Secure Flag

The cookie with a secure flag will only be sent over an HTTPS connection.(https://resources.infosecinstitute.com/securing-cookies-httponly-secure-flags/#gref)

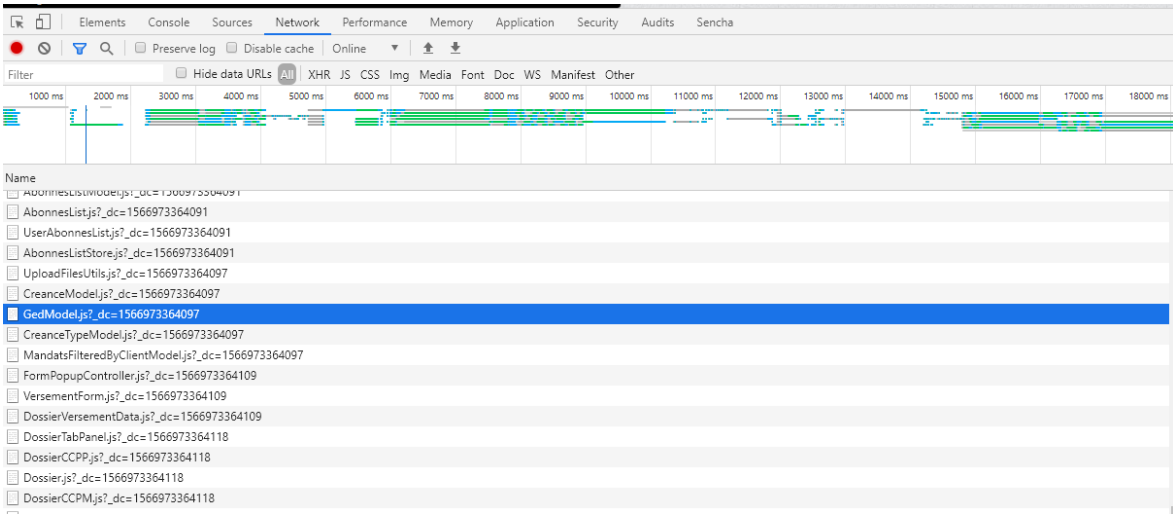
Cookies can be made secure by setting the httpOnly flag as this prevents client-side access to that cookie, however httpOnly flag here will prevent creation and manipulation of cookies on client-side. Given ext-js is extensively manipulating cookies (during login, subsituting users, desubsituting users etc), these functionalities will be impacted.

Steps:

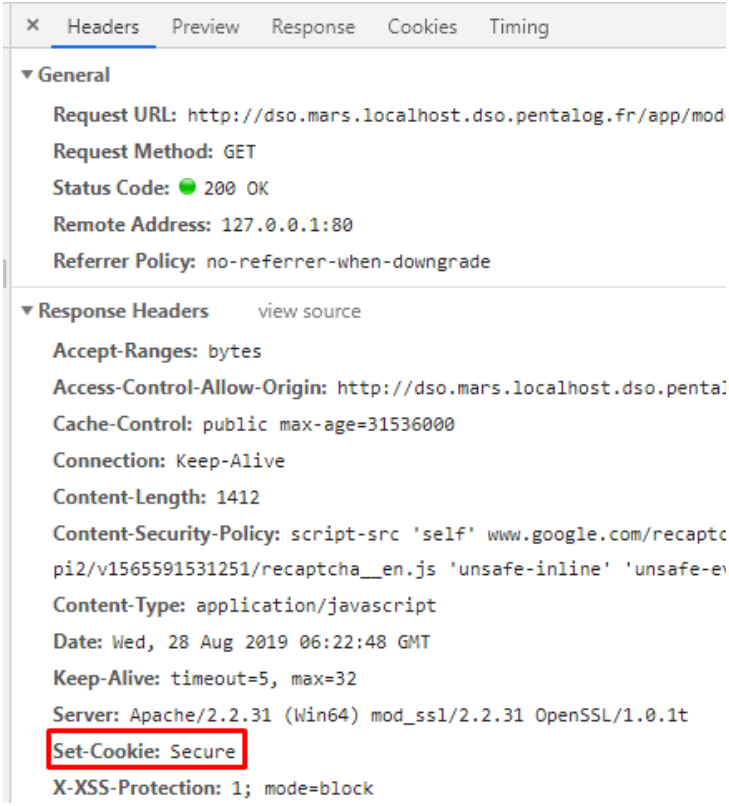
Configuration No.1:

- Open your **httpd.conf** (apache configuration file)
- Ensure that **LoadModule ssl_module modules/mod_ssl.so** and **LoadModule headers_module modules/mod_headers.so** are uncommented.
- Next, locate the section **#'Main' server configuration**
- Add this line to code below it, **Header set Set-Cookie Secure**
- Restart Apache
- Test as follows:

    - Open Chrome developper tool (Ctrl + Shift + i)
    - Click on the **"Network"** tab and choose any of JS file as shown below:

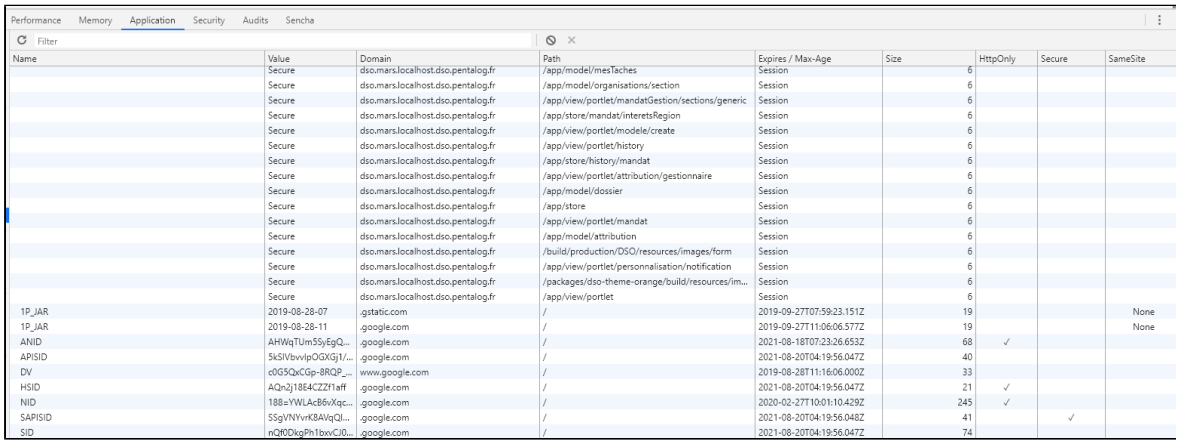


    - Then choose the **"Headers"** section for that file located to the right-hand-side



The set-cookie in your Http Header is now set to secure

- Another way to test it is by going to the **"Application tab" Cookies Expand Select URL**
- A tick will appear in front of the cookies in the **HttpOnly** or the **Secure** column and secure will be attributed them as shown below:



- **Resource**: https://resources.infosecinstitute.com/securing-cookies-httponly-secure-flags/

<u>Configuration No 2.</u>

Back-End Modification:

Files:

- C:\Workspace\marsservice\MandatService\impl\target\MandatService\WEB-INF\web.xml
- C:\Workspace\marsservice\MandatService\impl\src\main\webapp\WEB-INF\web.xml
- C:\Workspace\marsservice\SupervisionService\impl\src\main\webapp\WEB-INF\web.xml

Add the following lines of code in the **<session-config>** tag.

```
<session-config>
  <session-timeout>30</session-timeout>
  <cookie-config>
    <!-- <http-only>true</http-only> -->
    <secure>true</secure>
```

```
    </cookie-config>
</session-config>
```