La sécurité informatique : focus sur les menaces les plus communes et leurs solutions

Nous avons publié en février un article résumant les principaux risques liés au manque de sécurité des sites internet. Il y était précisé que les pirates informatiques prenaient le contrôle des sites internet et de leurs serveurs par l'intermédiaire de failles dans le code source. L'exemple d'exploitation de faille dans cet article était l'énumération d'identifiants, mais ce n'était qu'une possibilité parmi de nombreuses autres, plus ou moins faciles à mettre en place mais toutes dangereuses.

On peut séparer ces menaces informatiques et les solutions pour s'en protéger en deux catégories : les problèmes de configuration, dont les sites sont responsables et qui facilitent grandement le travail des pirates, et les attaques en elles-mêmes qui utilisent notamment ces failles. Pour une protection optimale de votre site, il faut donc coupler une bonne configuration de sécurité de son site avec des outils externes couvrant toutes les éventualités possibles.

1. Mauvaises configurations de sécurité

1.1. Principaux cas observés et risques

Avant même de pouvoir parler d'attaques et d'outils de protection, il est important de se pencher sur la configuration de sécurité même du site. En effet, de nombreux problèmes peuvent être réglés à ce niveau. De trop nombreux sites ont encore de mauvaises configurations de sécurité sur leurs composants tiers ou réseau, leurs comptes utilisateurs, leurs fichiers, entre autres. Les pirates utilisent alors les failles pour obtenir des accès frauduleux ou acquérir des connaissances sur le système.

1.1.1. Utilisation de composants avec des vulnérabilités connues

On peut citer deux problèmes majeurs liés à un manque de sécurité dans la configuration du site. Le premier est l'utilisation de composants avec des vulnérabilités connues. Il existe de nombreuses situations pouvant y mener (manque d'information, de temps, de ressources, perte de contrôle sur le développement du site…). Or, c'est laisser la porte de votre site ouverte aux pirates ! Même si ce point paraît trivial et évident, il faut donc y faire attention.

De plus, même si un composant n'est pas vulnérable à un moment donné, il pourra ne plus l'être dans le futur. Un état de sécurité doit donc toujours être considéré comme temporaire.

1.1.2. Manque de contrôle des accès au niveau fonctionnel

Le deuxième problème majeur concernant la configuration est le manque de contrôle des accès aux fonctions. Le concept est le suivant : un programme web se base sur des échanges entre le client (navigateur) et le serveur hébergeant le site internet. L'échange peut également passer par des

services tiers, les fameux webservices (par exemple, un connecteur de paiement). Si les accès aux fonctions du serveur ou du webservice sont mal contrôlés, un pirate pourra mettre la main dessus et utiliser ces fonctions à sa guise. En conséquence, le pirate pourra avoir accès à une base de données, effectuer de la fraude au paiement, faire tomber un site…

1.1.3. Exposition des données : un risque majeur

Comme on l'a vu, l'un des risques majeurs est l'exposition de données sensibles telles que les informations confidentielles de la société et celles touchant son réseau interne, les données clients… Les conséquences peuvent être catastrophiques, pour l'image de l'entreprise, son business, et également pour ses clients eux-mêmes.

1.2. Configuration : les bonnes pratiques pour sécuriser votre site

Pourtant, quelques règles simples dans la configuration du site permettent d'acquérir un niveau de protection développé :

- Mise à jour régulière des composants du site (logiciels et librairies) pour éviter l'utilisation de composants avec des vulnérabilités connues.
- Protection des données :
  - La création d'une politique claire de sécurité, avec un classement par criticité des données et une protection adaptée à chaque niveau permet d'éviter les pertes graves de données
  - Le « Store only what you need » (stocker uniquement des données strictement nécessaires au fonctionnement du site sur les machines exposées) diminue les risques en cas d'intrusion
  - Le chiffrement des données permet de ne pas perdre d'informations en clair en cas d'attaque
- Protection des accès :
  - La mise en place de droits stricts sur les comptes utilisateurs, les fichiers, les fonctions, etc… et le filtrage des accès par IP ou login/mot de passe sont nécessaires
  - L'utilisation de mots de passe forts, couplée à un changement régulier de ceux-ci, évite qu'ils soient devinés facilement
- Sécurité entre le navigateur et le serveur :
  - L'utilisation de protocoles chiffrés (HTTPS) permet d'éviter la mise sur écoute des requêtes entre votre serveur et le navigateur client
  - Il ne faut jamais faire reposer sa sécurité sur le navigateur, et toujours tout gérer du côté serveur. Cela rend votre site bien moins accessible aux pirates.
- Ne pas négliger la sécurité des pages inutilisées

2. Les attaques

Malgré la mise en place de ces bonnes pratiques, des attaques diverses peuvent toujours avoir lieu. Si leur but est, ici également, du vol de données (surtout celles des utilisateurs), les techniques, elles, diffèrent. Nous allons maintenant détailler quelques-unes de ces attaques les plus répandues sur le web.

2.1. Violation de gestion et d'authentification de session

Ce type d'attaque consiste à accéder, sur un site internet, à une session d'un autre utilisateur ou à un compte administrateur, et donc d'avoir accès à des informations sensibles voire même à toute la base de données du site. Ces attaques se basent sur l'utilisation de la session en elle-même, via un mot de passe trop faible ou bien un jeu sur l'association cookies/identifiant du compte par exemple. C'est en se connectant sur ces comptes auxquels il n'a pas accès que le pirate récupérera des données.

Nous allons préciser dans les points suivants deux types de méthodes pour obtenir ces résultats.

2.1.1. Les injections

Ce sont les attaques les plus communes car elles sont très simples et très dangereuses. Dans un formulaire d'authentification sur un site, un pirate renseignera à la place du mot de passe par exemple une requête en langage SQL (le plus souvent). Celle-ci, si elle n'est pas bloquée, sera envoyée au serveur et lui permettra d'accéder au compte dont il a rentré l'identifiant (par exemple 'admin'), sans avoir besoin du mot de passe. L'attaquant pourra donc potentiellement avoir accès à tous les autres comptes, donc à toute la base de données !

2.1.2. Références Directes non Sécurisées à un Objet

Là encore, le pirate pourra avoir accès à n'importe quel compte, mais par l'intermédiaire de l'URL. Il y a un risque si celle-ci affiche en clair le numéro d'identifiant du compte connecté, et que le site n'a pas assez contrôlé ses droits de session. L'attaquant changera alors simplement le numéro d'identifiant à la fin de l'URL par exemple de 34 à 35, et aura accès aux informations du compte 35 qui n'est pas le sien.

2.2. Le Cross-Site Scripting (XSS)

Très simples à mettre en place, ces attaques ont pour but d'infecter les visiteurs d'un site. Le concept est le suivant : le pirate, s'il n'en est pas empêché, va placer sur ce site du langage informatique pur, souvent du Javascript, afin que celui-ci soit lu et interprété par le navigateur des visiteurs. Le simple fait qu'ils soient sur la page leur fera, par exemple, télécharger un virus afin que le pirate puisse utiliser leurs ressources, ou voler leurs cookies et autres données. Cela peut être transparent, et si personne ne s'en rend compte, l'attaque peut rester active sur de longues durées.

2.3. Les attaques trompant le visiteur

2.3.1. Falsification de requêtes intersite (CSRF)

Cette faille affecte les sites dont les fonctionnalités sont connues, comme les applications web open source (Wordpress) ou les services ouverts au public (Facebook, Gmail…). Si un visiteur est connecté sur l'application et qu'il va sur un site maîtrisé par un pirate, puis clique sur un certain lien, alors le pirate enverra vers le compte de l'utilisateur, sur l'application vulnérable, une requête malveillante. Il aura cette possibilité justement parce qu'il connaît tous les paramètres à inclure dans la requête, et que l'application l'acceptera comme l'une des siennes. Les conséquences peuvent aller du changement de mot de passe au vol total d'une base de données.

2.3.2. Redirections et Renvois non validés

De la même manière, ces attaques trompent le visiteur d'un site. Le pirate va utiliser une redirection légitime du site, qui renvoie normalement de l'une de ses pages vers une autre, pour transférer le visiteur sur un site que le pirate contrôle, simplement en changeant l'URL de redirection. Ce site « pirate » est souvent à l'image du site initial afin que le visiteur ne se doute de rien et renseigne des informations, que le pirate pourra alors exploiter.

3. Les solutions

Chez NBS System, nous avons un ensemble de règles que nous estimons vitales pour assurer la sécurité d'un site. C'est pourquoi notre Cloud de très haute sécurité CerberHost protège les sites à 99% contre les attaques les plus communes du web que nous avons citées ci-dessus. Voici nos solutions principales.

3.1. L'audit applicatif intrusif pré-production

Nos experts en sécurité réalisent, avant toute mise en production, un audit très minutieux du code du site. Ils recherchent particulièrement les failles « classiques », afin que les développeurs puissent les réparer. C'est notamment l'un des moyens de se protéger des failles et attaques suivantes :

- Toutes les mauvaises configurations de sécurité : les failles seront repérées en amont de la mise en production, et donc réparées avant que le site ne soit accessible au public.
- Falsifications de requêtes intersite : en plus de l'audit initial, il est de bonne mesure d'ajouter des paramètres aléatoires (aléas) dans chaque requête, afin que l'application n'accepte plus les requêtes envoyées par le pirate.
- Redirections et Renvois non validés : de même, en plus de l'audit il est conseillé de limiter le nombre d'URL de redirections possible afin que les pirates ne puissent pas en créer d'autres.
- Cross-Site Scripting
- Références Directes non Sécurisées à un Objet : l'audit repère les failles de manque de contrôle d'accès, afin de mettre en place une configuration de sécurité efficace couplant cookies/session/droits des utilisateurs vérifiant la légitimité de l'accès à une fonction. En parallèle, il est également conseillé de référencer les comptes avec des identifiants complexes, comme JRFkln01f2458 par exemple.

3.2. Le pare-feu applicatif NAXSI

Le pare-feu applicatif NAXSI, développé par NBS System, offre également une protection supplémentaire contre beaucoup de menaces web. Il contrôle notamment les requêtes HTTP, et bloque celles qui lui semblent malveillantes, afin de protéger les sites notamment contre :

- Injections SQL : interdiction des requêtes comprenant des caractères ou mots utilisés dans le langage SQL. En plus de cette protection, le Cloud sécurisé CerberHost possède également un analyser spécifique au SQL, qui enregistre et analyse toutes les requêtes. Si l'une d'entre elles renvoie un volume anormal de données, alors la requête sera conservée et bloquée.
- Cross-Site Scripting : interdiction des requêtes comprenant des caractères ou mots utilisés dans le langage Javascript

NAXSI est également équipé de l'outil Fail2ban, un anti-bruteforce qui empêche les requêtes répetées et limite le nombre de requêtes/échecs par seconde. Cela protège notamment des violations de gestion et d'authentification de session en général.

Ces deux caractéristiques couplées permettent de protéger efficacement les sites contre d'autres attaques :

- Mauvais contrôle des accès aux fonctions, par le blocage des tentatives de contournement du navigateur
- Références Directes non Sécurisées à un Objet, par la limitation des objets facilement accessibles.

Autre point important : NAXSI, grâce à son système de reconnaissance et d'analyse d'IP, repère celles qui sont douteuses ou malveillantes et les bloque tout simplement. Cela ajoute, entre autres, une protection de plus contre les mauvais contrôles des accès aux fonctions, puisque les IP malveillantes n'auront de toute façon pas accès aux fonctions même si celles-ci sont mal configurées.

3.3. Bilan : les protections de CerberHost

Ainsi, le couplage de l'audit intrusif de pré-production, de NAXSI et d'autres outils inclus sur l'offre CerberHost (non présentés dans ce document) permet de protéger les sites hébergés sous CerberHost de la majorité des attaques. Le Cloud propose également quelques protections de plus :

- Mise en place d'une double authentification contre les violations de gestion et d'authentification de session
- Choix ou validation du mot de passe par les experts de NBS System, pour éviter également ces violations ainsi que l'exposition de données sensibles en général
- Imposition par défaut de droits stricts sur les fichiers, pour une meilleure configuration de sécurité par défaut
- Transferts en protocoles sécurisés (ex : HTTPS), par défaut pour une meilleure protection des données
- Renforcement des Systèmes d'Exploitation par de nombreux plug-in ; ils vont s'auto-protéger contre la majorité des attaques
- Application permanente de corrections et patches par l'équipe R&D de NBS System, qui effectuent une veille sur les nouvelles attaques et failles pour une réactivité maximale

Pour vous renseigner plus en détails sur chacune de ces failles ou attaques, et mieux étudier leurs solutions, rendez vous sur le blog NBS System où vous retrouverez des articles détaillés sur chacun des points évoqués.

Pour plus d'information, contactez NBS System : communication@nbs-system.com
Myriam Fiévé - 01.58.56.25.99
Lucie Saunois – 01.58.56.60.84