**Problem :**

|  |  |
| --- | --- |
| **Strict Transport Security (HSTS)** | **Invalid**   **Server provided more than one HSTS header** |

SSL Result = A

**Solutions:**

* The problem is that we have 2 HSTS header going on right now, and we only want one.
  + HSTS will get either the value of the upstream (where port 3000 and our node is) or the configuration (nginx)
* One of them is placed in the server.conf provided on BeachBoard
* The other one is placed in a directory called “helmet”.

**Solution 1: Hide the HSTS from nginx ,**

**STEPS:**

1. Access the “server.conf” ( the code inside should be exactly the same as provided on BeachBoard) **sudo vim /etc/nginx/conf.d/server.conf**

* Technically, you could modify the “nginx.conf” in /**etc/nginx**. However, in the “nginx.conf” file right now, we already had “include **/etc/nginx/conf.d/\*.conf**. So the configuration would point to “server.conf”.

1. Then, you want to add this line **proxy\_hide\_header Strict-Transport-Security;**  BEFORE the line ( **add\_header Strict-Transport-Security “max-age = 63072000” always;** )

* This is to hide the Nginx HSTS header

1. Now restart the system
   * Restart nginx
   * Restart your node using **forever restart app.js**
     + This command has to be where your node app.js is stored
     + WE MUST restart node because if we don’t, it will always take the last node we did because of forever
       - We had to implement forever for our sever to keep running on the domain, or else it will result in a 502 bad gateway
2. Test your SSL Lab, should be A+

**Solution 2:  Delete the default hsts in helmet**

* Helmet was installed when you did “npm install”
* Helmet set various HTTP default headers to help secure our express server, and one of them is hsts.

**STEPS:**

1. Access the javascript file “index.js” of the directory “helmet”
   1. Cd to **app/simple-node-express-server/node\_modules/helmet**
2. Now use vim/nano to edit the file “index.js”:
   1. Look for :
      1. Where it says : “ var DEFAULT\_MIDDLEWARE = […]
         1. Comment out the ‘hsts’, inside the parameter
      2. Go down to where it says: helmet.hsts = require(‘hsts’) and comment it out
3. Now restart the system
   1. Restart nginx
   2. Restart your node using **forever restart app.js**
      1. This command has to be where your node app.js is stored
      2. WE MUST restart node because if we don’t, it will always take the last node we did because of forever
         1. We had to implement forever for our sever to keep running on the domain, or else it will result in a 502 bad gateway
4. Test SSL Lab, Should get an A+

**Solution 3:** Configure your app.js using the beach board file, and make nginx config back to original default