

Quelques activités de NSI en lien avec la cybersécurité

Formateurs NSI Rennes

mai 2023

Ceci est une ébauche de travail basée sur ce que nous avons fait le lundi 22 mars. Dans la perspective des formations à dispenser, peut-être faut-il se contraindre à montrer que les contenus proposés s'intègrent dans le programme sans le surcharger et expliquer autant que possible la plus-value qu'elles peuvent apporter.

Lors de ces formations, il faudrait également pouvoir mettre les collègues en situation élève pour qu'ils découvrent une activité en la pratiquant : cela les implique davantage et démontre qu'elle est parfaitement faisable et, espérons-le, intéressante.

1 Considérations générales

Nous proposons ici des activités qui

- entrent dans le cadre du programme officiel, de sorte qu'elles peuvent être menées sans empiéter sur les temps de cours ;
- adoptent un positionnement raisonnable en terme d'équilibre culture / technique : d'une part, il ne faut pas revoir une notion déjà étudiée par le passé à moins d'y ajouter quelque chose d'essentiel, d'autre part les notions rencontrées peuvent être intimidantes du point de vue technique ou mathématique, on essaie donc de s'en abstraire sans dénaturer l'activité.

2 Observation contextualisée d'une fonction de hachage

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() {  
  // On récupère la valeur de "fPassword"  
  let x = document.forms["myForm"]["fPassword"].value;  
  
  // si cette valeur correspond bien au motif désiré (voir plus bas)  
  if (x.match("(?=.*[a-z])(?=.*[A-Z])(?=.*[0-9])(?=.*[-/:-@\\[-`{~]).{8,16}$") = null){  
    alert("Le mot de passe doit contenir une minuscule, une majuscule, un chiffre,  
    un caractère spécial et comporter entre 8 et 16 caractères.");  
  
    // On vide le champ fPassword  
    document.forms["myForm"]["fPassword"].value = "";  
    return false;  
  }  
  
  // Si le mot de passe est valable, on ne l'envoie pas, on envoie son hash...  
  document.forms["myForm"]["fPassword"].value = SHA256(x);  
}
```

FIGURE 1 – code Javascript de la fonction de validation du formulaire

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

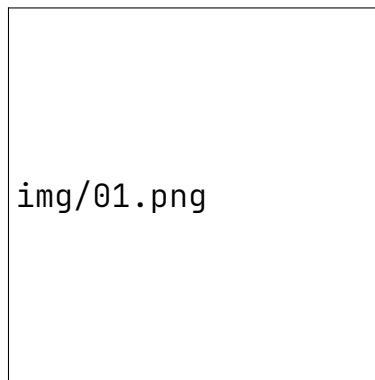
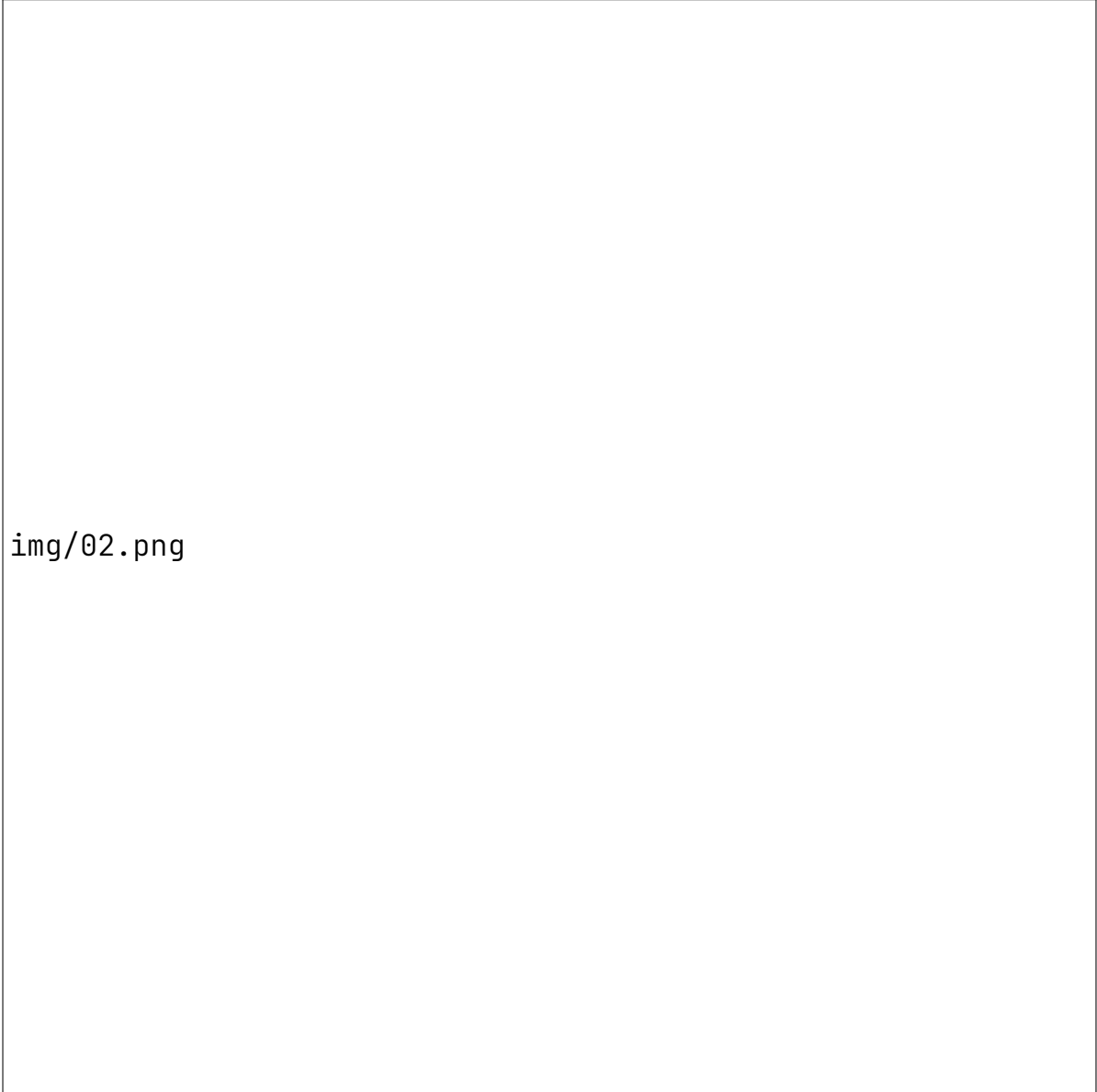


FIGURE 2 – validation du formulaire



img/02.png

FIGURE 3 – observation des données transmises *via* la méthode GET

3 Faire « comme HTTPS »

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 Interface graphique.

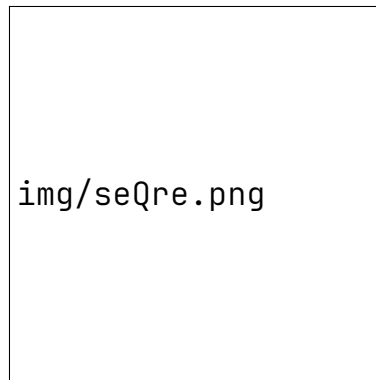


FIGURE 4 – interface minimaliste créée avec flet.

4 L'attaque de l'homme du milieu en débranché

Diffie Hellman avec des confettis ? Des paillettes ? Du sable ?
Diffie Hellman + homme du milieu
AES + homme du milieu RSA + homme du milieu

5 En plan

- 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 ?

RGS pour cookies

PSSI pour se former (long)

Chiffrer ou certifier est la réponse à l'homme du milieu ?

Man in the middle en débranché ?