés de nos utilisateurs et faciliter l'intégration de la sécurité dans le cycle de développement.

Le projet ThreatXplore est un effort continu pour améliorer la sécurité web et fournir aux utilisateurs des outils pratiques et efficaces pour protéger leurs pages web.

Planification et Gestion de Projet

Pour la planification du projet, nous avons adopté une méthodologie rigoureuse afin d'assurer une progression efficace et coordonnée à chaque étape. Pour une répartition claire des responsabilités et une gestion optimale des tâches, nous avons mis en place une matrice RACI adaptée à la planification du projet SI. Cette matrice permet de définir les rôles de chaque activité du projet : qui est Responsable, qui est Acteur, qui doit être Consulté et qui doit être Informé. Ainsi, chaque membre de l'équipe comprend précisément ses responsabilités et à qui il doit rendre compte.

La matrice RACI:

Tâches	Daniela Ceraku	Salla Diop
Création d'une BD avec des vulnérabilités incluses.	R	R
Mise en place d'un laboratoire vulnérable pour mener des tests	R	A, C, I
Création des scripts pour détecter les vulnérabilités web	R	A, C, I
Création d'une interface graphique pour l'application	R	A, C, I
Création de la page web en HTML et CSS (contenant plusieurs pages).	A, C, I	R
Création d'un serveur Flask pour faire la liaison du front-end avec le back-end	R	R
Création d'une version en CLI faisant appel aux scripts de détection	A, C, I	R

Création des scripts en JavaScript pour améliorer la page web	R	R
Optimisation du scan des vulnérabilités	R, A, C, I	A, C, I
Création des Dockerfiles pour faciliter l'installation pour l'utilisateur	R	A, C, I
Création de la documentation et du README	R, A, C, I	R, A, C, I

Nous avons mis en place un référentiel GitHub dédié au projet "ThreatXplore" (https://github.com/DanielaCe18/ThreatXplore) pour gérer l'ensemble de nos travaux. Ce référentiel est structuré avec un modèle spécifique pour les projets logiciels, et des issues y sont attribuées aux membres de l'équipe en fonction de leurs compétences et de leur disponibilité.

En utilisant ces outils, nous nous assurons que le projet progresse de manière organisée. La collaboration et la communication au sein de l'équipe sont ainsi facilitées, ce qui permet une résolution rapide des problèmes et nous aide à atteindre nos objectifs dans les délais impartis.

Conception du Projet

L’objectif de ce projet était de développer un scanner de vulnérabilités décliné en trois versions : une version web, une version en ligne de commande (CLI), et une version applicative. Dans un premier temps, nous avons sélectionné les vulnérabilités les plus pertinentes. Par la suite, nous avons conçu plus de 27 scripts de détection pour chaque vulnérabilité identifiée. Afin de garantir la fiabilité du scanner, nous avons utilisé deux des meilleurs environnements de test en matière de pentesting : bWAPP, installé sur nos machines, et les laboratoires en ligne de PortSwigger. Nos scripts ont réussi tous les tests de validation.

La page web du scanner offre plusieurs onglets : un onglet qui explique les vulnérabilités proposées ainsi que leur score CVSS, un onglet permettant de télécharger les versions CLI et applicative, un onglet sur nos profils, et enfin un onglet permettant d’effectuer le scan en choisissant parmi les 27 vulnérabilités disponibles. Le frontend de la page web est relié au serveur via Python Flask, permettant l’accès à l’interface web à l'adresse http://127.0.0.1:5000 une fois le serveur lancé.

La version applicative du scanner a été développée en utilisant la bibliothèque Tkinter de Python, offrant une interface utilisateur conviviale et intuitive. En conclusion, ce projet propose une solution robuste et complète pour la détection de vulnérabilités, adaptée à divers modes d'utilisation, tout en assurant un haut niveau de fiabilité grâce à des environnements de test rigoureux.

Fonctionnement

Notre scanner propose de détecter 27 vulnérabilités web parmi les plus pertinentes, y compris celles répertoriées par l'OWASP. Lorsque le scanner est lancé sur la page web cible, il effectue une analyse complète du code, des paramètres HTTP, des fichiers, etc. Si une vulnérabilité est détectée, elle sera affichée avec sa description et deux options : Blue Team et Red Team. La Blue Team fournira des mesures de prévention pour la vulnérabilité en question, tandis que la Red Team proposera des payloads, des conseils d'attaque et des informations sensibles.

Les vulnérabilités détectées incluent notamment SQL Injection (SQLi), Cross-Site Scripting (XSS), Cross-Origin Resource Sharing (CORS), Server-Side Template Injection (SSTI), Server-Side Request Forgery (SSRF), Cross-Site Request Forgery (CSRF), OS Command Injection, Local File Inclusion (LFI), Unrestricted File Upload, Web Crawler, SSL/TLS-related vulnerabilities, Certificate issues, XML External Entity (XXE), Path Traversal, Common Passwords, Account Lockout, Brute Force, Analysis of robots.txt, WHOIS Scan, Uncommon HTTP Methods, URL Redirections, Security Headers, et WebSocket Manipulation.

Pour installer les différentes versions du scanner, les utilisateurs peuvent utiliser les Dockerfiles disponibles sur le repository Git.

Perspectives

Pour continuer à améliorer notre projet "ThreatXplore" et répondre aux besoins évolutifs de nos utilisateurs, nous envisageons plusieurs améliorations supplémentaires, sous réserve que les fonctionnalités existantes soient bien établies et offrent une expérience utilisateur de qualité.

Nous prévoyons d'ajouter une fonctionnalité de Cyber Threat Intelligence : l'intégration d'une IA capable de se renforcer continuellement en effectuant des tests réguliers et en sauvegardant les résultats pour améliorer ses performances au fil du temps.

En outre, nous envisageons d'élargir la détection proactive à d'autres types de vulnérabilités. Bien que notre scanner propose actuellement la détection de 27 vulnérabilités et soit open source, contrairement à de nombreux scanners en ligne, nous pourrions ajouter davantage de vulnérabilités ou même établir une liaison avec l'OWASP pour intégrer chaque nouvelle vulnérabilité identifiée.

Ces améliorations visent à renforcer la capacité de "ThreatXplore" à offrir une solution de sécurité web robuste et évolutive, tout en maintenant un haut niveau de fiabilité et d'efficacité pour nos utilisateurs.

Conclusion

En conclusion, le projet "ThreatXplore" que nous développons pour notre troisième année en sécurité informatique vise à répondre à l'ensemble des exigences énoncées dans notre cahier des charges. Notre objectif est de créer une plateforme de détection des vulnérabilités efficace et complète.

Ce projet annuel reflète parfaitement notre parcours en sécurité informatique, nous permettant de renforcer nos compétences dans ce domaine crucial. Il nous offre l'opportunité de consolider nos connaissances en matière de sécurité des sites web, de tests d'intrusion, et de développement logiciel.

Travailler sur "ThreatXplore" nous prépare à relever les défis complexes associés à ce type de projet. Il nous permet d'acquérir une expérience pratique précieuse et de développer des compétences essentielles dans le domaine de la cybersécurité.

En résumé, le projet "ThreatXplore" représente une étape significative dans notre parcours académique et professionnel en cybersécurité, et nous sommes fières du travail accompli.