Version libre à http://www.owasp.org



OWASP Standard de Vérification de la Sécurité des Applications 2009







Avant-propos

Ce document définit quatre niveaux de vérification des applications Web. Les niveaux de sécurité des applications web sont orientés vers l'analyse des composants constitués des couches du modèle OSI (Open Systems Interconnection Reference Model), plutôt que vers la sous-couche du système d'exploitation ou les réseaux connectés. Chaque niveau décrit dans ce document inclut un ensemble d'exigences servant à vérifier l'efficacité des contrôles de sécurité qui protègent les applications web.

Cet ensemble d'exigences de vérification a été mis en place en fonction des objectifs suivants :

- Utiliser comme unité de mesure Fournir aux développeurs et aux propriétaires d'applications un repère permettant de mesurer le degré de confiance à accorder à leurs applications web.
- Utiliser comme guide Fournir un guide aux développeurs de contrôles de sécurité, pour savoir que mettre en place dans les contrôles afin de satisfaire aux exigences de sécurité des applications¹.
- Utiliser pour la négociation de solutions logicielles Fournir une base d'exigences pour les vérifications de sécurité des applications au sein de contrats et de négociations de solutions logicielles².

Les exigences de vérification ont été agencées pour satisfaire aux objectifs précédents, de manière à garantir que les architectures, implémentations et utilisations, appliquent des contrôles de sécurité valides. Ces exigences garantissent que les contrôles de sécurité utilisés par une application utilisent une stratégie de déni par défaut, qu'ils soient centralisés, qu'ils soient placé coté serveur, et qu'ils soient tous utilisés lorsque nécessaire.

Copyright et Licence

Copyright © 2008 - 2009 Fondation OWASP.



Ce document est publié sous la licence <u>Creative Commons Attribution</u>
<u>ShareAlike 3.0</u>. Pour toute réutilisation ou distribution, vous devez clairement faire apparaître les termes de licence de ce document.

¹ Pour plus d'informations concernant la construction et l'utilisation de contrôles de sécurité couvrant les spécifications ASVS, voir *Enterprise Security API (ESAPI)* (OWASP, 2009).

² Pour plus d'informations sur l'utilisation d'ASVS au sein de négociations de solutions logicielles, voir *Contract Annex* (OWASP, 2009).



Table des matieres
Introductionv
Préambulev
Remerciementsvii
Niveaux de vérifications de la sécurité des applicationsviii
Niveau 1 - Vérification automatique
Exigences de vérification détailléesxx
V1 - Exigences de documentation d'architectures sécurisée
Glossairexxxviii
Pour approfondir le sujetxl
Figures
Figure 1 - Niveaux OWASP ASVS
Figure 2 - Introduire la vérification dans votre cycle de développement (SDLC)vi
Figure 3 - OWASP ASVS Niveaux 1, 1A, et 1Bix
Figure 4 - OWASP ASVS Niveau 1 exemple d'architecture sécuriséex
Figure 5 - OWASP ASVS Niveaux 2, 2A, et 2Bxi
Figure 6 - OWASP ASVS Niveaux 2 exemple d'architecture sécuriséexiii
Figure 8 - OWASP ASVS Niveau 3 exemple d'architecture sécuriséexvi
Figure 7 - OWASP ASVS Niveau 3xv



Figure 9 - OWASP ASVS Niveau 4xvii
Figure 10 - OWASP ASVS Niveau 4 Exemple de code non examinéxix
Figure 11 - Contenu des rapports d'activité (reporting)xxxvi
Tableaux
Tableau 1 - Exigences de l'architecture sécurisée OWASP ASVS (V1)xxi
Tableau 2 - Exigences d'authentification OWASP ASVS (V2)xxii
Tableau 3 - Exigences de gestion de sessions OWASP ASVS (V3)xxiii
Tableau 4 - Exigences du contrôle d'accès OWASP ASVS (V4)xxv
Tableau 5 - Exigences de validation des entrées (input) OWASP ASVS (V5)xxvi
Tableau 6 - Exigences d'encodage/échappement des sorties (output) OWASP ASVS (V6)xxvii
Tableau 7 - Exigences cryptographiques OWASP ASVS (V7)xxviii
Tableau 8 - Exigences de gestion des erreurs et de journalisations OWASP ASVS (V8)xxix
Tableau 9 - Exigences de protections des données OWASP ASVS (V9)xxx
Tableau 10 - Exigences des communications sécurisées OWASP ASVS (V10)xxxi
Tableau 11 - Exigences de sécurité HTTP OWASP ASVS (V11)xxxii



Introduction

Le Projet Ouvert de Sécurité des applications Web (OWASP) est une communauté ouverte destinée à permettre au organisations de développer, acquérir et maintenir des applications de confiance. Tous les outils, documents, forums et chapitres OWASP sont gratuits, de sources libres, et à disposition de ceux qui veulent améliorer la sécurité des applications. Nous recommandons d'aborder la sécurité des applications comme un problème de personnes, de processus et de technologie, parce que l'approche la plus efficace de la sécurité des applications doit comprendre des améliorations dans chacun de ces domaines. Vous pouvez nous trouver à www.owasp.org.

OWASP est une nouvelle sorte d'organisation. Notre indépendance face aux pressions commerciales, nous permet de fournir une information impartiale, pratique et économique à propos de la sécurité des applications. OWASP n'est affilié avec aucune entreprise de technologies, bien que nous encouragions l'utilisation avertie des outils et technologies de sécurité commerciaux. Comme de nombreux projets logiciels « open-source », OWASP produit de nombreux outils et documentations dans une démarche collaborative et ouverte. La fondation OWASP est une entité à but non lucratif, ce qui assure le succès des projets sur le long terme.

L'objectif premier du projet de standard de vérification de la sécurité des applications (ASVS), est de normaliser la gamme de protection et le niveau de rigueur en vigueur, lorsque sont exécutés des vérifications de sécurité d'applications internet, tout en utilisant un standard ouvert et commercialement compatible. Le standard apporte une base pour tester aussi bien les contrôles de sécurité techniques des applications, que tous les contrôles de sécurité techniques de l'environnement, qui servent à protéger contre des vulnérabilités comme le Cross-Site Scripting (XSS) et les injections SQL.³ Ce standard peut être utilisé pour établir un niveau de confiance relatif à la sécurité des applications internet.

<u>Préambule</u>

Le standard OWASP ASVS définit les exigences de vérification et de documentation, relatifs aux fondamentaux de la protection et du niveau de rigueur requis. Le standard définit quatre niveaux hiérarchiques (e.g. le niveau 2 demande plus de protection et de rigueur que le niveau 1) comme décrit dans la figure ci-dessous.

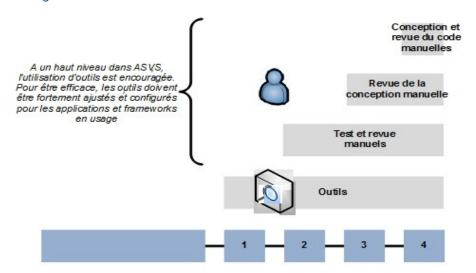


Figure 1 - Niveaux OWASP ASVS

³ Pour plus d'information sur les vulnérabilités communes des applications internet, voir le *OWASP Top Ten* (OWASP, 2007).



La vérification de la sécurité d'applications internet, est réalisée d'un point de vue logique en suivant (ou en essayant de suivre) les chemins d'entrée et de sortie d'une application ciblée, appelée la cible de vérification (Target of Verification ou TOV), et en exécutant des analyses le long de ces chemins. Les applications plus complexes prennent plus de temps à analyser, obligeant à des vérifications plus longues et plus couteuses. Les lignes de code ne sont pas le seul facteur qui détermine la complexité d'une application - différentes technologies requièrent typiquement différents nombres d'analyses. Les applications simples pourraient inclure par exemple des bibliothèques et des environnements de développement (framework). Les applications complexes pourraient inclure des applications Web 2.0 et de nouvelles technologies internet.

ASVS définit les éléments constituants pour les niveaux 1 et 2 (e.g. Les vérifications au niveau 1 requièrent d'accéder aux niveaux 1A et 1B). Par exemple, les applications pourraient prétendre à une conformité avec les niveaux 1A ou 1B au lieu du niveau 1, mais ce niveau reste plus faible que de revendiquer le niveau 1. Les exigence de vérification et de documentation sont définies dans ce standard de trois façons : les exigences de haut niveau, les exigences détaillées et les exigences de compte rendu. Les exigences de haut niveau définissent l'ensemble des exigences d'implémentation et de vérification de l'application. Les exigences détaillées définissent l'implémentation bas niveau de l'application, ainsi que les exigences de vérification (c-à-d, un point spécifique à vérifier). Les exigences de compte rendu définissent comment les vérifications de l'application, en accord avec le standard OWASP ASVS, doivent générer une documentation.

OWASP procure de nombreuses ressources, incluant ASVS, pour aider les organisations à développer et maintenir des applications sécurisées. Le standard OWASP ASVS, d'aide à la négociation de contrats (OWASP Contract Annex⁴), et OWASP ESAPI⁵, peuvent être utilisés pour améliorer votre cycle de vie de développement logiciel (Software Development Life Cycle SDLC), comme décrit dans la figure ci-dessous.

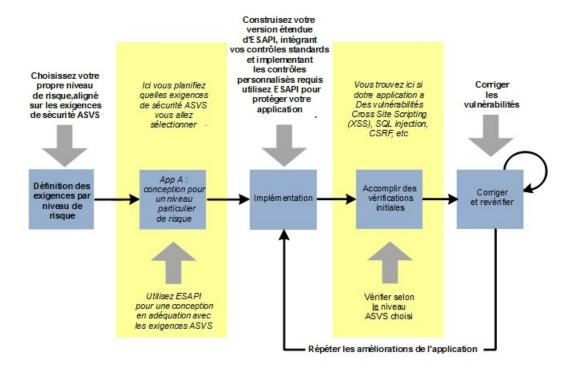


Figure 2 - Introduire la vérification dans votre cycle de développement (SDLC)⁶

⁴ Pour plus d'informations à propos des niveaux ASVS dans les contrats, voir *OWASP Contract Annex*.

⁵ Pour plus d'informations sur la manière de rendre ESAPI compatible avec votre application, voir OWASP *ESAPI* project (OWASP 2009).

⁶ Pour plus d'informations sur la manière d'introduire la sécurité dans votre cycle de vie de developpement logiciel, voir *OWASP CLASP* (OWASP 2008) ou *OWASP SAMM* Projects (OWASP 2009).



Remerciements

Nous remercions la fondation OWASP pour soutenir le OWASP Application Security Verification Standard Project durant le OWASP Summer of Code 2008.

Directeur de projet: ⁷ Mike Boberski (Booz Allen Hamilton)

Auteurs: 8 Mike Boberski (Booz Allen Hamilton), Jeff Williams

(Aspect Security), Dave Wichers (Aspect Security)

Traduction: Olivier Roquigny

Relecture: Jean-Philippe Teissier

Sponsors du

projet:





Booz | Allen | Hamilton

Nous remercions pour leur contributions: Pierre Parrend, relecteur du OWASP Summer of Code 2008; Andrew van der Stock (Aspect Security); Nam Nguyen (Blue Moon Consulting); John Martin (Boeing); Gaurang Shah (Booz Allen Hamilton); Theodore Winograd (Booz Allen Hamilton); Stan Wisseman (Booz Allen Hamilton); Barry Boyd (CGI Federal); Steve Coyle (CGI Federal); Paul Douthit (CGI Federal); Ken Huang (CGI Federal); Dave Hausladen (CGI Federal); Mandeep Khera (Cenzic); Scott Matsumoto (Cigital); John Steven (Cigital); Stephen de Vries (Corsaire); Dan Cornell (Denim Group); Shouvik Bardhan (Electrosoft), Dr. Sarbari Gupta (Electrosoft); Eoin Keary (Ernst & Young); Richard Campbell (Federal Deposit Insurance Corporation); Matt Presson (FedEx); Jeff LoSapio (Fortify Software); Liz Fong (National Institute of Standards and Technology); George Lawless (Noblis); Dave van Stein (ps_testware); Terrie Diaz (SAIC); Ketan Dilipkumar Vyas (Tata Consultancy Services); Bedirhan Urgun (TURKCELL); Dr. Thomas Braun (United Nations); Colin Watson (Watson Hall); Jeremiah Grossman (WhiteHat Security); et finalement, nous remercions la communauté vérifiant la sécurité des applications et ceux qui sont intéressés par une informatique internet de confiance pour leur conseils enthousiastes et leur assistance à travers cet effort.

⁷ Email: mike.boberski@owasp.org

⁸ Email: jeff.williams@owasp.org, dave.wichers@owasp.org



Niveaux de vérification de la sécurité des applications

Le standard ASVS définit quatre niveaux de vérification qui augmentent en largeur et en profondeur lorsque l'on monte la hiérarchie des niveaux. La largeur est définie dans chaque niveau par un ensemble d'exigences de sécurité qui doivent être appliquées. La profondeur de vérification est définie par l'approche et le niveau de rigueur requis dans la vérification de chaque exigence de sécurité. Les outils sont une part importante de chaque niveau ASVS. Dans les niveaux les plus hauts de ASVS, l'utilisation des outils est vivement encouragée. Mais pour être efficaces, les outils doivent être rigoureusement adaptés et configurés pour l'application et les framework utilisés. A chaque niveau, les résultats des outils doivent être vérifiés manuellement.

Il est de la responsabilité du vérificateur de déterminer si la cible de vérification (TOV) répond à toutes les exigences du niveau ciblé par la revue. Si l'application remplit toutes les exigences pour ce niveau, alors elle peut être considérée comme une application du niveau N OWASP ASVS, ou N est le niveau de vérification avec lequel l'application est compatible. Si l'application ne répond pas à toutes les exigences d'un niveau, mais répond à toutes les exigences d'un niveau inférieur de ce standard, on peut alors considérer qu'elle est compatible avec le niveau inférieur de vérification. Ce standard utilise le terme vérificateur pour désigner la personne ou l'équipe chargée de vérifier la compatibilité de l'application avec les exigences du standard OWASP ASVS.

Les spécifications pour une application peut requérir le niveau N OWASP ASVS, mais il peut aussi inclure des exigences additionnelles au détail, dépendant d'un niveau ASVS supérieur. Par exemple, une organisation de finance pourrait avoir une application vérifiée pour les risques de niveau 2 OWASP ASVS, mais pourrait aussi vouloir vérifier qu'aucun code malicieux n'ai pu être inclus(voir V13, niveau 4). D'autres organisations ou entreprises, peuvent appliquer un règlement ou une politique de sécurité particulière.

Il n'y a pas de niveau 0 de vérification. Pour accéder à un niveau, les vulnérabilités doivent être réparées (ou atténuées), et l'application doit être revérifiée.

Niveau 1 - Vérification automatique

Le Niveau 1 ("Vérification automatique") est généralement approprié pour des applications où un usage convenable des contrôles de sécurité est requis. Les menaces de sécurité seront généralement des virus, vers, (les cibles sont choisies au hasard à travers de larges scan, et impactent les plus vulnérables). La portée des vérifications inclues le code qui a été développé ou modifié durant la création de l'application.

Dans le niveau 1, la vérification implique l'utilisation d'outils automatisés ainsi que des vérifications manuelles. Ce niveau assure seulement une protection de sécurité partielle de l'application. La vérification manuelle n'est pas prévue pour rendre la sécurité de l'application complète, seulement pour vérifier que chaque découverte automatique est correcte et pas simplement une fausse alerte (false positive).

Il y a deux éléments constituants le niveau 1. Le niveau 1A utilise des outils pour scanner automatiquement les vulnérabilités de l'application (analyse dynamique), et le niveau 1B utilise des outils pour scanner automatiquement le code source (analyse statique). Les efforts de vérification peuvent utiliser chacun de ces composants individuellement, ou utiliser une combinaison de ces approches pour obtenir le niveau 1 complet. La structure de ces niveaux est décrite dans la figure ci-dessous.

⁹ Pour plus d'informations sur l'identification et l'estimation des risques associés aux vulnérabilités, voir le OWASP *Testing Guide* (OWASP 2008)



Tandis qu'il peut déterminer qu'une application accède au niveau 1A ou 1B, aucun de ces niveaux pris séparément ne procure le même niveau de rigueur et de protection qu'une application qui accède au niveau 1. Une application qui est de niveau 1, doit être de niveaux d'exigences 1A et 1B.

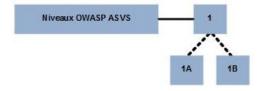


Figure 3 - OWASP ASVS Niveaux 1, 1A, et 1B

Vous trouverez ci-dessous les exigences minimales requise pour les niveaux 1, 1A, et 1B:

Portée de vérification

L1.1 La portée de vérification inclue tous les codes qui ont été créés ou modifiés pour la création de l'application.

Exigences de contrôle de sécurité des comportements

Aucun Il n'y a pas d'exigence particulière des contrôles de sécurité en rapport avec les décisions prises par les applications au niveau 1.

Exigence d'utilisation des contrôles de sécurité

Aucun Il n'y a pas d'exigence particulière en rapport avec le lieu ou les contrôles de sécurité sont utilisés dans l'application au niveau 1.

Exigences d'implémentation des contrôles de sécurité

Aucun Il n'y a pas d'exigence particulière pour la construction des contrôles de sécurité des applications au niveau 1.

Exigences de vérification des contrôles de sécurité

- L1.2 Scanner dynamiquement l'application en accord avec les exigences de niveau 1A, exposées dans la section « Exigences de vérification détaillées ».
- L1.3 Scanner le code source de l'application, en respectant les exigences du niveau 1B, exposées dans la section « Exigences de vérification détaillées ».

Les exigences de niveau 1 qui permettent l'une ou l'autre des vérifications techniques, doivent seulement être vérifiées par cette technique. De plus, si la suite d'outils de vérification sélectionnée n'a pas l'aptitude à vérifier une exigence de vérification spécifique, le vérificateur peut exécuter des vérifications manuelles pour combler cette lacune. 10 11

¹⁰ Pour plus d'informations à propos de vérifications manuelles dans le cadre de tests de pénétration manuels, voir le *OWASP Testing Guide* (OWASP, 2008).

¹¹ Pour plus d'informations à propos de vérifications manuelles dans le cadre de revues de code manuelles, voir le *OWASP Code Review Guide* (OWASP, 2008).



Exigences de rapport (reporting)

L1.4 Créer un rapport de vérification détaillant l'architecture de sécurité de l'application qui liste ses composants, et inclut les résultats des vérifications, dans le respect des exigences de la section « Exigences de rapport de vérification ».

Au niveau 1, les composants d'applications peuvent être vus comme des fichiers sources individuels, ou comme groupes de fichiers sources, bibliothèques, et/ou exécutables, comme décrit dans la figure ci-dessous. Au niveau 1, la liste n'a pas besoin d'être organisée autrement qu'en identifiant clairement les composants de l'application des composants de l'environnement informatique. L'application peut ainsi être perçue comme un groupe de composants plutôt que comme une seule entité monolithique. Le chemin qu'une requête d'utilisateur final peut prendre à travers l'application n'a pas besoin d'être identifiée ni documentée.

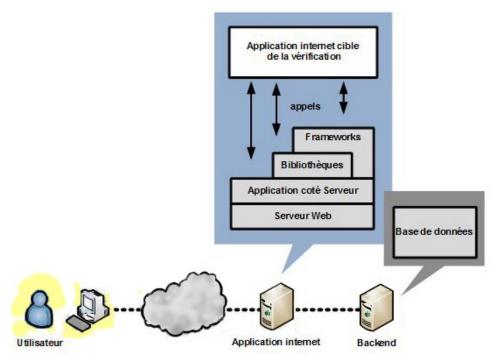


Figure 4 - Exemple d'architecture de sécurité de niveau 1 OWASP ASVS

Niveau 1A - Scans Dynamiques (Vérification automatique partielle)

Exigences de vérification de contrôles de sécurité par scans dynamiques

Les scans dynamiques, aussi connus comme « scan de vulnérabilités d'applications », consistent à utiliser des outils automatisés pour accéder aux interfaces d'applications pendant que l'application fonctionne, de sorte à découvrir des vulnérabilités dans les contrôles de sécurité. Il convient de noter que cela ne suffit pas pour déclarer une conception comme correcte, mais que c'est une vérification acceptable au niveau 1. La portée de vérification est définie par ces niveaux d'exigences d'architecture de sécurité.

- L1A.1 Scanner dynamiquement l'application en accord avec les exigences du niveau 1A, spécifiées dans la section « Exigences de vérification détaillées ».
- L1A.2 Vérifier les résultats de scan dynamiques utilisés dans les tests manuels de pénétration des applications et dans les revues de code. Les résultats automatiques non-vérifiés ne sont



pas considérés comme apportant une quelconque assurance, et ne sont pas suffisants pour qualifier une application au niveau 1 ASVS.

Plusieurs cas d'un type particulier de vulnérabilité, pouvant être répertoriées comme ayant la même origine, devraient être rassemblées dans une même alerte, dans le cas ou cela n'aurait pas déjà été fait par les outils de scan.

Niveau 1B - Scans de code source (Vérification automatique partielle)

Exigences de vérification des contrôles de sécurité des scans de code source

Le scan de code source, ou « analyse statique », consiste à utiliser des outils automatisés, pour chercher au travers du code source de l'application des motifs (patterns) qui représentent des vulnérabilités. Il est à noter que ce n'est pas suffisant pour vérifier que la conception, l'implémentation et l'utilisation des contrôles de sécurité soient véritablement efficaces, mais ces vérifications sont acceptables au niveau 1. La portée des vérifications est définie par les exigences de sécurité de la conception à ce niveau.

- L1B.1 Scanner le code source de l'application dans le respect des exigences du niveau 1B spécifié dans la section « Exigences de vérification détaillées ».
- L1B.2 Vérifier les résultats de scan de code source utilisant les tests manuels de pénétration d'application ou la revue de code. Les résultats automatisés non vérifiés ne sont pas censé apporter une quelconque assurance et ne sont pas suffisants pour qualifier une application pour le niveau 1 ASVS.

Plusieurs cas d'un type particulier de vulnérabilité, pouvant être répertoriés comme ayant la même origine, devraient être rassemblés dans une même alerte, dans le cas où cela n'aurait pas déjà été fait par les outils d'analyse de code.

Niveau 2 - Vérification manuelle

Le niveau 2 (« Vérification manuelle ») est approprié pour des applications qui gèrent des transactions personnelles, des transactions B2B (business to business), des informations de cartes de crédit, ou des informations personnelles. Le niveau 2 procure une assurance que les vérifications des contrôles de sécurité se font conformément aux spécifications et qu'ils fonctionnent correctement. Les menaces seront les virus, vers et des opportunistes simple qui utilisent des outils d'attaque préconçus. L'étendue des vérifications inclut tous les codes développés ou modifiés pour l'application, aussi bien que l'examen des tierces parties qui procure des fonctionnalités de sécurité à l'application. Il y a deux composants pour le niveau 2, comme décrit sur la figure ci-dessous.

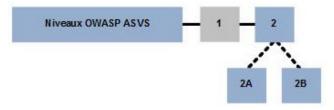


Figure 5 - Niveaux OWASP ASVS 2, 2A, et 2B

Si une application peut accéder au niveau 2A ou 2B, aucun de ces niveaux seul n'apporte la même rigueur ni le même niveau de protection que le niveau 2. D'autre part, alors que le niveau 2 englobe le niveau 1, il n'y a pas d'exigences d'utilisation d'outils automatisés pour accéder au niveau 2. Au



lieu de cela, le vérificateur a l'option d'utiliser seulement des techniques manuelles pour répondre aux exigences du niveau 2. Si des outils automatisés sont disponibles, le vérificateur peut les utiliser pour appuyer son analyse. Cependant, répondre à une exigence de niveau 1, ne signifie pas systématiquement que l'on répond à la même exigence de niveau 2, et ce parce que les outils automatiques n'apportent pas de preuves suffisamment solides, pour affirmer que l'exigence de niveau 2 a été satisfaite.

Les techniques manuelles sont supposées utiliser des outils. Cela peut inclure l'utilisation de toutes sortes d'analyses de sécurité ou d'outils de test, incluant les outils automatisés utilisés au niveau 1. Cependant, ces outils sont de simples aides à l'analyse, pour trouver et estimer si les contrôles de sécurité ont été vérifiés. De tels outils peuvent ou non exploiter une logique pour détecter les vulnérabilités des applications.

Ci-dessous les exigences de haut-niveau minimum pour les applications de niveau 2, 2A, ou 2B :

Étendue de la vérification

- L'étendue des vérifications inclut tout le code qui a été développé ou modifié pour créer l'application. Cette exigence est introduite au niveau 1.
- L'étendue des vérifications inclut le code de tous les frameworks, bibliothèques, tierces parties et fonctionnalités de sécurité des services qui sont appelés ou qui supportent la sécurité de l'application. C'est une nouvelle exigence du niveau 2.

Exigences de comportement des contrôles de sécurité

- L2.3 Vérifier que tous les contrôles de sécurité utilisent une approche de type « liste blanche ». C'est une nouvelle exigence au niveau 2.
- L2.4 Vérifier que l'examen des résultats des contrôles de sécurité et leurs répercussions ne puissent être contournés, en accord avec les niveaux d'exigences 2A et 2B spécifiés dans la section « Exigences de vérification détaillées ». C'est une nouvelle exigence au niveau 2.

Exigences d'utilisation des contrôles de sécurité

L2.5 Vérifier que les contrôles de sécurité sont utilisés partout où il y a lieu dans l'application, et que les implémentations sont concentrées du coté serveur, comme spécifié par les exigences de niveau 2 dans la section « Exigences de vérification détaillées ». C'est une nouvelle exigence du niveau 2.

Exigences d'implémentation des contrôles de sécurité

Aucun Il n'y a pas d'exigences quant à la conception des contrôles de sécurité de l'application au niveau 2.

Exigences de vérification des contrôles de sécurité

- L2.6 Exécuter des tests de pénétration sur l'application, conformément aux exigences de niveau 2A spécifiées dans la section « Exigences de vérification détaillée ». C'est une nouvelle exigence du niveau 2.
- L2.7 Exécuter une revue de code source manuelle sur l'application, conformément aux exigences du niveau 2B, spécifiées dans la section « Exigences de vérification détaillée ». C'est une nouvelle exigence au niveau 2.

Les exigences de niveau 2 qui permettent l'utilisation de différentes techniques de vérification, doivent seulement être vérifiées par une de ces techniques.



Le vérificateur devrait considérer les scans automatiques ou l'analyse de code comme partie de l'effort de vérification du niveau 2, mais les vérifications automatiques ne peuvent être utilisées en lieu et place des revues manuelles requises pour chaque exigence du niveau 2. Si les résultats de scans aident le vérificateur à travailler plus rapidement, ou à augmenter les résultats de la partie manuelle de la revue, ils peuvent être utilisés pour assister l'éxecution des vérifications de niveau 2.

Exigences de rapport (reporting)

L2.8 Créer un rapport de vérification qui décrit l'architecture de sécurité de l'application en groupant ses composants dans une architecture de haut niveau, et en incluant les résultats de la vérification conformément aux exigences de la section « Exigences de rapports de vérification ». Cela augmente les exigences de rapport introduits au niveau 1.

Au niveau 2, les composants des applications peuvent être définis en tant que fichiers sources individuels ou groupes, bibliothèques, et/ou fichiers exécutables organisés dans une architecture de haut niveau (par exemple composants Modèle-Vue-Contrôleur (MVC), composants de fonctionnalités métier, et composants de couches de données). Par exemple, le diagramme ci-dessous représente une application constituée d'un serveur d'applications, du code personnalisé, des bibliothèques, et une application de base de données, qui sont regroupés conformément à une architecture MVC. Au niveau 2, le chemin ou les chemins qu'une requête d'utilisateur peut prendre à travers l'application doit être documenté, comme décrit dans la figure ci-dessous. Cependant, tous les chemins peuvent ne pas être examinés.

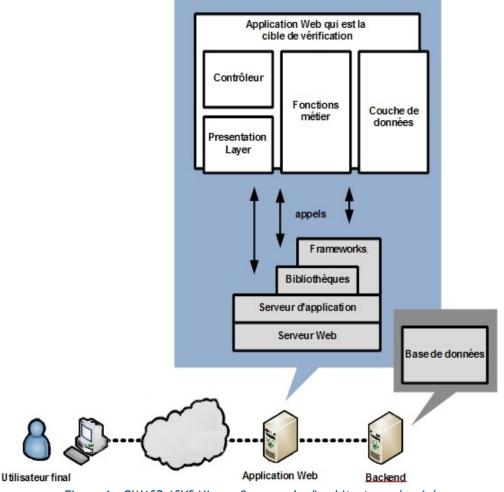


Figure 6 - OWASP ASVS Niveau 2, exemple d'architecture sécurisé



Niveau 2A - Tests de sécurité (Vérification manuelle partielle)

Exigences de vérification des contrôles de test de pénétration manuel des applications

Les tests de sécurité manuels des applications consistent à créer des tests dynamiques, pour vérifier la qualité de conception, l'implémentation, et l'utilisation des contrôles de sécurité d'une application. L'étendue de la vérification est définie par son niveau d'exigence de sécurité.

L2A.1 Exécuter des tests de sécurité manuels sur l'application, conformément aux exigences de niveau 2A spécifiées dans la section « Exigences de vérification détaillées ». C'est une nouvelle exigence au niveau 2.

Lorsque c'est approprié, le vérificateur peut utiliser l'échantillonnage (sampling) pour établir l'usage effectif d'un contrôle de sécurité. Le vérificateur peut documenter un type de vulnérabilité (pattern), ce qui permettra aux développeurs de retrouver et de réparer toutes les instances de ce type de vulnérabilité (pattern) dans la base logicielle. Plusieurs instances d'un type de vulnérabilité (pattern) qui peuvent être définis comme provenant d'une même source, devraient être combinées dans une même découverte.

Niveau 2B - Revue de code (Vérification manuelle partielle)

Exigences de vérification des contrôles de sécurité de revue de code manuelle

Les revues de code manuelles consistent à des recherches humaines et à l'analyse du code source de l'application afin de vérifier le design de l'application, son implémentation, et l'utilisation correcte des contrôles de sécurité. Une telle analyse est censé être assistée par des outils, Mais peut simplement associer des outils communs comme un éditeur de texte. L'étendue des vérifications est définie par les exigences de sécurité de ce niveau.

L2B.1 Exécuter une revue de code manuelle sur l'application conformément aux exigences du niveau 2B spécifié dans la section « Exigences de vérification détaillées ». C'est une nouvelle exigence au niveau 2.

Lorsque c'est approprié, le vérificateur peut utiliser l'échantillonnage (sampling) pour établir l'usage effectif d'un contrôle de sécurité. Le vérificateur peut documenter un type de vulnérabilité (pattern), ce qui permettra aux développeurs de retrouver et de réparer toutes les instances de ce type de vulnérabilité (pattern) dans la base logicielle. Plusieurs instances d'un type de vulnérabilité (pattern) qui peuvent être définis comme provenant d'une même source, devraient être combiné dans une même découverte.

Niveau 3 - Vérification de la conception

Le niveau 3 (« Vérification de la conception ») est approprié pour les applications qui manipulent des transactions significatives entre entreprises (business-to-business), incluant celles qui traitent des informations de santé, implémentent des des fonctions sensibles ou critiques, ou traitent d'autres types d'actifs sensibles. Les menaces sont typiquement des virus et vers, des attaquants opportunistes, ainsi que des attaquants déterminés (attaquants habiles et motivés, concentrés sur des cibles précises, utilisant des outils incluant ceux conçus spécialement pour le scan). L'étendue des vérifications inclut tout le code développé ou modifié pour l'application, aussi bien que l'examen de la sécurité de tous les composants extérieurs qui apportent à l'application des fonctionnalités de sécurité. Le niveau 3 s'assure que les contrôles de sécurité fonctionnent correctement et que ces contrôles soient utilisés dans chaque partie de l'application où ils doivent être appliqués pour faire



respecter la politique de sécurité de l'application. Le niveau 3 n'est pas fractionné en multiples composants, comme décrit dans la figure ci-dessous :



Figure 7 - Niveau 3 OWASP ASVS

Vous trouverez ci dessous les exigences minimales pour qu'une application accède au niveau 3 :

Étendue de la vérification

- L'étendue de la vérification comprend tout le code qui a été développé ou modifié afin de créer l'application. Cette exigence a été introduite au niveau 1.
- L'étendue de la vérification comprend tout le code des frameworks extérieurs, bibliothèques, et services de fonctionnalités sécurité qui sont invoqués par ou qui supportent la sécurité de l'application. Cette exigence a été introduite au niveau 2.
- L3.3 L'étendue de la vérification comprend tout le code des frameworks extérieurs, bibliothèques, et services associés à l'application. C'est une nouvelle exigence au niveau 3

Exigences de comportement des contrôles de sécurité

- L3.4 Vérifier que tous les contrôles de sécurité qui exécutent des examens de sécurité utilisent l'approche des listes blanches. Cet exigence a été introduite au niveau 2.
- L3.5 Vérifier que tous les contrôles de sécurité qui exécutent des examens de sécurité et des contrôles de sécurité ne puissent être contournés conformément au exigences du niveau 3 spécifiées dans la section « Exigences de vérification détaillées ». Cette exigence a été introduite au niveau 2.

Exigences d'utilisation des contrôles de sécurité

L3.6 Vérifier que tous les contrôles de sécurité soient utilisés partout ou c'est nécessaire au travers de l'application, et que leur implémentation est centralisée sur le serveur, conformément aux exigences du niveau 3 spécifiées dans la section « Exigences de vérification détaillées ». Cette Exigence a été introduite au niveau 2.

Exigences d'implémentation des contrôles de sécurité

Aucun Il n'y a pas d'exigences quand à la manière dont les contrôles de sécurité sont construits au niveau 3.

Exigences de vérification des contrôles de sécurité

- L3.7 Vérifier manuellement l'application conformément aux exigences de niveau 3 spécifiées dans la section « Exigences de vérification détaillées ». Cela accroit les exigences de vérification manuelles introduites au niveau 2.
- L3.8 Documenter l'architecture de sécurité et utiliser cette documentation pour vérifier que la conception correcte, et utiliser tous les contrôles de sécurité pour exécuter une modélisation des menaces. C'est une nouvelle exigence au niveau 3.



Exigences de rapports (Reporting)

L3.9 Créer un rapport de vérification qui décrit l'architecture de sécurité de l'application en groupant ses composants dans une architecture de haut niveau qui inclut les informations de modélisation des menaces, ainsi que les résultats de vérification conformément aux exigences de la section « Exigences de rapport de vérification (Reporting) ». Cela accroit les exigences de rapport (reporting) du niveau 2.

Au niveau 3, les composants d'application peuvent être définis soit en tant que fichier source individuel, soit en tant que groupe de fichiers sources, bibliothèques, et/ou fichiers exécutables qui sont groupés dans une architecture de haut niveau (par exemple composants MVC, composants de fonctions business, et composants de couches de données). Au niveau 3, les informations de modélisation d'agents et d'actifs de menaces doivent être fournies en plus. Le ou les chemins qu'une requête d'utilisateur doit prendre à travers une interface utilisateur doit être documentée, comme décrit dans la figure ci-dessous. Au niveau 3, *tous* les chemins potentiels à travers l'interface utilisateur de l'application doivent être examinés.

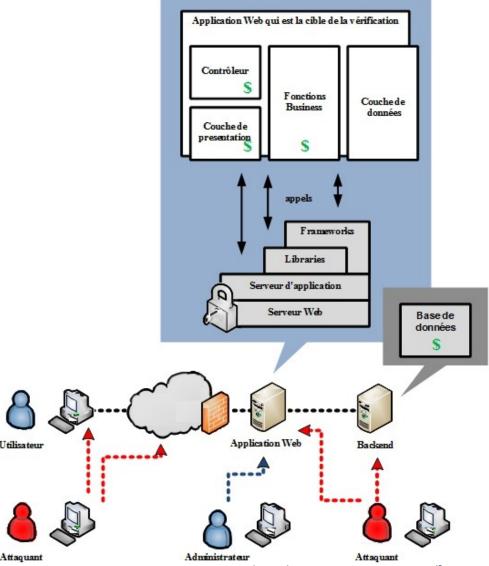


Figure 8 - Exemple d'architecture de sécurité de niveau 3 OWASP ASVS¹²

¹² Le Signe dollar indique les actifs dans le diagramme.



Niveau 4 - Vérification interne

Le Niveau 4 (« Vérifications internes ») est approprié pour les applications critiques qui doivent protéger la vie et la sécurité, des infrastructures critiques, ou des fonctions de défense. Le niveau 4 peut aussi convenir pour des applications qui manipulent des données sensibles. Le niveau 4 s'assure que les contrôles de sécurité fonctionnent correctement, que les contrôles de sécurité sont employés partout où la politique de sécurité de l'application le juge nécessaire, et que des pratiques de développement sécurisées sont employées. Les menaces sont caractérisées par des attaquants déterminés (attaquants habiles et motivés, concentrés sur des cibles précises et utilisant des outils spécialement conçus pour le scan). L'étendue des vérifications étend les compétences du niveau 3 pour inclure tous le code utilisé par l'application. Le niveau 4 n'est pas fractionné en multiples composants, comme décrit dans la figure ci-dessous :



Figure 9 - Niveau 4 OWASP ASVS

Vous trouverez ci dessous les exigences minimales pour qu'une application accède au niveau 4 :

Étendue de la vérification

- L'étendue de la vérification inclut tous le code développé ou modifié pour créer l'application. Cette exigence est introduit au niveau 1.
- L'étendue de la vérification inclut le code de tous les frameworks, bibliothèques de fonctions, et fonctionnalités de services sécurisés utilisés par ou procurant la sécurité de l'application. Cette exigence est introduite au niveau 2.
- L'étendue de la vérification inclut le code de tous les frameworks, bibliothèques de fonctions, et services associés à l'application. Cette exigence est introduite au niveau 3.
- L4.4 L'étendue de la vérification inclut tous le code associé à l'application, incluant les frameworks, bibliothèques de fonctions, environnement d'exécution, outils de développement, outils de compilation, ainsi que les outils de déploiement. L'étendue n'inclut pas le code de logiciel de plateforme, tel que serveur d'application, serveur de base de données, machine virtuelle, ou système d'exploitation, qui a été confronté à un important examen public. C'est une nouvelle exigence au niveau 4.

Exigence de comportement des contrôles de sécurité

- L4.5 Vérifier que tous les contrôles de sécurité qui exécutent des examens de sécurité utilisent une approche positive de listes blanches. Cette exigence est introduite au niveau 2.
- L4.6 Vérifier que tous les contrôles de sécurité qui exécutent des examens de sécurité ne peuvent être contournés conformément au exigences du niveau 4 spécifiées dans la section « Exigences de vérification détaillées ». Cette exigence a été introduite au niveau 2.

Exigence d'utilisation des contrôles de sécurité

L4.7 Vérifier que tous les contrôles de sécurité sont utilisés partout ou cela est nécessaire au travers de l'application, et que leur implémentation est centralisée sur le serveur, conformément aux exigences du niveau 4 spécifiées dans la section « Exigences de vérification détaillées ». Cette Exigence a été introduite au niveau 3.



Exigence d'implémentation des contrôles de sécurité

L4.8 Vérifier que l'application ne contient pas de code malicieux conformément aux exigences de niveau 4 spécifiées à la section « Exigences de vérification détaillées » C'est une nouvelle exigence au niveau 4.

Exigences de vérification des contrôles de sécurité

- L4.9 Vérifier manuellement l'application conformément aux exigences de niveau 4 spécifiées dans la section « Exigences de vérification détaillées ». Cela augmente les exigences de niveau 3
- L4.10 Documenter l'architecture de sécurité et l'utiliser pour vérifier la conformité de conception et l'utilisation de tous les contrôles de sécurité en exécutant des modélisations de menaces. Cette exigence est introduite au niveau 3.
- L4.11 Revoir manuellement tous le code développé ou modifié pour cette application pour le code malicieux¹³ conformément aux exigences de niveau 4 spécifiées dans la section « Exigences de vérification détaillées ». C'est une nouvelle exigence au niveau 4.

Exigences de rapport (Reporting)

L4.12 Créer un rapport de vérification qui décrit l'architecture de sécurité de l'application conformément aux exigences de niveau 3, qui englobe tous le code de l'application, et inclut les résultats des vérifications conformément aux exigences de la section « Exigences de rapports de vérification (reporting) » Cela augmente les exigences de rapports du niveau 3.

Au niveau 4, l'architecture de l'application devrait être examinée comme requis au niveau 3. Plus encore le niveau 4 exige que tout le code de l'application, incluant le code non explicitement examiné, soit identifié comme faisant partie de la définition de l'application, comme décrit dans la figure ci-dessous. Ce code doit inclure toutes les bibliothèques de fonctions, frameworks, ainsi que le code dont l'application dépend. Les vérifications précédentes de ces composants peuvent être réutilisées comme part d'un autre effort de vérification. Le code de la plateforme, comme celui du système d'exploitation, de la machine virtuelle, ou d'un noyau de bibliothèques de fonctions distribuées avec un environnement de machine virtuelle, serveur web, ou serveur d'applications ne sont pas concernés par le niveau 4. Par exemple les bibliothèques associées avec l'environnement d'exécution Java n'ont pas besoin d'être contrôlées au niveau 4.

¹³ Le code malicieux est différent d'un malware. Voir la définition du glossaire de code malicieux.





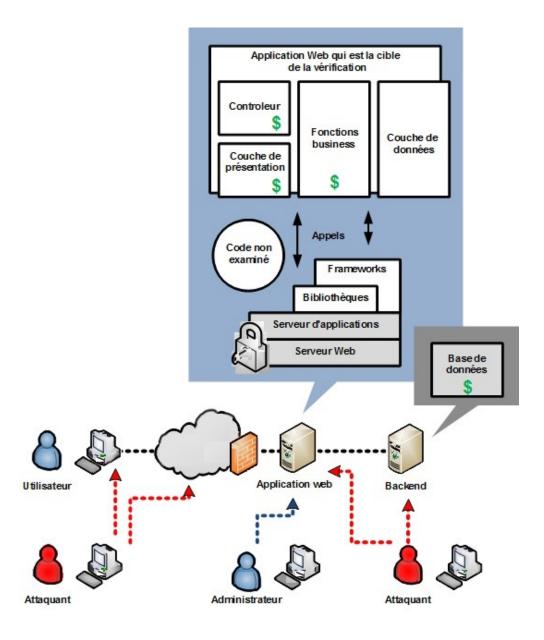


Figure 10 - Exemple de code non examiné niveau 4 OWASP ASVS

Interprétations et précédents d'exigences

Le standard OWASP ASVS est un document vivant. Si vous exécutez une vérification de sécurité d'application conformément à ce standard, alors vous devriez toujours revoir les articles qui peuvent être trouvés sur la page du projet OWASP ASVS qui se trouve à cette adresse : http://www.owasp.org/index.php/ASVS#Articles Below - More About ASVS and Using It . Les articles sur les pages du projet OWASP ASVS, apportent des clarifications des exigences, des verdicts d'ajouts d'exigences, ainsi que des conseils utiles.



Exigences de vérification détaillées

Cette section du standard OWASP Application Security Verification Standard (ASVS) définit les exigences de vérification détaillées qui sont dérivées des exigences de haut niveau pour chacun des niveaux définis dans ce standard. Chaque section ci-dessous définit un ensemble d'exigences de vérification détaillées groupées dans des zones apparentées.

Le standard ASVS définit les zones d'exigences de sécurité suivantes :

- V1. Architecture de sécurité
- V2. Authentification
- V3. Gestion de Sessions
- V4. Contrôle d'accès
- V5. Validations d'entrées
- V6. Encodage et échappement de sorties
- V7. Cryptographie
- V8. Gestion des erreurs et de la journalisation
- V9. Protection des données
- V10. Sécurité des communications
- V11. HTTP Sécurisé
- V12. Configuration de la sécurité
- V13. Recherche de codes malicieux
- V14. Sécurité interne

Pour chacune de ces zones, les exigences qui doivent être atteintes à chaque niveau de vérification spécifié, sont listées ci-dessous :

Niveau 1: Vérifications automatisées

Niveau 1A - Scans dynamiques (Vérification automatique partielle) Niveau 1B - Scans de code source (Vérification automatique partielle)

Niveau 2: Vérification manuelle

Niveau 2A - Test de sécurité (Vérification automatique partielle) Niveau 2B - Revue de code (Vérification automatique partielle)

Niveau 3: Vérification de la conception

Niveau 4: Vérification interne



V1 - Exigences de documentation de l'architecture de sécurité

Pour tous les niveaux ASVS, il est nécessaire de documenter les bases de l'architecture de sécurité, pour s'assurer de la totalité et de la précision (et de la reproductibilité lorsque des corrections sont nécessaires) des vérifications de sécurité exécutées. L'analyse peut être dirigée et les résultats pris en compte dans l'architecture de sécurité de haut niveau de l'application. Ces exigences commencent avec un niveau basique de détail de l'architecture de sécurité qui doit être atteint, et ce niveau de détail s'accroit avec chaque niveau. Le tableau ci-dessous définit les exigences de documentation de l'architecture de sécurité correspondantes s'appliquant aux quatre niveaux de vérification.

Tableau 1 - Exigences d'architecture de sécurité OWASP ASVS (V1)

	Exigence de vérification	Niveau 1A	Niveau 1B	Niveau 2A	Niveau 2B	Niveau 3	Niveau 4
V1.1	Vérifier que tous les composants de l'application sont identifiés (aussi bien les composants individuels que les groupes de fichiers sources, bibliothèques de fonctions, et/ou fichiers exécutables.	√	√	✓	√	✓	√
V1.2	Vérifier que tous les composants qui ne font pas partie de l'application, mais dont l'application dépend pour fonctionner, soient correctement identifiés.			✓	✓	✓	✓
V1.3	Vérifier qu'une architecture de haut niveau a bien été définie pour l'application ¹⁴			✓	✓	✓	✓
V1.4	Vérifier que tous les composants de l'application sont définis en termes de fonctions e-commerce et/ou de fonctions de sécurité qu'ils apportent.					✓	✓
V1.5	Vérifier que tous les composants qui ne font pas partie de l'application mais dont l'application dépend pour fonctionner, soient correctement définis en termes de fonctions e- commerce et/ou de fonctions de sécurité qu'ils apportent.					✓	√
V1.6	Vérifier que des informations de modélisation de menaces ont bien été apportées.					✓	✓

¹⁴ Le vérificateur peut créer ou documenter la conception de haut niveau si le développeur de l'application n'en a pas fournit.



V2 - Exigences de vérification d'authentification

Les exigences de vérification d'authentification définissent un ensemble d'exigences pour générer et gérer les jetons d'authentification utilisateur de manière sûre. Le tableau ci-dessous définit les exigences de vérification correspondantes de chacun des quatre niveaux de vérification.

Tableau 2 - Exigences d'authentification OWASP ASVS (V2)

	Exigence de vérification	Niveau 1A	Niveau 1B	Niveau 2A	Niveau 2B	Niveau 3	Niveau 4
V2.1	Vérifier que toutes les pages et ressources exigent bien une authentification excepté celles qui sont spécialement prévues pour être public.	✓	✓	✓	✓	✓	✓
V2.2	Vérifier que tous les champs de mot de passe n'affichent pas le mot de passe lorsqu'il est entré, et que l'auto-complétion est bien désactivée sur ces champs.	✓	✓	✓	✓	✓	√
V2.3	Vérifier que si un nombre maximum de tentatives d'authentification est atteint, le compte utilisateur est bloqué pendant un temps assez long pour dissuader une attaque par force brute.	√		✓	✓	✓	✓
V2.4	Vérifier que tous les contrôles d'authentification sont effectués du coté serveur.			✓	✓	✓	✓
V2.5	Vérifier que tous les contrôles d'authentification ont une implémentation centralisée (les contrôles incluent les bibliothèques qui font appel des services d'authentification externes).				√	√	✓
V2.6	Vérifier que tous les contrôles d'authentification échouent de manière sûre.			✓	✓	✓	✓
V2.7	Vérifier que la solidité de chaque jeton d'authentification est suffisante pour résister aux attaques et menaces typiques de l'environnement déployé.			✓	✓	✓	✓
V2.8	Vérifier que toutes les fonctions de gestion des comptes soient au moins aussi résistantes aux attaques que le principal mécanisme d'authentification.			✓	✓	✓	✓



V2.9	Vérifier que les utilisateurs peuvent changer en toute sécurité leur jeton d'authentification, en utilisant un mécanisme qui soit au moins aussi résistant au attaques que le principal mécanisme d'authentification.		√	✓	✓	✓
V2.10	Vérifier qu'une ré-authentification est exigée avant de permettre toute opération sensible.		✓	✓	✓	✓
V2.11	Vérifier que le jeton expire après une période donnée et configurable.		✓	✓	✓	✓
V2.12	Vérifier que toutes les authentifications soient journalisées.			✓	✓	✓
V2.13	Vérifier que les mots de passe des comptes contiennent un grain de sel qui soit unique au compte auquel il est rapporté (par exemple ID utilisateur) et qu'il soit hashé avant d'être stocké.			√	√	✓
V2.14	Vérifier que tous les jetons d'authentification servant à accéder des services externes à l'application soient chiffrés et stockés dans un endroit protégé (pas dans le code source).			√	✓	✓
V2.15	Vérifier que tous le code implémentant ou utilisant des contrôles d'identification n'est pas affecté par un code malicieux.					✓

V3 - Exigences de vérification de gestion des sessions

Les exigences de vérification de gestion des sessions, définissent un ensemble d'exigences pour utiliser de manière sûre : requêtes HTTP, réponses, sessions, cookies, en-têtes (headers) et la journalisation de sorte à gérer les sessions correctement. Le tableau ci-dessous définit les exigences de vérification correspondantes s'appliquant aux quatre niveaux de vérification.

Tableau 3 - Exigences de gestion des sessions OWASP ASVS (V3)

	Exigence de vérification	Niveau 1A	Niveau 1B	Niveau 2A	Niveau 2B	Niveau 3	Niveau 4
V3.1	Vérifier que l'implémentation du contrôle de gestion des sessions par défaut du framework est utilisé par l'application.	✓		✓	✓	✓	✓
V3.2	Vérifier que la session est invalidée quand l'utilisateur se déconnecte.	✓		✓	✓	✓	✓
V3.3	Vérifier que la session est invalidée après une période d'inactivité donnée et configurable(timeout).	✓		✓	✓	✓	✓



V3.4	Vérifier que les sessions sont invalidées après un temps maximum configurable indépendant de l'activité (temps de timeout absolu).					✓	✓
V3.5	Vérifier que toutes les pages qui requièrent une authentification pour y accéder possèdent un lien de déconnexion.	✓		✓	✓	✓	✓
V3.6	Vérifier que l'id de session n'est jamais communiqué autrement que par l'entête de cookie; particulièrement dans les URLs, messages d'erreurs ou journalisation. Cela inclut de vérifier que l'application ne permet pas la réécriture d'URL pour les cookies de session.		✓		✓	✓	✓
V3.7	Vérifier que l'id de session est changé à la connexion.			✓	✓	✓	✓
V3.8	Vérifier que l'id de session est changé à la re-connexion.			✓	✓	✓	✓
V3.9	Vérifier que l'id de session est changé ou détruit à la déconnexion.			✓	✓	✓	✓
V3.10	Vérifier que seul les ids de session générés par l'application sont reconnus comme valides par l'application.			✓		✓	✓
V3.11	Vérifier que les jetons de session d'authentification soient suffisamment long et aléatoires pour résister aux menaces typiques de l'environnement déployée.					✓	✓
V3.12	Vérifier que les cookies qui contiennent les jetons/ids de session d'authentification ont leurs domaine et chemin définit sur une valeur suffisamment restrictive pour ce site.					✓	✓
V3.13	Vérifier que tout le code utilisant ou implémentant les contrôles de gestion de sessions n'est pas affecté par un code malicieux.						✓

V4 - Exigences de vérification des contrôles d'accès

Les exigences de vérification des contrôles d'accès, définissent comment une application peut renforcer les contrôles d'accès de sorte à les rendre sûrs. Dans la plupart des applications, les contrôles d'accès doivent être exécutés en de multiples points à travers les différentes couches de l'application. Ces exigences définissent les points requis de vérification de contrôles d'accès pour les URLs, les fonctionnalités commerciales, les données, les services ainsi que les fichiers. Le tableau ci-dessous définit les exigences de vérification correspondantes qui s'appliquent pour chacun des quatre niveaux de vérification.



Tableau 4 - Exigences de contrôles d'accès OWASP ASVS (V4)

	Exigences de vérification	Niveau 1A	Niveau 1B	Niveau 2A	Niveau 2B	Niveau 3	Niveau 4
V4.1	Vérifier que les utilisateurs ne puissent accéder qu'aux fonctionnalités protégées pour lesquelles ils ont des autorisations spécifiques.	√	✓	✓	✓	✓	√
V4.2	Vérifier que les utilisateurs ne puissent accéder qu'aux URLs pour lesquelles ils possèdent des autorisations spécifiques.	✓		✓	✓	✓	✓
V4.3	Vérifier que les utilisateurs ne puissent accéder qu'aux fichiers de données pour lesquels ils possèdent des autorisations spécifiques.	✓		✓	✓	✓	✓
V4.4	Vérifier que les références directes aux objets sont protégées, de telle sorte que seuls les objets autorisés soient accessibles à l'utilisateur.	✓		✓	✓	✓	✓
V4.5	Vérifier que la navigation dans les répertoires est désactivée lorsqu'elle n'est pas délibérément autorisée.	✓		✓		✓	✓
V4.6	Vérifier que les utilisateurs ne peuvent accéder qu'aux services auprès desquels ils ont des autorisations spécifiques.			✓	✓	✓	✓
V4.7	Vérifier que les utilisateurs peuvent accéder seulement aux données pour lesquelles ils ont des autorisations spécifiques.			✓	✓	✓	✓
V4.8	Vérifier que les contrôles d'accès échouent de manière sécurisée.			✓	✓	✓	✓
V4.9	Vérifier que les règles de contrôle d'accès imposées par la couche de présentation sont renforcées du coté serveur.			✓	✓	✓	✓
V4.10	Vérifier que les attributs d'utilisateur et de données, ainsi que les informations de politique de sécurité utilisés par les contrôles d'accès ne peuvent être manipulés par un utilisateur sauf si c'est spécialement requis.			✓	√	✓	√
V4.11	Vérifier que tous les contrôles d'accès soient renforcés du coté serveur.			✓	✓	✓	✓



V4.12	Vérifier qu'il existe un mécanisme centralisé (incluant des bibliothèques qui appellent des services d'autorisation externes) pour protéger les accès de chaque type de ressource protégée.			✓	√	✓
V4.13	Vérifier que les limitations sur les entrées et les accès, imposées par les fonctions de l'application ne puissent être contournées (comme des limites de transactions journalières ou une séquence de tâches).		√	✓	✓	✓
V4.14	Vérifier que toutes les décisions de contrôles d'accès ainsi que toutes gestion d'erreur soient journalisées.			✓	✓	✓
V4.15	Vérifier que tout le code utilisant ou implémentant les contrôles d'accès ne soit pas affecté par du code malicieux.					✓

V5 - Exigences de vérification de la validation des entrées

Les exigences de vérification de la validation des entrées, définissent un ensemble d'exigences pour valider les entrées, de sorte à ce qu'elles puissent être utilisées de manière sécurisées au sein de l'application. Le tableau ci-dessous définit les exigences de vérification et d'assainissement correspondantes pour les quatre niveaux de vérification.

Tableau 5 - Exigences de validation des entrées OWASP (V5)

	Exigence de vérification	Niveau 1A	Niveau 1B	Niveau 2A	Niveau 2B	Niveau 3	Niveau 4
V5.1	Vérifier que l'environnement d'exécution n'est pas sujet aux débordements de tampon, ou que les contrôles de sécurité préviennent les débordements de tampons.	√	√	✓	√	✓	√
V5.2	Vérifier qu'un motif de validation positif est définit et appliqué à toutes les entrées.	✓	✓	✓	✓	✓	✓
V5.3	Vérifier que tous les échecs de validation d'entrée résultent dans un rejet de l'entrée ou un assainissement.	✓		✓	✓	✓	✓
V5.4	Vérifier qu'un type d'encodage des caractères, tel l'UTF-8, est spécifié pour toutes les sources d'entrées.			✓	✓	✓	✓
V5.5	Vérifier que toutes les validations d'entrées soient exécutées coté serveur.			✓	✓	✓	✓



V5.6	Vérifier qu'un seul contrôle de validation des entrées est utilisé par l'application pour chaque type de données qui est accepté.		✓	✓	✓
V5.7	Vérifier que tous les échecs de validation des entrées soient journalisés.		✓	✓	✓
V5.8	Vérifier que chaque entrée de données soient conforme en aval pour tous les décodeurs ou interpréteurs préalablement à la validation.			✓	✓
V5.9	Vérifier que tous les contrôles de validation des entrées ne soient pas affectés par du code malicieux.				✓

V6 - Exigences de vérification de l'encodage/échappement des sorties

Les exigences de validation de l'encodage/échappement des sorties, définissent un ensemble d'exigences pour vérifier que la sortie est correctement encodée de sorte à ce qu'elle soit sûre pour les applications externes. Le tableau ci-dessous définit les exigences de vérification correspondantes pour les quatre niveaux de vérification.

Tableau 6 - Exigences d'encodage / échappement des sorties OWASP ASVS (V6)

	Exigence de vérification	Niveau 1A	Niveau 1B	Niveau 2A	Niveau 2B	Niveau 3	Niveau 4
V6.1	Vérifier que toutes les données non fiables qui doivent sortir sous forme de HTML (incluant HTML éléments, HTML attributs, données Javascript, blocks CSS, et attributs d'URLs) soient correctement échappés en fonction du contexte.		√	√	√	√	✓
V6.2	Vérifier que tous les contrôles d'encodage/échappement des sorties soient implémentés coté serveur.			✓	✓	✓	✓
V6.3	Vérifier que les contrôles d'encodage/échappement des sorties protègent correctement tous les caractères qui ne sont pas connus pour être sûr pour l'interpréteur de destination.				✓	√	✓
V6.4	Vérifier que toutes les données non sûres qui doivent être envoyées à un interpréteur SQL utilisent une interface paramétrée, une déclaration préparée (prepared statements), ou qu'elles soient échappées correctement.				✓	✓	✓



V6.5	Vérifier que toutes les données non sûres qui sont envoyées en sortie vers du XML, utilisent une interface paramétrée ou soient correctement échappées.		✓	✓	✓
V6.6	Vérifier que toutes les données non sûres qui sont utilisées dans des requêtes LDAP soient échappées correctement.		✓	✓	✓
V6.7	Vérifier que toutes les données non sûres qui sont incluses dans des commandes de système d'exploitation soient correctement échappées.		✓	✓	✓
V6.8	Vérifier que toutes les données non sûres qui sont envoyées à un interpréteur non listé ci-dessus soient correctement échappées.		✓	✓	✓
V6.9	Vérifier que pour chaque type de sortie encodée/échappée exécutée par l'application, il n'y ait qu'un seul contrôle de sécurité pour ce type de sortie pour la destination prévue.			✓	✓
V6.10	Vérifier que tous le code utilisant ou implémentant des contrôles de validation de sorties, n'est pas affecté par du code malicieux.				✓

V7 - Exigences de vérification cryptographique

Les exigences de vérification de chiffrement définissent un ensemble d'exigences qui peuvent être utilisées pour vérifier le chiffrement d'une application, la gestion des clés, les nombres aléatoires, et les opération de hashage. Les applications devraient toujours utiliser des modules cryptographiques validés FIPS 140-2 ou validés par un standard équivalent (par ex. un standard non US). Le tableau ci-dessous définit les exigences de vérification correspondantes pour les 4 niveaux.

Tableau 7 - Exigences cryptographiques OWASP ASVS (V7)

	Exigence de vérification	Niveau 1A	Niveau 1B	Niveau 2A	Niveau 2B	Niveau 3	Niveau 4
V7.1	Vérifier que toutes les fonctions cryptographiques utilisées dans l'application soient implémentées coté serveur.			✓	✓	✓	✓
V7.2	Vérifier que tous les modules cryptographiques échouent de manière sûre.7			✓	✓	✓	✓



V7.3	Vérifier que l'accès à tout code secret maitre est protégé des accès non autorisés (un code secret est un jeton d'application stocké en texte brut sur le disque, et qui est utilisé pour protéger l'accès aux informations de configuration de la sécurité).		✓	✓	✓
V7.4	Vérifier qu'un grain de sel est ajouté lorsque les mots de passe sont hashés.		✓	✓	✓
V7.5	Vérifier que les erreurs des modules cryptographiques soient journalisés.		✓	✓	✓
V7.6	Vérifier que tous les nombres aléatoires, noms de fichiers aléatoires, GUIDs aléatoires, et chaines de caractères aléatoires soient générés par un module cryptographique, dont le générateur de nombres aléatoire soit approuvé, et dont les valeurs aléatoires ne puissent être prévues par un attaquant.		✓	✓	√
V7.7	Vérifier que les modules cryptographiques utilisés par l'application soient validées par le standard FIPS 140-2 ou un standard équivalent. (voir http://csrc.nist.gov/groups/STM/cmvp/validation.html).			✓	✓
V7.8	Vérifier que les modules cryptographiques opèrent dans leur contexte valide, conformément à leur politique de sécurité publique (voir http://csrc.nist.gov/groups/STM/cmvp/ validation.html).			✓	√
V7.9	Vérifier qu'il existe une politique explicite définissant la manière dont les clés cryptographiques sont gérées (par ex. générées, distribuées, révoquées, expirées) Vérifier que cette politique est correctement respectée.			✓	✓
V7.10	Vérifier que tout le code implémentant ou utilisant un module cryptographique n'est pas affecté par un code malicieux.				✓

V8 - Exigences de vérification de gestion des erreurs et de journalisation

Les exigences de vérification de gestion des erreurs et de journalisation, définissent un ensemble d'exigences qui peuvent être utilisées pour vérifier la recherche des évènements liés à la sécurité et l'identification d'attitudes menaçantes. Le tableau ci-dessous définit les exigences de vérification correspondantes qui s'appliquent au 4 niveaux de vérification.



Tableau 8 - Exigences de gestion des erreurs et de journalisation OWASP ASVS (V8)

	Exigence de vérification	Niveau 1A	au 1B	Niveau 2A	au 2B	eau 3	Niveau 4
	zagenee ze to meation	Nive	Niveau	Nive	Niveau	Niveau	Nive
V8.1	Vérifier que l'application n'envoie pas sur la sortie des messages d'erreurs ou des traces de pile contenant des informations sensibles qui pourraient aider un attaquant, incluant les ids de session et les informations personnelles.	✓	✓	✓	✓	✓	✓
V8.2	Vérifier que les erreurs coté serveur sont gérées sur le serveur.			✓	✓	✓	✓
V8.3	Vérifier que tous les contrôles de journalisation sont implémentés sur le serveur.			✓	✓	✓	✓
V8.4	Vérifier que la logique de gestion des erreurs refuse l'accès par défaut.			✓	✓	✓	✓
V8.5	Vérifier que les contrôles de sécurité de connexion permettent de journaliser les succès ET les échecs d'évènements qui sont identifiés comme liés à la sécurité.				√	✓	√
V8.6	Vérifier que chaque événement de journalisation inclut : 1. Un timestamp provenant d'une source de confiance. 2. Un niveau de gravité de l'évènement. 3. Une indication du fait que c'est un événement lié à la sécurité (si mélangé à d'autres journaux). 4. L'identité de l'utilisateur à l'origine de l'évènement (s'il y a un utilisateur lié à l'évènement) 5. L'adresse IP source de la requête associée à l'évènement. 6. Si l'évènement à réussi ou échoué. 7. Une description de l'évènement.				√	√	√
V8.7	Vérifier que tous les évènements qui incluent des données non sûres ne pourront produire du code exécutable dans le logiciel de lecture des journaux.				✓	✓	✓
V8.8	Vérifier que les journaux de sécurité soient protégés contre l'accès non autorisés et la modification.				✓	✓	✓



V8.9	Vérifier qu'il y a une seule implémentation de journalisation qui soit utilisée par l'application.		✓	✓	✓
V8.10	Vérifier que l'application ne journalise pas des donnée sensibles spécifiques à l'application qui pourraient aider un attaquant, incluant les ids de session utilisateur et les informations personnelle ou sensible.		✓	✓	✓
V8.11	Vérifier qu'un outil de journalisation soit disponible, permettant à l'analyste des rechercher d'évènements basées sur des combinaisons de critères de recherches à travers tous les champs du format d'enregistrement des journaux supportés par ce système.		✓	√	✓
V8.12	Vérifier que tous le code implémentant ou utilisant les gestions d'erreurs ou la journalisation ne soient pas affectés par du code malicieux.				✓

V9 - Exigences de vérification de la protection des données

Les exigences de vérification de la protection des données définissent un ensemble d'exigences qui peuvent être utilisées pour vérifier la protection des données sensibles (par ex. numéros de cartes de crédit, numéros de passeport, informations personnelles). Le tableau ci-dessous définit les exigences de vérification correspondantes qui s'appliquent à chacun des quatre niveaux de vérification.

Tableau 9 - Exigences de protection des données OWASP ASVS (V9)

	Exigence de vérification	Niveau 1A	Niveau 1B	Niveau 2A	Niveau 2B	Niveau 3	Niveau 4
V9.1	Vérifier que tous les formulaires contenant des informations sensibles ont désactivé les caches coté client, incluant les fonctionnalités d'autocomplétion.	✓	✓	✓	✓	✓	✓
V9.2	Vérifier que la liste des informations sensibles traitées par l'application est identifiée et qu'il existe une politique explicite pour le contrôle de l'accès à ces données, et le choix du moment ou ces données doivent êtrechiffrées (aussi bien au repos qu'en transit). Vérifier que cette politique est correctement appliquée.				√	✓	✓



V9.3	Vérifier que toute donnée sensible est bien envoyée au serveur dans le corps du message HTTP (les URLs ne sont jamais utilisées pour envoyer des données sensibles).		✓		✓	✓
V9.4	Vérifier que les caches ou copies temporaires de données sensibles envoyées au client soient protégéescontre les accès non autorisés, purgées / invalidées après que l'utilisateur autorisé ait accédé à ces données (l'entête no-cache et no-store Cache-Control doivent être utilisés).			√	✓	√
V9.5	Vérifier que tous les caches ou copies temporaires de données sensibles stockées sur le serveur soient protégées contre les accès non autorisés ou purgées/invalidées après que l'utilisateur autorisé ait accédé à ces données.			√	✓	√
V9.6	Vérifier qu'il y a une méthode pour supprimer chaque type de données sensibles de l'application à la fin de la période de rétention requise.				✓	✓

V10 - Exigences de vérification des communications sécurisées

Les exigences de vérification des communications sécurisées définissent un ensemble d'exigences qui peuvent être utilisées pour vérifier que toutes les communications avec une application soient correctement sécurisées. Le tableau ci-dessous définit les exigences de vérification qui s'appliquent pour chacun des quatre niveaux de vérification.

Tableau 10 - Exigences de communications sécurisées OWASP ASVS (V10)

	Exigence de vérification	Niveau 1A	Niveau 1B	Niveau 2A	Niveau 2B	Niveau 3	Niveau 4
V10.1	Vérifier qu'un chemin peut être créé depuis chaque AC de confiance vers chaque certificat de serveur TLS (Transport Layer Security), et que chaque certificat de serveur est valide.	✓		✓	√	✓	✓
V10.2	Vérifier que les échecs de connections TLS ne deviennent pas des connections non sécurisées.			✓		✓	✓



V10.3	Vérifier que TLS est utilisé pour toutes les connections authentifiées ou impliquant des données sensibles, ou des fonctionnalités sensibles (incluant les connexions externes et terminales).		✓	✓	✓
V10.4	Vérifier que les échecs de connexions TLS terminales soient journalisées.		✓	✓	✓
V10.5	Vérifier que les chemins de certificats soient créés et vérifiés pour chaque certificat client utilisant des ancres de confiance configurées et des informations de révocation.		✓	✓	√
V10.6	Vérifier que toutes les connexions à un système externe qui impliquent des informations ou des fonctionnalités sensibles soient authentifiés.		✓	✓	✓
V10.7	Vérifier que toutes les connexions à un système externe qui impliquent des informations ou des fonctionnalités sensibles utilisent un compte qui soit réglé pour avoir le minimum de privilèges nécessaire à l'application pour fonctionner correctement.		✓	✓	✓
V10.8	Vérifier qu'il n'y a qu'une seule implémentation standard de TLS qui soit utilisée par l'application et soit configurée pour opérer dans un moded'opération homologué (voir http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/FIPS1402IG.pdf).			√	√
V10.9	Vérifier qu'un encodage de caractères spécifique est définit pour toutes les connexions (par ex. UTF-8)			✓	✓

V11 - Exigences de vérification de sécurité HTTP

Les exigences de vérification de sécurité HTTP définissent un ensemble d'exigences qui peuvent être utilisées pour vérifier la sécurité relative aux requêtes, réponses, sessions, cookies, en-têtes, et journalisations HTTP. Le tableau ci-dessous définit les exigences de vérification correspondantes qui s'appliquent pour chacun des quatre niveaux de vérification.

Tableau 11 - Exigences de sécurité HTTP OWASP ASVS (V11)



	Exigence de vérification	Niveau 1A	Niveau 1B	Niveau 2A	Niveau 2B	Niveau 3	Niveau 4
V11.1	Vérifier que les redirections n'incluent pas de données non validées	✓	✓	✓	✓	✓	✓
V11.2	Vérifier que l'application n'accepte qu'un nombre définis de types de requêtes HTTP, tels que GET ou POST.	√	✓	✓	✓	✓	✓
V11.3	Vérifier que chaque réponse HTTP contient un entête Content-Type spécifiant un type d'encodage de caractères sûr (par ex. UTF-8).	1	✓	✓	✓	✓	✓
V11.4	Vérifier que le drapeau HTTPOnly est utilisé sur tous les cookies qui n'ont pas besoin d'être accédés par JavaScript.			✓	✓	✓	✓
V11.5	Vérifier que le drapeau de sécurité est utilisé sur tous les cookies qui contiennent des données sensibles, incluant le cookie de sessions.			✓	✓	✓	✓
V11.6	Vérifier que les entêtes HTTP ne contiennent que des caractères imprimables ASCII dans les requêtes et réponses.			✓	✓	✓	✓
V11.7	Vérifier que l'application génère un jeton aléatoire solide comme partie de tout lien ou formulaire associé à une transaction ou accédant à des données sensibles. Vérifier que l'application vérifie la présence du jeton contenu une valeur valide pour l'utilisateur courant lorsqu'il traite ces requêtes. 15					✓	✓

V12 - Exigences de vérification de la configuration de la sécurité

Les exigences de vérification de la configuration de la sécurité définissent un ensemble d'exigences qui peuvent être utilisées pour vérifier le stockage sécurisé de toutes les information de configuration qui déterminent le comportement lié à la sécurité de l'application. Le tableau cidessous définit les exigences de vérification correspondantes qui s'appliquent à chacun des quatre niveaux de vérification.

Tableau 12 - Exigences de configuration de la sécurité OWASP ASVS (V12)

¹⁵ Ces exigences décrivent le mecanisme requis pour défendre contre les attaques de typeCross Site Request Forgery (CSRF).



	Exigence de vérification	Niveau 1A	Niveau 1B	Niveau 2A	Niveau 2B	Niveau 3	Niveau 4
V12.1	Vérifier que toutes les informations de configurations liées à la sécurité sont stockées dans un endroit protégé des accès non-autorisés.				✓	✓	✓
V12.2	Vérifier que les accès à l'application soient refusés si l'application ne peut accéder aux informations de configuration de la sécurité.				✓	✓	✓
V12.3	Vérifier que tout changement dans la configuration de la sécurité gérée par l'application soit journalisé dans les journaux d'évènements de sécurité.					✓	✓
V12.4	Vérifier que le stockage de la configuration peut être ouvert dans un format lisible par un humain pour faciliter l'audit.						✓

V13 - Exigences de vérification de recherche de code malicieux

Pour le niveau 4, il est obligatoire de chercher le code malicieux, dans tous le code de l'application qui n'a pas encore été examiné après le niveau 3. Le tableau ci-dessous définit les exigences de recherche de code malicieux qui sont introduites au niveau 4.

Tableau 13 - Exigences de recherche de code malicieux OWASP ASVS (V13)

	Exigence de vérification	Niveau 1A	Niveau 1B	Niveau 2A	Niveau 2B	Niveau 3	Niveau 4
V13.1	Vérifier qu'aucun code malicieux n'est inséré dans tous le code qui a été développé ou modifié pour créer l'application. 16						✓
V13.2	Vérifier l'intégrité des codes interprétés, bibliothèques, exécutables et fichiers de configuration en utilisant des sommes de contrôle ou des hash.						✓

V14 - Exigences de vérification de la sécurité interne

¹⁶ Par ex. examiner les appels d'horloge système pour chercher les time bombs, fonction sans rapport avec l'objectif de l'application pour les back doors, chemin d'exécution (PATH) pour les Easter eggs, transactions financières pour une logique incorrecte qui pourrait révéler une attaque salami, ou d'autres type de code malicieux.



Les exigences de vérification de la sécurité interne définissent un ensemble d'exigences qui peuvent être utilisées pour vérifier que l'application se protège efficacement contre les défauts d'implémentation. Le tableau ci-dessous définit les exigences de vérification correspondante qui s'appliquent pour chacun des quatre niveaux vérification.

Tableau 14 - Exigences de sécurité interne OWASP ASVS (V14)

	Exigence de vérification	Niveau 1A	Niveau 1B	Niveau 2A	Niveau 2B	Niveau 3	Niveau 4
V14.1	Vérifier que l'application protège les attributs des utilisateurs et des données, et la politique d'information utilisée par les contrôles d'accès lors d'accès nonautorisé et de modifications.					√	✓
V14.2	Vérifier que les interfaces de contrôle de sécurité soient assez simples à utiliser pour que les développeurs les utilisent.						✓
V14.3	Vérifier que l'application protège correctement les variables et ressources partagées d'accès concurrents inapropriés.						✓

Exigences de rapport de vérification

Un rapport OWASP ASVS contient une description de l'application qui a été analysée en accord avec les exigences OWASP ASVS pour un niveau donné. Le rapport documente aussi le résultat de l'analyse, incluant tout correctif de vulnérabilité.

Les exigences de rapport ASVS définissent le type d'information qui doit être présent dans le rapport. Elles ne définissent pas la structure, l'organisation, le format, ni n'empêchent d'ajouter des informations supplémentaires dans le rapport.

Le type d'informations exigées par chaque partie des exigences de rapport ASVS peuvent être organisées conformément aux exigences d'un nommées, formatées, et vérificateur. Les exigences de Rapport rapport ASVS ont cours tant que les informations rapport devrait inclure tout ce qui est nécessaire pour requises sont présentes. Un comprendre l'analyse et ses résultats, ainsi que les informations de configuration, et des portions de code comme décrit dans la figure ci-dessous, qui devrait être utilisée lors de la conception du rapport. Description Architecture Résultats Page xxxviii

à vérifier

Échec d'authentification



Figure 11 - Contenu du rapport

R1 - Introduction du rapport

- R1.1 L'introduction du rapport doit apporter suffisamment d'informations pour pouvoir identifier le rapport et l'application qui est le sujet du rapport.
- R1.2 L'introduction du rapport doit résumer la confiance générale dans la sécurité de l'application.
- R1.3 L'introduction du rapport doit identifier les risques clés associés à l'utilisation de l'application.
- R1.4 L'introduction du rapport doit identifier les règles d'engagement associées avec l'exécution des vérifications ou ce qui contraint l'étendue des vérifications.

R2 - Description de l'application

R2.1 La description de l'application doit fournir une description suffisante pour la bonne compréhension de son fonctionnement et de son environnement.

R3 - Architecture de sécurité de l'application

R3.1 L'architecture de sécurité de l'application doit fournir des détails supplémentaires décrivant l'application, pour montrer au lecteur que l'analyse est précise et complète. Cette partie du rapport expose le contexte de l'analyse; les informations présentées dans cette section seront utilisées durant l'analyse pour identifier les contradictions. Cette partie du rapport doit apporter différents niveaux de détails, en fonction du niveau OWASP ASVS sélectionné pour l'analyse.



R4 - Résultats de vérification

R4.1 Ces résultats de vérification doivent présenter l'analyse qui a été faite conformément à la section « Exigences de vérification » du standard, incluant les descriptions des corrections de vulnérabilités requises, comme ci-dessous :

Tableau 15 - Contenu des résultats du rapport OWASP ASVS

Niveau	Succès	Échec		
Résultats niveau 1	 Verdict Outil de configuration si l'outil peut réaliser le contrôle, ou argumentation apportant des preuves et justifiant le verdict pour la totalité et la conformité. Un schéma des capacité des outils automatisés relativement au exigences de vérification détaillées. Une description de la configuration des outils et un schéma des capacités des outils ne doivent être fournis qu'une seule fois dans le rapport. 	 Verdict Emplacement (URL, paramètres ou fichier source avec son chemin, nom, et numéro de ligne(s). Description (incluant les informations de configuration si approprié). Évaluation du risque¹⁷ Explication du risque. 		
	Une description de la configuration des outils et un schéma des capacités des outils doivent être fournis dans le rapport.			

¹⁷ Pour plus d'informations à propos des risques et de l'estimation des risques associés aux vulnérabilités, voir le *Testing Guide* (OWASP, 2008).



Niveau	Succès	Échec			
Résultats niveau	Verdict	• Verdict			
2 - 4	Explication du verdict (une explication apportant des preuves de l'ensemble et de la conformité).	 Emplacement (URL, paramètres ou fichier source avec son chemin, nom, et numéro de ligne(s). Description (incluant les chemins à emprunter et les étapes à reproduire) Évaluation de risque (voir la « méthodologie d'évaluation de risque OWASP ») Explication du risque. 			

Glossaire

Contrôle d'accès - Restreindre l'accès à des fichiers, fonctionnalités, URLs, ou des données personnelles d'utilisateur ou de groupe.

Composant d'application - Un fichiers source ou groupe de fichiers source, bibliothèques de fonctions, et/ou exécutables, comme définit par le vérificateur pour une application particulière.

Sécurité d'application - Sécurité de niveau application axée sur l'analyse des composants qui comprennent les couches applicatives du modèle OSI (Open Systems Interconnection Reference Model), plutôt que par exemple, sur le système d'exploitation sous-jacent ou le réseau connecté.

Vérification de sécurité d'une application - Estimation technique d'une application conformément au standard OWASP ASVS.

Rapport de vérification de la sécurité d'une application - Un rapport qui documente les résultats d'ensemble ainsi que les analyses du vérificateur pour une application donnée.

Standard de vérification de la sécurité d'applications (ASVS) - Standard OWASP qui définit quatre niveaux de vérification de la sécurité des applications.

Authentification - Vérification de l'identité revendiquée par un utilisateur de l'application.

Vérification automatisée - Utilisation d'outils automatisés qui utilisent des signatures de vulnérabilités pour trouver des problèmes (outils d'analyses dynamiques, statiques ou les deux).

Porte dérobée (Back Doors) - Type de code malicieux qui permet à des utilisateurs non autorisés d'obtenir un accès.

Liste noire (Blacklist) - Liste de données ou d'opérations non permises, par ex. une liste de caractères non autorisés comme données d'entrée.

Critères communs (Common Criteria CC) - Standard pouvant être utilisé comme base de vérification de la conception et de l'implémentation des contrôles de sécurité des produits informatiques.

Communication sécurisée - Protection des données de l'application lorsqu'elles transitent entre les composants de l'application, entre clients et serveurs, et entre des systèmes externes et l'application.

Vérification de la conception - Estimation technique de larchitecture de sécurité d'une application.

Vérification interne - Estimation technique d'aspects spécifiques de l'architecture de sécurité d'une application conformément au standard OWASP ASVS.

Module Cryptographique - Matériel, logiciel, et/ou firmware qui implémente des algorithmes cryptographiques ou génère des clés cryptographiques.



Attaque de déni de service (DOS) - Inondation d'une application avec plus de requêtes qu'elle ne peut en gérer.

Vérification dynamique - Utilisation d'outils automatisés qui utilisent des signatures de vulnérabilités pour trouver des problèmes durant l'exécution de l'application.

Œufs de pâques (Easter Eggs)- Type de code malicieux qui ne s'exécute pas avant qu'un événement spécifique ne se produise.

Système externe - Service qui ne fait pas partie de l'application.

FIPS 140-2 - Standard qui peut être utilisé comme base pour la vérification de la conception et l'implémentation de modules cryptographiques.

Validation des entrées - Validation et mise sous forme canonique de données utilisateur non sûres.

Code malicieux - Code introduit dans le code d'une application à l'insu du propriétaire/développeur de l'application, qui détourne la politique de sécurité de l'application. Le code malicieux est différent des virus ou vers.

Malware - Code exécutable introduit dans une application durant son exécution, à l'insu de l'administrateur ou de l'utilisateur de l'application.

Open Web Application Security Project (OWASP) - Open Web Application Security Project (OWASP) est une communauté libre et ouverte dont l'objectif est d'améliorer la sécurité des applications logicielles. Notre mission est de rendre la sécurité des applications « visible », de sorte à ce que les particuliers et les organisations puissent prendre en connaissance de cause, des décisions liées au risques et à la sécurité des applications. Voir : http://www.owasp.org/

Validation des sorties - validation et mise sous forme canonique des sorties d'une application, vers les navigateurs et des systèmes externes.

OWASP Enterprise Security API (ESAPI) - Une bibliothèque libre et ouverte de toutes les méthodes sécurisées dont un développeur a besoin pour construire une application web sécurisé, voir : http://www.owasp.org/index.php/ESAPI

Méthodologie d'évaluation des risques OWASP - Méthodologie d'évaluation des risques conçue spécialement pour la sécurité des applications. Voir : http://www.owasp.org/index.php/How_to_value_the_real_risk

OWASP Guide des tests - Un document conçu pour aider les organisations à comprendre ce que comporte un programme de test, ainsi que les démarches à suivre pour le mettre en oeuvre. Voir : http://www.owasp.org/index.php/Category:OWASP_Testing_Project

OWASP Top Ten - Un document qui représente un large consensus à propos des attaques d'applications web les plus critiques. Voir : http://www.owasp.org/index.php/Top10

Positif - Voir Liste blanche (White list).

Attaque Salami - Type de code malicieux utilisé pour rediriger discrètement une petite quantité d'argent durant une transaction financière.

Architecture de sécurité - Abstraction de la conception d'une application, identifiant et décrivant où et comment les contrôles de sécurité sont utilisés, ainsi que l'endroit et la sensibilité des données.

Contrôle de sécurité - Fonctionnalité ou composant, exécutant un examen de sécurité.

Configuration de sécurité - Configuration de l'exécution d'une application, affectant la manière dont les contrôles de sécurité sont utilisés.

Vérification statique - Utilisation d'outils automatisés, faisant appels à des signatures de vulnérabilités, pour trouver les problèmes dans le code source de l'application.

Cible de vérification (Target of Verification TOV) - Si vous faites une vérification de la sécurité d'une application conformément aux exigences OWASP ASVS, la vérification se fera sur une



application particulière. Cette application est nommée la « cible de vérification », ou simplement TOV(*Target of Verification*).

Modélisation de menace - Technique consistant à développer une architecture de sécurité de plus en plus raffinée pour identifier les agents de menaces, zones de sécurité, contrôles de sécurité.

Bombe à retardement (Time Bomb) - Type de code malicieux qui ne s'exécute pas avant un certain délai ou une date.

Vérificateur - La personne ou l'équipe qui fait la revue de l'application conformément aux exigences OWASP ASVS.

Liste Blanche (Whitelist) - Liste de données ou d'opérations permises, par exemple une liste de caractères d'entrée de l'application valides.

Pour approfondir le sujet

OWASP est l'un des sites les plus important sur la sécurité des applications web. Le site OWASP héberge de nombreux projets, forums, blogs, présentations, articles et outils. De plus, OWASP héberge deux conférences majeures sur la sécurité des applications Web par an, et 80 chapitres locaux. Le projet OWASP ASVS peut être trouvé ici: http://www.owasp.org/index.php/ASVS

Les projets OWASP ci-dessous peuvent être très utiles aux utilisateur de ce standard :

- Projet Top Ten OWASP http://www.owasp.org/index.php/Top_10
- Guide de revue du code OWASP (Code Review Guide) http://www.owasp.org/index.php/Category:OWASP_Code_Review_Project
- Guide de tests OWASP (Testing Guide) http://www.owasp.org/index.php/Testing_Guide
- Projet OWASP Enterprise Security API (ESAPI) http://www.owasp.org/index.php/ESAPI
- OWASP Legal Project http://www.owasp.org/index.php/Category:OWASP_Legal_Project

De la même manière, les sites Web ci-dessous peuvent être très utiles aux utilisateur de ce standard :

- OWASP http://www.owasp.org
- MITRE Énumération des faiblesses communes Tendances des vulnérabilités, http://cwe.mitre.org/documents/vuln-trends.html
- Conseil des standards de sécurité PCI Éditeurs des standards PCI, correspondant aux organisations traitants les données des cartes de crédit, https://www.pcisecuritystandards.org
- Standard de sécurité des données (DSS) v1.1 https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf

LES ICONES CI-DESSOUS REPRESENTENT LES DIFFERENTES VERSIONS DISPONIBLES POUR CE DOCUMENT.

ALPHA: Une "version alpha" du document est une ébauche approximative, son contenu est en cours de développement jusqu'à la prochaine version publié.

BETA: Une "version beta" du document est un niveau supérieur de qualité, son contenu en cours de développement jusqu'à la prochaine version publié.

FINALE: Une "version finale" du document est le plus haut niveau de qualité de développement d'un document, c'est un produit fini.



VOUS ETES LIBRE



de partager - copier, distribuer et transmettre le travail



de modifier - adapter le travail

SOUS LES CONDITIONS SUIVANTES :



Attribution. Vous devez attribuer le travail de la manière spécifiée par l'auteur ou le bailleur de la licence (mais pas de sorte à ce qu'ils endossent votre travail ou son utilisation).



Partage à l'identique. - Si vous altérez, transformez, ou créez en utilisant ce travail, vous devez distribuer le travail résultant, sous une licence identique, similaire ou compatible avec la licence originale.



Le projet de sécurité des applications web (OWASP) est une communauté mondiale libre et ouverte, focalisée sur l'amélioration de la sécurité des applications logicielles. Notre mission est de rendre la sécurité des applications "visible", de sorte à ce que les gens et les organisations, puissent prendre des décisions éclairées à propos des risques de sécurité liés aux applications. Chacun est libre de participer au projet OWASP, et tous nos produits sont disponibles sous une licence logicielle libre et ouverte. La fondation OWASP organisation à but non lucratif qui assure la disponibilité continue de notre travail.

Sur la couverture : guêpes parasites, scarabées, et pucerons. Après que la femelle injecte un oeuf dans un hôte, la larve s'alimente doucement depuis cet hôte. Avec le temps l'hôte meurt, la larve elle, est devenue grande. Elle se transforme alors en chrysalide dans ou à coté de son hôte, parfois dans un cocon, pour sortir plus tard en guêpe adulte.