

# Secure Flag

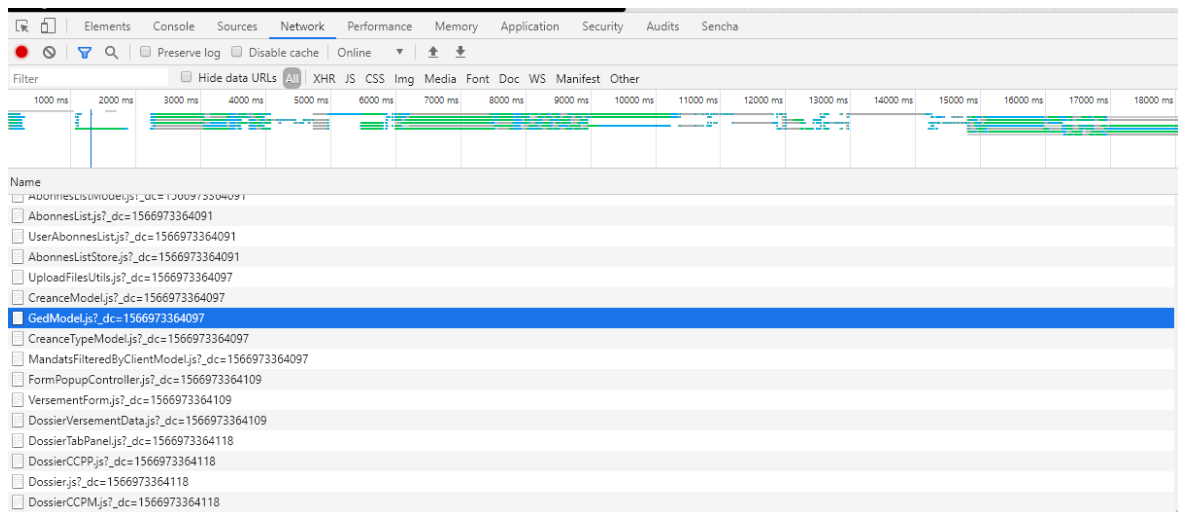
The cookie with a secure flag will only be sent over an HTTPS connection. (<https://resources.infosecinstitute.com/securing-cookies-http-only-secure-flags/#gref>)

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, substituting users, desubstituting 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 developer 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

Headers Preview Response Cookies Timing

▼ General

Request URL: http://dso.mars.localhost.dso.pentalog.fr/app/mod

Request Method: GET

Status Code: 200 OK

Remote Address: 127.0.0.1:80

Referrer Policy: no-referrer-when-downgrade

▼ Response Headers view source

Accept-Ranges: bytes

Access-Control-Allow-Origin: http://dso.mars.localhost.dso.penta

Cache-Control: public max-age=31536000

Connection: Keep-Alive

Content-Length: 1412

Content-Security-Policy: script-src 'self' www.google.com/recaptc  
pi2/v1565591531251/recaptcha\_\_en.js 'unsafe-inline' 'unsafe-e

Content-Type: application/javascript

Date: Wed, 28 Aug 2019 06:22:48 GMT

Keep-Alive: timeout=5, max=32

Server: Apache/2.2.31 (Win64) mod\_ssl/2.2.31 OpenSSL/1.0.1t

**Set-Cookie: Secure**

X-XSS-Protection: 1; mode=block

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:

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite
	Secure	dso.mars.localhost.dso.pentalog.fr	/app/model/mesTaches	Session	6			
	Secure	dso.mars.localhost.dso.pentalog.fr	/app/model/organisations/section	Session	6			
	Secure	dso.mars.localhost.dso.pentalog.fr	/app/view/portlet/mandatGestion/sections/generic	Session	6			
	Secure	dso.mars.localhost.dso.pentalog.fr	/app/store/mandat/interetsRegion	Session	6			
	Secure	dso.mars.localhost.dso.pentalog.fr	/app/view/portlet/modele/create	Session	6			
	Secure	dso.mars.localhost.dso.pentalog.fr	/app/view/portlet/history	Session	6			
	Secure	dso.mars.localhost.dso.pentalog.fr	/app/store/history/mandat	Session	6			
	Secure	dso.mars.localhost.dso.pentalog.fr	/app/view/portlet/attribu/gestionnaire	Session	6			
	Secure	dso.mars.localhost.dso.pentalog.fr	/app/model/dossier	Session	6			
	Secure	dso.mars.localhost.dso.pentalog.fr	/app/store	Session	6			
	Secure	dso.mars.localhost.dso.pentalog.fr	/app/view/portlet/mandat	Session	6			
	Secure	dso.mars.localhost.dso.pentalog.fr	/app/model/attribu	Session	6			
	Secure	dso.mars.localhost.dso.pentalog.fr	/build/production/DSO/resources/images/form	Session	6			
	Secure	dso.mars.localhost.dso.pentalog.fr	/app/view/portlet/personnalisation/notification	Session	6			
	Secure	dso.mars.localhost.dso.pentalog.fr	/packages/dso-theme-orange/build/resources/im...	Session	6			
	Secure	dso.mars.localhost.dso.pentalog.fr	/app/view/portlet	Session	6			
TP_JAR	2019-08-28-07	gstatic.com	/	2019-09-27T07:59:23.151Z	19			None
TP_JAR	2019-08-28-11	google.com	/	2019-09-27T11:06:06.577Z	19			None
ANID	AHWqTum5S5yEgQ...	google.com	/	2021-08-18T07:23:26.653Z	68	✓		
APISID	5kSVbvvpOGXGj1...	google.com	/	2021-08-20T04:19:56.047Z	40			
DV	cDG5QxCGp-BRQP...	www.google.com	/	2019-08-28T11:16:06.000Z	33			
HSID	AQn3j1864CZ21aff	google.com	/	2021-08-20T04:19:56.047Z	21	✓		
NID	188=FWL4g6vWq...	google.com	/	2020-02-27T10:01:10.439Z	245	✓		
SAPISID	5SgVNVwKSAIeq2...	google.com	/	2021-08-20T04:19:56.048Z	41			
SID	nc9RQXgPh1bwC0...	google.com	/	2021-08-20T04:19:56.047Z	74		✓	

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

## Configuration No 2.

### 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>
```