XSS

Saviez-vous que votre site web pourrait être vulnérable à une attaque XSS ? Découvrez les conséquences effrayantes de cette menace et apprenez comment vous en prémunir avant qu'il ne soit trop tard.

Presentation Par DURIZOT Héléna

LE CROSS-SITE SCRIPTING

Est une faille de sécurité qui permet à un attaquant d'injecter dans un site web un code client malveillant. Ce code est exécuté par les victimes et permet aux attaquants de contourner les contrôles d'accès et d'usurper l'identité des utilisateurs.

Il en existe 3 types.

DOM CROSS-SITE SCRIPTING

REFLECTED CROSS-SITE SCRIPTING

STORED CROSS-SITE SCRIPTING

Presentation Par DURIZOT Héléna

DOM CROSS-SITE SCRIPTING

Abréviation de "Cross-Site Scripting basée sur le modèle de document" en français, est une technique d'attaque informatique visant à injecter et exécuter du code JavaScript malveillant sur une page web, en exploitant des vulnérabilités dans le Document Object Model (DOM) de la page. Contrairement aux attaques XSS traditionnelles qui ciblent directement le contenu HTML, les attaques XSS DOM-based se concentrent sur la manipulation dynamique du DOM de la page, ce qui les rend plus difficiles à détecter.

L'attaquant parvient à injecter du code JavaScript malveillant dans la page web, souvent en exploitant des entrées utilisateur non sécurisées, puis ce code est interprété et exécuté par le navigateur du visiteur, provoquant des actions non autorisées ou indésirables.

S’en prévenir ?

Il est essentiel de mettre en place des pratiques de sécurité appropriées, comme **la validation des entrées utilisateur** et **l'échappement de données** pour prévenir les attaques XSS DOM-based et protéger les applications web contre ce type de menace.

Presentation Par DURIZOT Héléna

REFLECTED CROSS-SITE SCRIPTING

Une technique d'attaque utilisée pour injecter des scripts malveillants dans des sites web, qui sont ensuite renvoyés aux utilisateurs via des liens ou des entrées de formulaire.

Lorsqu'un utilisateur clique sur le lien ou soumet le formulaire, le script malveillant s'exécute dans le navigateur de l'utilisateur, compromettant ainsi la sécurité du site ou volant des informations sensibles, telles que des cookies d'authentification.

Explication

Cette attaque exploite les vulnérabilités des sites web qui n'ont pas correctement validé et échappé les données entrées par les utilisateurs, permettant ainsi l'exécution de code non autorisé dans le contexte du navigateur de la victime.

Presentation Par DURIZOT Héléna

STORED CROSS-SITE SCRIPTING

À l’aide des cookies générés et reliés à chaque utilisateur, l’attaquant usurpe l’identité de sa victime et à donc accès à toutes informations possédés par celle-ci.

Présentation

Presentation Par DURIZOT Héléna

Contexte

Nous voici sur le site ordi-pas-cher.com

Ce site est de type PME (Petite et Moyenne Entreprise) L’entreprise est nouvelle sur le marché du Marketplace en ligne spécialisé en ordinateur et ne possède pas de ressources nécessaires qui lui permettrais d’avoir des mesures de sécurité robustes.

Qui est **Bob** ?

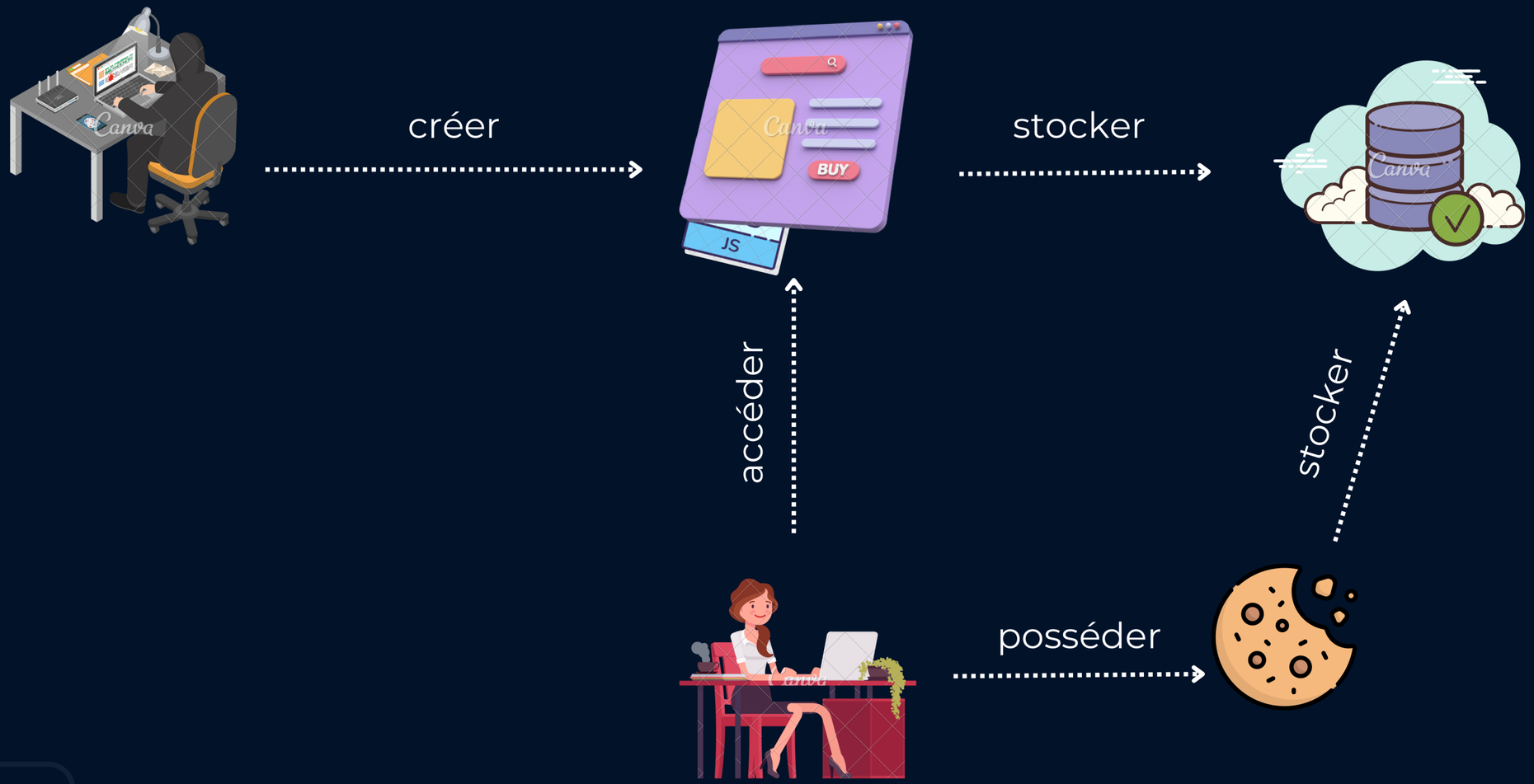
Ici il incarne un cyberattaquant ayant découvert une vulnérabilité à exploiter sur ordi-pas-cher.com , il exploiterais celle-ci en créant une fausse annonce juteuse pour attirer ses futures victimes en remplissant le formulaire d’annonce comme ceci.

Qui est **Alice** ?

Ici elle incarne notre victime qui est intéressé par l'annonce trafiqué de **Bob.**
Malheureusement pour elle lors de sa session de recherche elle tombe sur cette dernière et lorsqu'elle clique sur le lien pour voir les détails **sans le savoir** ses identifiants ont été envoyé à notre cyberattaquant, qui détient maintenant toutes les clés pour usurper parfaitement **Alice.**

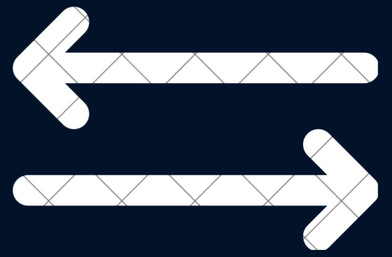
Comment ça se passe ?

Le plan



Comment ça se passe ?

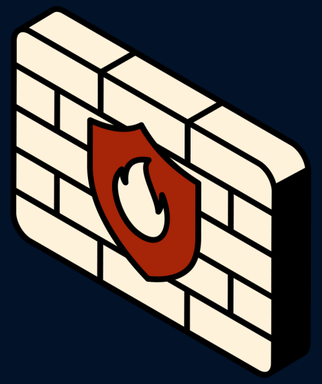
Après y avoir accéder



Sans le sans le savoir les cookies d'**Alice** ont été envoyés à **Bob**, qui peut maintenant prétendre qu'il est **Alice** sur le site et accéder au informations liés à son compte.

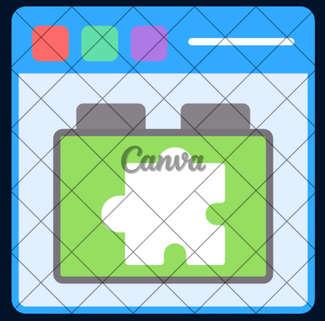
Presentation Par DURIZOT Héléna

Comment s’en protéger ?



Les pare-feu

Les pare-feu contre XSS sont conçus pour détecter et bloquer les tentatives d'injection de scripts malveillants dans le contenu web qui est envoyé aux utilisateurs.



Les plugins anti XSS

Les plugins anti-XSS servent à contrer ces attaques en identifiant, filtrant ou éliminant les scripts malveillants ou les données potentiellement dangereuses avant qu'elles ne soient rendues dans le navigateur de l'utilisateur.

La veille informatique

Elle consiste à surveiller activement les dernières tendances, les vulnérabilités, les outils et les techniques liées aux attaques XSS.

Presentation Par DURIZOT Héléna

Liens utilisé

https://www.youtube.com/watch?v=K43ur3cJ0Ps

https://www.youtube.com/watch?v=1Hr4_r2xQXY&t=17s

https://www.youtube.com/watch?v=cbmBDiR6WaY

https://www.youtube.com/watch?v=ABwS2MIxFPQ

https://youtu.be/GiqR9IXr_bU?t=304

Presentation Par DURIZOT Héléna

MERCI
ET FAITES ATTENTION À VOS