

Apache Basic Server Hardening

Apache Basic Server Hardening

Before hardening your Web Server you should make sure it works with its intended integrated purpose in a test environment. Otherwise you may spend lots of wasted time trouble-shooting.

So, assuming that your Web Server passes testing of its intended purpose, you may perform "Basic Hardening". Because this is "basic" I often perform these all at once and then test.

Here are some of the basic hardening steps I take today by default,

As with any security notes, I will write a disclaimer that there are more advanced ways to secure Apache. You can go as far as compiling your own custom version but that's out of scope for now.

Disable Server Information Banner

By default Apache provides extra information about your server when 403, 404, 502 or similar error pages are invoked. The information could be used to look up vulnerabilities on the particular version of Apache you are running.

If you visit a page that does not exist you will invoke a 404 error resulting in a page Not Found similar to below,

```
Not Found
The requested URL /invalidpage.html was not found on this server.
Apache/2.4.18 (Ubuntu) Server at www.bonsaiframework.com Port 80
```

Edit `/etc/apache2/conf-available/security.conf`,

`set ServerTokens Prod` - This turns off all the extra header information sent by Apache.

`set ServerSignatures Off` - Removes footer information from default apache pages. For example, page not found.

Older versions of Apache use `/etc/apache2/conf.d/security`

Restart Apache to take effect and verify by invoking a 404 again.

Disabling Unnecessary Modules

Less loaded, less vulnerabilities and you will also get performance increases too.

Disable Status Module

I found that you can save about 3MB of memory if the `status` apache module is disabled. Here's how to disable interactively,

```
sudo a2dismod
Your choices are: alias auth_basic authn_file authz_default authz_groupfile
authz_host authz_user autoindex cgid
                  deflate dir env filter jk mime negotiation proxy
proxy_http rewrite setenvif status substitute
Which module(s) do you want to disable (wildcards ok)?
NOTE: make sure you only disable the following one ONLY!!! type:
status
Module status disabled.
To activate the new configuration, you need to run:
    service apache2 restart
sudo service apache2 restart
```

Disable More Modules

Will flush this out some more ...

Turn off Default Website

...