



Building digital solutions for you

Référence :	BNI_ORION_DIAGNOSTIC-VV1.0-20230131.docx
Client :	BNI
Date de dernière modif. :	31-01-2023
Date de Diffusion :	31-01-2023
Version :	1
Nombre de pages :	20
Validation :	Mamisoa Ramanitrarivo
Auteur(s) :	Rado Andriandrantonavalona

BNI – ORION

Diagnostic et préconisations

Auteur(s) :	Validation(s) :
Rado Andriandrantonavalona	Mamisoa Ramanitrarivo

Sommaire

1 Avant-propos.....	1
1.1 Confidentialité du document.....	1
1.2 Historique des versions.....	1
1.3 Documents de référence	1
2 Cadre de la mission	1
3 Le processus d’audit.....	2
3.1 Démarche adoptée	2
3.1.1 Analyse « Statique » de la qualité	3
3.1.2 Scan « Dynamique » de la sécurité.....	3
3.1.3 Vérification des préconisations du dernier audit	3
3.2 Eléments de mesure	3
3.2.1 Priorité.....	3
3.2.2 Sévérité.....	4
3.2.3 Probabilité	4
3.2.4 Probabilité – Simplicité d’exploitation	5
3.2.5 Probabilité – Exposition.....	5
3.2.6 Impact.....	6
3.2.7 Impact – Conséquence	6
3.2.8 Impact – Complexité de correction	7
3.3 Gestion des sources.....	7
3.4 Suivi des corrections du premier audit	8
3.5 Résultat analytique du diagnostic en mode BlackBox et GrayBox	9
3.5.1 Analyse avec BURP en mode BlackBox.....	9
3.5.2 Analyse avec BURP en mode GrayBox.....	11
3.6 Résultat analytique du diagnostic en mode WhiteBox.....	12
3.6.1.1.1 Duplication de code	12
3.6.1.1.2 Vérification code	14

1 Avant-propos

1.1 Confidentialité du document

Le présent document est confidentiel et sa confidentialité consiste à :

- La non-divulgateion des dites informations auprès de tierces parties,
- La non-reproduction des informations, sauf accord de l'organisme audité,
- Ne pas profiter ou faire profiter tierces parties de ces informations en matière de savoir-faire,
- Considérer toutes les informations relatives à la production et au système d'information de l'organisme audité déclarées Confidentielles.

1.2 Historique des versions

Version	Date	Auteur
BNI_ORION_DIAGNOSTIC -VT0.1	17/01/2023	Rado Andriandrantonavalona
BNI_ORION_DIAGNOSTIC -VT0.2	26/01/2023	Rado Andriandrantonavalona Mamisoa Ramanitrarivo
BNI_ORION_DIAGNOSTIC -VV1.0	31/01/2013	Rado Andriandrantonavalona Mamisoa Ramanitrarivo

1.3 Documents de référence

Référence	Titre	Version	Description
Audit code ORION	Audit_code_orion	VV1.0	Rapport du dernier audit sur le projet ORION

2 Cadre de la mission

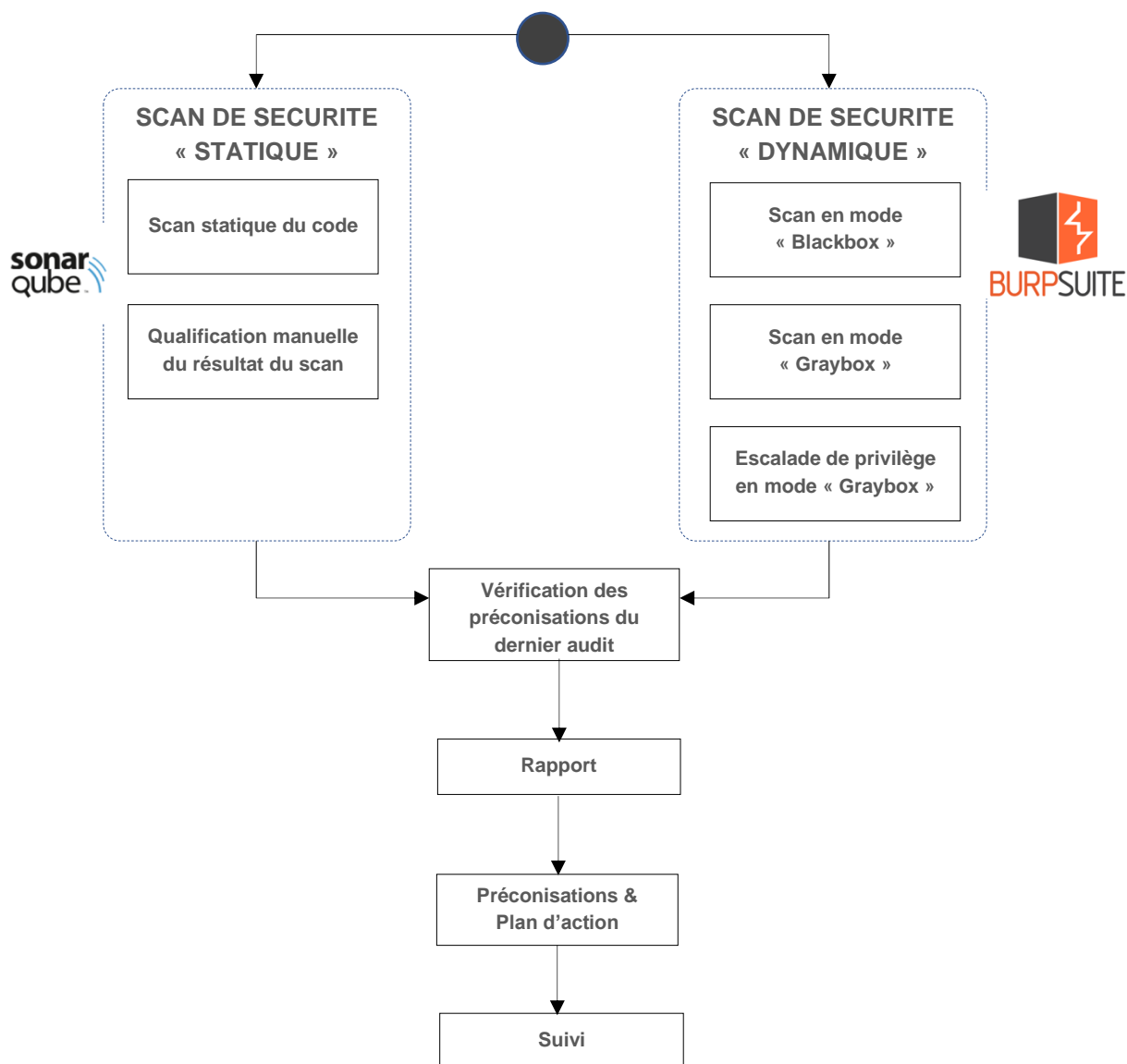
Dans le cadre de son projet de transformation digitale, la BNI souhaite faire un diagnostic de l'outil BNI ORION afin de valider son socle digital.

Ce document fournit :

- Diagnostic technique de l'outil ORION
- Des précautions afin des résorber les « dettes techniques » identifiées
- Suivi de la correction des précautions proposées lors du premier audit en 2020

3 Le processus d'audit

3.1 Démarche adoptée



3.1.1 Analyse « Statique » de la qualité

Il s'agit d'une analyse de codes sources des programmes sans l'exécuter. Les potentiels déficits sont détectés à partir de la façon dont le code a été écrit et structuré. Cette analyse dépend étroitement de la technologie et du langage de programmation utilisé.

3.1.2 Scan « Dynamique » de la sécurité

Il s'agit d'un « scan » effectué sur une instance en exécution de l'application. L'environnement scanné devrait être le plus proche possible de l'environnement de production en termes de :

- Version de l'application
- Ecosystème hôte (configuration et dimensionnement matériel du serveur, version de système d'exploitation, règles de flux entrant et sortant)
- Contenu de la base de données (qualité et quantité des informations)

Un scan en « **Blackbox** » est une tentative de détection des différentes failles ou tentative de casser ou d'outrepasser les dispositifs de sécurité en place, en ne disposant pas (ou en n'utilisant pas, si on en on a disposition) d'identifiants (login / mot de passe, badge, etc ...) valide sur le système tester

Un scan en « **Graybox** » est une tentative de détecter les différentes failles en accédant aux différentes fonctionnalités de l'application en utilisant des identifiants valides.

En mode « **Graybox** », un test d'escalade de privilèges consiste essayer d'outrepasser les dispositifs de sécurité et des restrictions tout en ayant un profil non adéquat (ayant le moins de droits et le plus restreint possible).

3.1.3 Vérification des préconisations du dernier audit

Vérification si les recommandations du dernier audit sont toutes appliquées et si d'autres se sont reproduit lors de la correction des bugs.

3.2 Eléments de mesure

Chaque point de diagnostic relevé sera évalué avec les métriques suivants :

* Les unités de mesure utilisées dans ce rapport ont été inspirées par et reprises des précédents audits de sécurité effectués par la société **Elysium Security**.

3.2.1 Priorité

NOTE		DESCRIPTION
TRES FAIBLE	INDEFINIE	La priorité du ou des constats est indéfinie. Leur sévérité n'est pas élevée et leur temps de correction nécessaire n'est pas rapide.
FAIBLE	LONG TERME	La priorité du ou des constats est à long terme. Soit leur sévérité est élevée mais leur temps de correction nécessaire est très considérable ou leur sévérité n'est pas élevée.

NOTE		DESCRIPTION
MOYEN	MOYEN TERME	La priorité du ou des constats est à moyen terme. Leur sévérité est élevée et leur temps de correction nécessaire est considérable.
FORT	COURT TERME	La priorité du ou des constats est à court terme. Leur sévérité est très élevée et leur temps de correction nécessaire est rapide.
TRES FORT	IMMEDIATE	La priorité du ou des constats est immédiate. Leur sévérité est très élevée et leur temps de correction nécessaire est très rapide.

3.2.2 Sévérité

NOTE		DESCRIPTION
TRES FAIBLE	SANS IMPORTANCE	La sévérité du ou des constats est sans importance. Leur réalisation est improbable et leur impact opérationnel/financier est très limité.
FAIBLE	LIMITEE	La sévérité du ou des constats est limitée. Leur réalisation est peu probable et leur impact opérationnel/financier est limité.
MOYEN	SUBSTANTIELLE	La sévérité du ou des constats est substantielle. Leur réalisation est probable et leur impact opérationnel/financier peut être élevé.
FORT	IMPORTANTE	La sévérité du ou des constats est importante. Leur réalisation est très probable et leur impact opérationnel/financier est élevé.
TRES FORT	TRES IMPORTANTE	La sévérité du ou des constats est très importante. Leur réalisation est extrêmement probable et leur impact opérationnel/financier est très élevé.

3.2.3 Probabilité

NOTE		DESCRIPTION
TRES FAIBLE	IMPROBABLE	La réalisation du ou des constats est improbable. Leur exploitation est difficile et leur surface et vecteurs d'attaques sont limités.
FAIBLE	PEU PROBABLE	La réalisation du ou des constats est peu probable. Soit leur exploitation est facile mais leur surface et vecteurs d'attaques sont limités ou leur exploitation est difficile.

NOTE		DESCRIPTION
MOYEN	PROBABLE	La réalisation du ou des constats est probable. Leur exploitation est facile et leur surface et vecteurs d'attaques peuvent être grands.
FORT	TRES PROBABLE	La réalisation du ou des constats est très probable. Leur exploitation est très facile et leur surface et vecteurs d'attaques sont grands.
TRES FORT	CERTAINE	La réalisation du ou des constats est certaine. Leur exploitation est très facile et leur surface et vecteurs d'attaques sont très grands.

3.2.4 Probabilité – Simplicité d'exploitation

NOTE		DESCRIPTION
TRES FAIBLE	TRES DIFFICILE	La réalisation du ou des constats est très difficile car le vecteur d'attaque n'est que théorique. Cela nécessite des ressources et expertise extrêmement importantes.
FAIBLE	DIFFICILE	La réalisation du ou des constats est difficile car le vecteur d'attaque n'a pas encore d'outils d'exploitation connus. Cela nécessite des ressources et une expertise très importante
MOYEN	PRESQUE FACILE	La réalisation du ou des constats est presque facile car le vecteur d'attaque a déjà des outils d'exploitation connus complexes qui nécessitent des ressources et une expertise importante.
FORT	FACILE	La réalisation du ou des constats est facile car le vecteur d'attaque a déjà des outils d'exploitation connus qui nécessitent peu de ressources ou d'expertise.
TRES FORT	TRES FACILE	La réalisation du ou des constats est très facile car le vecteur d'attaque a déjà des outils d'exploitation connus très simples qui ne nécessitent pas de ressources ou d'expertise.

3.2.5 Probabilité – Exposition

NOTE		DESCRIPTION
TRES FAIBLE	INTERNE PRIVILEGIE	La surface d'attaque du ou des constats est très petite. Leur réalisation nécessite un accès au réseau interne à l'environnement testé et un compte administrateur.
FAIBLE	INTERNE UTILISATEUR	La surface d'attaque du ou des constats est petite. Leur réalisation nécessite un accès au réseau interne à l'environnement testé et un compte utilisateur.

NOTE		DESCRIPTION
MOYEN	INTERNE	La surface d'attaque du ou des constats est normale. Leur réalisation ne nécessite qu'un accès au réseau interne à l'environnement testé.
FORT	EXTERNE UTILISATEUR	La surface d'attaque du ou des constats est grande. Leur réalisation nécessite un accès depuis l'internet avec un compte utilisateur sur l'environnement testé.
TRES FORT	EXTERNE	La surface d'attaque du ou des constats est très grande. Leur réalisation ne nécessite qu'un accès depuis l'internet sans compte utilisateur sur l'environnement testé.

3.2.6 Impact

NOTE		DESCRIPTION
TRES FAIBLE	SANS IMPORTANCE	L'impact du ou des constats est sans importance. Leur conséquence opérationnelle / financière est limitée et leur correction est simple.
FAIBLE	LIMITE	L'impact du ou des constats est limité. Leur conséquence opérationnelle / financière est peu élevée et leur correction n'est pas complexe.
MOYEN	SUBSTANTIEL	L'impact du ou des constats est substantiel. Leur conséquence opérationnelle/financière est élevée et leur correction n'est pas complexe.
FORT	IMPORTANT	L'impact du ou des constats est important. Leur conséquence opérationnelle/financière est très élevée et leur correction peut être complexe.
TRES FORT	TRES IMPORTANT	L'impact du ou des constats est très important. Leur conséquence opérationnelle/financière est extrêmement élevée et leur correction est très complexe.

3.2.7 Impact – Conséquence

NOTE		DESCRIPTION
TRES FAIBLE	SANS IMPORTANCE	Les conséquences du ou des constats sont sans importance. Leur réalisation aurait un impact opérationnel/financier limité.

NOTE		DESCRIPTION
FAIBLE	LIMITE	Les conséquences du ou des constats sont limités. Leur réalisation aurait un impact opérationnel/financier peu élevé.
MOYEN	SUBSTANTIELLE	Les conséquences du ou des constats sont substantiels. Leur réalisation aurait un impact opérationnel/financier élevé.
FORT	IMPORTANTE	Les conséquences du ou des constats sont importantes. Leur réalisation aurait un impact opérationnel/financier très élevé.
TRES FORT	TRES IMPORTANTE	Les conséquences du ou des constats sont très importantes. Leur réalisation aurait un impact opérationnel/financier extrêmement élevé.

3.2.8 Impact – Complexité de correction















NOTE		DESCRIPTION
TRES FAIBLE	DES HEURES	Les efforts de correction du ou des constats peuvent prendre des heures et les ressources nécessaires, technologiques ou humaines sont négligeables.
FAIBLE	DES JOURS	Les efforts de correction du ou des constats peuvent prendre des jours et les ressources nécessaires, technologiques ou humaines sont très peu importantes.
MOYEN	DES SEMAINES	Les efforts de correction du ou des constats peuvent prendre des semaines et les ressources nécessaires, technologiques ou humaines sont importantes.
FORT	DES MOIS	Les efforts de correction du ou des constats peuvent prendre des mois et les ressources nécessaires, technologiques ou humaines sont très importantes.
TRES FORT	DES ANNEES	Les efforts de correction du ou des constats peuvent prendre des années et les ressources nécessaires, technologiques ou humaines sont très importantes.

3.3 Gestion des sources

BNI dispose actuellement d'un gestionnaire de sources (GIT) avec un référentiel central (prgit01.tnr.bnici.com) qui est déjà un point très positif.

Néanmoins, pour avoir le code source à analyser, l'équipe l'a demandé au prestataire. Le risque est d'avoir un écart sur le code analysé et le code mis en prod.

3.4 Suivi des précautions du premier audit

Référence	Description	Etat	Observations
SECU-AUTH-001	Code contenant du mot de passe en dur et en clair		
SECU-AUTH-002	La méthode « OrionAuthenticationProvider::bindLDAPUser » renvoie toujours une valeur « true »		
SECU-SQLI-001	Concaténation de chaînes de caractère pour former les requêtes SQL		
SECU-XSSI-001	Utilisation d'API vulnérable permettant l'injection XSS via Email		
SECU-DOS-001	Utilisation d'« expressions régulières », à requalifier en profondeur et à justifier car expose à un risque de ReDOS (Regular Expression Denial Of Service)		
SECU-RCI-001	Utilisation de fonction d'évaluation, permettant l'exécution de « code arbitraire » côté client.		
SECU-CRYPTO-001	Utilisation de méthode de génération de nombre aléatoire non sécurisée, basée seulement sur l'horloge système		
SECU-CRYPTO-002	Utilisation de méthode de cryptage faible		
QA-MISC-001	Potentiel « NullPointerException »		
QA-MISC-002	« return » dans un bloc « finally »		
QA-MISC-003	Comparaison par égalité « == » de 2 références d'objet => Toujours « False »		
QA-MISC-004	Comparaison par méthode « equals » de 2 références de différents types		
QA-CONFIG-001	Configuration de CORS (Cross-RoginResource Sharing)		
QA-CONFIG-002	Cookie manipulable côté client		

3.5 Résultat analytique du diagnostic en mode BlackBox et GrayBox

3.5.1 Analyse avec BURP en mode BlackBox

Stricte sécurité de transport n'est pas forcée		ORION-CONF-001	
		SECU-HSTS-A01	
PRIORITE		MOYEN	
SEVERITE		FAIBLE	
PROBABILITE	MOYEN	EXPOSITION	MOYEN
		SIMPLICITE D'EXPLOITATION	MOYEN
IMPACT	FORT	CONSEQUENCES	MOYEN
		COMPLEXITE DE CORRECTION	FAIBLE
<u>Localisation</u> :			
<ul style="list-style-type: none">- Serveur de production- https://prorion01.tnr.bnictm.com:8443/orion/login.jsp			
<u>Autres localisations similaires</u> :			
<u>Description</u> : L'attaquant peut intercepter la requête de sa victime et la modifier.			
<u>Impacts</u> :			
<ul style="list-style-type: none">- Usurpation d'identité			
<u>Préconisation</u> :			
<ul style="list-style-type: none">- Ajouter l'option « preload » dans le HSTS header et l'envoyer vers le navigateur			
<u>Autres références</u> :			
<ul style="list-style-type: none">- Strict-Transport-Security- HSTS Preload Form			

L'option autocomplete est activée pour le champ password			ORION-CONF-002
			SECU-PASSW-A01
PRIORITE		MOYEN	
SEVERITE		FAIBLE	
PROBABILITE	MOYEN	EXPOSITION	MOYEN
		SIMPLICITE D'EXPLOITATION	MOYEN
IMPACT	FORT	IMPACT	FORT
		COMPLEXITE DE CORRECTION	FAIBLE
<u>Localisation</u> : <ul style="list-style-type: none">- Serveur de production- https://prorion01.tnr.bnclm.com:8443/orion/j_acegi_security_check;jsessionid=D3EAF8D8E43EE788EAC8BB97C82BFB0A			
<u>Autres localisations similaires</u> :			
<u>Description</u> : Certain navigateurs permet facilement de se souvenir du mot de passe de l'utilisateur.			
<u>Impacts</u> : <ul style="list-style-type: none">- Si le post est utilisé par plusieurs personnes, d'autre personne peut utiliser l'identifiant de la victime.			
<u>Préconisation</u> : <ul style="list-style-type: none">- Ajouter l'attribut « autocomplete = off » dans le formulaire ;- A voir avec la BNI si certains utilisateurs a besoin de cette fonctionnalité			
<u>Autres références</u> : <ul style="list-style-type: none">- CWE-200: Information Exposure			

3.5.2 Analyse avec BURP en mode GrayBox

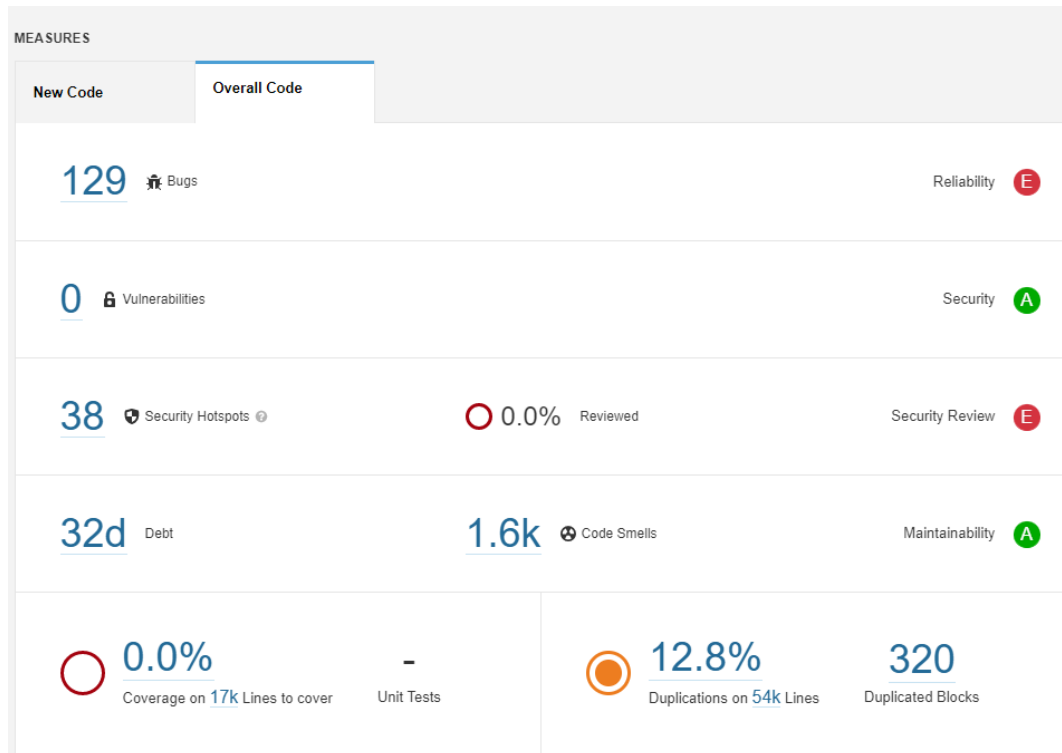
SQL injection possible		ORION-SQL-001	
		SECU-SQL-A01	
PRIORITE		MOYEN	
SEVERITE		FORT	
PROBABILITE	MOYEN	EXPOSITION	MOYEN
		SIMPLICITE D'EXPLOITATION	MOYEN
IMPACT	FORT	IMPACT	FORT
		COMPLEXITE DE CORRECTION	FAIBLE
<u>Localisation</u> : <ul style="list-style-type: none">- Serveur de recette- http://rcorion01.tnr.bnici.m.com:8080/orion/transaction/search			
<u>Autres localisations similaires</u> :			
<u>Description</u> : En ajoutant « (select*from(select(sleep(20)))a) » dans les paramètres de la recherche, le temps de réponse du serveur inclut le laps de temps d'arrêt.			
<u>Impacts</u> : <ul style="list-style-type: none">- Une attaque par injection d'une requête SQL peut			
<u>Préconisation</u> : <ul style="list-style-type: none">- Tout paramètre http doit être nettoyé avant utilisation- Les paramètres de requêtes SQL doivent être protégés			
<u>Autres références</u> : <ul style="list-style-type: none">- Web Security Academy: SQL injection- Using Burp to Test for Injection Flaws- Web Security Academy: SQL Injection Cheat Sheet			

3.6 Résultat analytique du diagnostic en mode WhiteBox

Le tableau suivant fournit de manière synthétique le résultat de l'analyse statique de la qualité du code. Les détails sont accessibles et explorables en mode interactif sur SONAR.

La notation de chaque axe varie de **A** (note la plus haute) à **F** (note la plus basse)

3.6.1.1.1 Duplication de code



Le taux de duplication de code est d'environ 12,8%

Exemple : src/main/com/soprabanking/amplitude/CustomerActivityField.java [ligne s 36 – 84] est dupliqué dans les fichiers suivants :

src/main/java/com/soprabanking/amplitude/AccountClass.java [ligne 36 – 84]
src/main/java/com/soprabanking/amplitude/AccountType.java [ligne 36 – 84]
src/main/java/com/soprabanking/amplitude/AdressFormat.java [ligne 36 – 84]
src/main/java/com/soprabanking/amplitude/AdressType.java [ligne 36 – 84]
src/main/java/com/soprabanking/amplitude/Branch.java [ligne 36 – 84]
src/main/java/com/soprabanking/amplitude/CentralBankCategory.java [ligne 36 – 84]
src/main/java/com/soprabanking/amplitude/ChamberOfCommerce.java [ligne 36 – 84]
src/main/java/com/soprabanking/amplitude/Country.java [ligne 36 – 84]
src/main/java/com/soprabanking/amplitude/CustomerFreeField1.java [ligne 36 – 84]
src/main/java/com/soprabanking/amplitude/CustomerFreeField2.java [ligne 36 – 84]
src/main/java/com/soprabanking/amplitude/CustomerFreeField3.java [ligne 36 – 84]
src/main/java/com/soprabanking/amplitude/CustomerProfile.java [ligne 36 – 84]
src/main/java/com/soprabanking/amplitude/CustomerQuality.java [ligne 36 – 84]
src/main/java/com/soprabanking/amplitude/CustomerREalEstateSituation.java [ligne 36 – 84]
...

La duplication de codes :

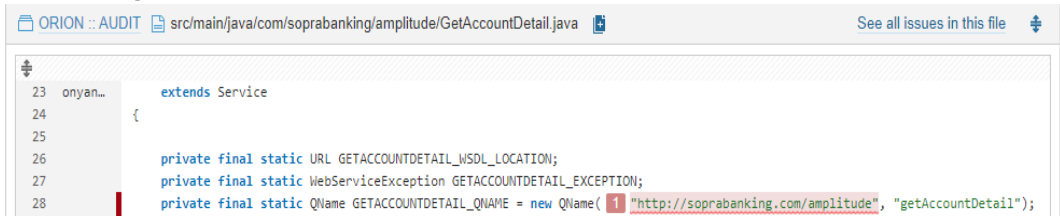

Réduit de manière considérable la « maintenabilité de ce dernier »

Est source potentiel de régression due à une modification effectuée sur un bloc dupliquée et non impliquée sur l'autre.

3.6.1.1.2 Vérification code

Risque de ressource non fermée			ORION-code-001
			Code-blocker-S01
PRIORITE		MOYEN	
SEVERITE		FORT	
PROBABILITE	MOYEN	EXPOSITION	FAIBLE
		SIMPLICITE D' EXPLOITATION	MOYEN
IMPACT	MOYEN	IMPACT	MOYEN
		COMPLEXITE DE CORRECTION	FAIBLE
Localisation : <ul style="list-style-type: none">- src/main/java/mg/bni/orion/dao/hibernate/liaison/LiaisonFODaoHibernate.java [ligne 259] <pre>192 public List<String> getListeCommentaires(String idLiaison){ 193 StringBuilder sql = new StringBuilder("select commentaire,@r AS _id, (SELECT @r := id_liaison_prec FROM audits_liaisons"); 194 sql.append(" WHERE id_liaison = _id and type_action='C') AS parent, @l := @l + 1 AS lvl "); 195 sql.append(" FROM (SELECT @r := ?, @l := 0, @cl := 0) vars, audits_liaisons h WHERE ifnull(@r,0) <> 0 and type_action='"); 196 List<String> parameters = new ArrayList<>(); 197 List<String> commentaires = new ArrayList<>(); 198 parameters.add(idLiaison); 199 Session session = getHibernateTemplate().getSessionFactory().getCurrentSession(); 200 Connection connection = ((SessionImpl) session).connection(); 201 PreparedStatement pstmt = null; 202 ResultSet rs = null; 203 try { 204 pstmt = connection.prepareStatement(sql.toString());</pre>			
Autres localisations similaires : <ul style="list-style-type: none">- src/main/java/mg/bni/orion/dao/hibernate/liaison/LiaisonFODaoHibernate.java [ligne 204]- src/main/java/mg/bni/orion/dao/hibernate/liaison/LiaisonFODaoHibernate.java [ligne 292]- src/main/java/mg/bni/orion/web/document/DocumentController.java			
Description : Une ressource a été ouverte et en cas d'erreur la ressource ne sera pas fermée correctement.			
Impacts : <ul style="list-style-type: none">- Possibilité d'avoir des fuites de mémoire.			
Préconisation : <ul style="list-style-type: none">- Fermer la ressource dans le bloc finally- Utiliser Try-with-resource			
Autres références : <ul style="list-style-type: none">- MITRE, CWE-459 - Incomplete Cleanup- MITRE, CWE-772 - Missing Release of Resource after Effective Lifetime- CERT, FIO04-J. - Release resources when they are no longer needed- CERT, FIO42-C.- Try With Resources			

Objet non sérialisable		ORION-code-003	
		CODE-CRIT-S01	
PRIORITE		MOYEN	
SEVERITE		FORT	
PROBABILITE	MOYEN	EXPOSITION	MOYEN
		SIMPLICITE D'EXPLOITATION	FAIBLE
IMPACT	MOYEN	IMPACT	MOYEN
		COMPLEXITE DE CORRECTION	FAIBLE
Localisation : <ul style="list-style-type: none">- src/main/java/com/soprabanking/amplitude/ErrorResponseFlow_Exception.java [ligne 22] <pre>7 /** 8 * This class was generated by the JAX-WS RI. 9 * JAX-WS RI 2.3.2 10 * Generated source version: 2.2 11 * 12 */ 13 @WebFault(name = "errorResponseFlow", targetNamespace = "http://soprabanking.com/amplitude") 14 public class ErrorResponseFlow_Exception 15 extends Exception 16 { 17 18 /** 19 * Java type that goes as soapenv:Fault detail element. 20 * 21 */ 22 private ErrorResponseFlow faultInfo;</pre>			
Autres localisations similaires : <ul style="list-style-type: none">- src/main/java/mg/bni/orion/model/ClientBni.java- src/main/java/mg/bni/orion/model/user/Client.java			
Description : Quand l'application tente d'enregistrer un objet non sérialisé, il y a de fort risque que l'action ne se fait pas et le programme crash.			
Impacts : <ul style="list-style-type: none">- Une fuite de mémoire exploitable en lançant plusieurs requêtes pour forcer le serveur à enregistrer l'objet sur le disque.- Les données non sérialisées peuvent être corrompu.			
Préconisation : <ul style="list-style-type: none">- Sérialiser l'objet			
Autres références : <ul style="list-style-type: none">- MITRE, CWE-594 - Saving Unserializable Objects to Disk			

Variable à mettre en constante		ORION-code-004	
		Code-CRIT-S02	
PRIORITE		MOYEN	
SEVERITE		FAIBLE	
PROBABILITE	FAIBLE	EXPOSITION	FAIBLE
		SIMPLICITE D'EXPLOITATION	FAIBLE
IMPACT	FAIBLE	IMPACT	FAIBLE
		COMPLEXITE DE CORRECTION	FAIBLE
Localisation : <ul style="list-style-type: none">- src/main/java/com/soprabanking/amplitude/ObjectFactory.java [ligne 28]			
			
Autres localisations similaires : <ul style="list-style-type: none">- src/main/java/com/soprabanking/amplitude/ObjectFactory.java [ligne 76]- src/main/java/com/soprabanking/amplitude/ObjectFactory.java [ligne 88]			
			
Description : Le texte est utilisé à plusieurs endroits			
Impacts : <ul style="list-style-type: none">- La modification de la valeur du texte risquera des oublies et sources de régressions.			
Préconisation : <ul style="list-style-type: none">- Remplacer le texte en utilisant une constante.			

Autres références :

-

Erreur non capturée		ORION-code-004	
		Code-CRIT-S03	
PRIORITE		MOYEN	
SEVERITE		MOYEN	
PROBABILITE	MOYEN	EXPOSITION	MOYEN
		SIMPLICITE D'EXPLOITATION	FAIBLE
IMPACT	FAIBLE	IMPACT	FAIBLE
		COMPLEXITE DE CORRECTION	FAIBLE

Localisation :

- src/main/java/mg/bni/orion/config/CustomPropertyPlaceholderConfigurer.java

src/main/java/mg/bni/orion/config/CustomPropertyPlaceholderConfigurer.java

Open in IDE

Get Permalink

```
21         try {
22             props.load(res.getInputStream());
23             Enumeration<?> propertyNames = props.getPropertyNames();
24             while (propertyNames.hasMoreElements()) {
25                 String propertyName = (String) propertyNames.nextElement();
26                 String propertyValue = props.getProperty(propertyName);
27                 Resource newR = new PathResource(propertyValue);
28                 newRes.add(newR);
29             }
30         } catch (IOException e) {
31             e.printStackTrace();
```

Autres localisations similaires :

- src/main/java/mg/bni/orion/dao/hibernate/liaison/LiaisonFODaoHibernate.java [ligne 213]
- src/main/java/mg/bni/orion/dao/hibernate/liaison/LiaisonFODaoHibernate.java [ligne 316]
- src/main/java/mg/bni/orion/dao/hibernate/user/UserFODaoHibernate.java [ligne 57]
- src/main/java/mg/bni/orion/dao/hibernate/user/UserFODaoHibernate.java [ligne 71]
- src/main/java/mg/bni/orion/service/OrionAuthenticationProvider.java [ligne 125]
- src/main/java/mg/bni/orion/service/OrionUserDetailsService.java [ligne 127]
- src/main/java/mg/bni/orion/util/CryptoUtil.java [ligne 52]
- src/main/java/mg/bni/orion/util/CryptoUtil.java [ligne 125]
- src/main/java/mg/bni/orion/util/Toolkit.java [ligne 167]
- src/main/java/mg/bni/orion/util/Toolkit.java [ligne 272]
- src/main/java/mg/bni/orion/web/document/DocumentController.java [ligne 113]
- src/main/java/mg/bni/orion/web/document/DocumentController.java [ligne 347]
- src/main/java/mg/bni/orion/web/document/DocumentController.java [ligne 349]
- src/main/java/mg/bni/orion/web/document/DocumentController.java [ligne 356]
- src/main/java/mg/bni/orion/web/user/UserController.java [ligne 214]
- src/main/java/mg/bni/orion/ws/client/GetAccountDetailClient.java [ligne 47]
- src/main/java/mg/bni/orion/ws/client/GetAccountDetailClient.java [ligne 94]
- src/main/java/mg/bni/orion/ws/client/GetCustomerDetailClient.java [ligne 56]
- src/main/java/mg/bni/orion/ws/client/GetCustomerDetailClient.java [ligne 103]

Description : L'erreur n'est pas capturée convenablement

Impacts :

- Affichage des informations sensibles en cas de crache

Préconisation :

- S'assurer que le niveau de traçage soit en erreur

Autres références :

- [CVE-2018-1999007](#)
- [CVE-2015-5306](#)
- [CVE-2013-2006](#)

Adresse IP codée en dure		ORION-code-005	
		Code-CRIT-S04	
PRIORITE		MOYEN	
SEVERITE		MOYEN	
PROBABILITE	MOYEN	EXPOSITION	MOYEN
		SIMPLICITE D'EXPLOITATION	FAIBLE
IMPACT	FAIBLE	IMPACT	FAIBLE
		COMPLEXITE DE CORRECTION	FAIBLE
Localisation : src/main/java/com/soprabanking/amplitude/GetAccountDetail.java [ligne 21]			
<div>src/main/java/com/soprabanking/amplitude/GetAccountDetail.java</div> <div>Open in IDE</div> <div>Get Permalink</div>			
<pre>11 import javax.xml.ws.WebServiceException; 12 import javax.xml.ws.WebServiceFeature; 13 14 15 /** 16 * This class was generated by the JAX-WS RI. 17 * JAX-WS RI 2.3.2 18 * Generated source version: 2.2 19 * 20 */ 21 @WebServiceClient(name = "getAccountDetail", targetNamespace = "http://soprabanking.com/amplitude", wsdlLocation = "http://10.161.129.149:8080/getAccountDetail?wsdl")</pre>			
Autres localisations similaires : src/main/java/com/soprabanking/amplitude/GetAccountDetail.java [ligne 34]			
<ul style="list-style-type: none">- src/main/java/com/soprabanking/amplitude/GetCustomerDetail.java [ligne 20]- src/main/java/com/soprabanking/amplitude/GetCustomerDetail.java [ligne 33]- src/main/java/mg/bni/orion/web/util/WebUtil.java [ligne 751]- src/main/java/mg/bni/orion/web/util/WebUtil.java [ligne 752]- src/main/java/mg/bni/orion/web/util/WebUtil.java [ligne 753]			
Description : Utilisation des adresses IP fixes dans le code			
Impacts : <ul style="list-style-type: none">- Risque de régression en cas changement de l'adresse- Une attaque par IP spoofing est favorable- Donner les informations du réseau à un hacker			
Préconisation : <ul style="list-style-type: none">- Changer en constante- Préférer les noms de domaine que l'adresse IP			
Autres références : <ul style="list-style-type: none">- CVE-2006-5901- CVE-2005-3725			