ApacheCon

# httpd Security Fundamentals

William A. Rowe, Jr.
wrowe@apache.org

Committer, Apache httpd Project
Sr Software Engineer, SpringSource

# Directives you know

- Use <Directory > and <Files > when this is what you mean
- <Location > is usually the wrong answer, except in a predictable rule

Alias /foo/ /path/to/bar/

<Location /foo> ...

# Modules you don't know

- Comment out (disable) all modules who's function is not required in the server.
- mod_imagemap vulnerability; why react to unused module vulnerability reports?

# Service Ports

- Listen 8080 – is this correct in your infrastructure?
- Bind private services privately, e.g.
  - Listen 10.1.1.115:8080
  - Listen 127.0.0.1:8080 – whenever sufficient!

# Denial of Service

- Consumption of server resources disproportionate to the client resources required

# Cross Site Scripting (XSS)

- Embedding excecutable script into page responses
- Allows referrer cookie to be stolen by referred site (referred by the script)
- Lazy programming the most common origin of these flaws
- Charset encoding is the most nefarious origin, UTF-7 especially

# Run-as-user

- Required on Windows
- NEVER on Unix

# Filesystem Protection

- On unix, special attention to logs/ directory and similar
- On all architectures, read only or nill access whenever possible



# Configuration Tricks

- Root-only-read passwords.conf

# SSL Issues

- Key file protection; 600
- SSLPassphraseDialog?

# Worker (event) MPM

- Multi-threads, multiple exposures

# mod_log_forensic

- Record +datum|request|headers upon receipt
- Record -datum upon completion (success)

# Mass Virtual Hosting

- Additional considerations
- Multiple owners within-process

# Non-security topics

- Example content; disable this!
- Options -FollowSymlinks
- .htaccess issues
- mod_perl, PHP run in-process

# Extra modules

- mod_security
- mod_suexec
- mod_fcgid

# Special Applications

- Admin apps, DAV and FTP spaces
- Create separate user/group and httpd invocation for these tasks
- BARE MINIMUM additional modules



# Watch for vulnerability alerts

- bugtraq@securityfocus.com
- announce@httpd.apache.org



# See Also

- http://httpd.apache.org/security_report.html
- http://httpd.apache.org/docs/2.2/misc/security_tips.html