

Meandering Through Apache

<http://www.ussg.io.edu/>

USSG UNIX SYSTEMS
SUPPORT GROUP

- Apache1 vs. Apache2
- Apache Security Tips & Tricks
- SSL & Certs
- Building mod_perl for apache1
- New ideas in securing PHP
- How is apache used at IU?

Apache1 vs. Apache2

- Apache1
 - stable, secure (compared to Apache2)
 - mod_perl better supported
- Apache2
 - Worker modules allow for threaded servers
 - IPv6 support
 - Disadvantage: Security track record

<http://www.ussg.io.edu/>

USSG UNIX SYSTEMS
SUPPORT GROUP

- Module Reduction

- Don't build in:

- `./configure --disable-module=<mod_name> ...`

- Comment out in `(httpd | apache).conf`

- For Apache1 Comment both “LoadModule” and “AddModule” entries

- Bare minimum Modules:
 - httpd_core / mod_access / mod_auth / mod_so
 - mod_dir / mod_log_config / mod_mime
 - Apache2: core / (prefork | worker)
- Useful modules:
 - mod_userdir – allow ~/user syntax
 - mod_cgi – allow cgi scripts
 - mod_alias – access directories outside docroot
 - mod_vhost_alias – vhost support

<http://www.ussg.io.edu/>

- Limit information leakage:
 - ServerTokens Full (Default)
 - Apache/2.0.52 (Gentoo/Linux) mod_perl/1.99_11 Perl/v5.8.4 mod_ssl/2.0.52 OpenSSL/0.9.7d Server at verbose.biguni.edu Port 80
 - ServerTokens Prod
 - Apache Server at quiet.smartuni.edu Port 80

- Track & Trace
- Place the following in Main Server Config, as well as each <Virtual Host> section
- RewriteEngine on
- RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
- RewriteRule .* - [F]

- Restrict .htaccess usage
 - <Directory />
 - AllowOverride None
 - </Directory>
 - <Directory /some/path>
 - AllowOverride AuthConfig Indexes
 - </Directory>

- Apache1
 - mod_ssl provides encryption via apache module
 - http://www.mod_ssl.org
 - mod_ssl version must match apache version
 - Example: 2.8.22-1.3.33
- Apache2
 - SSL built-in
- SSL & non-IP based Virtual Hosts

- <http://www.ossf.org/pkg/lib/mm/>
 - Shared Memory Allocation
 - Allows forked processes to share memory
 - Allows mod_ssl to use a RAM-based cache instead of disk based for performance
 - `./configure --disable-shared ; make ; make install`

Self Signed Certificates

- Create RSA key:
 - openssl genrsa -des3 -out server.key 1024
- Strip Passphrase from key:
 - openssl rsa -in server.key -out server.pem
 - YOU MUST PROTECT server.pem
- openssl req -new -key server.key -out server.csr
- openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt

<http://www.ussg.io.edu/>

USSG UNIX SYSTEMS
SUPPORT GROUP

- Building:
 - mod_perl, statically compiled
 - Configure mod_ssl
 - `cd mod_ssl-x.x.x-x.x.x`
 - `./configure -with-apache=../apache_1.3.xx`

- Configure mod_perl
 - perl Makefile.PL USE_APACI=1 EVERYTHING=1
DO_HTTPD=1 SSL_BASE=/path/to/openssl
APACHE_PREFIX=/path/to/apache
APACHE_SRC=../apache_1.3.xx/src
APACI_ARGS='--enable-module=ssl,--enable-
module=rewrite --disable-module=proxy'
 - Make && make test && make install
- Install apache
 - cd ../apache-1.3.xx; make install

- <http://www.hardened-php.net>
- Very new project
- Provides:
 - Canary Protection of critical data structures
 - Protection against internal format string exploits
 - Protection against arbitrary code inclusion
 - Syslog logging of attackers IP and attacked script
- Gentoo USE Flag “hardenedphp”

<http://www.ussg.io.edu/>

USSG UNIX SYSTEMS
SUPPORT GROUP

- Questions?
- What are you doing with apache?

<http://www.ussg.iu.edu/>

USSG UNIX SYSTEMS
SUPPORT GROUP