
Sécurité
Informatique

SOMMAIRE

Les différentes façon de tester ses applications

Afin de s'assurer du bon fonctionnement de notre application, il va falloir la tester. Pour cela différentes possibilités s'offrent à nous, ici nous parlerons des tests unitaires et fonctionnels.

Le test unitaire

Ce test nous permettra d'essayer des morceaux de code comme des fonctions en particulier afin de savoir si elles fonctionnent correctement. Le principe est d'isoler les parties de code pour vérifier l'attitude d'un objet et la logique. C'est en général lors de la phase de développement qu'on les met en place afin de s'assurer que le code fonctionne toujours correctement au fur et à mesure de l'avancée du projet. Il en sera de même pour les tests fonctionnels.

Le test fonctionnel

Un test fonctionnel est le test qui servira à tester automatiquement toutes les fonctionnalités de notre application, c'est-à-dire toutes celles qui étaient demandées dans le cahier des charges du projet. Par exemple, on pourra tester le fait qu'un membre puisse bien s'inscrire et se connecter correctement. Par ailleurs, au fur et à mesure que nous ferons évoluer l'application, les tests fonctionnels permettent de s'assurer que ces modifications n'impactent pas les autres fonctionnalités du site.

Les principales failles de sécurité d'un site web et comment s'en protéger

I - Les failles web les plus connues

La faille XSS

Une faille XSS consiste à injecter du code qui pourra être interprété directement par le navigateur Web. Ce dernier ne fera ainsi aucune différence entre le code du site et celui injecté par le pirate. Les effets sont bien entendu assez embêtants puisque vous risquez de faire face à des redirections vers un autre site, du vol de cookies ou encore une modification du code de votre page.

Pour vous protéger des XSS, vous devez remplacer les caractères pouvant être compris par le navigateur comme des balises par leur entité HTML. En procédant ainsi, le navigateur affichera mot à mot le caractère et ne cherchera plus à l'interpréter. En PHP, vous pouvez utiliser les fonctions htmlentities ou htmlspecialchar.

La faille upload

Cette faille peut apparaître lors de l'upload de fichiers sur un site : photo de profil, document pdf, image dans un message, etc. Elle profite de l'action effectuée pour mettre en ligne des fichiers malveillants PHP qui vont permettre au « hacker » de prendre le contrôle total de notre site.

Pour éviter cette vulnérabilité, il est important de :

- Empêcher les utilisateurs d'envoyer des fichiers lorsque cela n'est pas une fonction primordiale pour votre site ou application
- Interdire l'exécution de code depuis le dossier dans lequel sont stockés les fichiers uploadés sur votre site
- Vérifier et autoriser l'extension des fichiers que vous tolérez via une liste blanche

Injection SQL

Cette faille survient lors de la modification d'une requête SQL et consiste à injecter des morceaux de code non filtrés, généralement par le biais d'un formulaire. Cela revient à détourner la requête et lui faire faire autre chose que ce pour quoi elle a été conçue. Cette manipulation donne donc accès à vos données telles que les login, mots de passe ou adresses e-mail.

La faille include

Il s'agit d'une faille très dangereuse. Comme son nom l'indique, elle exploite une mauvaise utilisation de la fonction include. La plupart du temps, cette fonction est utilisée pour exécuter du code PHP qui se situe dans une autre page, permettant de se connecter à une base de données. Il existe deux type de failles include :

A distance : il s'agit de la faille include par excellence. C'est à la fois la plus courante et la plus facilement exploitable.
En local : cela revient à inclure des fichiers qui se trouvent sur le serveur du site. Une personne mal intentionnée pourrait donc s'emparer, assez facilement, de votre fichier contenant vos mots de passe.
Pour se protéger de cette faille, rien de mieux que de la tester ! Il vous suffit d'inclure une page qui n'existe pas. Si l'URL de celle-ci est vulnérable, un message d'erreur vous sera transmis venant de PHP.

II - Les failles humaines

En cybersécurité, il reste un phénomène contre lequel la meilleure solution de sécurité informatique au monde ne pourra jamais rien faire : l'erreur humaine.

Et pour cause, le facteur humain reste l'une des principales sources de cyberattaques en entreprise. On peut même souvent lire ou entendre que l'homme représente le maillon faible dans la chaîne de sécurité informatique.

L'utilisation d'une clé USB d'origine inconnue

Certains curieux ne vont pas hésiter à utiliser une clé USB trouvée par hasard afin de vérifier quels fichiers s'y trouvent. Un réflexe qui paraît complètement anodin, mais qui, en réalité, peut s'avérer dangereux.

Un cybercriminel peut facilement incorporer un fichier infecté au sein de cette clé USB afin de pénétrer le réseau d'une entreprise via le pc d'un collaborateur un peu trop curieux. Lui permettant ainsi d'accéder aux données confidentielles ou exploiter une faille et en faire profiter son réseau.

La revente de données sensibles

Aujourd'hui, l'information a une très grande valeur, notamment financière. Toutes les entreprises sont en possession de données sensibles et confidentielles qui peuvent susciter un grand intérêt, notamment de la part de certains concurrents.

Fabrication, schémas, plans, algorithmes, etc., nombreuses sont les informations pour lesquelles certains seraient prêts à offrir de l'argent. Et il est donc impératif pour une

entreprise de garder ces informations confidentielles. Et donc d'empêcher des collaborateurs en colère de céder à une impulsion criminelle et de saisir l'opportunité de revendre ce genre de données.

Le vol de données suite à un changement d'employeur

Autre exemple de fuite de données sensibles, les employés quittant une entreprise et emportant avec eux des fichiers confidentiels.

L'exemple le plus courant reste celui du commercial qui part pour la concurrence avec le fichier client de son ancien employeur. Un exemple basique, certes, mais qui correspond pleinement à ce que l'on peut appeler du vol de données.

L'impatience et la négligence de certains

Il faut impérativement avoir conscience que certains collaborateurs ne font preuve d'aucune patience avec l'outil informatique. Par exemple, nombreuses sont les personnes qui se passent des scans antivirus pour ne pas ralentir l'utilisation de leurs outils informatiques.

Autre exemple, tout aussi parlant, les personnes qui ne se sentent pas concernées par ce genre de sujets qu'est la sécurité informatique et qui ne respectent aucune consigne. Gestion des mots de passe hasardeuse, divulgation d'informations clés ou partage excessif de droits d'accès à des fichiers, ce type de comportement reste dangereux pour une entreprise.

Attention également aux dirigeants d'entreprise qui vont parfois se sentir « au-dessus » des problèmes de sécurité informatique et qui vont être les premiers à faire des erreurs ou à se montrer négligent.

C'est typiquement ce genre de profils qui va parfois encore plus loin en désactivant les mises à jour et les antivirus, affaiblissant la cybersécurité de leur entreprise sans réellement s'en rendre compte.

L'usurpation d'identité

L'usurpation d'identité arrive plus souvent et plus rapidement que l'on ne le croit. Il est arrivé, par exemple, que des hackers ou autres personnes malveillantes se fassent passer pour le dirigeant d'une entreprise par téléphone ou par mail afin de demander le transfert d'une grosse somme d'argent.

Autre exemple, celle du cybercriminel qui se fait passer pour un responsable IT et qui va demander les accès et mots de passe à un ou plusieurs salariés afin de pénétrer au sein d'un système. Prétextant ainsi un travail de maintenance ou la nécessité de ne pas se déplacer afin de gagner du temps.

Des exemples qui peuvent paraître trop gros pour être vrai, mais qui ont déjà coûté plusieurs millions d'euros à des structures dont les équipes ont été dupées.

failles, humaines, cybersécurité
Accéder à des contenus ou des sites à risques est très facile et très rapide sur le web aujourd'hui. Et de nombreux collaborateurs vont, sans le savoir, exposer leurs entreprises.

Comment ? Tout simplement en utilisant leurs ordinateurs professionnels pour aller sur un site de streaming ou télécharger des fichiers douteux, potentiellement malveillants.

Le silence des collaborateurs face à l'erreur

Aujourd'hui, un très grand nombre de collaborateurs passent sous silence les incidents qui ont pu survenir lors de leur utilisation de l'outil informatique.

Attaque, malware, escroqueries, beaucoup d'employés préfèrent taire de tels événements pour éviter toutes retombées ou remontrances. Exposant ainsi leurs structures à de potentiels dangers puisque rien n'est mis en place pour empêcher un programme malveillant de se propager.

Pour preuve, un récent sondage a révélé que dans près de 40% des entreprises mondiales, des salariés ont déjà gardé sous silence les incidents liés à la sécurité informatique (source : Kaspersky/ B2B international).

L'impact du BYOD (Bring Your Own Device) ou le fléau de l'utilisation d'appareils personnels

Saviez-vous que selon une récente étude, plus de la moitié des incidents de sécurité en entreprise proviennent de la perte d'appareils par les employés ?

On ne compte plus le nombre d'employés qui vont utiliser un appareil personnel pour accéder à des fichiers et données professionnelles. Smartphone, ordinateur et tablette vont ainsi être utilisés pour consulter un mail, lire un fichier ou accéder au cloud d'une entreprise.

Pourtant, ces appareils ne sont souvent pas sécurisés et peuvent donc être source d'importantes failles. Pire encore, si l'appareil est perdu ou volé, il est très facile de remonter aux informations professionnelles consultées si ces dernières n'ont pas été protégées.

Les erreurs classiques : SPAM et phishing

Faille la plus courante dans la sécurité informatique d'une entreprise, l'ouverture d'un spam reste une erreur qui se répète trop régulièrement.

On ne compte plus les collaborateurs qui, par curiosité, vont ouvrir les pièces jointes d'e-mail d'expéditeurs inconnus ou remplir les champs d'un formulaire frauduleux. Exposant ainsi leur entreprise à des failles dangereusement compromettantes.

Les bonnes pratiques à suivre pour sécuriser une application

Première bonne pratique : installer un pare-feu réseau et utiliser des DMZ

Mettre en place un pare-feu réseau est indispensable pour cloisonner les couches au sein de zones démilitarisées différentes (DMZ). Il est important de contrôler l'ouverture des flux sur ces pare-feu. Par exemple, il est absolument déconseillé d'ouvrir des flux depuis Internet vers la couche « données », cela irait à l'encontre de la sécurité du modèle 3 tiers car les couches « présentation » et « application » sont contournées.

Deuxième bonne pratique : chiffrer les flux

Il est aussi important de vérifier que les flux inter couches soient chiffrés à l'aide de protocoles tels que le HTTPS. Cela permet d'éviter des attaques de l'homme du milieu au sein de ce modèle. Il est à noter qu'il est très important de sensibiliser les utilisateurs à vérifier le certificat du site web. Cela permet d'éviter qu'un utilisateur se retrouve sur un site pirate.

Troisième bonne pratique : limiter les protocoles à risque

Certains protocoles fortement utilisés au sein des environnements Microsoft sont vecteurs de propagations virales. Par exemple, le protocole Netbios est à éviter au sein d'une infrastructure. Si toutefois, il faut ouvrir ce type de flux, il convient de parfaitement cloisonner les différents éléments et de mettre en place un plan d'actions en cas d'attaques virales (par exemple, la possibilité de pouvoir arrêter ce type de flux rapidement en cas de danger à l'aide d'un poste d'administration lui aussi cloisonné). La mise en œuvre d'IPS est aussi un moyen intéressant pour contrer les attaques qui pourraient être véhiculées par ce type de flux.

Quatrième bonne pratique : installer un pare-feu applicatif (WAF ou *Web Application Firewall* en anglais)

Cet équipement est déployé en amont de la couche présentation afin de filtrer les attaques applicatives potentielles, telles que des injections SQL ou les failles XSS.

Le pare-feu applicatif permet de se protéger contre les failles de l'OWASP (*Open Web Application Security Project* en anglais), qui est un organisme qui recense les dix risques de sécurité applicatifs les plus critiques sur Internet.

Cinquième bonne pratique : privilégier une authentification forte

Une authentification faible de type nom d'utilisateur et mot de passe pourrait permettre à un attaquant de réaliser une attaque par force brute et ainsi de pouvoir accéder à l'application directement depuis Internet. Néanmoins, certains logiciels libres comme *fail2ban* peuvent empêcher les attaques par force brute. Ce système surveille les journaux des applications et bannit les adresses IP qui ont un trop grand nombre d'échecs d'authentification.

Les sources à suivre pour rester informé sur les nouvelles failles

- https://vigilance.fr/?langue=1 (est l'une des sources francophones les plus utiles, avec des bulletins technologiques en français, une base assez complète et plusieurs flux RSS pour suivre les publications plus facilement).
- https://www.cert.ssi.gouv.fr/ (le centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques, qui dépend de l'ANSSI, est la base de données officielle française autour des vulnérabilités. C'est aussi une source indispensable de bonnes pratiques).
- http://www.livehacking.com/ (est la référence du Hacking éthique. C'est une mine de données et d'informations présentées sous un axe très hacker).
- l'extension daily.dev : https://chrome.google.com/webstore/detail/dailydev-news-for-busy-de/jlmpjdjjbgclbocgajdjefcidcncaied (extension permettant de rester informé sur les dernières nouveautés dans le domaine de la programation informatique)