vumetric
CYBERSÉCURITÉ

JOURNÉE SUR LA SÉCURITÉ APPLICATIVE (ISACA / UNIVERSITÉ LAVAL)

LES TESTS D'INTRUSION DANS LE CADRE DU CYCLE DE DÉVELOPPEMENT APPLICATIF

Présenté par

Patrick Chevalier

CISSP, CISA, CSSLP, GIAC, CPTE, CEH

Associé, conseiller principal

pchevalier@vumetric.com

30 NOVEMBRE 2017

Qui suis-je ?

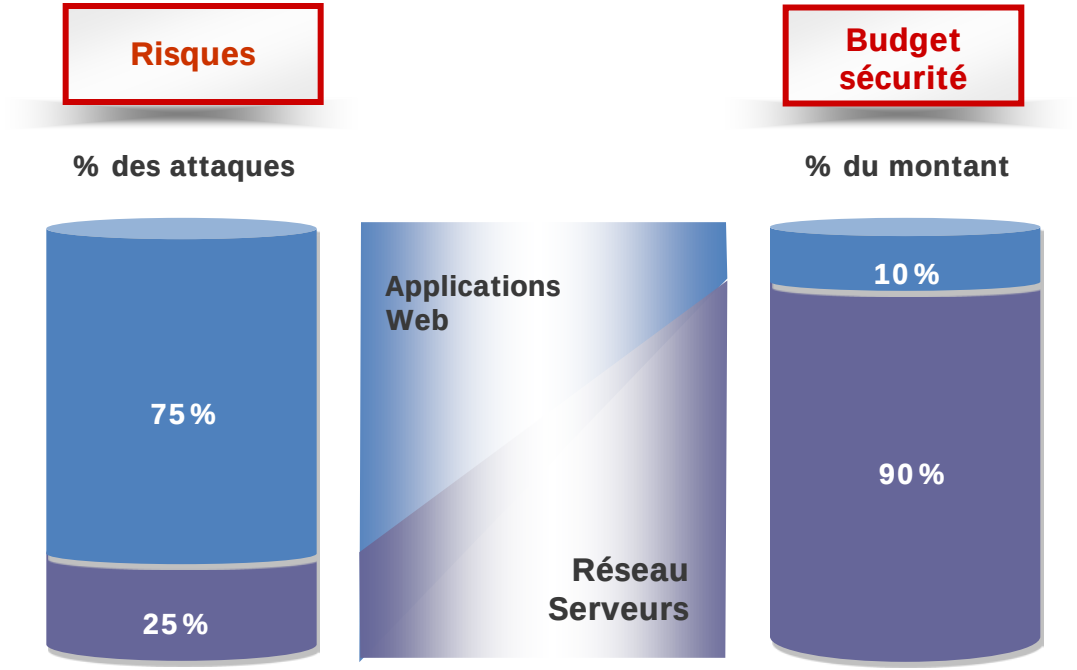
- Patrick Chevalier, CISSP, CISA, CSSLP, GIAC
- Conseiller principal @ **Vumetric**
  - Tests d'intrusion (1000+ projets)
  - Cybersécurité
  - R&D
- ~20 ans d'experience en sécurité

Agenda

- Introduction et mise en contexte
- Pourquoi effectuer des tests d’intrusion
- Postionnement des tests dans le SDLC
- Standards et certifications
- Conclusion
- Période de questions

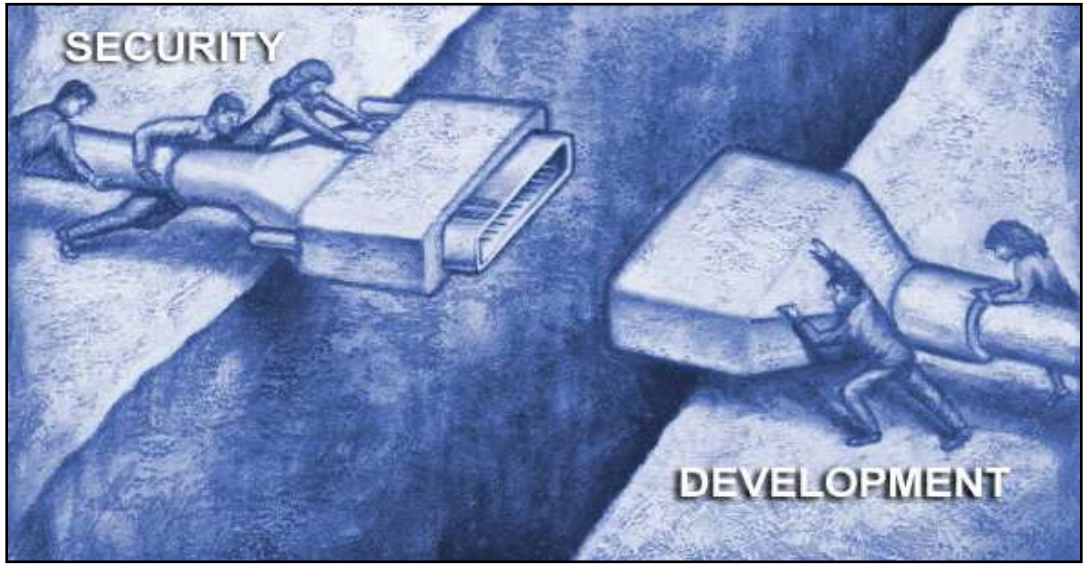
Sondage éclair !

- Qui a déjà participé à des tests d'intrusion ?
  - À titre de testeur ou dans le cadre d'un projet de développement

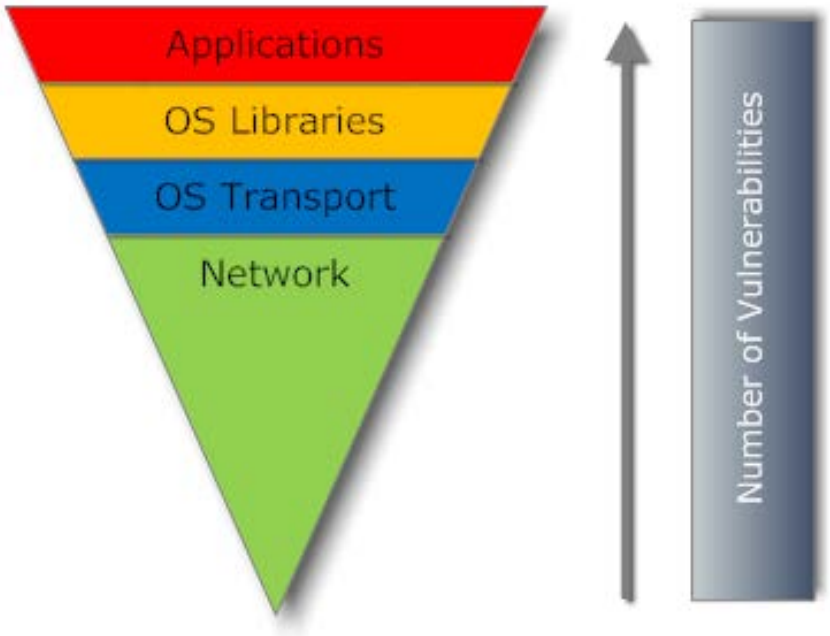


"75% of All Attacks are Directed at the Web Application Layer"

Gartner



Peu de développeurs possèdent des connaissances en sécurité et inversement, peu de professionnels en sécurité possèdent des connaissances en développement…



La sécurité applicative est malheureusement le talon d'Achille de plusieurs organisations…

Pourquoi la sécurité applicative est-elle un enjeu d'actualité ?

- Cause première
  - Les développeurs ne sont pas formés aux meilleures pratiques de développement sécuritaire
  - Les développeurs et gestionnaires sont rarement conscients des enjeux de sécurité
  - Les contrôles de sécurité réseau (pare-feu, IDS, etc.) ne protègent pas la couche applicative
- État actuel
  - Il existe un fossé de communication entre la sécurité et le développement
  - Le contexte des projets de développement est souvent peu propice à l'intégration d'activités de sécurité
  - La réalisation de tests d'intrusion est une pratique relativement établie, bien qu'elle se limite souvent à un test avant la mise en production d'une application stratégique

Quelques mythes très répandus…

- Notre application est protégée par un pare-feu…
- Notre application Web utilise le chiffrement SSL…
- Notre application Web ne présente aucun intérêt pour les pirates…
- Notre analyseur de vulnérabilité automatisé n'a rien identifié…
- La sécurité de l'application Web est la responsabilité des intervenants de l'infrastructure TI…
- Notre application Web est hébergée chez un fournisseur externe, la sécurité n'est pas notre responsabilité…
- Un test d'intrusion annuel est suffisant…

Pourquoi effectuer des tests d'intrusion ?

- Mesurer l'état de sécurité d'un système
- Identifier la présence de vulnérabilités
- Valider l'efficacité des contrôles de sécurité en place
- Se conformer à certaines exigences (ex: PCI-DSS)

Quelques incidents…

le journal de québec

LOJIQ - Des milliers de renseignements personnels exposés aux pirates

Avril 22, 2014

La faille relevée par notre source concerne une brèche de sécurité sur le portail web des Offices jeunesse internationaux du Québec (LOJIQ). L'organisme gouvernemental chapeaute les échanges et projets étudiants des Québécois de moins de 35 ans à l'étranger.

Les données sensibles sont nombreuses : passeport, date de naissance, adresse, téléphone, courriel, nom des parents, documents d'assurance, billet d'avion. Même les dates de séjour à l'étranger y étaient affichées, une information précieuse pour les pirates qui s'adonnent aussi au cambriolage. Chaque pirate pouvait piger 25 dossiers confidentiels parmi les milliers de l'organisme.

Quelques incidents…

LA PRESSE

Le site d'embauche de McDonald's Canada piraté

21 mars 2017

McDonald's du Canada a annoncé vendredi que son site internet « carrières » avait été piraté, compromettant ainsi les renseignements personnels d'environ 95 000 candidats qui avaient postulé depuis trois ans pour un emploi.

Les candidats touchés sont ceux qui ont postulé en ligne entre mars 2014 et mars 2017, indique le géant de la restauration rapide. Selon McDonald's, les demandes d'emploi exigent de fournir des renseignements personnels comme le nom, l'adresse, l'adresse courriel, le numéro de téléphone, l'historique d'emploi «et autres renseignements usuels de candidature».

McDonald's du Canada assure que ses formulaires de demande d'emploi n'exigent pas de donner le numéro d'assurance sociale, des renseignements bancaires, ni des renseignements sur la santé. L'entreprise soutient qu'« à l'heure actuelle, rien n'indique que les renseignements saisis ont servi à un usage inadéquat ».

Quelques incidents…

le journal de montreal

Les infos personnelles de nos stars exposées par erreur

5 juillet, 2014

Une bévue informatique a rendu accessibles des milliers de renseignements confidentiels sur les artistes québécois ainsi qu'une foule de documents à diffusion interne de leur syndicat.

Le problème concerne le site internet de l'Union des artistes. Les documents exposés regroupent notamment des adresses de résidence et de courriel ou les numéros de téléphone personnels de milliers d'artistes comme Gregory Charles, Raymond Bouchard, Chantal Fontaine, Micheline Lanctôt, Guylaine Tremblay, Anaïs Favron, Luck Mervil et Edgard Fruitier.

Découverte par hasard par l'une de nos sources, la faille découlait du bottin de l'UDA sous forme électronique. Sur ce document à diffusion restreinte, de nombreux artistes y affichent leurs coordonnées personnelles au lieu de celles de leur agent. Seuls les membres de l'UDA, les producteurs et les journalistes, en payant, peuvent se le procurer.

Quelques incidents…

Bell hack attack that affected more than 20,000 customers shows rising security threat

February 4, 2014

Hackers disclosed more than 20,000 of Bell Canada's small-business customer usernames and passwords last weekend, the latest reminder that users and companies alike need to start taking data protection more seriously.

An examination of how the data breach likely happened shows the risk users face when companies they share their information with don't take crucial steps to safeguard it.

BCE Inc.-owned Bell Canada confirmed Sunday that 22,421 usernames and passwords and five valid credit-card numbers were posted online after what it called an "illegal hacking" of an Ottawa-based third-party IT supplier.

The telecommunications company insists its own systems, "operate with the highest standards of data security with encryption and other data and system protections."

The problem in this case seems to have arisen due to poor practices on the part of the unnamed supplier.

Quelques incidents…

LE HUFFINGTON POST

Site du ministère de l'Éducation piraté: On a honte de notre gouvernement!

4 avril, 2012

Le site Web du ministère de l'Éducation, du Loisir et du Sport a été la proie des grévistes étudiants en ce vendredi après-midi.

Des étudiants auraient en effet piraté la page d'accueil, où les visiteurs pouvaient y lire l'expression «On a honte de notre gouvernement». Plus bas, une fenêtre de conversation Twitter était affichée, illustrant tous les gazouillis concernant la grève étudiante avec les identifiants #ggi ou encore #non1625.

Cette tactique des étudiants s'ajoute aux événements survenus en cette journée de grève mouvementée; une manifestation a dégénéré lors du Salon Plan Nord tenu à Montréal. Jean Charest a également tenu des propos de mauvais goût quant aux étudiants «cognant à la porte» dudit Salon.

Quelques incidents…

leSoleil

Le site Internet de la Sécurité publique piraté

21 mai 2012

(Québec) Les sites Internet de la Sécurité publique du Québec et du Commissaire à la déontologie policière ont été piratés en début d'après-midi, hier. Les pirates pourraient avoir agi en réaction à la loi 78, qui restreint le droit de manifester.

La page d'accueil des deux sites avait été remplacée par la devise du groupe de pression Anonymous : «Nous sommes Anonymes. Nous sommes Légion. Nous ne pardonnons pas. Nous n'oublions pas. Redoutez-nous.»

Les deux sites étaient toujours inaccessibles au moment de mettre sous presse. D'autres sites du gouvernement, dont celui de l'aide financière aux études et du ministère de l'Éducation, du Loisir et du Sport, étaient également hors service dans la journée de lundi.

Exemples récents...

le journal de montreal

Le site internet de la ville de Sherbrooke piraté «au nom d'Allah»

31 aout 2015

Le site internet de la Ville de Sherbrooke a été piraté par un groupe qui prétend être une cyber armée islamiste turque. C'est la section «données ouvertes» du site internet de la Ville qui a été touchée. Le problème a été détecté lundi matin.

Les pirates n'avaient pas seulement accès aux données déjà publiques de la Ville. Ils ont aussi été en mesure de déjouer les responsables de la sécurité du site en devenant un véritable administrateur de la gestion de la page web. Ils ont aussi publié un long message terroriste.

«Nous condamnons les massacres en Égypte et en Palestine contre des musulmans innocents. Nous serons vos anges de la mort des non-croyants de l'Islam», écrit le groupe, ajoutant revendiquer «au nom d'Allah».

Ce n'est pas la Ville qui héberge cette section de son propre site internet, mais plutôt un sous-traitant.

Quelques incidents…

TVA Nouvelles

Des archives du site Canoë.ca ont été piratées

12 septembre 2017

Le site Canoë.ca a été la cible d'un acte de piratage touchant certaines de ses banques d'archives datant de 1996 à 2008, a annoncé mardi MédiaQMI.

Des renseignements personnels, provenant potentiellement d'un million d'usagers francophones et anglophones, pourraient avoir été obtenus par les pirates. Cependant, ces renseignements ne comportaient pas de numéros de cartes de crédit, ni de numéros d'assurance sociale, a tenu à préciser MédiaQMI.

«L'analyse a révélé que les banques de données piratées contenaient des renseignements personnels (...) tels que des noms, des adresses courriel et postales ainsi que des numéros de téléphone », a indiqué MédiaQMI, dans un communiqué.

«Canoë.ca tient à exprimer ses plus sincères excuses envers ses usagers et assure que tous les efforts sont présentement déployés afin de retracer et de communiquer avec les personnes concernées par cet accès illégal de données recueillies au cours de la période 1996-2008», a indiqué MédiaQMI.

Audit, analyse, tests d’intrusion ?

- Quelle est la différence entre :
  - Balayage de vulnérabilité
  - Test d’intrusion
  - Revue de code
  - Audit de sécurité
- Plusieurs utilisent ces termes de manière interchangeable
- Au-delà de la sémantique, il existe des différences importantes

Audit, balayage, tests d'intrusion ?

- Balayage de vulnérabilité (Scan)
  - Test exécuté par le biais d'un outil automatisé
- Test d'intrusion
  - Test visant à compromettre la sécurité d'un système, combine l'utilisation d'outils automatisés et de tests manuels
- Revue de code
  - Révision du code source d'une application afin d'identifier les vulnérabilités à la source
- Audit de sécurité
  - Évaluation du niveau de sécurité d'un système face à un standard ou un référentiel externe

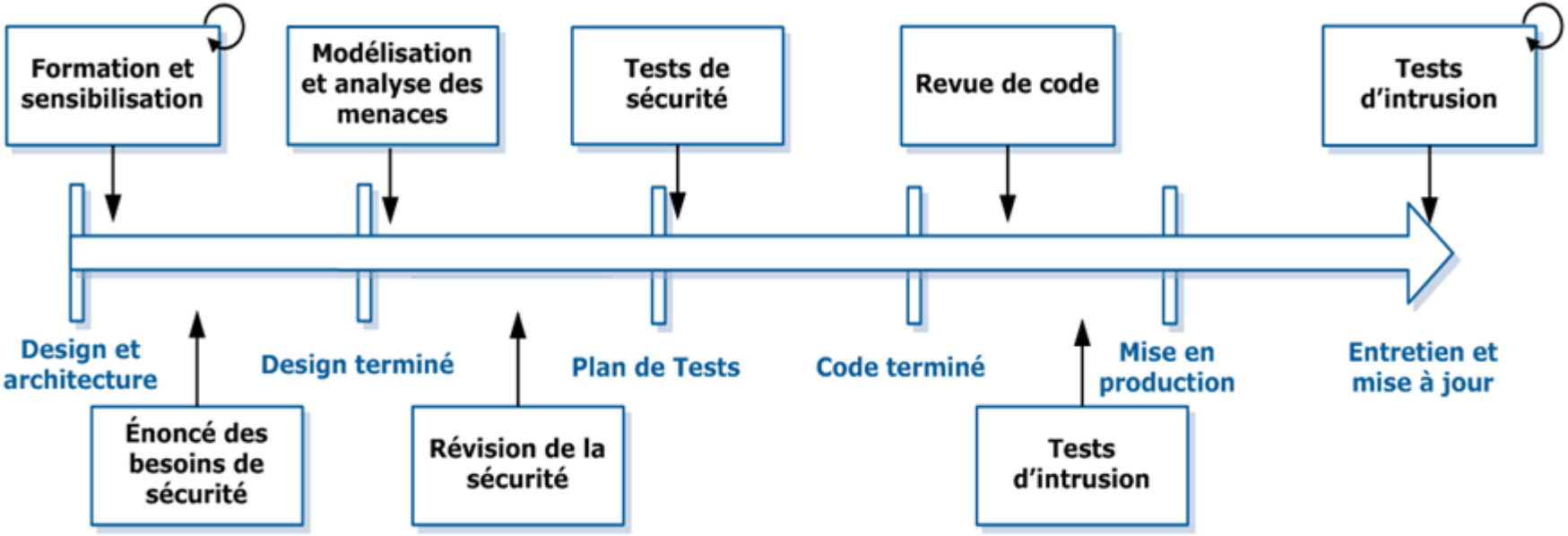
Approches de test

- Black box
  - Test à l'aveugle, vise à simuler la perspective d'un attaquant ne possédant aucune information sur la cible
- White box
  - Test avec partage d'information complet (documentation, code source, etc.)
- Grey box
  - Approche mixte, partage d'information partiel, souvent incrémentielle…

Outils de balayage automatisés

- ex: Nessus, AppScan, WebInspect, Acunetix, etc.
- Couverture partielle des vulnérabilités
  - Entre 30% à 40% des failles
  - Ne teste pas les vulnérabilités situées au niveau de la logique d'affaires
  - Généralement moins efficace qu'un test d'intrusion
- Présence potentielle d'un nombre élevé de faux positifs
- Nécessite un encadrement rigoureux si exécuté en production

Tests de sécurité dans le cycle de développement



Principales phases de réalisation d’un test d’intrusion

1. Planification et préparation
2. Reconnaissance
3. Identification des vulnérabilités
4. Exploitation
5. Analyse des résultats et évaluation des risques
6. Rédaction du rapport

Quelques conseils...

- Les tests de sécurité doivent faire partie intégrante du cycle de développement
- Il faut prévoir les efforts (et les budgets) lors de la planification initiale du projet de développement
- En fonction du projet, il faut considérer de cibler autant l'infrastructure, les systèmes que l'application
- Effectuer des tests sur une base régulière ou lors d'étapes prédéfinies, ex :
  - Avant la mise en production
  - Lors de changements majeurs
- Procéder par échantillonnage si nécessaire

Principaux risques

- Impact sur la disponibilité et l'intégrité des systèmes et des données
- Débordement des tests
- Mauvaise couverture des tests, faux sentiment de sécurité
- Présence de faux positifs
- Perception négative des constats
  - Ex: suite à l'identification de vulnérabilités critiques
- Aucun suivi des recommandations

Fournisseur externe: Questions à poser

- Références de clients satisfaits œuvrant dans le même secteur que votre organisation?
- Font-ils une distinction entre une analyse de vulnérabilité et un test d’intrusion, les tests d'infrastructures réseau et d'applications?
- Expérience et certifications professionnelles reconnues?
- Possibilité d'obtenir un exemple de rapport?
- Politique concernant la confidentialité des informations?

Certifications

- SANS GIAC Web Application Penetration Testing (GWAPT)
- ISC^2 Certified Secure Software Lifecycle Professional (CSSLP)
- SANS GIAC Certified Penetration Tester (GPEN)
- Offensive Security Certified Professional (OSCP)
- EC-Council Certified Ethical Hacker (CEH)
- EC-Council Licensed Penetration Tester (LPT)
- ISECOM OSSTMM Professional Security Tester (OPST)

Standards

- OWASP Top 10 Most Critical Web Application Security Risks
- OWASP Open Web Application Security Project Testing Guide
- OWASP Software Assurance Maturity Model (SAMM)
- OWASP Application Security Verification Standard (ASVS)
- MITRE Common Weakness Enumeration (CWE)
- MITRE Common Attack Pattern Enumeration and Classification (CAPEC)

Conclusion

- Les tests de sécurité doivent être intégrés au sein du cycle de développement
- À défaut de tout tester, il est nécessaire de déterminer les applications nécessitant une attention particulière en terme de sécurité
- Possibilité de combiner les différents types de tests afin d'obtenir une couverture adéquate de la cible
- Plus que tout, il est essentiel de former et de sensibiliser les développeurs aux enjeux de sécurité
  - Les ressources de l'OWASP sont la meilleure porte d'entrée
  - Considérer la participation au chapitre OWASP-Québec!

vumetric

Merci de votre attention!

Patrick Chevalier
CISSP, CISA, CSSLP, GIAC, CPTE
pchevalier@vumetric.com

1-877-805-RISK