Ruben BATTOCCHIO
13/11/2025

Cybersécurité

I. Introduction

Dans ce TP,nous allons voir ce qu'est la veille technologique et l'audit de sécurité des applications web. Nous allons regarder les méthodes et les outils pour se tenir informé des évolutions technologiques. Nous allons ensuite mettre en pratique l'audit de sécurité d'un site web à l'aide d'outils spécifiques, et utiliser des services de vérification pour proposer des mesures de sécurité.

II. Exercice 1

Objectif de la veille technologique	vérifier que les auteurs d'information sont fiables	les auteurs d'information sont fiables s'assurer que les sources sont fiables	s'assurer que les informations sont neutres et pas détournées.	Vérifier que les données sont exacte et basé sur des faits prouvé	s'assurer que les informations sont mis à jour régulièrement	Choisir des informations pertinentes pour et utiles pour la protection des…
Source d'information	Crédibilité de l'auteur	Fiabilité de la source	Objectivité de l'information	Exactitude de l'information	Actualité de l'information	Pertinence de l'information
Exemples: sites web…	organisation internationale	ANSSI	site d'actualité technique,	données techniques	alertes et vulnérabilités mises à jour en temps réel	exemple de site bancaire sécurisé à analyser pour la veille

Evaluation	4	4	3	4	4	4

III. Exercice 2

	Outil de collecte de l'information	Outil de traitement de l'information	Outil de curation de l'information	Outil de partage des résultats
Nom de l'outil	Google Alerts	Excel	OneNote	GoogleDoc
Avantages	Automatisation de la collecte d'information	Permet d'extraire et analyser des données	Organise et regroupe les ressources pertinentes	Collaboration en temp réel, facilité d'accès
Inconvénients	peut générer des informations inutiles	nécessite certaines compétences techniques	peut devenir compliqué si trop d'information	Risque des pertes de données en cas d'erreurs humaines

IV. Exercice 3

OWASP ZAP : Outil gratuit qui scanne les vulnérabilités web en interceptant les requêtes, idéal pour détecter les failles courantes.
W3AF : Framework open-source avec de nombreux plugins pour auditer et attaquer les applications web afin de repérer diverses vulnérabilité

V. Exercice 4

Test effectué pour le site : OWASP ZAP (https://www.intruder.io)

Critères d'analyse	Google Safe Browsing	URLVoid
Malware	Vérifie si le site contient des malwares (virus, trojans). aucun contenue suspect détécter	Cherche si le site est listé pour des malwares. ✅Rien Trouvé
Spam	Vérifie si le site est associé à du contenu spam. aucun contenue suspect détécter	Recherche dans des bases de données de sites spams. ✅Rien Trouvé
Phishing	Vérifie si le site imite un autre site pour voler des infos. aucun contenue suspect détécter	Vérifie si le site est signalé pour du phishing. ✅Rien Trouvé
Taux de réputation	Vérifie la réputation du site selon Google. aucun contenue suspect détécter	Vérifie la réputation dans plusieurs bases de données. ✅Rien Trouvé
Listes noir	Vérifie si le site est sur des listes noires (ex. Google). aucun contenue suspect détécter	Consulte des bases de données de listes noires. ✅Rien Trouvé

VI. Exercice 5

Note à l'attention de M.Schmitt

Suite à la défiguration du site de M@Banque, il est essentiel d'informer vos clients sur les moyens de vérifier l'intégrité du site web afin de leur donner confiance. Mais surtout d'éviter qu'ils ne soient victimes de cyberattaque, de malwares ou de fraude. La confiance des clients est primordiale et permet de ramener encore plus de clients. Une action simple et rapide est donc nécessaire pour assurer leur sécurité.

Nous vous recommandons de mettre en place une solution de vérification continue de l'intégrité du site à l'aide des outils d'audit de sécurité. Ces outils permettent de détecter toute anomalie sur le site. Ex: une infection par malware, une attaque par phishing… Parmi les outils les plus efficaces, vous pouvez utiliser :

- OWASP ZAP
- W3AF

Mais aussi des outils qui vous permettront d'effectuer des contrôles réguliers :

- Google Safe Browsing
- UrlVoid

Ces outils offriront un panel complet pour identifier les vulnérabilités et maintenir la sécurité du site. Vous pourrez donc rassurer les clients sur la fiabilité du site.

De plus, vous pouvez faire ce qu'on appelle une veille technologique afin de répertorier chaque semaine / mois les modifications effectuées sur le site. Cela permet d'avoir une trace écrite claire, nette et précise de l'historique du site.

VII. conclusion

Dans ce Tp nous avons découvert des outils et des services qui nous permettent d'identifier des malwares, attaques… sur un site. Mais aussi des outils afin d’effectuer une veille technologique pour répertorier ici, l'avancée du site dans le temps.