

MÉTHODOLOGIE D'ÉVALUATION D'APPLICATIONS WEB

L'**OWASP** (Open Web Application Security Project) est un projet de sécurité communautaire impliquant différents intervenants de tous les milieux. En d'autres mots, c'est la communauté qui crée des documents accessibles et libres de droits tels que des articles, des méthodologies, des outils etc.

La fondation OWASP est un organisme à but non lucratif qui n'est associé à aucune compagnie d'informatique. Les documents les plus reconnus de l'OWASP, sont: « The OWASP guide to building secure web applications v2 » et le « OWASP TOP 10 ».

Afin de procéder à une évaluation de sécurité rigoureuse, **Gardien Virtuel** effectue une vérification des sites web en fonction du guide de l'OWASP. Ce guide relate, entre autres, les bonnes pratiques en création de site Internet et les analystes de **Gardien Virtuel** l'utilisent afin de valider la sécurité d'un site web. Ensuite, il y a une validation de chacune des pratiques durant laquelle tout manquement et toute faille de sécurité sont relevés. Voici donc un court résumé des différentes catégories de tests ainsi qu'une explication des impacts rattachés.

Catégorie de test	Explication des impacts
<i>Paramètres reçus</i>	Chaque paramètre d'une application correspond à une ouverture potentiellement exploitable par un pirate. Les caractères reçus ainsi que le traitement effectué sont à risque. Un attaquant peut utiliser une faille pour attaquer directement une application ou un serveur utilisé par l'application Web en se basant sur les informations reçues de ce dernier.
<i>Contrôles d'accès</i>	Il est possible pour un attaquant de visionner des fichiers sensibles ou d'utiliser des fonctions non autorisées si les contrôles présents sont défectueux.
<i>Gestion des sessions</i>	Un attaquant peut-il voler l'identité d'un autre utilisateur ou d'en modifier les paramètres d'accès afin d'obtenir des accès non autorisés?
<i>Script d'attaque croisée (XSS)</i>	Une attaque réalisée avec succès peut fournir un faux contenu à un client floué ou permettre de découvrir de l'information sur ce client.
<i>Surcharge de mémoire tampon</i>	L'application ne valide pas toutes les informations entrées. Une application vulnérable peut cesser de fonctionner ou permettre à l'attaquant d'en prendre le contrôle.
<i>Injection de commande</i>	Une autre application externe reçoit des paramètres sans en valider leur contenu. Un risque de modification de ces paramètres ou d'ajout de valeurs est donc présent.
<i>Gestion des erreurs</i>	Toutes informations fournies à l'utilisateur concernant une erreur survenue ne doit rien contenir à propos de cette application ou des chemins qu'elle utilise.
<i>Journalisation</i>	L'objectif de la journalisation consiste à retrouver l'origine d'un événement dans une application. Sans une journalisation adéquate des erreurs, les attaques peuvent passer inaperçues pour les administrateurs de systèmes.
<i>Chiffrement</i>	Il est fréquent de voir les modules de cryptographie être mal utilisés (mauvaise configuration ou chiffrement faible) causant ainsi une faiblesse de protection.

Source : http://www.owasp.org/index.php/OWASP_Testing_Guide_v2_Table_of_Contents

**Avez-vous besoin d'évaluer vos applications web ?
Contactez-nous dès aujourd'hui pour une évaluation gratuite !**

ANALYSE D'APPLICATIONS WEB : LA MÉTHODOLOGIE GARDIEN VIRTUEL INC.

En sécurité des TI, il n'est pas toujours évident de spécifier le coût et le délai pour un service. Cette difficulté est accrue lorsqu'on traite d'applications web puisque c'est encore moins quantifiable que de travailler avec du matériel informatique (postes de travail, serveurs, routeurs, etc.) qui nous permet habituellement de faire des estimations de coûts plus précises.

Pour tenter de résoudre ce problème et de satisfaire les clients, **Gardien Virtuel** a développé trois niveaux de notre méthodologie d'analyse d'applications web. Vous trouverez donc ci-dessous nos meilleurs estimés en termes de « délais ». Le seul moyen d'avoir une idée encore plus précise est que le client fournisse par écrit à **Gardien Virtuel** toutes les informations pertinentes à l'application elle-même (nombre de pages, nombre de formulaires etc.)

TYPES	LE « LÉGER »	LE « CLASSIQUE »	« L'APPROFONDI »
<i>Délai d'exécution (estimé⁽²⁾)</i>	2 à 5 jours	4 à 8 jours	9 jours et plus
<i>Sommaire descriptif</i>	Très large et peu profond (vise 60% des vulnérabilités)	Large et profond (vise 85% des vulnérabilités)	Large et très profond (vise 95% des vulnérabilités)
<i>Balayage automatisé des vulnérabilités</i>	✓	✓	✓
<i>Validation des faux positifs</i>	✓	✓	✓
<i>Test OWASP : Top 10 seulement</i>	✓	✓	✓
<i>SANS Top 20</i>	✓	✓	✓
<i>Test OWASP : complet</i>		✓	✓
<i>Validation des faux négatifs</i>		✓	✓
<i>Évaluation de la sécurité du serveur</i>		✓	✓
<i>Test manuel de sécurité</i>		✓	✓
<i>Analyse du code source (recensement des failles et faiblesses potentielles)</i>			✓

1) Certains détails peuvent changer sans préavis

2) Ces données représentent nos meilleurs estimés. Le délai réel peut varier selon la complexité.

Pour toute question veuillez contacter **Marco Estrela** par email: mestrela@gardienvirtuel.ca ou par téléphone au 514.907.5107 x707

