Security of Server-Side Web Applications

Summary

School of Computing
Napier University, Edinburgh, UK
Module Leader: Uta Priss

November 2006

Outline

General Security

Webserver security

PHP security

Security Engineering

see “patterns & practices Security Engineering Index” (msdn.microsoft.com)

- Security objectives
- Threat modeling
- Security design guidelines
- Security architecture and design reviews
- Security code reviews
- Security testing
- Security deployment reviews

Webserver security

- disallow server-side includes
- disallow indexes
- only store files in the public_html directory if they really need to be there
- security through obscurity

Webserver security (continued)

Apache's mod_security

- place Apache in a chroot directory
- POST filtering based on headers, values, IP addresses
- POST payload analysis
- restrict the use of certain HTML tags (e.g. <script>)
- prevent SQL injection ("delete", "insert")
- prevent SHELL commands
- etc

Of course, the server will run slower and use more memory

Other server functions

- Email: protect against spam and phishing
- install email server on different machine from webserver if possible
- don't allow the www user to send email
- HTACCESS
  useful for group-based restriction to part of site
  not very useful for login/registration of users
- database
  DB security and script security need to be integrated
  prevent SQl injection

PHP security

- Use appropriate functions:
  htmlspecialchars(); strip_tags(); add_slashes();
  mysql_real_escape_string(); etc
- apply “hardening” patch to PHP before installing
- PHP safe_mode
  restrict file access, executable directory, disable functions etc