­­

PROJET SYNTHÈSE

IFT606 – Sécurité & cryptographie

Présenté à

M. Marc Verreault

M. Mohammed Ouenzar

Par

Kevin Boisvert – 16086334

Denis Ahmed Samson Abel

Jean-François Breton

Samuel Perron-Desrochers

UNIVERSITÉ DE SHERBROOKE

02 août 2018

# Description et buts du projet

# OWASP + description de ce qu’on a fait pour prévenir

* **A1-Injection** -> mettre «‘ or ‘’=’» dans login et password pour connexion
* **A2- Broken Authentication** -> Force users to use a strong password policy. Stored username and password values should be salted and hashed, in addition to being encrypted. An authenticated user of the site wants to let their friends know about the sale. The user e-mails the link above without realizing they are also giving away their session ID. When the friends use the link they use the user’s session and credit card. (https://hdivsecurity.com/owasp-broken-authentication-and-session-management)
* **A3-Sensitive data exposure** -> Password fields sont caches
* **A4-XML External Entities** ->
* **A5-Broken Access Control** ->
* **A6-Security Misconfiguration** ->
* **A7-Cross-Site Scripting (XSS)** ->
* **A8-Insecure Deserialization** ->
* **A9-Using Components with Known Vulnerabilities** ->
* **A10-Insufficient Logging&Monitoring** ->

# Distribution des rôles

# Outils utilisés