Authentifications
Gestion des Sessions
Contrôle d'Accès

Le point de vue d' OWASP ASVS
(Application Security Verification Standard)

Philippe Léothaud : chez BeeWare depuis 2003, d'abord en charge de l'offre Web SSO puis CTO depuis 2006

Bee Ware :

- éditeur d'un WAF depuis 2001
- solution de WebSSO depuis 2003
- outil d'Application Security Assessment depuis 2005
- Gateway XML complète depuis 2007

Aujourd'hui, regroupement de toutes ces fonctionnalités sur une plate-forme unique : **i-Suite**

But : fournir aux Systèmes d'Information une gamme de modules pilotés par une console centralisée couvrant l'intégralité des besoins techniques des infrastructures applicatives métier :

- sécurité
- contrôle d'accès
- manipulation des flux
- optimisation de la bande passante
- haute disponibilité et répartition de charge
- audit et monitoring des flux.

Qu'est-ce que ASVS

- Unité de mesure du niveau de sécurité d'une application Web
- Liste exhaustive des contrôles à mettre en place pour garantir un niveau de sécurité donné
- Base d'exigences pour la contractualisation des vérifications de sécurité.

Quelles réponses apporte l'ASVS

- Quels contrôles de sécurité sont nécessaires pour garantir à mon application le niveau de sécurité attendu ?
- Quelles doivent être les parties couvertes et le niveau d'exigence lors de ces contrôles de sécurité ?
- Quel est le niveau de sécurité d'une application Web ?

Exigences de vérification de l'ASVS

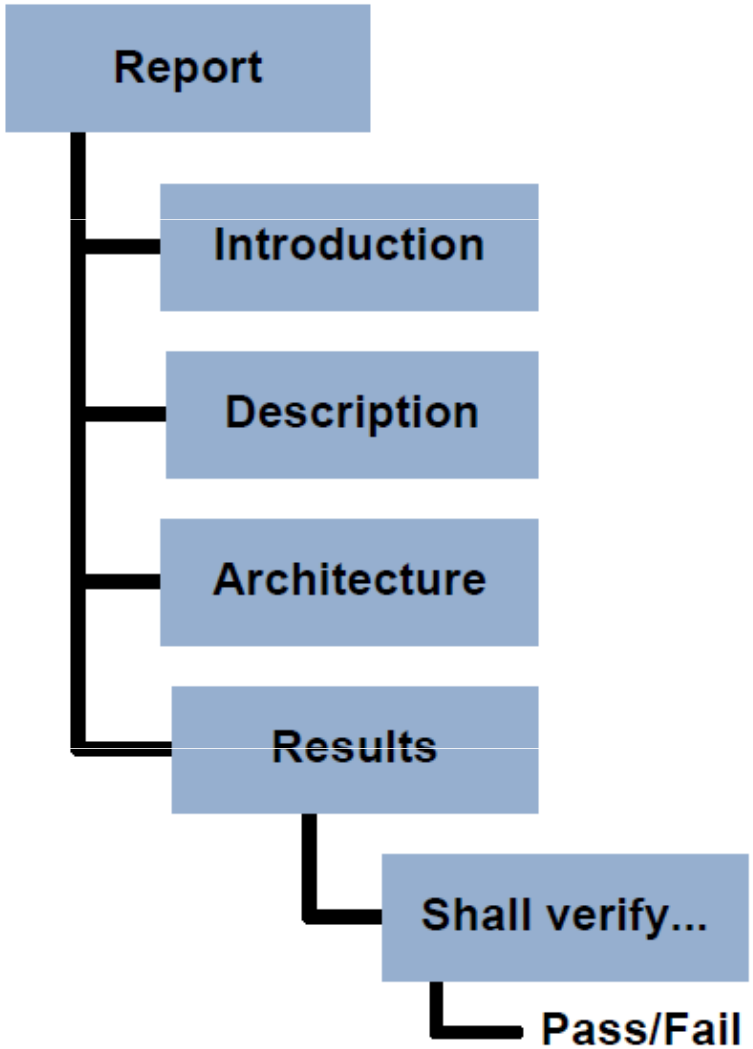
- Exigences d'architecture
- Exigences de vérification de la sécurité

	Level 1A	Level 1B	Level 2A
Shall verify…	✓	✓	✓
Shall verify…			✓
Shall verify…			
Shall verify…	✓		✓

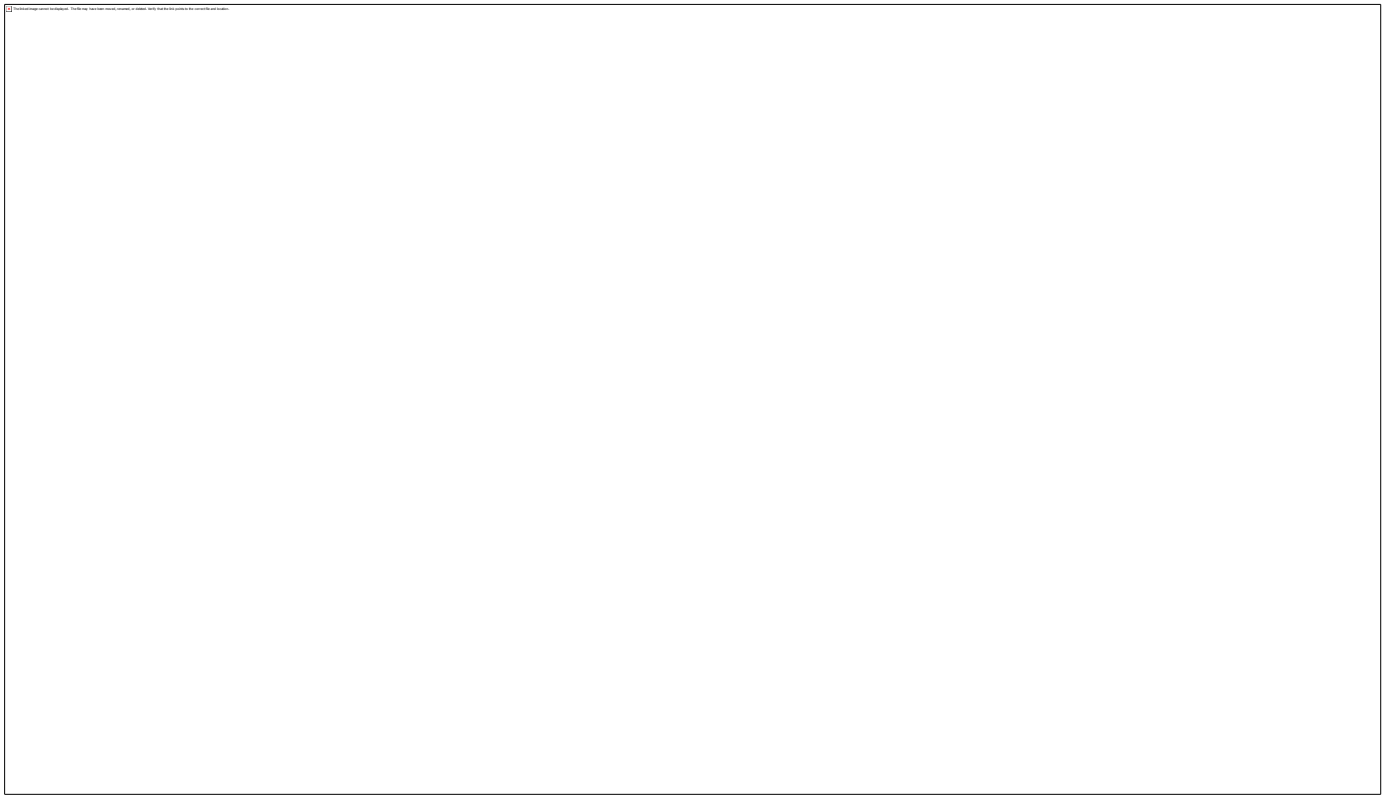
➢ **Liste détaillée des vérifications à effectuer, par niveau**

Exigences de reporting de l'ASVS

- R1 –Introduction
- R2 – Description de l'application
- R3 – Approche architecturale
- R4 – Résultats de la vérification



Les niveaux de vérification de l'ASVS

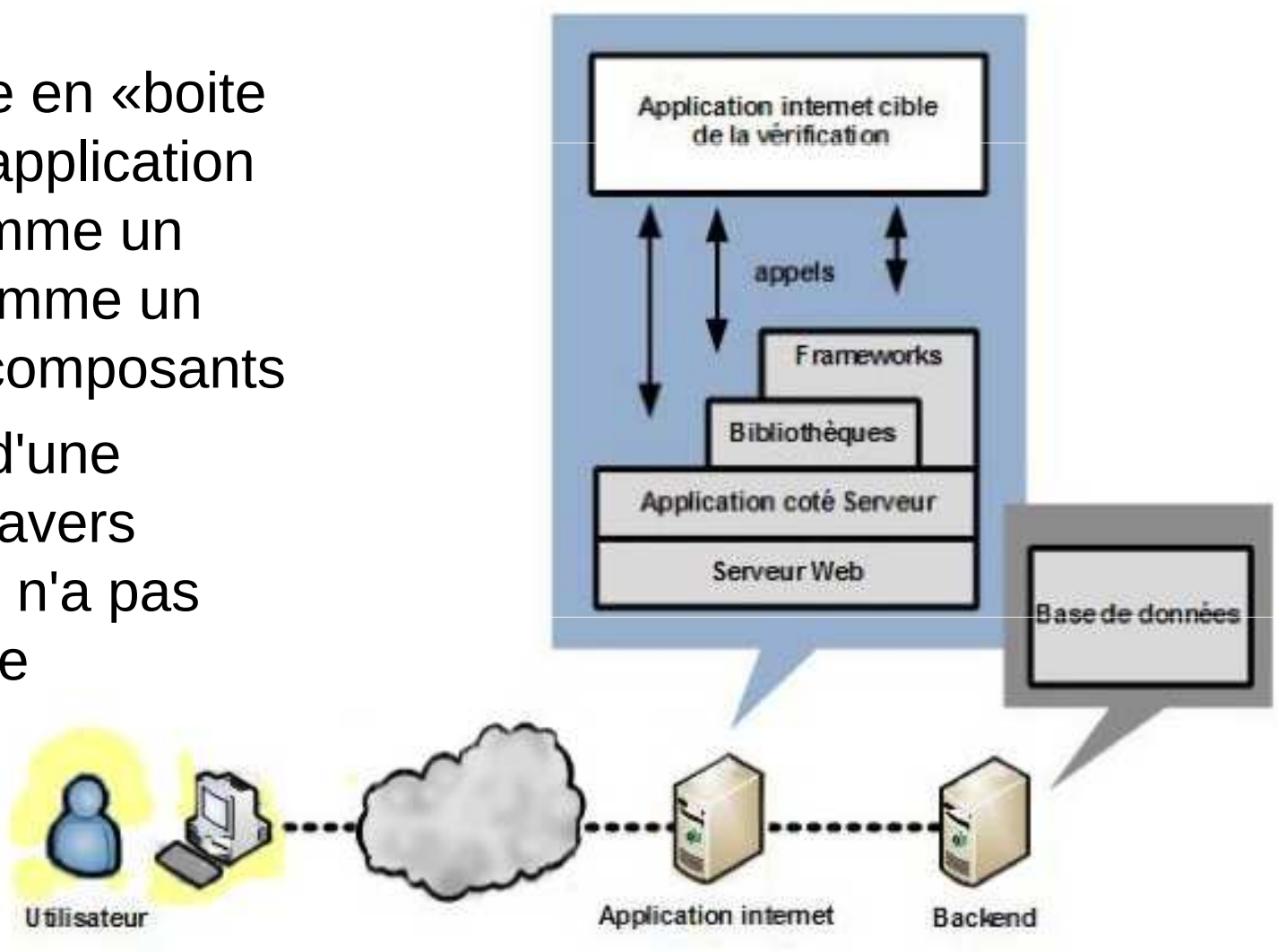


Définition des niveaux

- Niveau 1 – Vérification automatisée (vérification partielle de l'application)
  - Niveau 1A –Scan dynamique
  - Niveau 1B – Analyse du code source
- Niveau 2 – Vérification manuelle (vérification partielle de l'application)
  - Niveau 2A – Test d'intrusion
  - Niveau 2B – Revue de code
- Niveau 3 – Vérification de la conception
- Niveau 4 – Vérification des fonctions internes

Niveau 1 en détail

- Vérification automatisée en «boite noire» de l'application vue soit comme un tout, soit comme un groupe de composants
- Le chemin d'une requête à travers l'application n'a pas besoin d'être documenté



Niveau 1A et niveau 1B

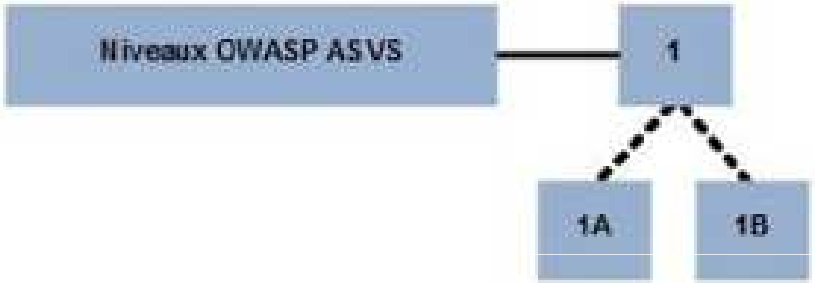


Figure 3 - OWASP ASVS Niveaux 1, 1A, et 1B

- Niveau 1A

  Analyse dynamique partielle

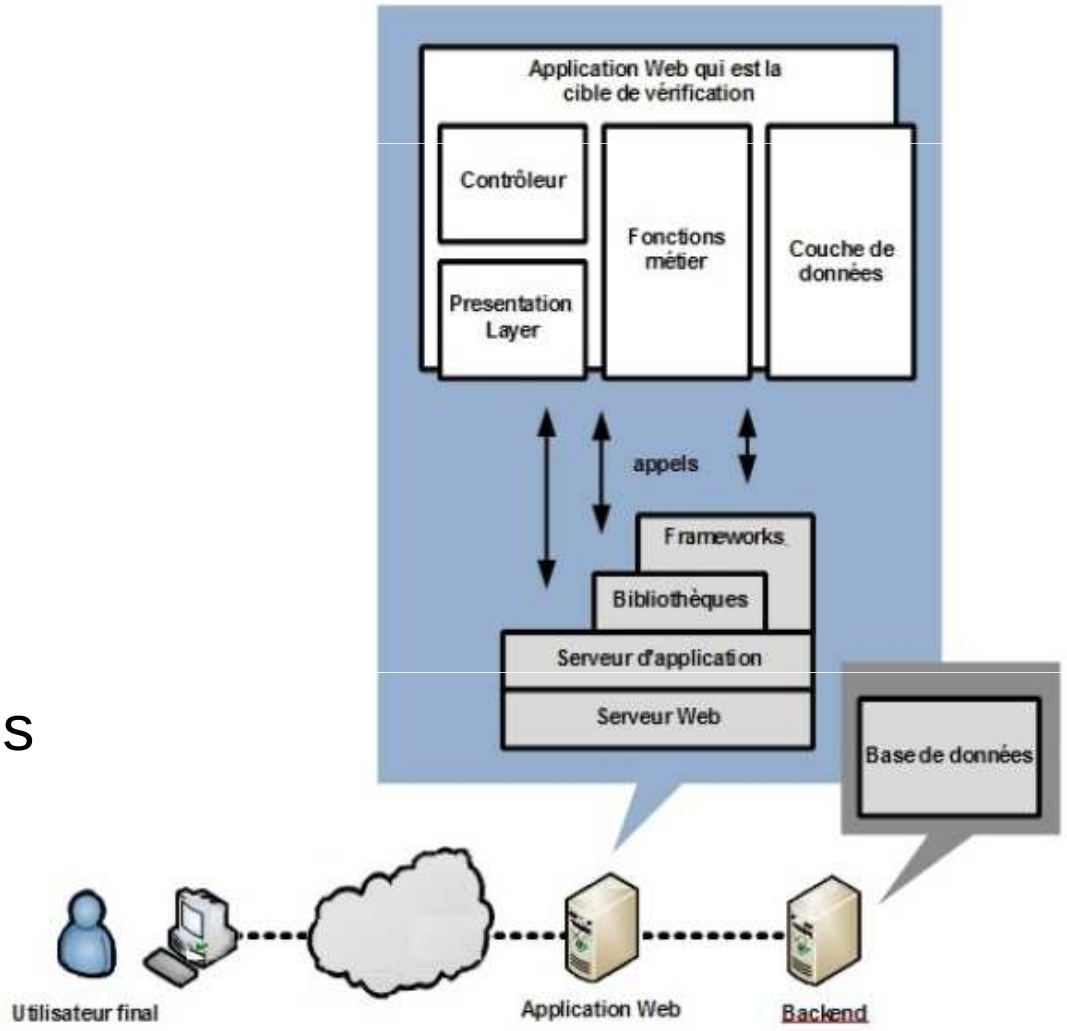
- Niveau 1B

  Analyse partielle du code source

Les 2 sont nécessaires pour obtenir un niveau 1 complet

Niveau 2 en détail

- Vérification manuelle d'une application vue comme un groupe de composants organisés selon une architecture de haut niveau
- Les chemins des requêtes testées à travers l'application doivent être documentés



Niveau 2A et niveau 2B

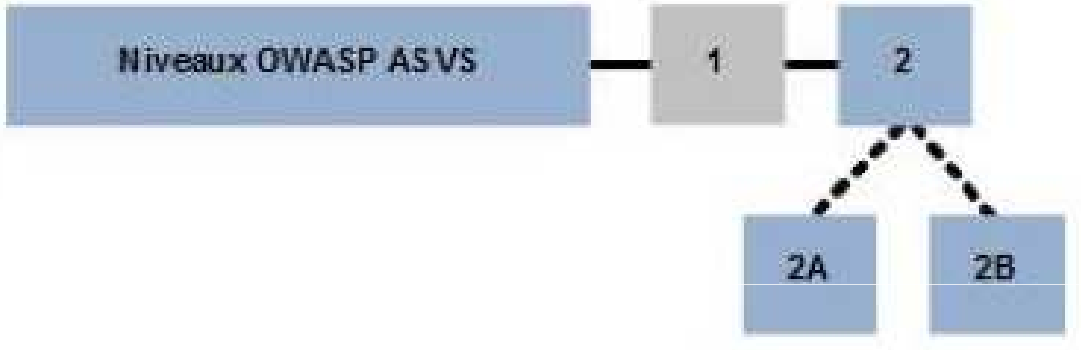


Figure 5 - Niveaux OWASP ASVS 2, 2A, et 2B

- Niveau 2A

Tests de pénétration manuels

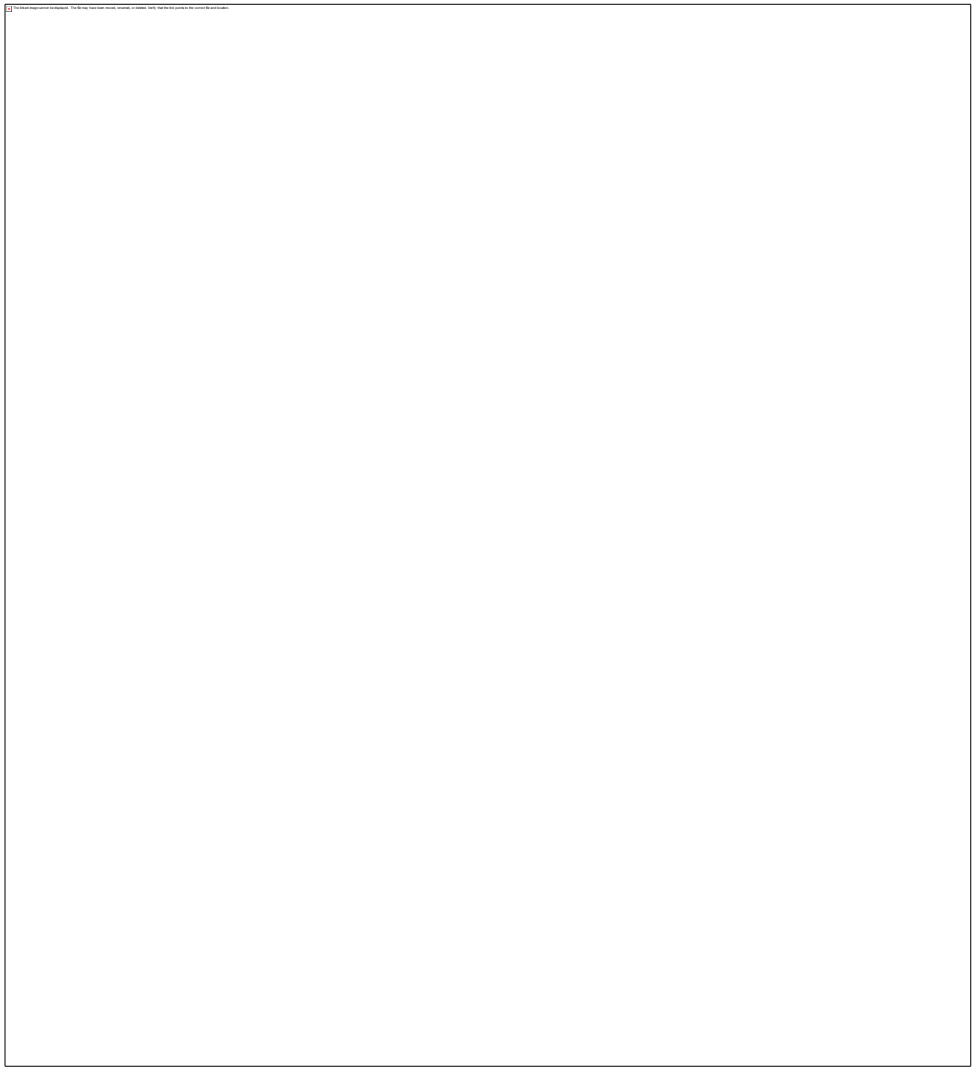
- Niveau 2B

Revue manuelle du code source

Les 2 sont nécessaires pour obtenir un niveau 2 complet.

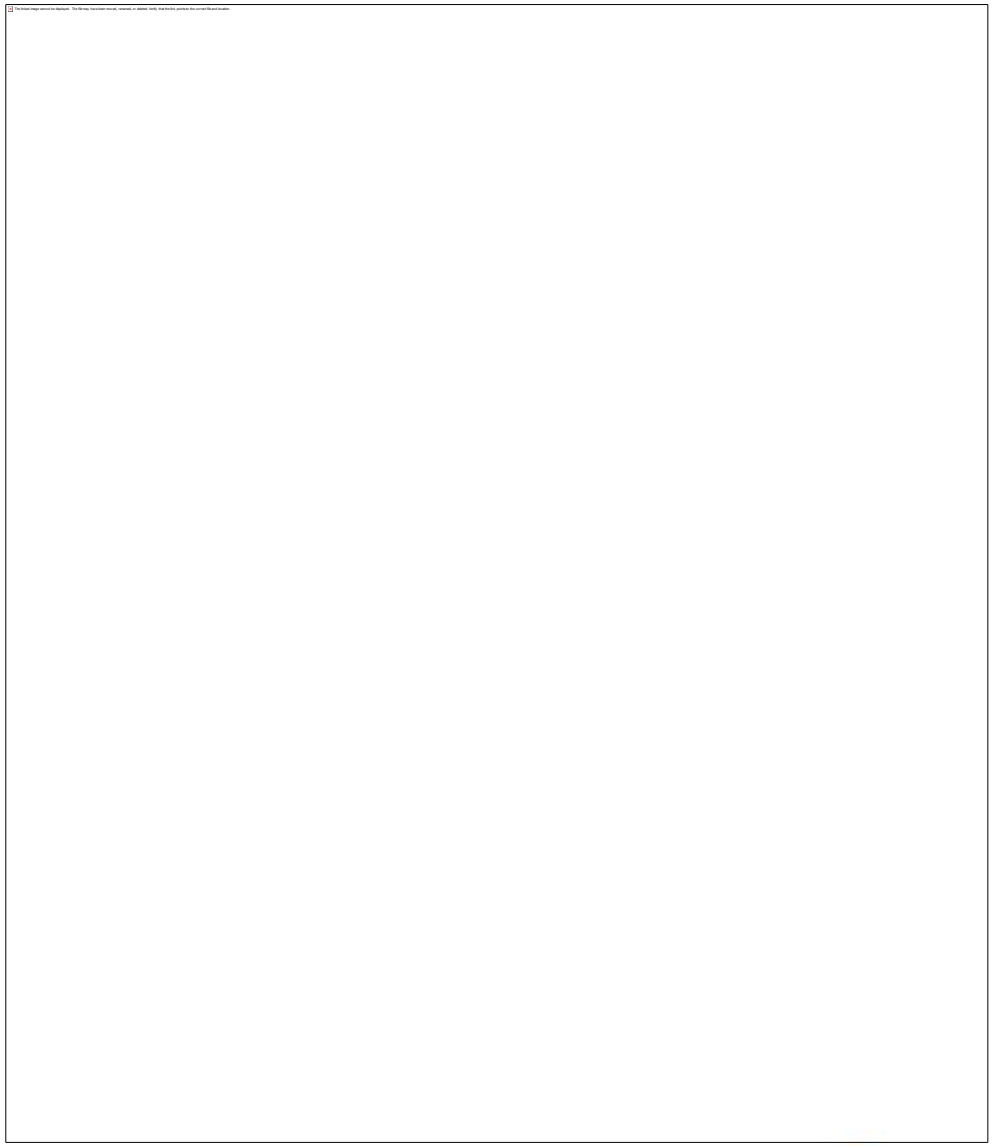
Niveau 3 en détail

- En plus du niveau 2, modélisation des menaces contre les assets critiques et vérification de la conception
- Tous les chemins des requêtes à travers l'application doivent être documentés

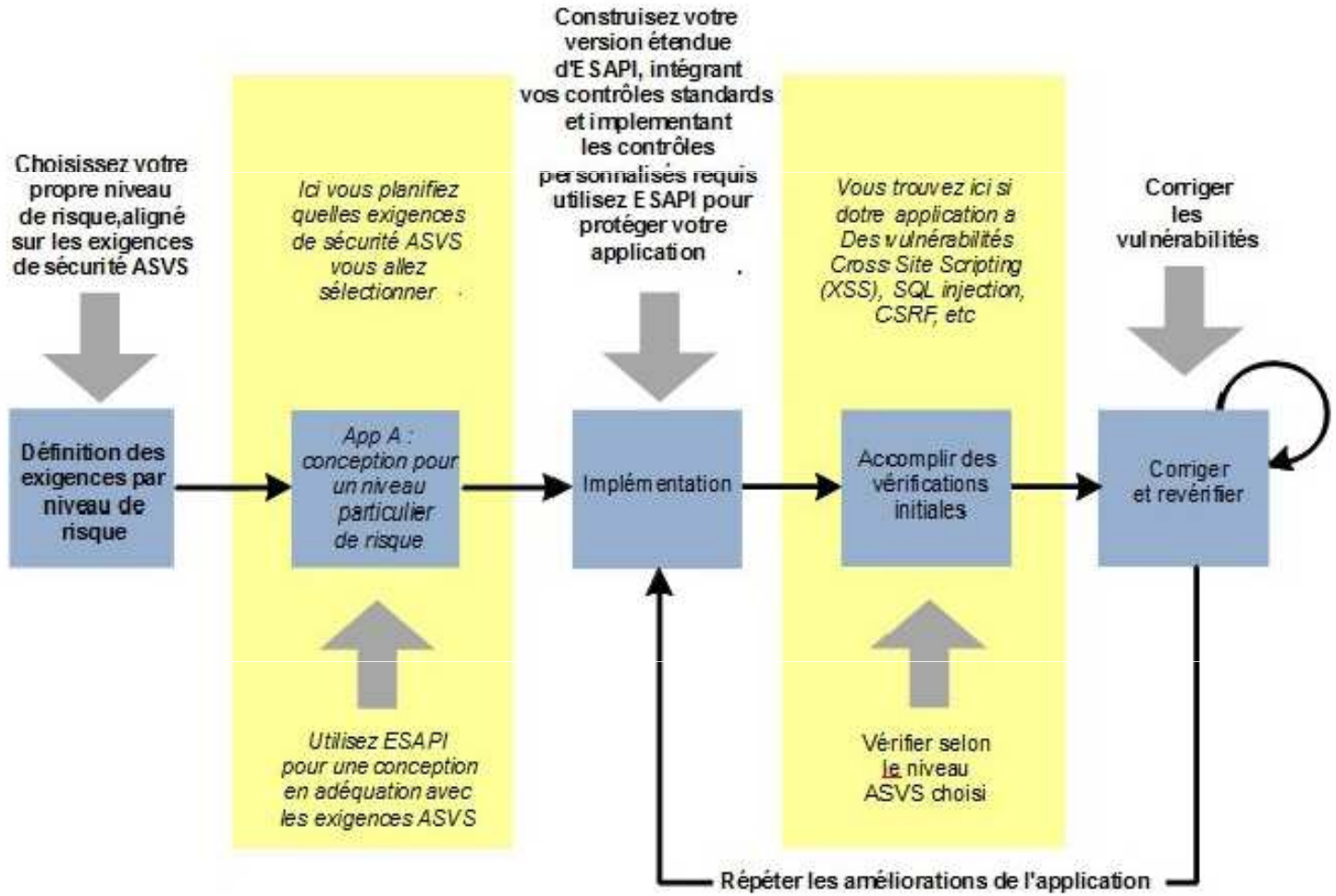


Niveau 4 en détail

- En plus du niveau 3, prise en compte du code des librairies et des frameworks



ASVS dans le Cycle de Vie des Développements



Les 14 familles d’exigences

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

Authentification

« Les exigences de vérification d'authentification définissent un ensemble d'exigences pour générer et
gérer les jetons d'authentification utilisateur de manière sûre »

Authentification

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.			✓	✓	✓	✓

Authentification

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.						✓

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 »

Gestion des sessions

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.			✓	✓	✓	✓

Gestion des sessions

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.						✓

Contrôle d’accès

« 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 »

Contrôle d'accès

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.			✓	✓	✓	✓

Contrôle d’accès

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.						✓