**Titre :**

« Comment l’entête de réponse HTTP Content-Security-Policy peut sauver votre soirée en amoureux »

**Contenu :**

Cette « présentation » est dans le prolongement de la présentation « [Transformez votre navigateur en piège à pirate avec les en-têtes de sécurité http](https://www.youtube.com/watch?v=dvx-Gr9DO_8)» faites à la session 2022 de VOXXED. Elle a pour objectif de faire découvrir l’entête de réponse http Content-Security-Policy et, comment, il peut être utilisé pour réduire l’exploitabilité d’une vulnérabilité, de type injection HTML/JavaScript, de façon significative.

Cette présentation ne requiert pas d’avoir vu celle de 2022. En effet, le but sera de poser un contexte où un test de sécurité remonte une vulnérabilité de type « injection JavaScript » (aussi appelé [XSS](https://portswigger.net/web-security/cross-site-scripting/) et ici de type [Stored](https://portswigger.net/web-security/cross-site-scripting/stored)) avec une criticité haute sur une application. L’application en question étant importante pour la société dans la mesure où elle permet aux clients de passer des commandes de produits. Le responsable sécurité et le responsable métier mettent la pression sur les équipes de développement et d’infrastructure dans le sens où le premier veut que l’on fixe la vulnérabilité au niveau du code vulnérable et le second ne veut pas d’un nouveau déploiement car on est en période de solde et donc, aucune indisponibilité ou nouveau bug ne doit venir perturber les clients. La présentation montera, au travers de différent étapes successive, comment on peut utiliser l’entête de réponse HTTP Content-Security-Policy pour rendre la vulnérabilité difficile à exploiter et donc, par extension, diminuer son risque. Permettant ainsi de contenter les deux responsables selon leurs contraintes respectives et, ainsi, vous permettre de passer la soirée avec votre moitié.

**Abstract :**

Nous sommes le jour de votre anniversaire de rencontre, qui par le plus grand des hasards tombe un vendredi :

1. Le restaurant préféré de votre moitié est réservé !
2. Vous avez prévenu le restaurant de l’occasion et, tout est prêt, pour cette soirée importante pour vous deux !
3. Vos collègues sont au courant que, quoi qu’il arrive, à 16h00 « pétante » vous décollez !

Il est 10h, lors du point d’équipe…

Chef : « Le responsable sécurité a demandé à me rencontrer car nous avons reçu le rapport de l'évaluation de sécurité de l'application utilisée par notre client pour commander nos produits. Une vulnérabilité a été identifiée permettant d'injecter du JavaScript pour usurper la session de l'utilisateur ! C’est la panique car on doit déployer, mardi prochain à 06h00, la dernière version afin de proposer les dernières fonctionnalités pour la période de solde. »

Nous : « On ne savait même pas qu’une évaluation de sécurité était prévue…Sympa de prévenir… »

Chef : « Le responsable sécurité me demande de fixer maintenant et le responsable métier m’interdit de modifier la base de code avant la release de mardi. Je suis coincé, vous avez une idée ? »

Nous : « Nous avons entendu parler, durant un podcast, d’un entête de réponse HTTP appelé Content-Security-Policy, peut être que cela peut aider ? »

Chef : « Jetez-y un œil et faites-moi part des options possibles afin de nous sortir de là ! »

Notre conte de fée maléfique commence ici…

**Argumentaire :**

Cette présentation permet la découverte, via un cas concret et ludique, d'une fonctionnalité de sécurité supportée par tous les navigateurs modernes. Cela peut permettre à une équipe de développement de pouvoir, "trouver un compromis », dans le cas de la découverte d'une vulnérabilité côté navigateurs afin de ne pas décaler une mise en production. Les entêtes de sécurité HTTP, plus particulièrement, le Content-Security-Policy est un sujet encore mal connu des équipes de développements du point de vue de leurs existences et des leurs apports par rapport au volet exploitabilité d'une vulnérabilité.