Sécurité des sites et des applications web

I. Les différentes failles techniques possibles :

A. Failles serveur

■ SSRF : le Server-Side Request Forgery (SSRF 6) est l'équivalent, côté serveur, du CSRF. Il s'agit, pour un attaquant, de demander au serveur vulnérable d'effectuer des requêtes vers des destinations choisies par l'attaquant en profitant éventuellement des privilèges du serveur (par exemple, l'accès à un réseau privé) ;

Comme pour toute vulnérabilité faisant intervenir un contrôle sur les paramètres envoyés par le client, l'utilisation d'une liste blanche est privilégiée, c'est-à-dire n'autoriser que les ressources explicitées et refuser tout le reste. Il faudra alors définir :

Les noms DNS et/ou adresses IP autorisées
En l'absence de localhost et 127.0.0.1, cela empêchera l'accès aux services/fichiers du serveur.
L'accès illégitime au réseau interne sera empêché.
Les protocoles autorisés
L'utilisation de file://, sftp://, sera alors empêchée.

B. Failles au niveau du code

Exemples de vulnérabilités récurrentes et solutions :

■ XSS : une attaque Cross-Site Scripting (XSS 4) consiste en l'injection de données dans une page web dans le but de provoquer un comportement particulier du navigateur qui interprète cette page. Les données injectées ont la forme de langages interprétés par le navigateur tels que JavaScript ou HTML. Une attaque XSS cible les utilisateurs du site et vise en général à récupérer des secrets émis ou reçus par ceux-ci (sessions, coordonnées, mots de passe, informations bancaires, etc.), ou bien à effectuer des actions en leur nom ;

Pour se protéger contre les failles XSS, nous avons deux solutions principales, selon le contexte :

Supprimer tout contenu HTML de la saisie dans le formulaire
Neutraliser les caractères formant les balises HTML
Si on souhaite neutraliser les caractères formant les balises HTML de ce qui est récupéré lors de la saisie, nous pourrons utiliser l'instruction

"htmlspecialchars" dont le rôle est de neutraliser certains caractères (&, ", <...) en les remplaçant par leurs codes (&...) ou "htmlentities" dont le rôle est de modifier toutes les balises HTML.

■ CSRF : Cross-Site Request Forgery (CSRF 5) est une classe d'attaques qui force un utilisateur à exécuter, à son insu, des actions privilégiées sur une application tierce sur laquelle il est authentifié. Ce type d'attaques a lieu lors de la navigation sur un site piégé qui émet des requêtes vers un site de confiance, mais vulnérable au CSRF ;

Les exploitants de site peuvent également protéger leurs visiteurs : les agresseurs peuvent lancer des attaques Cross Site Forgery lorsqu'ils ont une connaissance précise des formulaires correspondants et des requêtes HTTP. Lorsqu'un facteur aléatoire entre en jeu, l'hacker doit généralement capituler. Le site Web peut, par exemple, produire un jeton unique (une séquence de caractères aléatoire) et alors l'insérer dans la requête HTTP. Lorsque le serveur reçoit une requête ne contenant aucun jeton valide (ou un jeton invalide), la requête est alors automatiquement rejetée.

Dans le cas des banques en ligne, un processus de double authentification est prévu : avant que l'utilisateur puisse exécuter un virement, il doit saisir un numéro de transaction (TAN) non disponible sur le site. Cette technique protège des CSRF, mais aussi d'autres attaques. En effet, même si un hacker parvenait à voler vos données d'accès, il ne pourrait pas exécuter de virement sans cette seconde authentification.

En théorie, l'en-tête référant offre une première couche de protection. Cette partie de la requête HTTP indique d'où provient la requête. Les sites Web peuvent ainsi filtrer les sources inconnues. Par le passé, l'en-tête référant a toutefois révélé des failles. Les extensions de navigateur, telles que les logiciels de blocage de fenêtres publicitaires, modifient ou suppriment l'en-tête référant. Les utilisateurs choisissant ce type de configuration ne peuvent alors plus exploiter l'offre du site.

■ SQLi : l'injection SQL (SQLi 7) consiste en la transmission de code malveillant parmi les données entrantes qu'un serveur web utilise pour formuler une requête à destination d'une base de données. Cette classe d'attaques occasionne une perte de contrôle sur les données en base, ce qui peut mener à leur exfiltration, altération ou suppression ;

Le bind des paramètres en PDO permet de se protéger de ces attaques.

■ LFI/RFI: Local/Remote File Inclusion ou faille d'include est une classe de vulnérabilités qui repose sur l'intervention de fichiers dont l'inclusion n'est pas prévue par l'application. Ces fichiers, qu'ils soient locaux à l'application (LFI) ou distants mais accessibles via celle-ci (RFI) peuvent être directement la cible de l'attaque s'ils sont confidentiels, ou bien être utilisés comme moyens d'attaque, dans le cas de l'inclusion de code par exemple.

Pour se prémunir des attaques LFI, il n'y a pas d'autre manière que de filtrer et valider les entrées utilisateurs. Il ne faut jamais inclure/exécuter directement une entrée utilisateur !

Pour le cas des RFI, il est possible de désactiver le support en passant la valeur des directives "allow_url_open" et "allow_url_include" à "Off".

Vous pouvez bloquer l'utilisation des wrappers en installant l'extension Suhosin pour PHP (sauf si "allow_url_include" = "On").

Les fonctions suivantes renverront "false" si un wrapper est utilisé dans le nom du fichier :
file_exists, is_file, filesize

■ XXE : les injections de type XML External Entity (XXE 8) reposent sur l'utilisation de fonctionnalités dangereuses de la spécification XML, qui permettent le chargement de données externes par l'interpréteur XML. Exploiter une XXE peut donc déboucher sur du LFI/RFI ou bien directement sur de l'exécution de code arbitraire.

Il existe un moyen de désactiver les entités externes dans tous les langages. Il s'agit généralement d'une balise binaire vrai/faux. Par exemple, dans un analyseur XML PHP, le code ressemblerait à ceci :libxml_disable_entity_loader (true) .

En conclusion :
La protection contre ces menaces passe à la fois par des mesures préventives de sécurisation des sites web, par leur maintien en condition de sécurité, par la mise en place de mécanismes permettant de détecter les tentatives d'attaques et par l'organisation régulière de tests d'intrusion et d'audits de sécurité.

II. Le facteur humain dans la sécurité informatique

90 % des cyberattaques et des violations de données résultent d'un comportement ou d'une erreur humaine, et non d'une défaillance technologique. (consultant Willis Towers Watson, 2017). La mobilisation accrue des employés peut permettre de remédier efficacement à la violation délibérée des protocoles de sécurité et de prévenir les incidents de sécurité causés par une négligence.

Pour être plus précis, une étude menée en 2016 a révélé que 22 % des violations de données étaient le résultat d'activités malveillantes d'employés, et 65 % de négligences.

Trois raisons courantes expliquant l'indifférence des employés à l'égard de la sécurité informatique.

1. Le changement de mentalités sur la propriété et la confidentialité des données : La Génération Y réutilise les mots de passe plus que tout autre groupe démographique, et 60 % acceptent les connexions avec des

inconnus « la plupart du temps ». 72 % de la Génération Y estiment que les données sur lesquelles elle travaille lui appartiennent.

2. Un sujet sensible et compliqué :
   La majorité des utilisateurs d'Internet ne comprend tout simplement pas les dernières normes et meilleures pratiques de sécurité. De plus, certains programmes de sécurité impliquent l'installation d'applications ou l'accès à des appareils personnels. Finalement, les employés se sentent mal à l'aise face à cette atteinte à leur vie privée.
   3. Une communication et une collaboration de mauvaise qualité avec les services informatiques : Les équipes informatiques ont beau élaborer les meilleurs plans de sécurité qui soient, leurs efforts restent vains si ces derniers ne sont pas compris du reste de l'organisation.

La cyber sécurité nécessite une approche en trois volets associant la technologie, les processus et les personnes.
En matière de protection des organisations contre les menaces internes et externes, promouvoir l'adoption d'initiatives de sécurité et de réduction des risques via une meilleure mobilisation des employés est l'un des meilleurs investissements qu'un responsable informatique puisse faire.

L’objectif est de pouvoir faire prendre conscience aux collaborateurs qu’ils sont eux aussi impliqués dans la sécurité et que la sécurité est l’affaire de tous au sein de l’entreprise.

Les outils de sensibilisation : happening de nuit qui imitent l’intrusion de voleurs d’informations et notent votre desk en fonction de son organisation et de sa sécurité, opérations de phishing factices pour entraîner les employés à les reconnaître ou tout simplement intrusion d’un étranger sans badges qui va parcourir l’intégralité des locaux.

La sécurité de l’information et sa gestion telles que mentionnées par la norme ISO/CEI : 27001 doivent être continuellement améliorées.

Pourquoi cette norme ? La norme fournit un cadre pour la mise en œuvre d’un système de gestion de la sécurité de l’information (SMSI). Elle vise à mettre en place un système de gestion de la sécurité dans l’entreprise et à assurer son amélioration continue selon le cycle « Plan – Do – Check – Act », dans un périmètre prédéfini.

La gestion basée sur les risques nécessite un engagement fort de la direction : non seulement pour valider ces risques, mais aussi pour fournir les ressources – financières, humaines et techniques – nécessaires à la mise en œuvre des plans d’action.

III. Tester ses applications

Le test d'intrusion externe simule le comportement d'un tiers malveillant n'ayant aucune connaissance préalable de votre Système d'Information et qui essaie d'y accéder depuis Internet. Ce test est communément appelé test en « black box » (boite noire). Cet audit est réalisé sans aucune information préalable délivrée par le client.
Pour les sites ou les applications qui requièrent une authentification, nous pouvons poursuivre les tests en mode « Grey Box » ou boîte grise qui consiste en l'utilisation d'un compte lambda fournit par le client et à partir duquel nous allons essayer d'élever nos privilèges et tenter d'accéder à des zones interdites afin de simuler des actes malveillants.

Le test d'intrusion interne consiste en la simulation d'actes malveillants qui pourraient être commis par un tiers connecté au système d'information de l'entreprise. Les profils de cette personne varient :
Consultant travaillant dans vos locaux à partir de son propre laptop et connecté à votre réseau (Lan / Wi-Fi)
Consultant utilisant votre infrastructure (matériels et ressources) pour réaliser sa mission ;
Stagiaire à qui vous avez confié un poste avec des droits restreints ;
Un utilisateur type de votre réseau.

IV. Les bonnes pratiques à suivre pour sécuriser

l'ANSSI, l'Agence nationale de la sécurité des systèmes d'information, publie régulièrement des "bonnes pratiques", afin de permettre aux administrateurs et architectes de votre SI de se tenir à jour régulièrement. Utiliser ces bonnes pratiques pour réfléchir sur les futures améliorations de l'architecture de votre SI.
Il est nécessaire de planifier une amélioration continue de l' architecture Systèmes et réseaux. Il faut donc être particulièrement vigilant sur les problèmes de conception à la base.

La CNIL, sur son site web demande une attention particulière sur 10 points :

- Appliquez une politique de mots de passe rigoureuse. Ne soyez pas la victime d'un pirate suite à une gestion trop laxiste des mots de passe. Auditez toujours la qualité de vos mots de passe, forcez par l'application de politique la robustesse et faites attention aux mots de passe par défaut des composants matériels et logiciels que vous intégrez ;

- Concevez toujours une procédure de création et de suppression des comptes utilisateurs. Ne laissez pas un ancien salarié mécontent, par exemple, s'en prendre à votre SI ;

- Sécurisez vos postes de travail. Ces terminaux sont les plus exposés, notamment parce que les salariés ne les emploient pas toujours comme un outil de travail. Vérifiez donc antivirus et logiciels d'intrusion ;

- Identifiez les accès à fichiers. Définissez toujours des politiques d'accès rigoureuses à vos différents services, afin que chaque personne ne puisse avoir accès qu'aux informations qu'elle doit manipuler ;

- Soyez vigilant sur la confidentialité des données, notamment vis-à-vis de vos prestataires ;

- Sécurisez votre réseau local. Appliquez des politiques de chiffrement des flux, mettez en place des pare-feux, des IDS. Contrôlez toujours les points d'accès à votre réseau ;

- Sécurisez vos accès physiques. Ce point rejoint le précédent. Vous ne pouvez pas garantir l'intégrité d'un système si tout le monde y a physiquement accès ;

- Anticipez les pertes et les divulgations. Avant même que cela ne vous arrive, prévoyez des mesures de sauvegardes, de protection par chiffrement, de destruction de vos anciens disques durs ;

- Anticipez et formalisez votre politique de sécurité des systèmes d'information. Nous en revenons toujours à la base. Il vous faut formaliser vos exigences en matière de sécurité ;

- Sensibilisez vos utilisateurs aux risques et à la "loi informatique et libertés".

V. Veille : Les sources à suivre pour rester informé sur les nouvelles failles

-

La veille sécurité s'attarde essentiellement sur les vulnérabilités. Ce sont ces dernières qui sont responsables de la réalisation de la menace. Un processus de veille s'analyse en une recherche méticuleuse des vulnérabilités.
Les vulnérabilités sont référencées et classées au niveau mondial. Il existe un système mis en place par le MITRE, organisation à but non lucratif américaine. Ce système est le CVE, pour Common Vulnerabilities and Exposures.

Il faut vous tenir au courant de tous les CVE, les qualifier vis-à-vis de votre système d'information et planifier des interventions, tout en prévoyant un suivi de vos

interventions. Vous pourrez vous aider pour cela d'un logiciel de gestion des correctifs, nous y reviendrons plus tard.

Vous pourrez consulter les bulletins les plus courants :
Les CERT, pour Computer Emergency Response Team, sont des centres d'alerte pour les attaques informatiques.

Les trois CERT français :

Le CERT-FR, centre gouvernemental de veille, d'alertes et de réponses aux attaques informatiques pour l'administration ;

Le CERT RENATER pour le secteur universitaire ;

Le CERT-IST pour l'industrie, les services et le tertiaire.

Le CERT de l'Union européenne : CERT-EU ;

Les autres CERT, comme les CERT étrangers :

maCERT, Direction générale de la sécurité du Maroc ;

CISA via le National Cyber Security and Communications Integration Center.

Les entités françaises réputées pour leur expertise, comme Vigilance d'Orange.

Sites sur la Cyber sécurité à suivre :

- Le CERT-FR
- L'ANSSI
- Zataz.com
- L'Usine Digitale
- Silicon.fr
- IT Security Guru
- Security Weekly
- Infosecurity

VI. Protection des données : RGPD

Le sigle RGPD signifie « Règlement Général sur la Protection des Données » . Le RGPD encadre le traitement des données personnelles sur le territoire de l'Union européenne.

Le contexte juridique s'adapte pour suivre les évolutions des technologies et de nos sociétés (usages accrus du numérique, développement du commerce en ligne…).

Ce nouveau règlement européen s’inscrit dans la continuité de la Loi française Informatique et Libertés de 1978 et renforce le contrôle par les citoyens de l’utilisation qui peut être faite des données les concernant.

Il harmonise les règles en Europe en offrant un cadre juridique unique aux professionnels. Il permet de développer leurs activités numériques au sein de l’UE en se fondant sur la confiance des utilisateurs.

En effet, le RGPD s’applique à toute organisation, publique et privée, qui traite des données personnelles pour son compte ou non, dès lors qu'elle est établie sur le territoire de l’Union européenne ou que son activité cible directement des résidents européens.
Ainsi, si vous traitez ou collectez des données pour le compte d’une autre entité (entreprise, collectivité, association), vous avez des obligations spécifiques pour garantir la protection des données qui vous sont confiées.