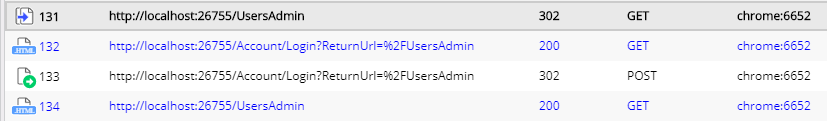
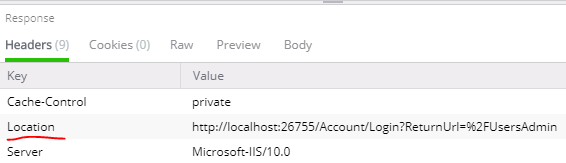
ASP.NET Identity Login HHTP Analysis

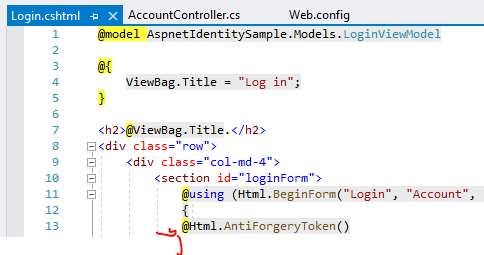
1. Redirect to Login page

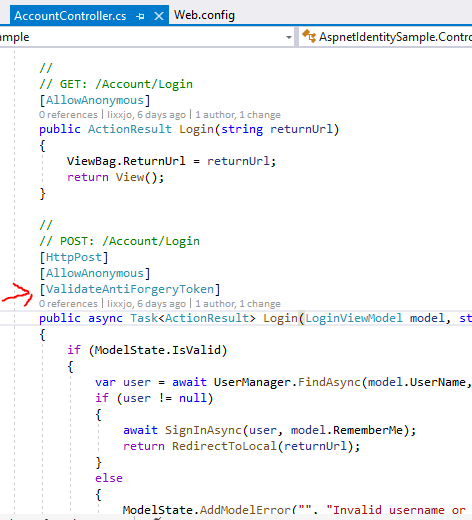


* The Hyper Text Transfer Protocol (HTTP) 302 Found redirect status response code indicates that the resource requested has been temporarily moved to the URL given by the Location header. In the above screen shot, browser got redirected to /UsersAdmin page
* Because of Form Authentication, /UsersAdmin redirects to /Account/Login page
* The response from /UsersAdmin contains a Location in its Header

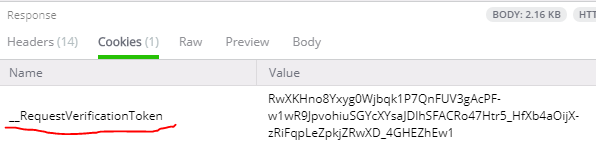


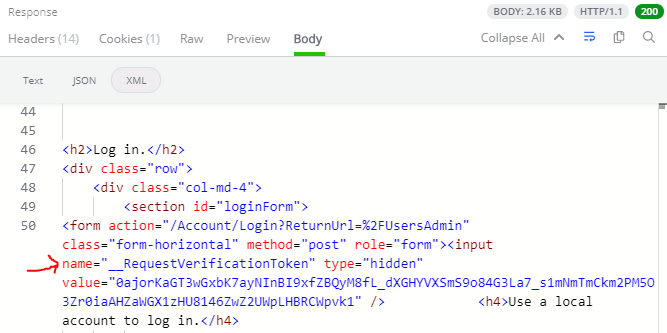
* Browser redirects to the Location using GET action, /Account/Login page uses AntiForgeryToken



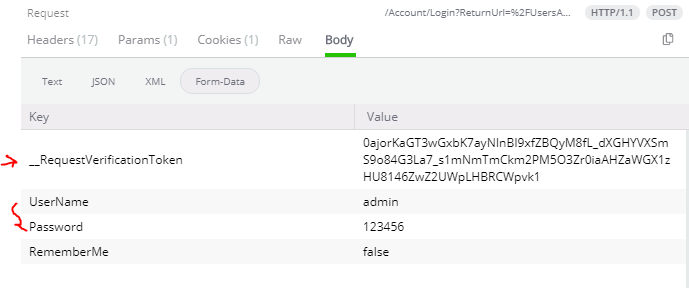


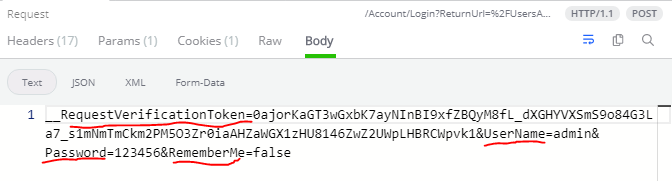
* HtmlHelper.AntiForgeryToken() generates the “\_\_RequestVerificationToken” Cookie as well as the hidden field “\_\_RequestVerificationToken”, here is the Response Header and Body from /Account/Login

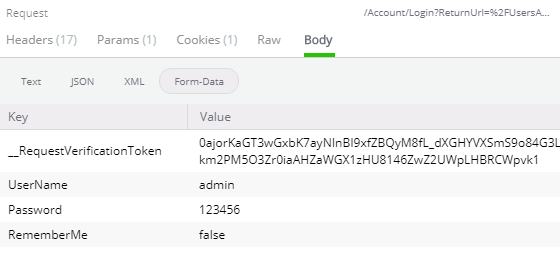


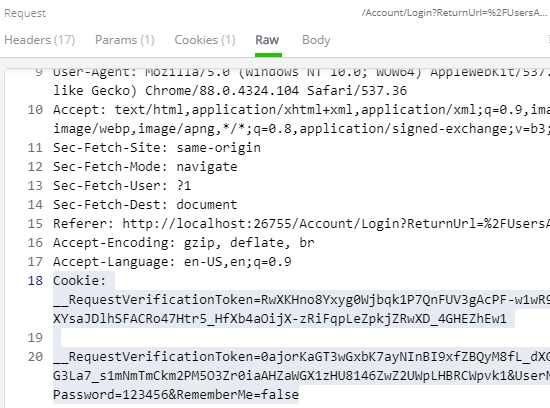


* When user inputs User name and Password and submits (POST) back to /Account/Login, the request header contains the “\_\_RequestVerificationToken” Session Cookie (expires when session ends) and also the hidden field “\_\_RequestVerificationToken”

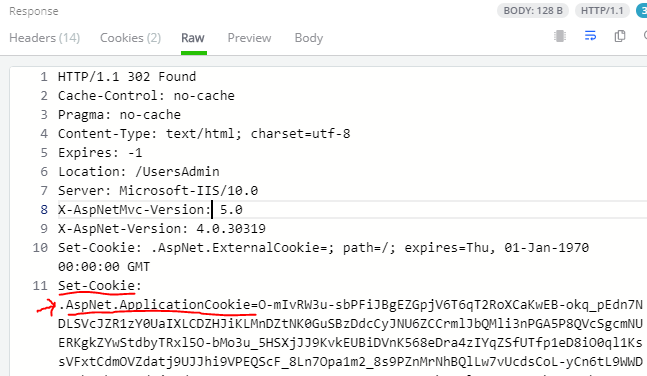


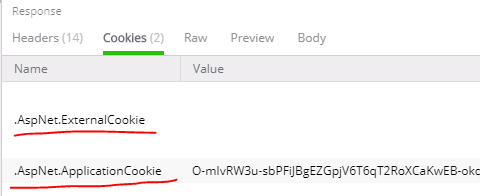






* Since Authentication successful, Response will generate the Session Cookie:

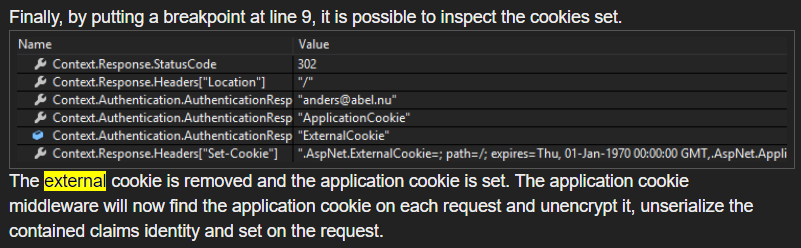




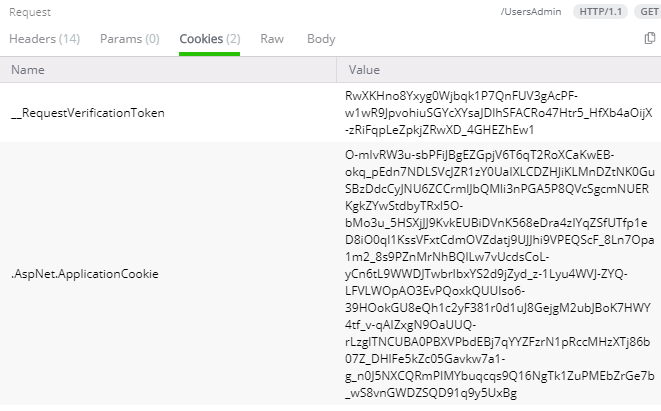
Where :

* .AspNet.ExternalCookie is for External Login using ASP.NET OWIN

For External Cookie refer to <https://coding.abel.nu/2014/06/understanding-the-owin-external-authentication-pipeline/>



* .AspNet.ApplicationCookie is the Session Cookie
* HTTP 302 Redirect page back to /UsersAdmin, and from now on, there is always 2 cookies on the Request Header:



* Whenever we submit data (POST) back to the server, there will be also a “\_\_RequestVerficationToken” hidden fields for preventing “Cross site Request Forgery” (CSTF) attack.