

Test - Sécurité en ingénierie du logiciel : Le cadre des Web Services

19 décembre 2003

1 P. Théorique/pratique : Web Services

- (1) Réalisez un rapide historique des origines dans l'industrie informatique pour placer le décor des "Services Web" ?
- (2) Ecrivez un document XML pour décrire un stockage d'un carnet d'adresses (nom, prénom, adresse,...) ?
- (3) Ecrivez un exemple XML-RPC d'échange(s) entre le serveur "carnet d'adresse" et un client utopique (question(s) et réponse(s)) ?

(Les méthodes disponibles sont `AddressBook.Lookup(string textLookup, int maxReturn)` et `AddressBook.Add(struct addressEntry, boolean overwrite)`)

- (3.a) Recherche de l'entrée "Josianne" via `AddressBook.Lookup` en HTTP vers le serveur `lookup.bonbonshop.fr`,
- (3.b) Ajout de l'entrée (2) (en réalisant le mapping XML dans une structure propre à XML-RPC) en HTTP (via SSL) avec une authentification HTTP Basic (login :josianne Password :m!guel65).

2 P. Théorique/pratique : Sécurité en ingénierie logiciel

- (4) Nommez les grandes pratiques lors de la création et l'élaboration d'un logiciel et de son architecture pour limiter les risques liés à la sécurité ? (p.ex. les pratiques utilisées dans le MTA Postfix)
- (5) Nommez les raisons de l'écriture de logiciels peu sûres ? (les raisons ne sont pas uniquement techniques)
- (6) Que pensez-vous de la sécurité de cette application CGI ? Pouvez-vous imaginer des modifications relatives à la sécurité de cette application ? Bonus : Ecrivez une version alternative dans un langage existant ou en pseudo-code ?

```

1 #!/usr/local/bin/perl
2 # finger gateway
3
4 require 'cgi-lib.pl';
5 print &PrintHeader;
6 if (&ReadParse(*in)) {
7     print "<pre>\n";
8     print '/usr/bin/finger $in{'username'} `';
9     print "</pre>\n";
10 }
11 else {
12     print "<html> <head>\n";
13     print "<title>Finger Gateway</title>\n";
14     print "</head>\n<body>\n";
15     print "<h1>Finger Gateway</h1>\n";
16     print "<form method=POST>\n";
17     print "<p>User@Host:"
18     print "<input type=text name=\"username\">\n";
19     print "<p><input type=submit>\n";
20     print "</form>\n";
21     print "</body> </html>\n";
22 }
23

```

3 P. Pratique : Web Services en production

- (7) Une société dispose d'un nouveau serveur applicatif 'Web Services'. Ce serveur utilise une base de données via une interface distante localisée dans le réseau de l'entreprise et utilise SOAP (via un serveur Apache HTTP/SSL) pour les connexions clients venant d'Internet.
 - (7.a) Shématisez une infrastructure réseau pour garantir une bonne sécurité de ce système 'Web Services'.
 - (7.b) Décrivez les flux de communication entre les différents composants suivant votre nouvelle infrastructure.
 - (7.c) L'application SOAP ne dispose pas encore d'une méthode pour protéger l'intégrité du message SOAP. Pouvez-vous imaginer des solutions possibles ?
 - (7.d) Décrivez les risques potentiels de l'application 'Web Services' concernant les attaques venant d'Internet.
 - (7.e) Vous êtes responsable du serveur HTTP, quelles sont les bonnes pratiques de sécurisation de ce serveur ? (dans les grandes lignes)
- (8) Il n'y pas de question 8.