* Utilisation d’une mesure : fournir aux développeurs d'applications et aux propriétaires d'applications un critère permettant d'évaluer le degré de confiance qui peut être placé dans une application web.
* Utilisation d’un guide : fournir des conseils aux développeurs sur ce qu'il faut intégrer comme contrôles de sécurité afin de satisfaire aux exigences de sécurité des applications.

**Présentation Générale (Easy)**

Structure d’accueil

Sujet

* Présentation
* Contexte
* Problematique(s) et Objectif(s)

**Analyse et Conception**

Analyse (Pré analyse)

* Etat Art (Ok)
* Etude de l existant securite parlant de
  + existant en matiere d architecture
  + existant en matiere de procedure (processus de developpement)
  + existant technique (code)
* Parler des besoins de securite dans Hubso :
  + Que faut il securiser ?
  + Menaces et Vulnerabilites
* Critiques sur l existant en se basant sur le niveau de securite attendue et ce qui est fourni ou implemente par l exisant + Rapports d’audit doit pavoir des elements sur ce qui se fait en ce moment lors du developpement d’applications + ce qu il y a comme methodologie de developpement + mesures de securite en cours + failles de securite + recommendation + Evaluation des risques (Méthodologie d’evaluation des risques OWASP)
  + Critiques sur l architecture :
  + Critiques sur la methodologie de developpement : risque
  + Critiques sur la partie applicative (technologies, failles des frameworks utilises comme angular js par ex, les codes qui ouvrent des failles de securite cad mauvaises pratiques
* Propositions de Solutions
  + Definir des politiques de securite
    - Aspects organisationnels
      * sauvegarde + restauration
    - Facette processus
      * methodologie scrum mixed to security
    - Facette personnes (developpeur)
      * Guide des bonnes pratiques + politiques mots de passe + politiques de gestion des informations sensibles + politique de chiffrements + serveur d auth + pare feux
      * mettre en place les environnements securises framework applicant owasp + outils de securite)
* Mise en œuvre
  + Definir une architecture securisee type owasp ( repartition des serveurs + protocoles (prendre en compte les services externes et les web services internes )
  + Essayer de faire des remarques sur comment adapter le Processuss de developpement afin qu il puisse prendre en charge les considerations de securite (voir comment mettre en place un processus de developpement prenant en charge les risques de secutite mixed to scrum maybe + prendres des sources sur Article sur la modélisation Menace/risque disponible sur les sources suivantes <https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology> + <https://www.owasp.org/index.php/Threat_Risk_Modeling> + <http://www.fairinstitute.org/learn-fair> + <https://msdn.microsoft.com/en-us/library/aa302419.aspx>)
  + Guide des bonnes pratiques en se basant sur top 10
  + Mettre en place une application web JEE conforme au minimum au top 10 owasp
  + Mettre en place une application mobile JEE conforme au minimum au top 10 owasp

Conception

* Etat Art (Ok)
* Etude de l existant securite parlant de
  + existant en matiere d architecture
  + existant en matiere de procedure (processus de developpement)
  + existant technique (code)
* Critiques sur l existant en se basant sur le niveau de securite attendue et ce qui est fourni ou implemente par l exisant + Rapports d’audit qui doit avoir des elements + Ce qui se fait en ce moment lors du developpement d’applications + ce qu il y a comme methodologie de developpement + mesures de securite en cours + failles de securite + recommendation + Evaluation des risques (Méthodologie d’evaluation des risques OWASP)
  + Critiques sur l architecture :
  + Critiques sur la methodologie de developpement : risque
  + Critiques sur la partie applicative (technologies, failles des frameworks utilises comme angular js par ex, mauvaises pratiques)
* Parler des besoins de securite dans Hubso :
  + Que faut il securiser ?
  + Menaces et Vulnerabilites
* Propositions de Solutions
  + Definir des politiques de securite
    - Aspects organisationnels
      * sauvegarde + restauration
    - Facette processus
      * methodologie scrum mixed to security
    - Facette personnes (developpeur)
      * Guide des bonnes pratiques + politiques mots de passe + politiques de gestion des informations sensibles + politique de chiffrements + serveur d auth + pare feux
      * mettre en place les environnements securises applicant owasp + outils de securite (api de securite)
* Mise en œuvre
  + Definir une architecture securisee type owasp ( repartition des serveurs + protocoles (prendre en compte les services externes et les web services internes )
  + Essayer de faire des remarques sur comment adapter le Processuss de developpement afin qu il puisse prendre en charge les considerations de securite (voir comment mettre en place un processus de developpement prenant en charge les risques de secutite mixed to scrum maybe + prendres des sources sur Article sur la modélisation Menace/risque disponible sur les sources suivantes <https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology> + <https://www.owasp.org/index.php/Threat_Risk_Modeling> + <http://www.fairinstitute.org/learn-fair> + <https://msdn.microsoft.com/en-us/library/aa302419.aspx>)
  + Guide des bonnes pratiques en se basant sur top 10
  + API sécurité basée sur top 10
  + Mettre en place une application web JEE conforme au minimum au top 10 owasp
  + Mettre en place une application mobile JEE conforme au minimum au top 10 owasp

0