<https://geekflare.com/apache-web-server-hardening-security/> [**Primary document**]

<https://www.digitalocean.com/community/tutorials/how-to-create-an-ssl-certificate-on-apache-for-centos-7>

* **Update Apache**

|  |
| --- |
| sudo yum update httpd |

* **Disable ServerSignature and ServerTokens:** 
  + /etc/httpd/conf/httpd.conf
  + This prevents Apache version, OS version and other sensitive info from being displayed.
  + Add the following to the file:

|  |
| --- |
| ServerSignature off  ServerTokens prod |

* **Disable TraceEnable**
  + **?**

|  |
| --- |
| TraceEnable off |

* **Ensure directory access is restricted**
  + Look for the following code block. Be sure Require all is set to denied, and not granted.

|  |
| --- |
| <Directory />  AllowOverrride none  Require all denied </Directory> |

* **Disabling browser directory browsing**
  + Prevent attackers from browsing directory paths
* **Etag disable**
  + Prevent attacks from obtaining Inode numbers, child processes and other sensitive information
* **Running Apache with a non privileged account**
  + This helps prevent attackers from accessing anything else, should Apache be compromised.
  + Remember that one process will always be root for apache anyway, because root is required to start Apache on port 80.
* **Protect the bin and conf directories by changing permissions**
  + (Could not find bin for httpd anywhere, bare in mind this is guide for apache on Ubuntu systems, so directories may vary in location)
* **System Settings Protection**
  + Make sure the root directory configuration (<Directory />) is set to not allow any overrides.
* **HTTP Request Methods**
  + Preventing users from exploiting HTTP methods.
* **Cookie with HttpOnly and Secure flag**
* **Clickjacking attack**