Deux activités en lien avec la cybersécurité

NSI

23 mai 2023

Sécurisation des communications NSI1

Contenu

Contenu

But : Faire constater aux élèves ce qui est effectivement transmis au serveur lors de la validation d'un formulaire comportant des données sensibles.

Contenu

But : Faire constater aux élèves ce qui est effectivement transmis au serveur lors de la validation d'un formulaire comportant des données sensibles.

Lien avec le cours : Complètement en phase avec le volet IHM de première.

Contenu

But : Faire constater aux élèves ce qui est effectivement transmis au serveur lors de la validation d'un formulaire comportant des données sensibles.

Lien avec le cours : Complètement en phase avec le volet IHM de première.

Partie technique : Du HTML et du Javascript, très simple, une fonction de hachage est exposée *pour s'en servir*.

Contenu

But : Faire constater aux élèves ce qui est effectivement transmis au serveur lors de la validation d'un formulaire comportant des données sensibles.

Lien avec le cours : Complètement en phase avec le volet IHM de première.

Partie technique : Du HTML et du Javascript, très simple, une fonction de hachage est exposée *pour s'en servir*. Un travail d'observation des fonctions de hachage peut être fait avec la librairie standard de Python.

```
    function validateForm() {
let x = document.forms["myForm"]["fPassword"].value; // On
↪  récupère la valeur de "fPassword"

if (x.match("^(?=.*[a-z])(?=.*[A-Z])(?=.*[0-9])(?=.*[
↪  -/:-@\[-`{-~]).{8,16}$") == null)

    // la ligne du dessus verifie ci cette valeur correspond
↪  bien au motif désiré (voir plus bas)
{
    alert("Le mot de passe doit contenir une minuscule, une
↪  majuscule, un chiffre, un caractère spécial et " +
        "comporter entre 8 et 16 caractères.");
    document.forms["myForm"]["fPassword"].value = ""; // On vide
↪  le champ fPassword
    return false;
}
document.forms["myForm"]["fPassword"].value = SHA256(x); // Si
↪  le mot de passe est valable, on ne l'envoie pas
// on envoie son hash...
}
```

Le code de la fonction SHA256 figure après le code ci-dessus, pour observation par l'élève.

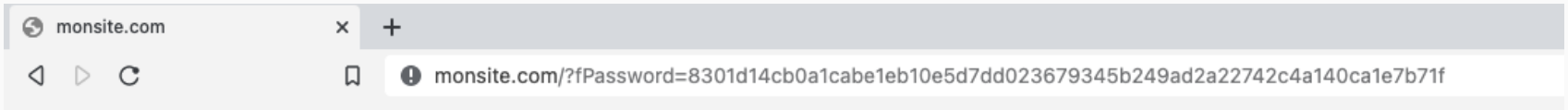
Le code de la fonction SHA256 figure après le code ci-dessus, pour observation par l'élève.

On valide le mot de passe...

Le code de la fonction SHA256 figure après le code ci-dessus, pour observation par l'élève.

On valide le mot de passe...

@



C'est son empreinte qui est transmise.

Sécurisation des communications NSI2

Contenu

Contenu

But : Faire connaître et utiliser les algorithmes de chiffrements.

Contenu

But : Faire connaître et utiliser les algorithmes de chiffrements.

Lien avec le cours : On fait comme le protocole HTTPS : une donnée est encryptées avec AES (encryptage symétrique), la clé de cryptage est encodée en RSA.

Contenu

But : Faire connaître et utiliser les algorithmes de chiffrements.

Lien avec le cours : On fait comme le protocole HTTPS : une donnée est encryptées avec AES (encryptage symétrique), la clé de cryptage est encodée en RSA.

Partie technique :

Contenu

But : Faire connaître et utiliser les algorithmes de chiffrements.

Lien avec le cours : On fait comme le protocole HTTPS : une donnée est encryptées avec AES (encryptage symétrique), la clé de cryptage est encodée en RSA.

Partie technique :

- utilisation de bibliothèques de cryptographie ;

Contenu

But : Faire connaître et utiliser les algorithmes de chiffrements.

Lien avec le cours : On fait comme le protocole HTTPS : une donnée est encryptées avec AES (encryptage symétrique), la clé de cryptage est encodée en RSA.

Partie technique :

- utilisation de bibliothèques de cryptographie ;
- on peut expliquer les algorithmes *sans les prouver* ;
- les élèves peuvent créer une petite UI.

Contenu

But : Faire connaître et utiliser les algorithmes de chiffrements.

Lien avec le cours : On fait comme le protocole HTTPS : une donnée est encryptées avec AES (encryptage symétrique), la clé de cryptage est encodée en RSA.

Partie technique :

- utilisation de bibliothèques de cryptographie ;
- on peut expliquer les algorithmes *sans les prouver* ;
- les élèves peuvent créer une petite UI.

Interface minimaliste créée avec `flet`.

D’autres pistes ?

Autres pistes

Autres pistes

- Travail en première sur les critères de sécurité d'un mot de passe.
- Est-ce que c'est possible de faire un fil rouge ?
- Explorer autour des cookies.
- l'homme du milieu.
- les certificats ?