Pratique recommandée en sécurité de l'information

PR-061

Tests d'intrusions et de vulnérabilités

Québec

Tests d’intrusions et de vulnérabilités

Cette publication a été réalisée par
le Sous-secrétariat du dirigeant principal de l'information
et produite en collaboration avec la Direction des communications.

Vous pouvez obtenir de l'information au sujet
du Conseil du trésor et de son Secrétariat
en vous adressant à la Direction des communications
ou en consultant son site Web.

Direction des communications
Secrétariat du Conseil du trésor
5e étage, secteur 500
875, Grande Allée Est
Québec (Québec) G1R 5R8

Téléphone : 418 643-1529
Sans frais : 1 866 552-5158

communication@sct.gouv.qc.ca
www.tresor.gouv.qc.ca

Dépôt légal – 2014
Bibliothèque et Archives nationales du Québec

ISBN 978-2-550-71124-7

Table des matières

Remerciements

Le Secrétariat du Conseil du trésor remercie l'équipe de réalisation et le groupe de travail interministériel pour leur participation et le travail accompli.

Équipe de réalisation

Mohamed Darabid, coordonnateur
Secrétariat du Conseil du trésor

Lyonel Vallès, chargé de projet
Socheat Sonn, conseiller
Secrétariat du Conseil du trésor

Groupe de travail interministériel

Daniel Landry
Sureté du Québec

Carmen St-Laurent
Bureau de décision et révision

Mohamed Nasr
Régie du logement

Diane Archambault
TéléQuébec

Hind Belqorchi
Curateur public du Québec

Alain R. Pagé
Régie de l'énergie

Notes à l'intention du lecteur

Note 1 :	Pour ne pas alourdir le texte, le masculin est utilisé comme générique dans le présent document.
Note 2 :	Le terme « organisme public » ou « organisme » désigne un ministère ou un organisme, qu'il soit budgétaire ou autre que budgétaire, ainsi que tout organisme du réseau de l'éducation, du réseau de l'enseignement supérieur ou du réseau de la santé et des services sociaux. [Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement].
Note 3 :	Bien que les éléments du présent guide soient applicables à la plupart des organismes publics, il convient pour chaque organisme public de les adapter à son contexte et aux risques qui lui sont propres.
Note 4 :	Certains termes ou acronymes sont définis à leur première apparition dans le texte. Ces définitions sont également présentées à l'annexe A – Acronymes, sigles et définitions.

1. Introduction

Le présent guide propose une pratique recommandée visant à soutenir les organismes publics dans la mise en œuvre de tests d'intrusions et de vulnérabilités, et ce, en application du paragraphe g) de l'article 7 de la Directive sur la sécurité de l'information gouvernementale. Il présente une vue d'ensemble des tests d'intrusions et de vulnérabilités ainsi que les étapes à suivre pour la réalisation de ces tests.

1.1 Contexte

Le présent guide a été réalisé en application de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement et de la Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics, ces deux textes mettant la sécurité de l'information au cœur des priorités gouvernementales. Le guide prend aussi appui sur les quatre documents structurants suivants, ayant permis d'asseoir les fondements du nouveau cadre de gouvernance de la sécurité de l'information :

- ✓ La directive sur la sécurité de l'information gouvernementale énonce, au paragraphe g) de l'article 7, que les organismes publics doivent « s'assurer de la réalisation de tests d'intrusion et de vulnérabilité, annuellement ou à la suite d'un changement majeur susceptible d'avoir des conséquences sur la sécurité de l'information gouvernementale »;
- ✓ Le cadre gouvernemental de gestion de la sécurité de l'information complète les dispositions de la directive sur la sécurité de l'information gouvernementale, en précisant l'organisation fonctionnelle de la sécurité de l'information ainsi que les rôles et responsabilités sur les plans gouvernemental et sectoriel;
- ✓ L'approche stratégique gouvernementale 2014-2017 en sécurité de l'information fixe les cibles gouvernementales en matière de sécurité de l'information pour les trois prochaines années, y compris la mise en œuvre, par les organismes publics, de tests d'intrusions et de vulnérabilités.
- ✓ Le cadre de gestion des risques et des incidents à portée gouvernementale présente, entre autres éléments, une approche novatrice de gestion des risques susceptibles de transcender le périmètre d'un organisme public, et, ainsi, d'avoir des conséquences à l'échelle gouvernementale.

1.2 Objectifs

Le présent guide sert de référence pour les organismes publics appelés à mettre en œuvre des tests d'intrusions et de vulnérabilités. Il couvre l'ensemble des étapes requises dans un contexte d'évaluation de la sécurité de l'information, y compris :

- ✓ la sécurité des logiciels et des progiciels;
- ✓ la sécurité des infrastructures technologiques;
- ✓ la sécurité physique (bâtiments).

Toutefois, le guide ne couvre pas :

- ✓ les revues de code et les revues d'architecture;
- ✓ les entrevues telles que les interrogatoires.

1.3 Public cible

Le document est à l'usage des organismes publics appelés à effectuer des tests d'intrusions et de vulnérabilités. Il vise particulièrement les intervenants dont les responsabilités sont énoncées dans le cadre gouvernemental de gestion de la sécurité de l'information. Il s'agit, notamment :

- ✓ des responsables organisationnels de la sécurité de l'information (ROSI);
- ✓ des conseillers organisationnels en sécurité de l'information (COSI);
- ✓ des coordonnateurs organisationnels de gestion des incidents (COGI);
- ✓ des Intervenants dans des domaines connexes à la sécurité de l'information (responsables de la sécurité physique, spécialistes en gestion des risques, vérificateurs internes, responsables de l'accès à l'information et de la protection des renseignements personnels, responsables de la continuité des services, détenteurs de l'information, spécialistes en technologie de l'information, etc.).

1.4 Organisation du document

Outre ce chapitre, le présent guide en comprend quatre autres :

- ✓ Le deuxième chapitre présente une vue d'ensemble des tests d'intrusions et de vulnérabilités, dont un bref historique, les motivations, les vecteurs d'attaques et les stratégies de tests;
- ✓ Le troisième chapitre décrit les grandes étapes d'un test d'intrusions et de vulnérabilités. On y retrouve notamment les phases de planification, de découverte, d'exploitation et de rapport;
- ✓ Le quatrième chapitre propose un certain nombre de critères quant aux compétences requises pour effectuer des tests d'intrusions et de vulnérabilités;
- ✓ Le cinquième et dernier chapitre conclut le document et introduit l'étape de gestion et de correction des vulnérabilités découvertes à l'étape de mise en œuvre des tests d'intrusions et de vulnérabilités.

2. Les tests d'intrusions et de vulnérabilités

Dans le domaine de la sécurité de l'information, un test consiste à soumettre un ou plusieurs systèmes[1] à différentes conditions, en vue de comparer la réaction du système au comportement escompté dans le but de découvrir l'existence de vulnérabilités.

Les tests d'intrusions et les tests de vulnérabilités diffèrent de par leur objectif. En effet, un test de vulnérabilités a pour objectif de déceler des vulnérabilités connues sur des systèmes, tandis qu'un test d'intrusions a pour objectif de simuler une attaque, par la découverte et l'exploitation de vulnérabilités. En d'autres mots, un test d'intrusions, en plus d'identifier des vulnérabilités, exploite celles-ci dans le but de vérifier les impacts réels des intrusions.

Le présent guide suit une règle fondamentale de sécurité : un organisme est aussi sécuritaire que son système le plus faible[2]. En effet, les pirates informatiques utilisent généralement les vecteurs d'attaques[3] les plus vulnérables pour atteindre leurs objectifs. Il est donc important de considérer cette règle pour toutes les sections qui suivent afin que les tests d'intrusions et de vulnérabilités apportent réellement une valeur ajoutée à l'organisme public désirant effectuer cet exercice.

2.1 Historique

Le besoin de protéger l'information a toujours été une préoccupation importante des organismes publics et privés. Cependant, l'année 2000 a particulièrement marqué le domaine des tests d'intrusions et de vulnérabilités. En effet, en décembre de l'année 2000, une première méthodologie de tests d'intrusions a été publiée par *l'Open Source Security Testing Methodology Manual (OSSTMM)*[4]. Les techniques utilisées pour effectuer les tests de cette nature devenaient ainsi mieux encadrées et plus structurées.

C'est à partir de l'année 2004 que le crime informatique s'est orienté davantage vers le développement de code malicieux[5]. Les pirates informatiques se sont mis à s'attaquer massivement aux postes de travail et aux appareils mobiles. Le monde de la sécurité de l'information est alors entré dans l'ère des réseaux de zombies (*botnets*)[6].

Aujourd'hui, les attaques sont de plus en plus ciblées[7], c'est-à-dire que le code malicieux développé est personnalisé en fonction de la cible. Les tendances et les techniques utilisées par des personnes malveillantes ont grandement évolué et ont influencé, par le fait même, les divers types de tests d'intrusions et de vulnérabilités.

1. Objet pouvant être évalué lors de tests d'intrusions ou de vulnérabilités, notamment un composant réseau, une application, un service, un bâtiment, un individu, etc.
2. https://buildsecurityin.us-cert.gov/bsi/articles/knowledge/principles/356-BSI.html
3. Les vecteurs d'attaques seront traités au point 2.3 du présent chapitre.
4. http://www.isecom.org/research/osstmm.html
5. http://download.microsoft.com/download/1/A/7/1A76A73B-6C5B-41CF-9E8C-33F7709B870F/Microsoft_Security_Intelligence_Report_Special_Edition_10_Year_Review.pd
6. Réseau d'ordinateurs personnels, transformés en zombies, qui sont utilisés par des personnes ou des groupes malveillants, à l'insu de leurs propriétaires, pour, par exemple, envoyer massivement des pourriels ou pour lancer anonymement des attaques contre d'autres systèmes.
7. http://www.nist.gov/itl/upload/BITS-Malware-Report-Jun2011.pdf

2.2 Les motivations

La protection adéquate des systèmes et de l'information constitue la principale source de motivation des organismes publics pour effectuer des tests d'intrusions et de vulnérabilités. Plus précisément, ces tests visent à :

- ✓ Répondre à une obligation gouvernementale. À titre d'exemple, le paragraphe g) de l'article 7 de la Directive sur la sécurité de l'information gouvernementale stipule que le dirigeant d'un organisme public doit « s'assurer de la réalisation de tests d'intrusion et de vulnérabilité, annuellement ou à la suite d'un changement majeur susceptible d'avoir des conséquences sur la sécurité de l'information gouvernementale, et en dégager les priorités d'actions et les échéanciers afférents »;
- ✓ Valider la conformité à une norme. Par exemple, pour satisfaire aux exigences de la norme PCI[8], un environnement doit être testé au minimum annuellement ou après un changement significatif de l'environnement;
- ✓ Connaître ou vérifier l'état de la sécurité de l'infrastructure technologique (postes, serveurs, réseaux, etc.);
- ✓ Valider la sécurité d'un système avant sa mise en production ou pendant son développement (codification, paramétrisation, etc.).

2.3 Les vecteurs d'attaque

Les vecteurs d'attaques constituent les points d'entrée qu'un attaquant pourrait utiliser pour s'introduire dans les systèmes d'une organisation. Les systèmes informatiques, les bâtiments et même les humains sont des vecteurs d'attaques qui peuvent être utilisés afin de compromettre un système.

Le tableau 1 dresse la liste des vecteurs d'attaques les plus communs.

8. https://www.pcisecuritystandards.org/pdfs/infosupp_11_3_penetration_testing.pdf

Tableau 1 – Vecteurs d'attaques

Vecteur	Exemple
Infrastructure exposée à Internet et infrastructure interne de l'organisation	Systèmes soutenant les applications, notamment les pare-feu, les routeurs, les commutateurs, les points d'accès et les serveurs pour les services accessibles de l'extérieur du périmètre de sécurité[9].
Application	Produits applicatifs de type client lourd[10], Web, mobiles, services Web, qu'ils soient conçus maison ou achetés (logiciels et progiciels).
Solution de sécurité	Systèmes ayant pour objectif de protéger les infrastructures ou les applications[11].
Bâtiment (sécurité physique)	Cartes d'accès, jetons, processus d'accès au bâtiment, processus de demande d'accès, absence de gardiens de sécurité pour surveiller l'accès au bâtiment, etc.
Humain	Comprend particulièrement l'ingénierie sociale. Par exemple, une personne malveillante pourrait abuser de la confiance d'un employé ou d'un dirigeant. Elle pourrait aussi mettre à l'épreuve un gardien de sécurité, un membre du personnel de l'entretien ménager, etc.

Les vecteurs d'attaque utilisés par les pirates informatiques sont nombreux. Il est donc judicieux de bien sélectionner les systèmes à tester en fonction de leur criticité et du niveau de confort par rapport aux mesures de sécurité qui les protègent. La diversification des vecteurs d'attaques permet de rehausser la sécurité d'un grand nombre de systèmes, couvrant ainsi la sécurité de l'information qu'un organisme public détient dans l'exercice de ses fonctions.

2.4 Les stratégies de tests

Pour chacun des vecteurs identifiés au point précédent, il existe plusieurs stratégies pour effectuer un test d'intrusions et de vulnérabilités. En effet, différentes caractéristiques peuvent influencer la nature des tests, par exemple :

- ✓ le niveau d'information disponible;
- ✓ le niveau d'accès utilisateur;
- ✓ le niveau d'accès réseau.

9. On retrouve notamment les serveurs Web tels qu'*Internet Information Services* (IIS), *Apache* et *ngnix*, les services de noms tels qu'*Active Directory* (AD) et BIND, les services de messagerie tels que *Microsoft Exchange, Dovecot, Postfix, Sendmail, Lotus Notes*, les services et protocoles d'accès distant tels que *Point-to-Point Tunneling Protocol* (PPTP), *Layer 2 Tunneling Protocol* (L2TP), *Internet Protocol Security* (IPSec) et *OpenVPN*.
10. Un client lourd, dans une architecture client-serveur, est un logiciel qui comporte des fonctionnalités complexes. À l'inverse du client léger, le client lourd ne dépend du serveur que pour l'échange des données dont il prend en charge l'intégralité du traitement.
11. On retrouve notamment les solutions de surveillance telles que les systèmes de détection d'intrusions (IDS), les systèmes de prévention d'intrusions (IPS), les filtres de contenu (*Websense, Blue Coat*, etc.) et les pare-feu applicatifs (*Apache mod_security, Netscallers*, etc.).

2.4.1 Le niveau d'information disponible

Un organisme public peut vouloir réaliser différents types de tests en fonction de l'information qu'il désire rendre disponible afin de découvrir l'existence de vulnérabilités.

Le tableau 2 décrit les trois principaux types de tests que l'on propose sur le marché et le niveau d'information disponible associé.

Tableau 2 – Type de tests en fonction du niveau d'information (inspiré du NIST[12])

Type	Description
Test de base (Boîte noire)	Ce type de test ne nécessite aucune connaissance sur la structure interne et l'implantation des systèmes à tester. Une description du système à haut niveau ainsi qu'une connaissance de base des spécifications fonctionnelles sont suffisantes pour ce type de test. Le test de base permet de déterminer si les mécanismes de sécurité en place sont fonctionnels et de s'assurer qu'aucune erreur évidente n'est présente.
Test concentré (Boîte grise)	Ce type de test nécessite quelques connaissances sur la structure interne et l'implantation des systèmes à tester. En plus d'une description du système à haut niveau et d'une connaissance de base des spécifications fonctionnelles, quelques renseignements sur l'architecture et les interactions avec les systèmes connexes sont nécessaires. Le test concentré permet de déterminer, avec plus de certitude, si les mécanismes de sécurité en place sont fonctionnels ainsi que de s'assurer qu'aucune erreur évidente n'est présente et que la mesure de sécurité s'exécute comme il se doit.
Test complet (Boîte blanche)	Ce type de test nécessite des connaissances importantes sur la structure interne et l'implantation des systèmes à tester. En plus des spécifications fonctionnelles et d'une description à haut niveau du système, on doit également connaître l'architecture complète, les divers schémas, le code source et toute information nécessaire à la compréhension du système. Le test complet permet de déterminer, avec certitude, si les mécanismes de sécurité en place sont fonctionnels ainsi que de s'assurer qu'aucune erreur évidente n'est présente, que la mesure de sécurité s'exécute comme il se doit, sur une base continue et cohérente, et qu'il existe un soutien pour l'amélioration continue de l'efficacité de la mesure.

La stratégie de tests se détermine, dans un premier temps, en fonction de la motivation de l'organisation et de l'envergure des tests à réaliser. Par exemple, pour obtenir une vue sommaire de la sécurité d'un parc informatique, un test de base pourrait s'avérer un bon choix. Par contre, pour tester en profondeur un système tel qu'un extranet ou pour tester un changement majeur apporté à une architecture, un test concentré ou complet est habituellement plus opportun.

2.4.2 Le niveau d'accès utilisateur

Un organisme public peut vouloir simuler différents niveaux d'accès utilisateur dans sa stratégie de tests. Par exemple, pour un système exposé sur Internet, il pourrait être intéressant de personnifier un utilisateur anonyme, un client accédant à son information ou encore un administrateur du système.

Le tableau 3 décrit trois exemples de niveaux d'accès utilisateur qui peuvent être retenus dans le cadre de tests d'intrusions et de vulnérabilités.

12. *National Institute of Standards and Technology*, USA, http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf

Tableau 3 – Niveau d'accès utilisateur

Accès	Description
Anonyme	L'accès anonyme représente un accès à un système, sans identité ou privilèges. Par exemple, pour une solution de courriel Web exposé, la rigueur du formulaire d'authentification pourrait être testée avec ce niveau d'accès.
Accès de base	L'accès de base représente un accès à un système, avec une identité, mais avec peu de privilèges. L'accès en tant que citoyen au système ClicSÉQUR[13] serait un bon exemple. La rigueur des sessions ou la confidentialité de l'information d'un citoyen connecté pourraient être testées avec ce niveau d'accès.
Accès privilégié	L'accès privilégié représente un accès à un système, avec une identité et des privilèges élevés. Ce niveau d'accès est intéressant pour tester la sécurité des rôles. À titre d'exemple, un organisme public pourrait tester si un rôle « administrateur des infrastructures » peut accéder à des données plus sensibles que celles nécessaires à ses fonctions, comme des numéros d'assurance sociale ou des données concernant les salaires des employés de l'organisation.

Dans la définition de la stratégie de tests, la sélection du niveau d'accès utilisateur s'effectue également en fonction de la motivation de l'organisation, mais principalement en fonction de la criticité des systèmes à tester. Par exemple, dans une situation où un organisme public suspecte des comportements louches de la part de ses employés ou de ses clients, il pourrait, au moyen d'un ensemble de tests, vérifier si les mécanismes de contrôle d'accès en place sont suffisamment restrictifs.

2.4.3 Le niveau d'accès réseau

Un organisme public peut également vouloir simuler différentes attaques selon le niveau d'accès réseau de ses clientèles.

Le tableau 4 présente les niveaux d'accès réseau que peut retenir un organisme public dans le cadre de tests d'intrusions et de vulnérabilités.

Tableau 4 – Niveau d'accès réseau

Accès	Description
Externe	Pour effectuer les tests à l'extérieur du périmètre de sécurité, une ou plusieurs adresses IP (*Internet Protocol*) publiques sont prédéterminées. Un organisme public peut ainsi prétendre être, par exemple, un client, un employé connecté à distance ou un employé connecté à un réseau sans fil.
Interne	Pour effectuer les tests à l'intérieur du périmètre de sécurité, un organisme public teste les différents systèmes à partir de son réseau interne. Ce point de vue est idéal pour simuler une attaque ou une infection du poste d'un employé, tester des mécanismes internes tels que les filtres de contenu Web[14] et les accès physiques ou encore simuler de l'ingénierie sociale.

La sélection du niveau d'accès réseau s'effectue en fonction des motivations de l'organisation et, principalement, de l'accessibilité des systèmes à tester. Par exemple, pour un test réaliste simulant une

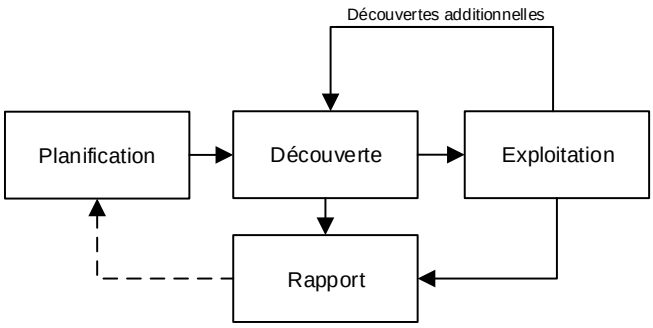
13. https://www.clicsequr.gouv.qc.ca/sqaq-aide/web/FichierAide/fr/services.html
14. Mécanismes de sécurité permettant de déterminer les contenus Web qui seront disponibles à partir d'un ordinateur.

attaque à partir d'Internet, un accès à partir de l'extérieur du périmètre de sécurité est de mise. Par contre, de nos jours, les attaques proviennent en grande partie de l'interne[15]. Ainsi, en cas de changements organisationnels majeurs ou en fonction de l'exposition aux risques, les tests effectués à partir de l'intérieur d'un organisme public sont également nécessaires.

3. Les étapes d'un test d'intrusions et de vulnérabilités

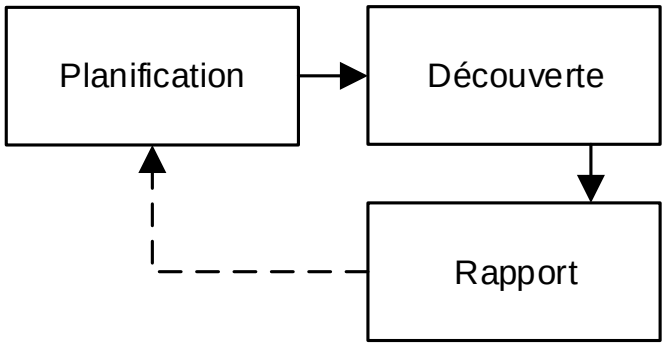
Il existe plusieurs méthodologies pour réaliser des tests d'intrusions. Les méthodologies les plus utilisées sont sommairement présentées à l'Annexe D. La figure 1 présente les grandes étapes d'un test d'intrusions, selon la perspective du NIST[16]. On y retrouve les étapes de planification, de découverte, d'exploitation et de rapport.

Figure 1 – Étapes de mise en œuvre d'un test d'intrusions (inspiré du NIST)



Ces étapes couvrent l'ensemble des éléments à considérer lors de tests d'intrusions. De plus, comme nous l'avons précédemment mentionné, un test de vulnérabilités n'inclut pas l'exploitation de vulnérabilités. La figure 2 illustre les étapes d'un test de vulnérabilités.

Figure 2 – Étapes de mise en œuvre d'un test de vulnérabilité



15. http://www.sans.org/reading_room/whitepapers/incident/protecting-insider-attacks_33168
16. http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

3.1 Planification

L'étape de planification est d'une grande importance et les éléments à couvrir sont nombreux. En effet, une bonne planification permet de déterminer les objectifs et de faciliter la réalisation des étapes subséquentes.

Un organisme public doit donc clairement définir les objectifs des tests à réaliser. Pour ce faire, il pourra s'inspirer de ses motivations et des vecteurs d'attaques présentés au point 2.3 du chapitre 2.

C'est également lors de l'étape de planification qu'est établie la stratégie de tests. Cette stratégie sera composée de l'ensemble des caractéristiques des tests d'intrusions et de vulnérabilités présentées au point 2.4 du chapitre 2. Par exemple, pour obtenir un avis global sur la situation de la sécurité d'un segment de réseau, un test de base pourrait être suffisant. Par contre, pour valider la rigueur des mécanismes de sécurité d'un système critique pour la mission d'une organisation, un test complet serait un meilleur choix.

Par ailleurs, les objectifs influencent aussi les efforts à consentir et les coûts à engager. Pour reprendre l'exemple précédent, un mécanisme de sécurité peut être testé en 2 jours-personnes ou en 8 jours-personnes, selon le niveau de profondeur recherché et la complexité du système.

3.1.1 Considérations relatives aux prestataires de services

Un organisme public peut faire appel à des prestataires de services spécialisés dans les tests d'intrusions et de vulnérabilités pour le soutenir lors de l'étape de planification, afin qu'il puisse élaborer une stratégie optimale de tests. Le cas échéant, des consultations avec les détenteurs de systèmes et les principaux intervenants[17] en sécurité de l'information de l'organisme public permettront de bien cibler les systèmes à tester.

Lorsqu'un organisme public désire faire affaire avec des prestataires de services spécialisés, plusieurs éléments sont à prendre en considération lors de la préparation des devis. À cet effet, le chapitre 4 propose plusieurs considérations au niveau des compétences techniques requises et des solutions logicielles potentielles. Il est également important, à cet égard, de bien définir les rôles et les responsabilités ainsi que les règles d'engagement des parties, lors de l'élaboration du document d'appel d'offres, du contrat ou de l'entente. Les deux prochains points portent sur ces éléments.

17. Principaux intervenants : ROSI, COSI et COGI.

3.1.2 Identification des intervenants

Tableau 5 – Rôle des intervenants d'un organisme public (inspiré du cadre gouvernemental de gestion de la sécurité de l'information au Québec.

Rôles	Implication
Dirigeant d'un organisme public Dirigeant réseau de l'information Dirigeant sectoriel de l'information Responsable organisationnel de la sécurité de l'information Conseiller organisationnel en sécurité de l'information Coordonnateur organisationnel de gestion des incidents Détenteur de l'information Responsable de la vérification interne Responsable de l'accès à l'information et de la protection des renseignements personnels Responsable de l'architecture de sécurité de l'information Comités de sécurité Responsable de la continuité des services Responsable de la sécurité physique Responsable de la gestion des technologies de l'information Responsable de la gestion documentaire Responsable de l'éthique Responsable du développement ou de l'acquisition de systèmes d'information	L'implication de ces intervenants à l'étape de planification permet de couvrir l'ensemble des besoins de l'organisation en matière de sécurité. De par leurs connaissances, ces intervenants ont un rôle important à jouer lors des étapes de planification et de découverte. Ils sont appelés à contribuer à la détermination de la portée, de l'environnement et des stratégies des tests. De plus, certains intervenants, comme le responsable de la gestion documentaire ou le responsable de l'accès à l'information et de la protection des renseignements personnels, peuvent être appelés à communiquer avec le prestataire lors de la phase de découverte. Enfin, le responsable de la gestion des technologies de l'information doit être impliqué dans la phase de découverte, afin de transmettre aux prestataires ses connaissances sur les systèmes. De plus, il doit être informé des résultats, afin que les vulnérabilités identifiées soient éventuellement corrigées.

Du côté du prestataire de services, on retrouve typiquement un chargé de projet, qui effectue la gestion de l'intervention, ainsi qu'une équipe technique de réalisation, spécialisée dans le domaine. Le chapitre 4 propose plusieurs considérations en matière de compétences techniques de l'équipe de réalisation.

3.1.3 Règles d'engagement

Il est recommandé aux organismes publics d'évaluer l'opportunité de préciser les règles d'engagement des parties lors de l'élaboration du document d'appel d'offres, du contrat ou de l'entente.

À cet effet, le Tableau 6 propose plusieurs indications qui peuvent être utiles selon la nature des tests à réaliser.

Tableau 6 – Règles d'engagement à considérer

Règle d'engagement	Explication
Système	Les systèmes d'information à tester doivent être clairement identifiés. Par exemple, on doit dresser une liste des segments réseaux, des adresses IP, de noms d'hôte, des adresses URL (Uniform Resource Locator), des personnes et même des bâtiments à tester. Comme nous l'avons énoncé au point 2.3, les systèmes à tester sont les systèmes les plus susceptibles d'être attaqués, particulièrement ceux qui gèrent de l'information sensible. Ainsi, une attention particulière doit être accordée aux systèmes de missions et aux systèmes qui leur sont interreliés.
Stratégies de tests	Les caractéristiques décrites au point 2.4 doivent être précisées : ✓ le niveau d'information disponible; ✓ le niveau d'accès utilisateur; ✓ le niveau d'accès réseau. Dans un même projet, différentes stratégies peuvent être appliquées à différents systèmes.
Effort	En fonction des objectifs, des systèmes et des stratégies de tests sélectionnées, on peut procéder à une estimation du nombre de jours à allouer par système. À titre d'exemple, une infrastructure technologique peut être testée en 10 jours-personnes, mais peut aussi être testée en 100 jours-personnes.
Environnement	Le choix de l'environnement a un impact direct sur l'intégrité des résultats. Il est habituellement préférable d'effectuer les tests dans l'environnement de production (ou l'équivalent). Toutefois, les tests d'intrusions et de vulnérabilités peuvent compromettre l'environnement. L'utilisation d'un environnement inférieur tel qu'un environnement de test ou de développement est donc parfois nécessaire.
Plage horaire	Il est possible de restreindre les heures lorsque les tests risquent de nuire à la mission de l'organisme. Toutefois, cette restriction peut limiter le réalisme des tests.
Changement de prestataire	Afin d'assurer la qualité et l'intégrité des tests, il est préférable d'effectuer un changement périodique de prestataire. De plus, l'utilisation de plusieurs prestataires peut s'avérer intéressante pour obtenir un plus large éventail d'expertise.
Mode de facturation	Les modalités de facturation doivent être judicieusement sélectionnées en fonction des stratégies retenues et précisées.
Exploitation de vulnérabilité	Il est recommandé de ne pas exiger de contraintes à l'exploitation de vulnérabilités, car celles-ci peuvent nuire au réalisme des tests. Par exemple, au lieu d'interdire l'exploitation de vulnérabilités des systèmes jugés critiques, les tentatives d'exploitations pourraient être faites lors de plages horaires moins critiques, après avoir avisé les intervenants concernés. Ainsi, si un problème survient lors de l'exploitation, la situation est prise en charge rapidement, minimisant ainsi les impacts.
Relève	Une capacité de relève du personnel peut être demandée aux prestataires de service. En plus d'assurer une expertise en quantité suffisante, la relève permet le remplacement rapide des intervenants au besoin.

Échéancier	L'échéancier permet d'obtenir une vue d'ensemble des tests qui seront effectués, de l'orchestration de ceux-ci, ainsi que du temps alloué pour chacun. Les périodes critiques, c'est-à-dire les périodes pendant lesquelles il est essentiel que les systèmes soient en fonction, doivent être précisées au besoin.
Bien livrable	La description des biens livrables doit être clairement définie. Le point 3.3.5 contient plusieurs éléments d'information qui doivent nécessairement se retrouver dans le rapport ou dans les documents connexes.
Stratégie de transfert d'expertise	Il est important d'établir une stratégie de transfert d'expertise, afin de garantir une prise en charge adéquate, par l'organisme public, des solutions proposées.
Documentation pour la réalisation	En fonction de la nature des tests, une documentation adéquate doit être fournie au prestataire, au démarrage des travaux. Par exemple, une liste des adresses IP pourrait être suffisante pour des tests de base, alors que les documents d'architecture pourraient être requis pour des tests concentrés ou complets.
Processus d'escalade	Un processus doit être établi afin d'informer rapidement les intervenants concernés lorsque des vulnérabilités critiques sont identifiées ou lorsqu'un incident survient.
Moyen de communication	Les moyens de communication doivent être clairement établis afin de réduire les ambiguïtés et les incompréhensions à propos des vulnérabilités identifiées lors des tests. Par exemple, de l'information sensible peut être transmise par courriel sécurisé, tandis que des suivis peuvent être effectués par téléphone. Pour des situations d'urgence, un pont téléphonique ou une conférence vidéo peuvent également être mis en place. De plus, un outil de chiffrement doit être identifié afin d'assurer l'intégrité et la confidentialité des documents échangés.
Infonuagique (*Cloud Computing*)	Si des infrastructures sont hébergées chez des tiers, il est important de prendre entente avec les hébergeurs avant de procéder aux tests, afin d'éviter tout conflit ou toute interprétation. Par exemple, un hébergeur pourrait rendre indisponible un service par souci d'attaque sur son infrastructure pendant les tests, s'il n'en n'est pas informé.

La planification des travaux doit tenir compte des règles d'engagement définies. Elle doit également être suffisamment flexible pour permettre des ajustements en fonction des résultats obtenus en cours de réalisation. En effet, le nombre et le type de vulnérabilités n'étant pas connus au démarrage des travaux, des ajustements seront possiblement requis afin d'assurer le respect des échéances et des budgets, tout en assurant une qualité optimale et une documentation complète.

3.2 Découverte

Cette étape consiste en la prise de connaissance du fonctionnement du système mis à l'épreuve ainsi qu'en la découverte de vulnérabilités.

3.2.1 Types de vulnérabilités

Les vulnérabilités sont catégorisées par type. Cette catégorisation permet, entre autres, de visualiser rapidement les conséquences d'une vulnérabilité identifiée. Le tableau 7, inspiré du *National Vulnerability Database* (NVD[18]), dresse la liste des principaux types de vulnérabilités connus à ce jour.

Tableau 7 – Type de vulnérabilités (inspiré de NVD19)

Type de vulnérabilité	Explications
Mécanisme d'authentification	Échec à authentifier adéquatement les utilisateurs.
Gestion de la session	Échec à créer, stocker, transmettre et protéger adéquatement l'information sensible de sessions telle que les mots de passe.
Permissions, privilèges et contrôle d'accès	Échec à appliquer les permissions et autres restrictions d'accès aux ressources, ou problème de gestion de privilèges.
Tampon	Dépassement de tampon, causé par une mauvaise gestion de celui-ci, permettant d'insérer plus d'information que la limite possible et créant ainsi une potentielle injection de code en mémoire.
Cross-Site Request Forgery (CSRF)	Échec à vérifier qu'une requête Web effectuée par un utilisateur provient de lui-même.
Cross-Site Scripting (XSS)	Échec d'un site à valider, filtrer ou encoder adéquatement l'information envoyée par un utilisateur avant de la lui retourner.
Cryptographie	Utilisation d'un algorithme de chiffrement non sécuritaire ou mauvaise utilisation d'un algorithme.
Parcours de chemin d'accès	Échec à valider adéquatement les chemins d'accès, permettant d'accéder à des fichiers en dehors du ou des répertoires prévus.
Injection	Échec à valider les données d'utilisateurs ou les téléchargements de fichiers, permettant l'exécution de code arbitraire sur le système[20].
Configuration	Mauvaise configuration d'un système de l'organisation, permettant une utilisation non sécuritaire de celui-ci.

18. Le *National Vulnerability Database*, version 2.2 (NVD), est un centre de données américain basé sur les normes de gestion des vulnérabilités. Ces données permettent, notamment, l'automatisation de la gestion des vulnérabilités, de l'évaluation des mesures de sécurité et de leur conformité. Les données du NVD comprennent, entre autres, des listes de contrôle de sécurité, des failles de sécurité logicielles connues, des erreurs de configuration, des noms de produits et des mesures d'impact.
19. http://nvd.nist.gov/cwe.cfm#cwes
20. On y retrouve notamment les injections SQL, LDAP, XPATH, XSS, CSRF, REGEX et toute forme de code exécutable ou de langage interprétable.

Fuite d'information	Exposition d'information système, sensible ou privée.
Situation de compétition (*Race Conditions*)	Défaut d'un système, caractérisé par un résultat différent selon l'ordre dans lequel agissent les composants et clients du système.
Architecture	Défaut de conception qui n'est pas causé par un problème d'implantation ou de configuration.

Ainsi, les types de vulnérabilités potentiellement présentes diffèrent en fonction des systèmes à mettre à l'épreuve[21].

De plus, un test peut être restreint à certains types de vulnérabilités. Par exemple, pour un test de vulnérabilité Web, les essais pourraient être restreints aux dix vulnérabilités les plus importantes identifiées par un organisme reconnu tel l'OWASP[22] (*Open Web Application Security Project*).

3.2.2 Prise de connaissances des systèmes

Cette étape consiste à prendre connaissance des systèmes à tester, ce qui permet de découper les systèmes en composants. À ce stade, une analyse des systèmes et de la documentation disponible permet de déterminer les principaux éléments nécessaires à la recherche de vulnérabilités :

- ✓ les types de services

  Par exemple, un service Web, un service de courriel entrant/sortant, un service de messagerie instantanée, un service de base de données, etc.

- ✓ les produits utilisés pour offrir le service

  Par exemple, pour un service de base de données, on retrouve, entre autres, MySQL, MS SQL Server, PostgreSQL, etc.

- ✓ la version des produits utilisés

  Par exemple, pour le produit MS SQL Server, il existe, entre autres, les versions 2000, 2005, 2008, 2012, et, pour chacune, il pourrait y avoir des révisions ou des ensembles de services (*service packs*).

Pour un test de base, un balayage des adresses IP peut être effectué, afin d'identifier les services disponibles et d'obtenir le plus d'information possible sur ceux-ci. Un balayage consiste à tester un certain nombre de ports, sur un ensemble d'adresses IP, dans le but de déceler des services accessibles et fonctionnels qui pourraient être vulnérables.

Pour un test concentré ou complet, en plus d'un balayage, la lecture de la documentation, appuyée par des échanges avec les intervenants concernés (questions et réponses), est habituellement suffisante pour comprendre le fonctionnement des services. Toutefois, il revient à l'organisme public de répondre adéquatement aux questions, dans un temps raisonnable, en fonction du niveau d'information rendu disponible préalablement, afin que le prestataire ait les connaissances requises pour déceler un maximum de vulnérabilités.

Ainsi, une fois que tous les composants susceptibles de contenir des vulnérabilités sont identifiés, la recherche de vulnérabilités proprement dite peut débuter.

21. Par exemple, les failles de type XSS et CSRF sont applicables seulement à des sites Web auxquels ont accédé des navigateurs, et non des clients lourds, c'est-à-dire des logiciels qui échangent automatiquement de l'information avec un serveur, mais dont l'intégralité du traitement est assurée par eux-mêmes.
22. https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

3.2.3 Identification des vulnérabilités

Les techniques utilisées pour déceler des vulnérabilités sont nombreuses. Celles-ci dépendent notamment du contexte de l'organisation, des systèmes, de l'expertise disponible et de la stratégie de tests, y compris le niveau d'information disponible, le niveau d'accès utilisateur et le niveau d'accès réseau. En outre, ces techniques se catégorisent en deux grandes familles, l'approche automatisée et l'approche manuelle.

Approche automatisée

L'approche automatisée consiste à utiliser des outils, souvent appelés balayeurs de vulnérabilités (*scanners*), qui ont la capacité d'effectuer un nombre élevé de tests en peu de temps. Cette technique, également appelée « balayage », permet d'analyser un certain nombre de problèmes dans le but de découvrir des vulnérabilités. Par exemple, pour tester un site Web, un balayeur de vulnérabilités de sites Web pourrait être utilisé afin d'effectuer un balayage rapide du serveur Web. Ce type d'outils permet de découvrir des problèmes de configuration majeurs et facilement identifiables. Par contre, ce type d'outils ne serait pas en mesure de déceler des vulnérabilités applicatives ou des vulnérabilités propres au produit utilisé. Un autre outil serait alors nécessaire pour identifier les vulnérabilités à ce niveau.

Par ailleurs, les tests ne doivent pas s'arrêter aux outils automatisés, puisque ceux-ci ne tiennent pas suffisamment compte du contexte du système, identifient des faux positifs[23], ne contiennent pas l'ensemble des tests ou sont incapables de détecter certaines vulnérabilités. De plus, les filtres de sécurité tels que les pare-feu applicatifs peuvent également influencer le fonctionnement des outils. Par exemple, dans la situation décrite à l'Annexe V, un pare-feu applicatif protège une application contre l'injection de certains caractères spéciaux, nécessaires à quelques attaques, rendant la découverte de vulnérabilités difficile au moyen d'outils automatisés. Par contre, l'analyse manuelle de divers comportements permet de déceler une vulnérabilité et de l'exploiter.

Approche manuelle

L'approche manuelle consiste à analyser, au moyen d'outils spécialisés, chaque composant en profondeur et, surtout, dans le contexte de leur environnement. Pour reprendre l'exemple précédent, dans le but de tester une page d'authentification, il est possible, entre autres, d'utiliser un serveur mandataire (*proxy*), outil permettant d'intercepter des requêtes et réponses afin de les lire ou de les modifier avant leur envoi. Il est également possible d'effectuer des injections directement dans les champs d'une page Web, simplement en utilisant un navigateur Web, comme dans l'exemple de l'Annexe IAnnexe V.

Il est important de mentionner que l'approche manuelle requiert des connaissances avancées en Web, en programmation et en base de données, en plus des compétences en sécurité de l'information décrites au chapitre 4. Bref, bien que l'approche manuelle soit plus complexe, c'est l'approche qui est la plus efficiente.

De manière générale, lorsque des tests sont envisagés par un organisme public, celui-ci devrait s'attendre à ce que 20 % du temps soit consacré à l'approche automatisée et que 80 % du temps soit dédié à l'approche manuelle.

L'étape suivante s'applique seulement aux tests d'intrusions. Dans le cas d'un test de vulnérabilités, le lecteur pourra passer directement au point 3.3.5 – Rapport.

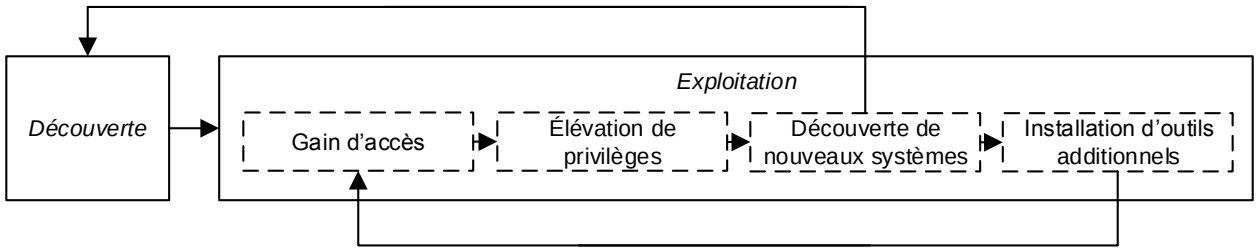
23. Par exemple, un service est identifié comme étant vulnérable, mais ne l'est pas.

3.3 Exploitation

L'étape d'exploitation relative aux tests d'intrusions a pour objectif d'infiltrer le système mis à l'épreuve jusqu'à ce que le niveau d'accès souhaité soit acquis, en exploitant les vulnérabilités précédemment décelées et en utilisant des techniques utilisées par les attaquants malveillants. Il est important de rappeler que cette étape doit être soigneusement réalisée et que la règle d'engagement concernant l'exploitation de vulnérabilités doit être rigoureusement respectée.

La figure 3 présente le découpage de l'étape d'exploitation en quatre sous-étapes.

Figure 3 – Les sous-étapes de l'exploitation



3.3.1 Gain d'accès

Le gain d'accès consiste à obtenir un accès non autorisé à de l'information ou à un système, à la suite d'une ou de plusieurs exploitations de vulnérabilité. Par exemple, il est possible d'exploiter une vulnérabilité de type « dépassement de tampon » et d'obtenir un accès direct à un service. Il est également possible d'effectuer une simulation de campagne d'hameçonnage (*phishing*) ou encore une attaque par ingénierie sociale, afin d'inciter un utilisateur à cliquer sur un lien malveillant ou à ouvrir un document permettant l'exécution de code malveillant et la prise de contrôle d'un poste.

3.3.2 Élévation de privilèges

Des techniques d'élévation de privilèges pourraient être utilisées pour passer d'un compte utilisateur à un compte administrateur. Les techniques d'élévation de privilèges sont nombreuses. Pour reprendre l'exemple précédent, il est possible que l'accès acquis lors de la compromission du poste ne soit pas suffisant pour accéder à des données sensibles, comme le rechercherait un attaquant.

3.3.3 Découverte de nouveaux systèmes

À la suite d'une élévation de privilèges positive, il est requis d'effectuer une nouvelle activité de découverte. Dans notre exemple, le poste pris en contrôle pourrait servir de tremplin pour s'attaquer à d'autres systèmes non ciblés initialement par les tests. Si ces systèmes n'étaient pas compris dans la portée préalablement identifiée, il est recommandé d'évaluer l'opportunité de poursuivre les tests plus en profondeur et de revoir le plan de travail, le cas échéant.

3.3.4 Installation d'outils additionnels

Finalement, il est à considérer, tout comme le ferait un attaquant, d'examiner la possibilité d'installer une « porte dérobée » (*backdoor*), c'est-à-dire des outils additionnels pour maintenir l'accès au système. Par exemple, si le poste de travail était mis à jour ou redémarré pendant les tests, l'accès au poste pourrait être perdu. L'installation d'outils additionnels offre donc plus de stabilité pour poursuive les essais et simuler de nouvelles attaques. Bien entendu, ces outils doivent être désinstallés à la fin de l'intervention.

3.3.5 Rapport

Le rapport est le principal bien livrable produit à la suite des tests d'intrusions et de vulnérabilités. Ce rapport doit être rédigé avec une grande rigueur, puisque ce document permet d'appuyer les décisions relatives à l'acceptation des solutions recommandées et de remédier aux vulnérabilités décelées.

Bien que le niveau de détails varie en fonction de l'envergure et de la profondeur des tests, un rapport de tests d'intrusions et de vulnérabilités doit minimalement contenir les éléments d'information suivants :

- ✓ les objectifs du mandat;
- ✓ la portée du mandat;
- ✓ le contexte du mandat;
- ✓ la démarche d'évaluation du risque;
- ✓ la démarche d'identification des vulnérabilités;
- ✓ une description détaillée de chacun des tests effectués, concluants ou non, et les résultats obtenus;
- ✓ une documentation détaillée de chaque vulnérabilité identifiée l'Annexe V en donne un exemple complet);
- ✓ des recommandations générales.

Il est également intéressant, si l'organisme public le juge à propos :

- ✓ de déterminer et de documenter les forces et les faiblesses des mesures de sécurité examinées, afin d'appuyer les recommandations et d'éclairer l'organisme public dans le cadre de sa prise de décision;
- ✓ de documenter les vulnérabilités potentiellement présentes qui n'ont pu être exploitées, tel un potentiel de déni de services (*denial of services ou DoS*) dans un environnement de production;
- ✓ de produire un rapport synthèse, de type sommaire de gestion, complet et d'interprétation facile par la haute direction;
- ✓ de préparer une présentation à l'intention de la haute direction;
- ✓ de rédiger un journal des activités dans le cadre de tests sur un environnement de production, en précisant la date et l'heure ainsi que la nature de chaque activité effectuée par le prestataire, notamment les balayages et les attaques.

4. Compétences techniques et solutions logicielles

Le chapitre 4 a pour objectif d'encadrer le choix d'un prestataire de services.

4.1 Compétences

Les prestataires offrant des services de tests d'intrusions et de vulnérabilités doivent être sélectionnés judicieusement. En effet, il est important de prendre en considération l'expérience et l'expertise du prestataire de services en fonction des systèmes à tester. De plus, l'approche préconisée par le prestataire doit s'appuyer sur les standards et les meilleures pratiques du domaine, afin d'assurer que les techniques qu'il utilise seront comparables à celles utilisées par un attaquant, ce qui garantit ainsi des tests réalistes et pertinents.

Le personnel du prestataire de services doit démontrer deux qualités essentielles, soit une mentalité d'attaquant et de bonnes connaissances techniques.

La mentalité d'attaquant ne s'acquiert pas naturellement et elle est difficile à démontrer. Cependant, un nombre important d'années d'expérience dans le domaine de la sécurité de l'information et, plus particulièrement, une expérience probante et récente en réalisation de tests d'intrusions et de vulnérabilités contribuent à forger cette mentalité.

Les connaissances techniques s'acquièrent principalement par des recherches soutenues et des expérimentations ainsi que par des réalisations dans ce domaine ou des mandats en sécurité de l'information de nature technique.

Un bon équilibre entre le nombre d'années d'expérience et la pertinence des réalisations du personnel du prestataire de services est donc essentiel pour la réalisation de tests d'intrusions et de vulnérabilités concluants[24].

4.2 Certifications de soutien

Les certifications en sécurité relatives aux tests d'intrusions et de vulnérabilités sont également à considérer, puisqu'elles assurent que le personnel du prestataire possède une connaissance minimale des méthodologies, des techniques et des divers types d'outils disponibles dans ce domaine. Un organisme public pourra ainsi prendre en considération certaines certifications, en plus de l'expertise et de l'expérience du personnel du prestataire de services.

Ceci étant dit, il est essentiel de bien identifier les certifications relatives aux tests d'intrusions et de vulnérabilités. Par exemple, bien que la certification *Certified Information Systems Security Professional* (CISSP) couvre presque tous les volets du domaine de la sécurité informatique, elle est peu pertinente dans un contexte de tests d'intrusions et de vulnérabilités. En effet, la réalisation de tests nécessite principalement des compétences techniques et pointues. L'Annexe VI présente les certifications les plus pertinentes associées à la réalisation de tests d'intrusions et de vulnérabilités.

Les certifications de produits devraient également être prises en compte lorsque des produits précis doivent être testés[25].

4.3 Logiciels et outils

Le domaine de la sécurité de l'information évolue rapidement et il en va de même pour les outils. Année après année, les outils sont remplacés par de nouveaux, plus sophistiqués et plus rapides. De plus, le domaine des tests d'intrusions et de vulnérabilités étant de plus en plus complexe, le nombre d'outils se multiplie[26].

24. Par exemple, pour tester la sécurité d'un appareil CISCO, un candidat ayant deux ans d'expérience en configuration d'appareils CISCO et deux ans d'expérience en sécurité de l'information est préférable à un candidat ayant uniquement quatre ans d'expérience en configuration d'appareils CISCO ou à un candidat ayant uniquement quatre ans d'expérience en sécurité de l'information.
25. Par exemple, pour tester la sécurité d'appareils CISCO, une certification telle que *Cisco Certified Network Associate* (CCNA) est un atout.
26. À titre d'exemple, la distribution Kali (http://www.kali.org/), un système d'exploitation spécialisé en tests d'intrusions et investigations, comprend plus de 500 outils à ce jour (http://secpedia.net/wiki/List_of_tools_in_BackTrack).

4.4 Considérations supplémentaires

Le personnel effectuant des tests d'intrusions et de vulnérabilités peut être amené à accéder à de l'information extrêmement sensible. Dans ce contexte, une vérification des antécédents criminels du personnel qui sera affecté aux tests d'intrusions et de vulnérabilités est recommandée.

De plus, il est également recommandé que le personnel qui sera affecté aux tests d'intrusions et de vulnérabilités ne soit pas intervenu dans la sécurisation des systèmes visés, afin d'assurer une neutralité complète des travaux et des résultats en découlant.

Conclusion

En conclusion, la sécurité de l’information restera un enjeu majeur pour les organismes publics du Québec pendant encore des décennies et les attaques ciblant les systèmes gouvernementaux seront toujours plus furtives et plus complexes. Il est donc essentiel de procéder à des évaluations périodiques de la sécurité des systèmes informatiques. Un moyen efficace d’évaluer la sécurité de l’information consiste à réaliser périodiquement des tests d’intrusions et de vulnérabilités.

Lorsqu'il est bien intégré aux processus de l’organisation et réalisé à l’aide de techniques d’actualité représentatives de la réalité du moment, à la manière d'un attaquant, le test d’intrusions et de vulnérabilités est un excellent moyen de vérifier le fonctionnement adéquat et la rigueur des mesures de sécurité mises en place.

L’étape suivant la mise en œuvre de tests d’intrusions et de vulnérabilités consiste à gérer les vulnérabilités décelées, que ce soit en préconisant la mise en place des solutions recommandées ou en acceptant les risques. Bien que cette étape requière de nouveaux efforts, elle est essentielle dans une perspective d’amélioration continue. Ainsi, la réalisation de tests d’intrusions et de vulnérabilités, en plus d'être conforme au paragraphe g) de l’article 7 de la directive sur la sécurité de l’information gouvernementale, permettra de rehausser la sécurité des systèmes informatiques d’un organisme public.

ANNEXE I Lexique

Le tableau 8, présenté ci-après, décrit brièvement les termes propres au domaine de la sécurité de l'information ou au contexte du présent guide.

Tableau 8 – Lexique des termes

Terme	Définition
Prestataire	Entreprise ayant les compétences d'effectuer des tests d'intrusions et de vulnérabilités.
Test	Exercice consistant à soumettre un ou plusieurs systèmes à différentes conditions, afin de comparer la réaction du système au comportement escompté, dans le but de découvrir l'existence de vulnérabilités des mesures de sécurité.
Test de vulnérabilités	Test consistant à déceler des vulnérabilités, sur des cibles préalablement identifiées, dans un contexte précis et selon une portée prédéfinie où les vulnérabilités sont documentées, mais ne sont pas exploitées.
Test d'intrusions	Test consistant à simuler une attaque en identifiant des vulnérabilités et en exploitant celles-ci, de manière récursive, afin de tester en profondeur les mécanismes de sécurité. Tout comme les tests de vulnérabilités, les vulnérabilités sont documentées, en plus des attaques simulées.
Logiciel malveillant *(malware)*	Logiciel malveillant ayant des objectifs malicieux.
Système	Objet pouvant être évalué lors de tests d'intrusions ou de vulnérabilités, notamment un composant réseau, une application, un service, un bâtiment, une personne, etc.
Réseau de zombies (*botnet*)	Réseau d'ordinateurs personnels, transformés en zombies, qui sont loués par des personnes ou des groupes malveillants, à l'insu de leurs propriétaires, pour, par exemple, envoyer massivement des pourriels ou pour lancer anonymement des attaques de déni de services.
Filtre de contenu	Mécanisme de sécurité permettant de déterminer les contenus Web qui seront disponibles à partir d'un ordinateur.

ANNEXE II Références

BITS. *Malware Risks and Mitigation Report*, juin 2011. [en ligne]. [http://www.nist.gov/itl/upload/BITS-Malware-Report-Jun2011.pdf] (consulté le 04 juillet 2014)

ISECOM. *Open-Source Security Testing Methodology Manual*, version 2.2, 2006. [en ligne]. [http://isecom.securenetltd.com/osstmm.en.2.2.pdf] (consulté le 04 juillet 2014)

NIST. *Guide to Information Security Testing and Assessment*, Special Publication 800-115, le 18 décembre 2008. [en ligne]. [http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf] (consulté le 04 juillet 2014)

NIST. *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*, (révision 1), juin 2010. [en ligne]. [http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf] (consulté le 04 juillet 2014)

OWASP Foundation. *OWASP Testing Guide*, version 3, 2008. [en ligne]. [https://www.owasp.org/images/5/56/OWASP_Testing_Guide_v3.pdf] (consulté le 04 juillet 2014)

PENETRATION TESTING EXECUTION STANDARDS (PTES). version Beta, 2011-03-06. [en ligne]. [http://www.pentest-standard.org/] (consulté le 04 juillet 2014)

SECRÉTARIAT DU CONSEIL DU TRÉSOR. *Démarche d'accompagnement dans la détermination des mesures de sécurité*, document de travail, version 0.7, avril 2013.

SECRÉTARIAT DU CONSEIL DU TRÉSOR. *Directive sur la sécurité de l'information gouvernementale*, janvier 2014.

ANNEXE III Outils de tests d'intrusions

Le tableau 9, présenté ci-après, donne des exemples d'outils utilisés pour effectuer des tests d'intrusions.

Tableau 9 – Exemple d'outils utilisés lors de tests d'intrusion (inspiré du guide NIST SP 800-115[27])

Famille d'outil	Exemple
Identification de cibles et de vulnérabilités	
Test applicatif	CIRT Fuzzer, Fuzzer 1.2, NetSed, Paros Proxy, Burp Suite, WebScarab, DirBuster, Peach, Fiddler, w3af, IronWASP, soapui, wsscanner et ws-attacker
Identification réseau	Autonomous System Scanner, Ettercap, Firewalk, Netdiscover, Netenum, Netmask, Nmap, P0f, Tctrace, et Umit
Identification de services et de ports	Amap, AutoScan, Netdiscover, Nmap, P0f, Umit, et UnicornScan
Balayage de vulnérabilités	Firewalk, GFI LANguard, Hydra, Metasploit, Nmap, Paros Proxy, Burp Suite, DirBuster, Snort, OpenVAS et SuperScan
Balayage de réseaux sans fil	Airsnarf, Airsnort, BdAddr, Bluesnarfer, Btscanner, FakeAP, GFI LANguard, Kismet, et WifiTAP
Attaques actives	
Cassage de mots de passe	Google, Hydra, Medusa, John the Ripper, RainbowCrack, Rcrack, SIPcrack, SIPdump, TFTP-Brute, THC PPTP, VNCrack, hashcat, et WebCrack
Accès distants	IKEProbe, IKE-Scan, PSK-Crack, et VNC_bypauth
Exploitation de vulnérabilités	Ettercap, Metasploit, Burp Suite et tout script de preuve de concept que l'on retrouve sur Internet
Attaques passives	
Capture réseau	Dsniff, Ettercap, Kismet, Mailsnarf, Msgsnarf, Ntop, Phoss, SinFP, SMB Sniffer et Wireshark
Intégrité de fichiers	Autopsy, Foremost, RootkitHunter, et Sleuthkit Target Identification and Analysis

27. http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

ANNEXE IV Méthodologie des tests

Le tableau 10, présenté ci-après, donne une liste non exhaustive des méthodologies de tests d'intrusions disponibles sur le marché.

Tableau 10 – Méthodologies de tests

Méthodologie	Étapes
OSSTMM[28]	Les grandes étapes d'OSSTMM sont les suivantes : ✓ Phase d'induction ✓ Phase d'interaction ✓ Phase d'enquête ✓ Phase d'intervention
OWASP[29]	Les grandes étapes du guide de tests d'OWASP sont les suivantes : ✓ Préalable au développement ✓ Pendant la conception ✓ Pendant le développement ✓ Pendant le déploiement ✓ Maintenance et opérations
PTES[30]	Les grandes étapes de PTES sont les suivantes : ✓ Interactions de préengagement ✓ Collecte de renseignements ✓ Modélisation des menaces ✓ Analyse de la vulnérabilité ✓ Exploitation ✓ Postexploitation ✓ Rapports
NIST[31]	Les grandes étapes du guide de tests d'intrusions du NIST sont les suivantes : ✓ Planification ✓ Découverte ✓ Attaque ✓ Rapport

28. http://www.isecom.org/mirror/OSSTMM.3.pdf
29. https://www.owasp.org/images/5/56/OWASP_Testing_Guide_v3.pdf
30. http://www.pentest-standard.org/
31. http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

SANS[32]	Les grandes étapes du SANS sont les suivantes : ✓ Planification et préparation ✓ Collecte d'information et analyse ✓ Identification des vulnérabilités ✓ Tentative d'intrusion ✓ Analyse et rapport ✓ Nettoyage
SDLC[33]	Les grandes étapes de SDLC sont les suivantes : ✓ Entraînement ✓ Prérequis ✓ Conception ✓ Implantation ✓ Vérification ✓ Sortie ✓ Réponse

32. http://www.sans.org/reading_room/whitepapers/auditing/conducting-penetration-test-organization_67
33. http://www.microsoft.com/security/sdl/process/training.aspx

ANNEXE V Exemple d'exploitation de vulnérabilités

La présente annexe a pour objectif d'illustrer un exemple de format de bulletin de vulnérabilités et de démontrer un exemple d'exploitation complet. Les textes en italique décrivent le contenu des sections.

Cet exemple provient d'un laboratoire de tests simulant une page d'authentification Web d'un système, protégé par un pare-feu applicatif, vulnérable à une injection SQL et permettant l'ouverture d'une session administrateur en contournant le système d'authentification.

Contournement du système d'authentification par injection SQL

Composants

Cette section doit donner une liste précise des composants affectés par la vulnérabilité.

Le composant vulnérable est :

- ✓ le formulaire d'authentification à l'adresse http://exemple.gouv.qc.ca

Sommaire de gestion

Cette section s'adresse à des personnes ayant un profil moins technique. Par conséquent, le langage est adapté afin de faciliter la compréhension de la vulnérabilité.

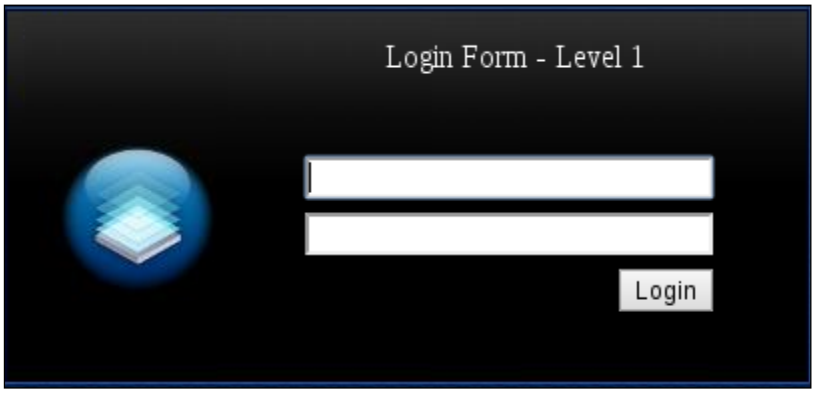
Le système Web interagit avec un gestionnaire de base de données sous la forme de requête SQL. Une requête SQL permet notamment d'ajouter, de modifier et de supprimer des données ainsi que d'y accéder. Or, une requête SQL construite à partir de données non validées fournies par un utilisateur constitue une faille de sécurité. En effet, un utilisateur malveillant pourrait fournir des données qui permettraient de modifier la requête SQL, ce qui, entre autres, pourrait donner accès à des entrées de la base de données ou occasionnerait une altération du comportement du système. Dans le cas présent, la vulnérabilité permet à un utilisateur malveillant de contourner le système d'authentification et d'ouvrir une session sur le système, en tant qu'administrateur.

Détails techniques

Cette section comporte des explications techniques permettant de comprendre la problématique en profondeur et de reproduire le problème. Ces détails doivent être complets, tout en excluant l'information explicite telle que des mots de passe.

Pour débuter, la vulnérabilité se situe au niveau du formulaire, illustré à la Figure 4, présentée ci-dessous.

Figure 4 – Formulaire d'authentification du système



La présence d'un pare-feu applicatif et de l'injection SQL a été détectée à l'aide de la technique du test à données aléatoires ou *fuzzing*[34], en utilisant des outils maison. Par exemple, les caractères « = » ainsi que les parenthèses sont bloqués par l'application, comme le démontrent la Figure 5 et la Figure 6.

Figure 5 – Tentative d'injection en utilisant le caractère « = »

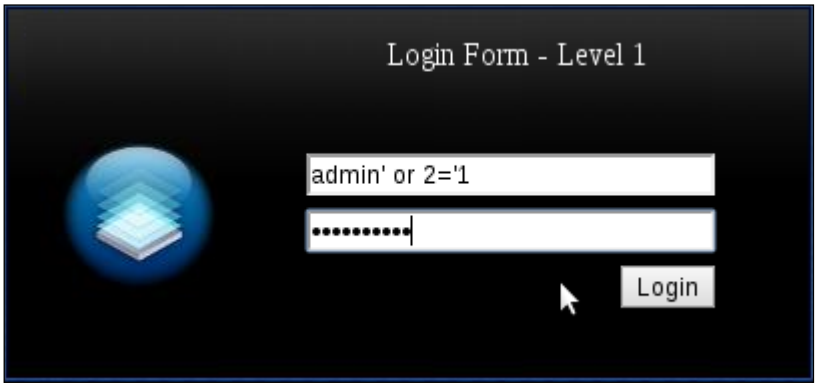
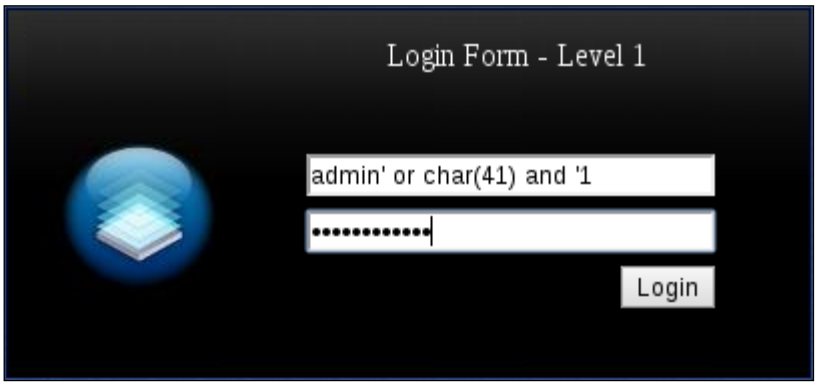


Figure 6 – Tentative d'injection en utilisant les parenthèses



34. Le *fuzzing* ou *fuzz testing* est une méthode de test, souvent automatisée ou semi-automatisée, qui consiste à entrer de l'information invalide, inattendue ou aléatoire dans un programme, afin de déceler les erreurs, les fuites de mémoire ou tout autre problème de code.

En effet, les deux tentatives d'injections précédentes retournent un message d'erreur, indiquant que des caractères invalides sont envoyés, comme l'illustre la figure 7. Pour cette raison, les tentatives d'injections SQL envoyées préalablement par des outils automatisés ont échoué.

Figure 7 – Erreur envoyée par le pare-feu applicatif

Ensuite, diverses tentatives d'injection manuelle ont permis de découvrir la présence d'une vulnérabilité applicative. En effet, certaines injections modifient le comportement de la page. Par exemple, l'injection illustrée à la figure 8 causait une erreur d'utilisateur ou de mot de passe invalide, comme l'illustre la figure 9.

Figure 8 – Injection avec un seul champ dans la requête

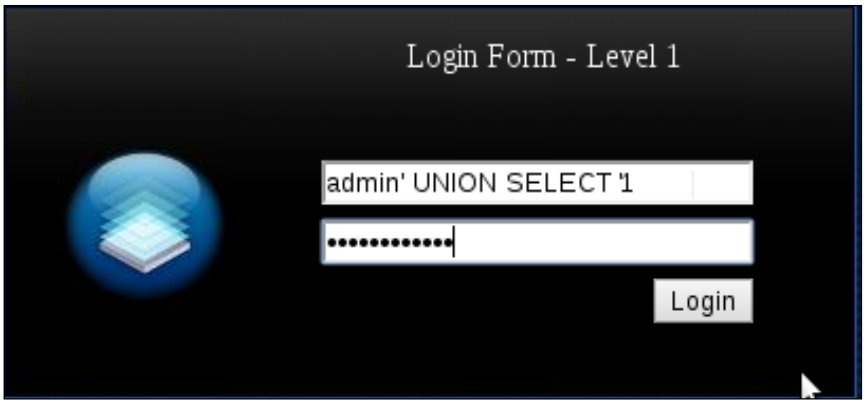


Figure 9 – Erreur envoyée lors d'une injection avec un seul champ

Par contre, l'injection de la figure 10, présentée ci-après, indique un mot de passe invalide pour l'utilisateur « admin » et l'utilisateur « 2 », comme l'illustre la figure 11.

Figure 10 – Injection avec trois (3) champs dans la requête

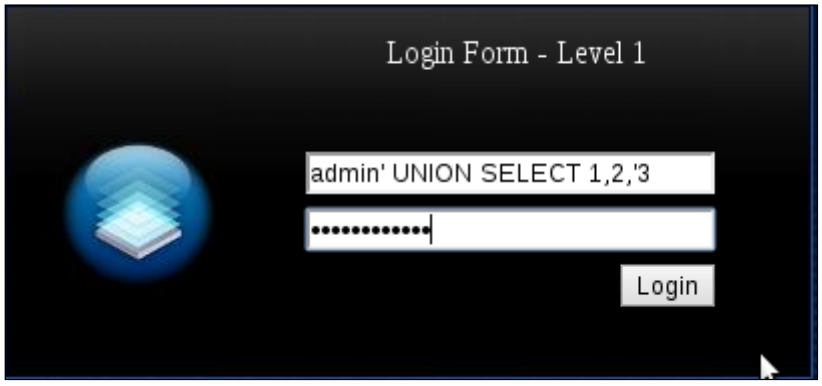
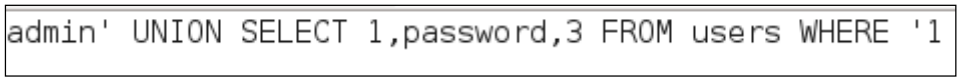


Figure 11 – Erreur retournée lors d'une injection à trois (3) champs

En mettant en corrélation les deux injections précédentes et les erreurs retournées par ces attaques, on peut affirmer, non seulement que l'utilisateur « admin » existe, mais aussi que l'application est vulnérable aux injections SQL, malgré le pare-feu applicatif; plus précisément, on observe que le deuxième champ de la requête SQL est retourné à l'utilisateur. Ainsi, il suffit de modifier l'injection, de manière à retourner le champ mot de passe de comptes dans la table utilisateurs, comme l'indique la figure 12.

Figure 12 – Injection SQL permettant l'affichage d'information sensible



Le résultat de l'injection est illustré à la figure 13, présentée ci-après. On peut remarquer que les mots de passe sont hachés, c'est-à-dire rendus illisibles par une fonction de hachage. L'algorithme utilisé est potentiellement celui de SHA-1, en raison du nombre de caractères affichés.

Figure 13 – Résultat de l'injection SQL précédente

Une tentative de cassage du mot de passe a été faite pour évaluer la rigueur des mots de passe. À l'aide de l'outil « hashcat », le mot de passe a été cassé en moins de huit minutes, sur un poste de travail standard, comme l'illustrent la figure 14 et la figure 15.

Figure 14 – Ligne de commande utilisée pour casser le mot de passe

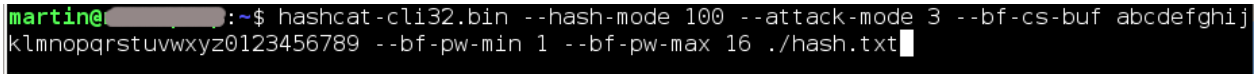
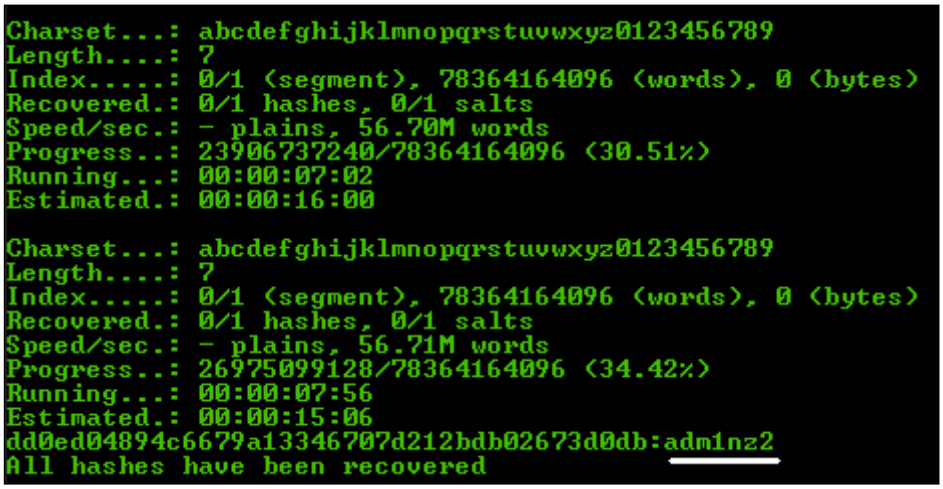
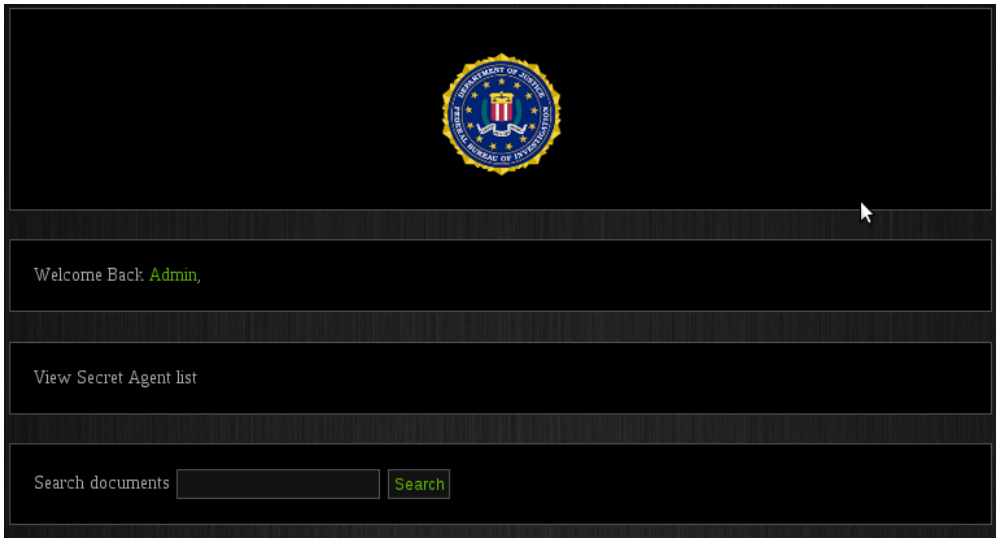


Figure 15 – Résultat de « hashcat » : le mot de passe est cassé



Ainsi, en exploitant la vulnérabilité d'injection SQL, il a été possible d'accéder au système, tout en ignorant le compte d'utilisateur ou le mot de passe, comme le démontre la Figure 16.

Figure 16 – Accès à l'application



Analyse

Cette section présente l'analyse permettant d'évaluer le risque, en fonction de la probabilité que la vulnérabilité soit exploitée et de son impact. L'analyse doit être mise en contexte selon la criticité du composant et la mission de l'organisation.

Considérant que :

- ✓ la vulnérabilité peut être exploitée avec très peu de connaissances;
  - Aucune connaissance préalable du compte d'utilisateur ou du mot de passe n'était nécessaire à l'exploitation
- ✓ le système Web est exposé;

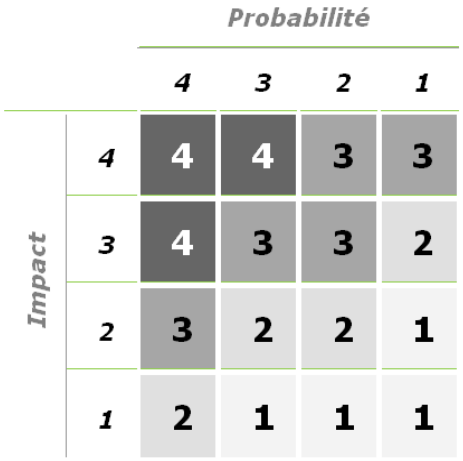
- la probabilité qu'une menace cause des dommages en exploitant cette vulnérabilité est jugée « Élevée » (3).

Considérant que :

- ✓ l'exploitation de cette vulnérabilité rend possible un déni de services du système, par corruption de données;
- ✓ l'exploitation de cette vulnérabilité rend possible l'accès à de l'information confidentielle;
- ✓ l'exploitation de cette vulnérabilité rend possible la modification d'information contenue dans la base de données;
  - l'impact à l'effet qu'une menace cause des dommages en exploitant cette vulnérabilité est jugé « Élevé » (3).

Ainsi, en utilisant la matrice d'analyse de risque illustrée à la figure 17, le risque est jugé « Élevé » (3).

Figure 17 – Matrice de calcul de la gravité du risque



Le tableau 11 présente un résumé de l'analyse de risque.

Tableau 11 – Sommaire de l'analyse de risque

	Impact	Probabilité	Risque
Disponibilité	Élevé (3)	Élevé(3)	Élevé(3)
Intégrité	Élevé (3)		
Confidentialité	Élevé (3)		

Recommandations

Cette section propose des pistes de solutions pour permettre de corriger la vulnérabilité. Celles-ci peuvent être précises ou plus larges, selon le problème et les composants touchés.

Tout d'abord, il est recommandé de rehausser la sécurité du pare-feu applicatif. De nombreux caractères peuvent être bloqués de manière à protéger l'application contre les injections SQL, tout en permettant l'envoi de caractères légitimes, nécessaires au fonctionnement de l'application. Par exemple, les

caractères apostrophe (‘), guillemets (‘’) et soustraction (-) pourraient être ajoutés à la liste des caractères protégés.

De plus, il est recommandé, avant d'effectuer tout traitement d'information, de valider les entrées envoyées par les utilisateurs, afin que ces entrées ne soient pas interprétées, mais bien utilisées comme elles se doivent.

Enfin, il est recommandé d'utiliser des mots de passe plus rigoureux. En effet, un mot de passe de sept (7) caractères et ne comprenant pas de caractères spéciaux n'est pas sécuritaire, puisqu'il peut être cassé dans un temps raisonnable par des outils gratuits et faciles à utiliser.

Références

Cette section présente les références permettant au lecteur d'en connaître davantage sur la vulnérabilité.

Date de dépôt du bulletin

Cette section indique la date à laquelle le bulletin a été déposé.

ANNEXE VI Certifications pertinentes

Le tableau 12 présente les certifications les plus pertinentes associées à la réalisation de tests d'intrusions et de vulnérabilités.

Tableau 12 – Certifications pertinentes pour la réalisation de tests d'intrusions et de vulnérabilités

Institution	Certification
Offensive Security[35]	Offensive Security Certified Professional (OSCP) Offensive Security Wireless Professional (OSWP) Offensive Security Certified Expert (OSCE) Offensive Security Exploitation Expert(OSEE) Offensive Security Web Expert (OSWE)
SANS[36]	GIAC Penetration Tester (GPEN)
EC-Council[37]	Certified Ethical Hacker (CEH)

35. http://www.offensive-security.com/
36. http://www.sans.org/
37. http://www.eccouncil.org/

Secrétariat
du Conseil du trésor
Québec

Au cœur de l'administration publique