

Securing websites with hardened Apache configuration and mod-security

Linh Vu

Physics IT
School of Physics,
the University of Melbourne

About me

- Web/database administration officer of the School of Physics, UniMelb.
- LAMP developer, with a passion for web standards, CSS/XHTML, accessibility and usability.
- Very paranoid webmaster.

Why harden Apache?

- Relaxed “out of the box” configuration
- Firewall and IDS don't provide complete protection
- Web applications can't always be trusted
 - undiscovered security issues
 - Third party apps outside of your control
 - Forgotten old apps!

Web application vulnerabilities

- SQL injection
- Shell command execution
- Email form header/subject injection
- XSS – Cross site scripting attack
- Comment spams

Consequences

- Leak sensitive database info – identity theft
- Database, files and content destroyed
- Rooted servers/sites become spam zombies
- Phishing scams sneakily inserted on websites
 - Paypal “donation” buttons
 - Bogus links

Part 1

- Hardened Apache configuration for deploying websites
 - Base config
 - mod_access: restrict access to sensitive locations
 - mod_access_rbl: Realtime Blackhole List
 - mod_rewrite – the swiss army knife of apache

Part 2

- `mod_security` – the open source web application firewall
 - Installation
 - Basic rules
 - Internal chroot apache
 - Integration with firewall/IDS and anti-virus scanner
 - Signatures and updates
 - Protections and examples
 - False alarms and exclusions

Hardening Apache

- Terminologies:
 - server config: `/etc/apache2/apache2.conf`
 - virtual host: `<VirtualHost 66.66.66.66:80>stuff</VirtualHost>`
 - directory: `<Directory “/path/to/dir”>stuff</Directory>`
 - htaccess: `.htaccess` files – not recommended

Base configuration for Apache

- Limit requests per process:

Server config

```
<IfModule prefork.c>
```

```
    StartServers      5
```

```
    MinSpareServers  5
```

```
    MaxSpareServers  10
```

```
    MaxClients       20
```

```
    MaxRequestsPerChild 10000 # Default 0 - unlimited
```

```
</IfModule>
```

Base configuration - PHP

- Restrict scripts to certain directories

```
php_admin_value open_basedir “/path/to/site:/tmp:/usr/share/php:.”
```

- Hide errors (on production sites)

```
php_admin_value display_errors 0
```

- Log errors

```
php_admin_value log_errors 1
```

```
php_admin_value error_log “/path/to/site/php-error.log”
```

mod_access

- Deny access to config directories and files

```
<Directory "/var/www/myblogs.com/wp-includes">
```

```
    Deny from all
```

```
</Directory>
```

```
<Files "wp-config.php">
```

```
    Deny from all
```

```
</Files>
```

mod_access

- Restrict access to admin areas for known ips/users only

```
<Directory "/var/www/myblogs.com/wp-admin">
```

```
    Order allow,deny
```

```
    Allow from 123.123.123.1
```

```
    ErrorDocument 403 "Site down, server not working."
```

```
</Directory>
```

- Use “Satisfy Any” in combination with mod_auth_* for external users requiring login to view the section

mod_access_rbl

- RBL – Realtime Blackhole List
 - open relays
 - known sources of spam
 - zombies/rooted systems
 - open proxies
 - Worms/viruses with built-in spam engines
- Provider: Spamhaus.org

mod_access_rbl

- Install: patch mod_access with the rbl patch

http://www.gotroot.com/tiki-view_blog_post.php?blogId=&postId=34

Server Config:

Order allow,deny

Allow from all

Deny via sbl-xbl.spamhaus.org

- Can mirror spamhaus list in your local DNS server (annual service fee)

mod_rewrite

- Nice URL

`/au/vic/collingwood v.s`

`/directory.php?country=au&state=vic&suburb=collingwood`

- Force input checks before applications get them,
plus hiding your script

RewriteEngine On

```
RewriteRule ^/products/([a-z0-9_-]+)/([0-9]+)$  
/product_info.php?category=$1&prod_id=$2 [L]
```

mod_rewrite

- Or: really hide your script

```
# ezpublish
```

```
RewriteEngine On
```

```
RewriteRule !(^/design|^/var/.*/storage|^/var/storage|^/var/.*/cache|^/var/cache|^/extension/.*/design|^/kernel/setup/packages|^/packages|^/share/icons).*\.(gif|css|htc|jpg|png|jar|js|ico|pdf|swf)$ /index.php
```

- Force SSL/https:

```
RewriteEngine On
```

```
RewriteCond %{SERVER_PORT} !^443$
```

```
RewriteRule ^/(secure1|secure2)/(.*) https://%{SERVER_NAME}/$1/$2  
[L,R]
```

mod_rewrite

- Block hot linking

RewriteEngine On

RewriteCond %{HTTP_REFERER} !^\$

RewriteCond %{HTTP_REFERER} !^http://mysite.com/.*\$ [OR,NC]

RewriteCond %{HTTP_REFERER} !^http://www.mysite.com/.*\$
[OR,NC]

RewriteRule .*\. (gif|GIF|jpg|JPG|png|PNG)\$
http://mysite.com/images/bloodyleechers.jpg [L,R]

- Other uses: see Apache URL rewriting guide on <http://httpd.apache.org>

Mod-Security: the open source web application firewall

- Intrusion detection and prevention engine for web applications
- Apache module, scan web streams for known and unknown attacks
- Installation:
 - package manager: apt-get, yum, portinstall etc.
 - compile from source:
 - get apache development package (apache2-dev)
 - **apxs2 -cia mod_security.c**

mod-security: basic rules

- Logging

- SecFilterEngine On
- SecFilterDefaultAction "deny,log,status:500"
- SecAuditEngine RelevantOnly
- SecAuditLog /var/log/apache2/audit_log

- Server signature

SecServerSignature " "

SecServerSignature "Microsoft-IIS/5.0"

SecServerSignature "honeypot"

mod-security: nikto scan

- `./nikto.pl -h <host-ip> -g`
- without mod-security:

Server: Apache/2.0.53 mod_python/3.1.3 Python/2.4.1 PHP/4.3.10-10 (etc.)

- with mod-security:

Server ID string not sent

Server does not respond with '404' for error messages (uses '500').

<internal server error 500 html message>

mod-security: URL encoding and chroot apache

- URL encoding
 - SecFilterCheckURLEncoding On
 - SecFilterCheckCookieFormat On
 - SecFilterCheckUnicodeEncoding Off
 - SecFilterForceByteRange 1 255
- internal chroot apache
 - SecChrootDir /chroot/var/www
 - SecChrootLock /var/lock/modsecurity-chroot.lock
 - # provided that: ln -s /chroot/var/www /var/www
 - # Path outside chroot same as inside chroot

mod-security: integration w/ firewall/IDS and anti-virus scanner

- **with APF – Advanced Policy Firewall**

```
SecFilterDefaultAction "pass,exec:/usr/local/bin/mod_security.php"  
#!/usr/bin/php -q  
$msg .= "DOMAIN NAME    : " . $_SERVER["HTTP_HOST"] . "\n";  
$msg .= "ERROR          : " . stripslashes($_SERVER  
    ["HTTP_MOD_SECURITY_MESSAGE"]) . "\n";  
exec("/etc/apf/apf -d " . $_SERVER["REMOTE_ADDR"]);  
mail("webmaster@mysite.com", "Security Monitor - Intrusion Alert",  
    $msg); // Or log to database for later analysis
```

- **with ClamAV – comes with utility script**

mod-security: signatures and updates

- Needs frequently updated rules to keep up with the baddies.
- Provider: gotroot.com
- Protection:
 - Blacklists
 - Known rootkits/worms
 - Search engine hacks
 - Webapp vulnerabilities
 - Bad UserAgents, etc.

mod-security: blacklists, rootkits and worms

- Comment spams, zombie boxes, known attacks
- Not needed if using mod_access_rbl
 - SecFilterSelective REMOTE_ADDR 195\.18\.128\.230
 - SecFilterSelective REMOTE_ADDR 200\.118\.69\.30
 - SecFilterSelective REMOTE_ADDR "218\.188\.23\.162"
- Known rootkits/worms
 - #remote perl execution with .pl extension
 - SecFilterSelective REQUEST_URI "perl .*\.pl(\s|\t)*\;"
 - #zencart exploit
 - SecFilterSelective REQUEST_URI "/ipn\.php\?cmd="

mod-security: “Google Hacks”, bad UserAgents

- “Google Hacks” signatures

```
SecFilterSelective HTTP_REFERER "Powered.*PHPBB.*2\0\.\ inurl:"  
"id:350002,rev:1,severity:2,msg:'PHPBB 2.0 Google Recon attempt'"
```

```
SecFilterSelective HTTP_REFERER "SquirrelMail version 1\4\4.*inurl:src  
ext\.php"
```

- Bad UserAgents

#XSS in the UA field

```
SecFilterSelective HTTP_USER_AGENT "<(.\s|\n)?(script|about|applet|  
activex|chrome|object)(.\s|\n)?>.*<(.\s|\n)?(script|about|applet|activex|  
chrome|object)"
```

mod-security: bad UserAgents

- Bad UserAgents

#PHP code injection attack

```
SecFilterSelective HTTP_USER_AGENT "(<\?php|<[[:space:]]*\?  
[[:space:]]*php)"
```

```
SecFilterSelective HTTP_USER_AGENT ".*HTTP_GET_VARS"
```

#XML RPC exploit tool

```
SecFilterSelective HTTP_USER_AGENT "xmlrpc exploit"
```

#Web leaches

```
SecFilterSelective HTTP_USER_AGENT "Web Downloader"
```

mod-security: webapp vulnerabilities

- **Generic PHP exploit signatures**

```
SecFilterSelective THE_REQUEST "\;(chr|fwrite|fopen|system|chr|passthru|
  popen|proc_open|shell_exec|exec|proc_nice|proc_terminate|proc_get_status|
  proc_close|pfssockopen|leak|apache_child_terminate|posix_kill|posix_mkfifo|
  posix_setpgid|posix_setsid|posix_setuid|phpinfo)\(.*\)\";\"
  \"id:300007,rev:1,severity:2,msg:'Generic PHP exploit pattern denied'\"
```

- **Prevent SQL injection in cookies**

```
SecFilterSelective COOKIE_VALUES \"((select|grant|delete|insert|drop|alter|
  replace|truncate|update|create|rename|describe)[[:space:]]+[A-Z|a-z|0-9|\\*| \\,|]+
  [[:space:]]+(from|into|table|database|index|view)[[:space:]]+[A-Z|a-z|0-9|\\*| \\,|]
  UNION SELECT.*\\'.*\\'.*,[0-9].*INTO.*FROM)\"
  \"id:300011,rev:1,severity:2,msg:'Generic SQL injection in cookie'\"
```

mod-security: webapp vulnerabilities

#Generic PHP remote file inclusion attack signature

```
SecFilterSelective REQUEST_URI "\.php\?" chain
```

```
SecFilter "(http|https|ftp)\:/" chain
```

```
SecFilter "(cmd|command)=(cd|\\;|perl |python |rpm |yum |apt-get |emerge |lynx |  
links |mkdir |elinks |cmd|pwd|wget |id|uname|cvs |svn |(s|r)(cp|sh) |net(stat|cat) |  
rexec |smbclient |t?ftp |ncftp |curl |telnet |gcc |cc |g\+\+\ |whoami|\.|/killall |rm \-  
[a-z|A-Z])"
```

```
SecFilterSelective REQUEST_URI "\.php\?" chain
```

```
SecFilter "(http|https|ftp)\:/" chain
```

```
SecFilter "(cmd|command)=.*(cd|\\;|perl |python |rpm |yum |apt-get |emerge |lynx |  
links |mkdir |elinks |cmd|pwd|wget |id|uname|cvs |svn |(s|r)(cp|sh) |net(stat|cat) |  
rexec |smbclient |t?ftp |ncftp |curl |telnet |gcc |cc |g\+\+\ |whoami|\.|/killall |rm \-  
[a-z|A-Z])"
```

mod-security: other rules

- Proxy scan
- Apache2
- Windows server protection

mod-security: false alarms and exclusions

- False alarms: especially with SQL injection
- Exclusions:

```
<LocationMatch "/index.php?name=PNphpBB2&file=posting&mode=reply.*">  
  SecFilter "[[:space:]]+(select|grant|delete|insert|drop|alter|replace|truncate|update|  
    create|rename|describe)[[:space:]]+[A-Z|a-z|0-9|\*| |\\,]+[[:space:]]+(from|into|  
    table|database|index|view)[[:space:]]+[A-Z|a-z|0-9|\*| |\\,]" pass,nolog  
</LocationMatch>  
  
<Location /path/to/foo/>  
  SecFilterRemove 1001 1002 30039 # rule ids  
</Location>
```

Recommended reading

- <http://www.apachesecurity.net> - Author: Ivan Ristic
- <http://www.modsecurity.org> - By the same author
- <http://www.gotroot.com> - the Prometheus Group - maintainers of modsecurity signatures