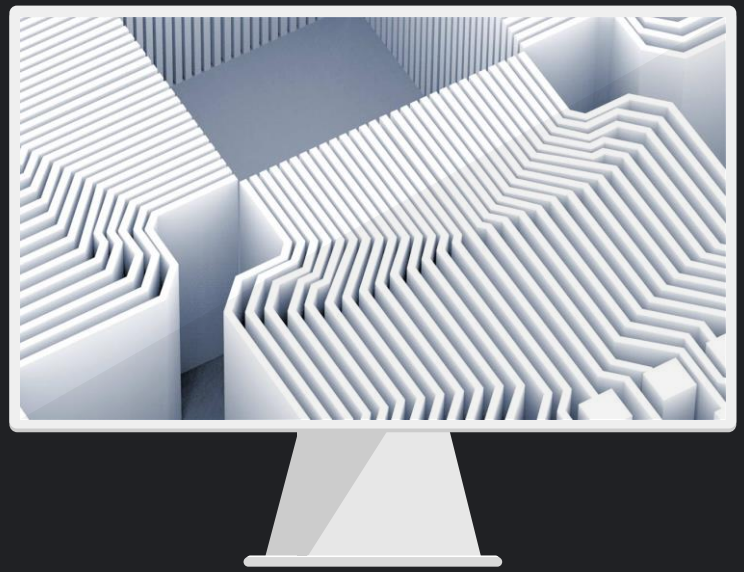
Cross-Site Scripting

Faille XSS

Sommaire



- Qu’est-ce que c’est ?
- Différentes attaques XSS
- Formatage / Exemple
- Déroulement d’une attaque
- Risques et Préventions
- Quiz

Qu'est ce que c'est?

- **Cross-Site Scripting est une faille de sécurité qui permet à un attaquant d'injecter dans un site web un code client malveillant.**

- **L'attaquant peut se servir du XSS pour diffuser un malware, réécrire le contenu du site, perturber des réseaux sociaux et hameçonner les identifiants ou la session d'un utilisateur.**

Source : NordVPN

3 types d'attaques XSS

Attaques XSS stockées

- La plus dévastatrice, le pirate va envoyer un contenu malicieux dans une application web, qui va le stocker, le contenu malicieux sera retourné dans le navigateur des autres utilisateurs lorsqu'ils iront sur le site.

Attaques XSS reflétées

- Les attaquants utilisent des liens malveillants, des emails de phishing et d'autres techniques d'ingénierie sociale pour inciter les victimes à effectuer une demande au serveur.

Attaques XSS sur le DOM

- L'attaquant manipule l'environnement du navigateur du client (Document Object Model) et place une charge utile dans le contenu de la page. La principale différence est que, puisque la charge utile malveillante est stockée dans l'environnement du navigateur, elle peut ne pas être envoyée côté serveur. De cette façon, tous les mécanismes de protection liés à l'analyse du trafic échoueront.

Source : Kaspersky

Formatage / Exemple

Quand vous naviguez sur un site de commerce électronique, une personne malveillante peut identifier une vulnérabilité qui permet d'intégrer des balises HTML dans la section des commentaires du site. Les balises intégrées deviennent ainsi un élément permanent de la page, ce qui amène le navigateur à les inclure avec le reste du code source chaque fois que la page est ouverte.

Nagios XI / 10 Mars

Source : cert.ssi.gouv.fr

Déroulement de l'attaque

Script /Champs de texte (par exemple : Forum)

Chargement de la page

Enregistrement du code malveillant dans la base de données.

Dès que la page est chargée, l'utilisateur exécutera le code à son insu

Risques

Redirection

- Le pirate redirige le client vers un site de phishing, ainsi lui octroyant des données personnelles.

Action sur le site

- Ruiner l'image du site, la sécurité étant faillible. Sa réputation sera endommagée.

Vol d'informations

- Avoir accès à vos données (typiquement cookies, clé de session, identifiants) lui permettant de les réutiliser / les vendre.

Facile d'utilisation

- Un simple script pourrait faire de gros dégâts.

Prévention

Utilisateurs

- Pas de confiance de l'utilisateur
- Navigateurs sécurisés, Logiciels mis à jour régulièrement permet également de limiter ces risques.
- Pare-feu

PHP

- Différentes fonctions php pour protéger ces champs
  - htmlentities()
  - htmlspecialchars()

Source : php.net / nordvpn

Quizz

- **http://take.quiz-maker.com/QQECMFQD6**

Déroulement de l'attaque

Script /Champs de texte (par exemple : Forum)

Chargement de la page

Enregistrement du code malveillant dans la base de données.

Dès que la page est chargée, l'utilisateur exécutera le code à son insu

Sources

- Kaspersky.fr
- Google Alerts
- Feedly
- ANSSI
- php.net
- nordvpn.net
- wikipedia.org
- cert.ssi.gouv.fr

Merci de votre écoute !