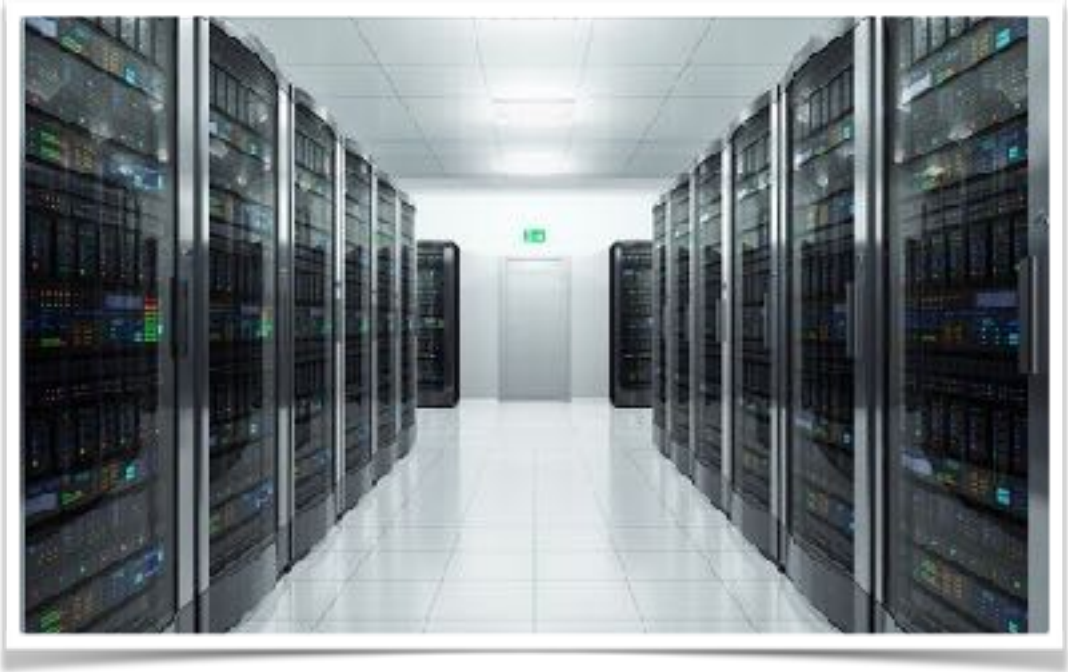
Hébergements

ce qu'il faut savoir



Que fait l'hébergeur pour vous ?

Beaucoup pense que c'est juste une machine quelque part ou l'on pose ces dossiers. un serveur c'est un gros cloud.

Et bien non pas seulement ...

Effectivement l'hébergement sert à stocker les fichiers et dossiers qui contient votre site internet. Mais pas uniquement, il est composé de trois grandes parties qui rendent votre site lisible sur le web.

1

DOMAINES

rendre compréhensible votre nom de domaine

2

WEB

rendre vos fichiers interprétables sur la toile

3

SÉCURITÉ

éviter et neutraliser les attaques que subissent les sites

Failles XSS

XSS (plus officiellement appelée Cross-Site Scripting) est une faille permettant l'injection de code HTML ou JavaScript dans des variables mal protégées.

Failles CSRF

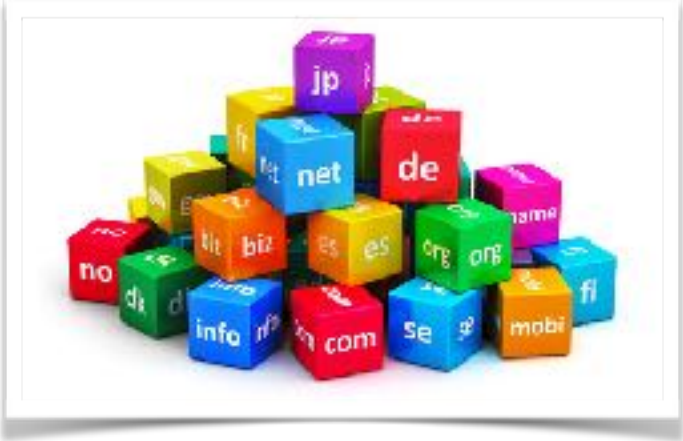
La faille CSRF ("Cross site request forgery") est très souvent assimilée à la XSS alors que ces deux failles sont diamétralement opposées. Quand la XSS cherche à dérober des informations personnelles de l'utilisateur, la CSRF cherche à lui faire exécuter des actions à son insu directement sur son ordinateur.

Injection SQL

C'est une méthode d'attaque très connue. Il consiste à modifier une requête SQL en injectant des morceaux de code non filtrés, généralement par le biais d'un formulaire.

1. Domaines

Un nom de domaine est un « masque » sur une adresse IP. Le but d'un nom de domaine est de retenir et communiquer facilement l'adresse d'un ensemble de serveurs (site web, courrier électronique, FTP). Par exemple, cebb-innovation.eu est plus simple à mémoriser que 65.128.39.40



Mais comment les navigateurs web savent quelle est mon adresse IP ? »

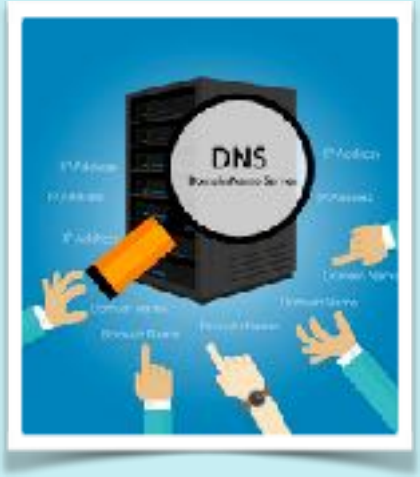
C'est là qu'interviennent les serveurs DNS. Ils sont partout sur le web et reçoivent des requêtes de noms sans arrêt. Quand vous ouvrez votre navigateur et que vous tapez : cebb-innovation.eu et que vous tapez ensuite "entrez" , votre ordinateur envoie de nombreuses requêtes à plusieurs serveurs DNS en leur demandant qui connait l'adresse IP correspondantes à ce nom. Dès qu'un serveur lui répond, le navigateur sait qu'il doit aller sur le réseau 65.128.39.40 et récupère les fichiers et dossiers qui y sont présents et vous les affichent.

Bien évidemment votre hébergeur doit faire connaitre votre ip de domaine et l'avoir transmis à un nombre des serveurs conséquents pour que votre site s'affiche le plus vite possible. Cette opération a besoin d'être effectuée très régulièrement car des serveurs de DNS se créent et disparaissent régulièrement.

LIAISON DOMAINE ET SERVEURS DNS

Les noms de domaines sont achetés et réservés pour une durée minimale d'un an et renouvelables. Par conséquence, la liaison subit les mêmes contraintes.

De plus chaque domaines possède une quantité d'espace disque et de bande passante bien définie qui lui servent à alimenter et réguler son traffic.



2. Web

Cette partie comprend votre site internet mais pas seulement il y a énormément de données et de paramètres qui ont besoin d'être configurer pour que votre site internet soit visible et lisible par les navigateurs web.

Il y a entr'autre :

1- Un compte qui gère les fonctions de votre hébergement,

2- Le gestionnaire de fichiers pour interpréter le code source de votre site coté serveur

3- Les comptes FTP pour pouvoir envoyer des fichiers sur le site

4- Les systèmes de sauvegardes pour que votre site puisse être disponibles même en cas de panne du serveur

5- Le système de gestion de base de données

6- Les comptes de messagerie

7- Les systèmes de logs pour connaitre les visiteurs, les types de requêtes envoyées …

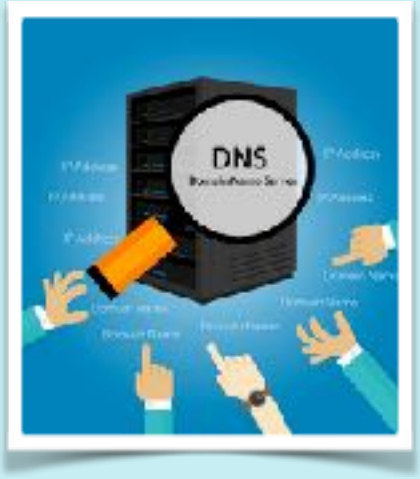
8- Les pages d'erreur 501-505-401-404

9- Le services de mise à jour du site

AUTRES FONCTIONS

La plupart des autres fonctions pour le web sont un lien entre les serveurs et le site pour la gestion des sous domaines, des domaines parqués, les alias de domaines et les redirections.

C'est d'ailleurs le cas pour les domaines en .fr, .com et .net du site cebb-innovation.eu qui redirige tous vers celui-ci.



3. Sécurité

Cette partie est totalement invisibles pour les clients des hébergeurs et pourtant dès qu'il y a un problème, cela vient presque toujours de là.

Comme pour le chapitre précédent, nous allons voir ce qui est utilisé pour protéger un site internet et son hébergement.

Il y a entr'autre :

1- La confidentialité des répertoires

2- Le système de chiffrement des messages envoyés et reçus

3-Authentification de mails

4- Système de contrôle des "flags" de mails et de fichiers

5- Chiffrement de toutes les données d'échange serveur-clients

6- Logiciels de statistiques avec alertes de routines ou sur-exposition

7- Logiciels de lecture de connections simultanées et d'utilisation de UC du serveur

8- Contrôle des Accès SSH

9- Bloqueur d'adresse IP

10- Possibilité de mettre en SSL ou TLS les données, les connections et le site

11- Logiciel anti-Hotlinks (évite de se faire prendre sa bande passante sur les images)

12- Logiciel de protection anti Leeching (idem hotline mais pour les codes source et fichiers)

13- Scanning journaliers des fichiers

14- Gestionnaire d'utilisateurs pour éviter de laisser n'importe qui se connecter au site

15- Logiciels et scanner anti failles (XXS, Include, Upload, SQL, CSRF, CRLF, Force brute, session, Buffer overflow ….)

Pour résumer, comme vous pouvez le voir l'hébergement d'un site internet ce n'est pas que mettre des fichiers sur un ordinateur et puis mettre à jour des textes et des images.

Si vous avez des questions sur ce document,

n'hésitez pas à me contacter à l'adresse mail suivantes : contact@paint-design.fr

Merci d'avoir pris le temps de lire ce document et bonne journée à vous.