

Rapport de TP : M@Banque

Sommaire

I. Introduction	1
II. Le travail à réaliser	1
III. Conclusion	4

I. Introduction

Nous avons pour objectif d'explorer les solutions et outils permettant d'auditer efficacement un site web, afin de détecter les vulnérabilités et garantir l'intégrité numérique de M@Banque. Pour ce faire, nous réaliserons plusieurs exercices pratiques.

II. Le travail à réaliser

1) Voici le tableau d'organisation complété de la veille technologique :

Objectifs de la veille technologique	Identifier les experts du domaine	Garantir la véracité des outils	Sélectionner des informations neutres	Valider la fidélité des caractéristiques techniques.	Trouver les dernières versions et mises à jour de l'outil.	Répondre directement au besoin d'audit.
Sources d'informations	Crédibilité de l'auteur	Fiabilité de la source	Objectivité de l'information	Exactitude de l'information	Actualité de l'information	Pertinence de l'information
Exemple : site web	www.n26.com	www.n26.com	www.n26.com	www.n26.com	www.n26.com	www.n26.com
Evaluation	3	3	2	3	4	3

2) J'ai donc fait un tableau

	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 (Alertes par courriel)	Feedly	Scoop.it!	Slack
Avantages	Simplicité d'utilisation	Possibilité de filtrer par pertinence et de marquer les articles les plus importants.	Possibilité d'ajouter des commentaires	Diffusion rapide et ciblée vers des canaux spécifiques (Mme Schmitt, équipe technique). Historique des échanges.
Inconvénients	Les résultats sont souvent très génériques	Le traitement reste limité	La version gratuite a des limitations importantes	Le message peut se perdre dans les autres discussions du canal.

3)

Après mes recherches, j'ai identifié deux outils d'audit de sécurité pour les sites web : **Burp Suite** et **Nessus**.

Burp Suite est un outil pour les tests de sécurité des applications web. Il agit comme un proxy entre le navigateur et l'application, ce qui permet aux auditeurs d'intercepter, d'analyser et de modifier le trafic. Cette approche facilite la détection de vulnérabilités que les scanners automatiques ne repèrent pas toujours.

Nessus, quant à lui, est l'un des plus anciens et des plus utilisés scanners de vulnérabilités. Il sert principalement à identifier les failles au niveau de l'infrastructure qui héberge un site web. Grâce à lui, on obtient une vue d'ensemble des risques liés à l'environnement d'hébergement.

4) Voici le tableau comparatif des audits de sécurité de site Web.

Critères d'analyse	Google Safe Browsing n26.com	URLvoid n26.com
Malware	Non	Non
Spam	Non	Non
Blacklist	Non	Non
Défiguration	Non	Non
Sécurisé	Oui	Oui

Résultats des sites :

Google Safe Browsing









Vérifier l'état du site

www.n26.com

État actuel

✓ **Aucun contenu suspect détecté**

URLvoid

Engine	Result
 Artists Against 419	✓ Nothing Found
 Avira	✓ Nothing Found
 AZORult Tracker	✓ Nothing Found
 Badbitcoin	✓ Nothing Found
 Bambenek Consulting	✓ Nothing Found
 BitDefender	✓ Nothing Found
 c_APT_ure	✓ Nothing Found
 CERT Polska	✓ Nothing Found

5)

Madame Schmitt,

Dans le cadre de notre engagement pour la sécurité de nos clients, nous souhaitons les rassurer sur l'intégrité de notre site M@Banque et sur la protection de leurs données personnelles. Il est naturel que certains se posent des questions sur la sécurité de la plateforme, notamment concernant les risques de virus, de malwares ou de tentatives de phishing.

Afin de garantir une transparence totale, nous avons choisi de leur proposer une solution simple et fiable : Google Safe Browsing. Cet outil, développé par Google, est utilisé par des millions d'internautes pour vérifier la sécurité des sites web. Nous demandons à nos clients de réaliser cette vérification par eux-mêmes, ce qui leur permettra de confirmer que M@Banque est un site sûr, exempt de toute menace.

Cette vérification est très facile à effectuer et démontre clairement que notre site n'est pas piégé, qu'il ne contient aucun malware et qu'il ne tente pas de voler leurs informations personnelles. Il est important de préciser que nous n'avons rien à cacher et que cette démarche vise à offrir une transparence totale.

Les clients peuvent effectuer cette vérification à l'aide du lien suivant :

[Google Safe Browsing - Vérification de sécurité de M@Banque](#)

Nous vous remercions de bien insister sur ce point de transparence et de sécurité dans votre communication auprès des clients.

Cordialement,

CHELLE

III. Conclusion

En conclusion, ce TD m'a permis de comprendre qu'une bonne protection d'un site web commence par une veille technologique régulière. J'ai également découvert qu'il existe une large gamme d'outils

pour évaluer la sécurité d'un site, allant des solutions complexes destinées aux experts jusqu'à des outils simples comme Google Safe Browsing. Mais ce que j'ai surtout retenu, c'est que face à un problème, la priorité est de communiquer rapidement et de manière transparente, en fournissant des preuves claires et accessibles, pour rassurer les clients et restaurer leur confiance. J'ai pris 2h à faire ce TP, j'ai bien aimé le faire car je trouvais ce TP relativement simple.