TD2 : attaques logicielles

Exercice 1 :

1) Un site Web offre une interface d'inscription pour recevoir les nouveautés du site. Un utilisateur qui tape une adresse de la forma *@*.* est automatiquement accepté (* représente un ensemble de caractères). Donner une attaque exploitant ce formulaire et l'expliquer?

Etape 1	Etape 2	Etape 1

2) Un site Web offre l'interface d'inscription suivante où un nouvel utilisateur doit remplir la quatrième zone de texte en utilisant les caractères affichés sous un format difficile à trouver d'une façon automatique (par un ordinateur). Précisez l'utilité de procéder ainsi pour l'inscription des utilisateurs ?

1) Donner deux vulnérabilités de ce programme C et les expliquer à l'aide d'exemples.

```
int main(char* argc, char** argv)
 {
   char cmd[100] = "/usr/bin/cat "; // commande « cat »
   char filename[20];
   strcpy (filename, argv[1]);
   strcat(cmd, filename);
   system(cmd); // appel système
}
```

Exercice 2

2) Soit le bout de code BC1 suivant implémenté au niveau d'un serveur. Expliquer comment un client peut exploiter ce code pour lancer une attaque ? Donner deux conséquences possibles.

BC1 :

```
Void mycopy (char * input) {
char buffer[20];
strcpy(buffer,input);
}
int main(int argc, char * argv[]) {
    mycopy(argv[1]) ;
}
```

3) Soit le bout de code BC2 suivant implémenté au niveau d'un serveur. Expliquer comment un client peut exploiter ce code pour lancer une attaque ? Comment peut-on améliorer ce code pour le rendre sécurisé?

BC2 :

```
$login = Request.Form("login")
$password = Request.Form("password")
SELECT * FROM users WHERE Login=$login AND Password=$password
```

Exercice 3 [4pts]:

Nous nous intéressons à l'évaluation du risque d'un site web d'une entreprise. Pour simplifier le travail, nous considérons une seule attaque qui ne peut être lancé que par des entités (utilisateurs Internet) ayant des compétences réseaux et logiciels. Ces entités cherchent à nuire aux propriétaires du site web plutôt que d'avoir des récompenses. L'exécution de l'attaque ne nécessite aucun droit d'accès et aucune ressource. Bien qu'aucune information sur le point faible à exploiter par l'attaque ne soit disponible et que les propriétaires du site avaient mis en place des détecteurs d'intrusions incorporés dans l'application, il est facile de déterminer et d'exploiter ce point faible.

Comme conséquences de l'attaque en question, de nombreuses données critiques peuvent être divulguées ou corrompues. Cependant peu de services, jugés secondaires, seront interrompus et les propriétaires du site auront probablement une certaine traçabilité sur ce qui s'est passé. Sur le plan d'affaires, l'attaque peut causer des effets significatifs sur les bénéfices annuels et peut endommager la réputation de l'entreprise. De plus, une violation haute de la conformité des services du site ainsi qu'une atteinte aux vies privées de milliers de personnes seront observés.

Questions :

En se basant sur la méthode OWASP, déterminer la gravité du risque de l'attaque en question. Expliquer ?