STI

Application de messagerie

Nikolaos Garanis, Nemanja Pantic

Vulnérabilités

- CSRF
  - Possible sur tous les formulaires
- XSS
  - Dans les messages envoyés
- Autorisation
  - Modifications des messages d'autres utilisateurs
- Simplicité des mots de passe
  - Absence de vérification sur leur complexité
- Authentification
  - Mot de passe pas demandé lors de son changement

Démo

CSRF via XSS Autorisation

Fix

- CSRF
  - Génération d'un token pour chaque affichage d'un formulaire
- XSS
  - Utilisation de la fonction PHP `htmlspecialchars()`
- Authentification
  - Demande du mot de passe (actuel) lors de son changement
- Autorisation
  - Vérifier que le destinataire du message est l'initiateur de la requête

Questions ?