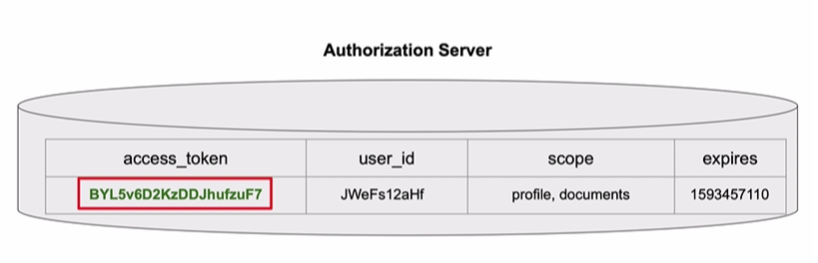
1. **Identifier Type Access Token**

(Preferable in our case as we are already generating the session id and we will generate the identity Token along with Session ID to make it more secure)

One Way is we can use the same Session ID but along with that we can add a table on Authorization Server ,

Where Table is like having details of user\_id , scope and expires...

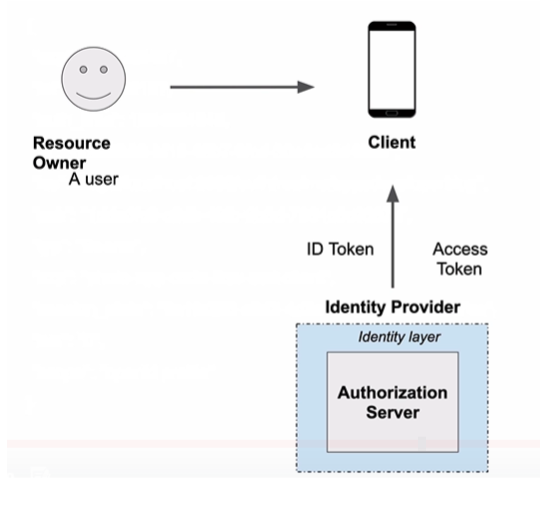
Also we can get integrate the ehcache to get the details between our Auth server and the client.



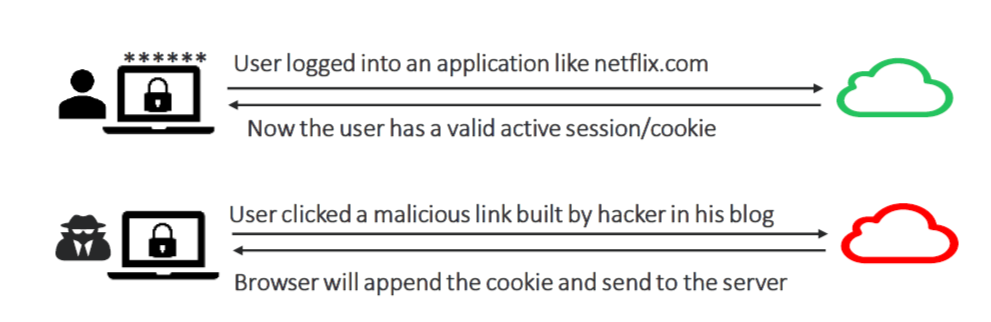
So the Client application will have now 2 tokens

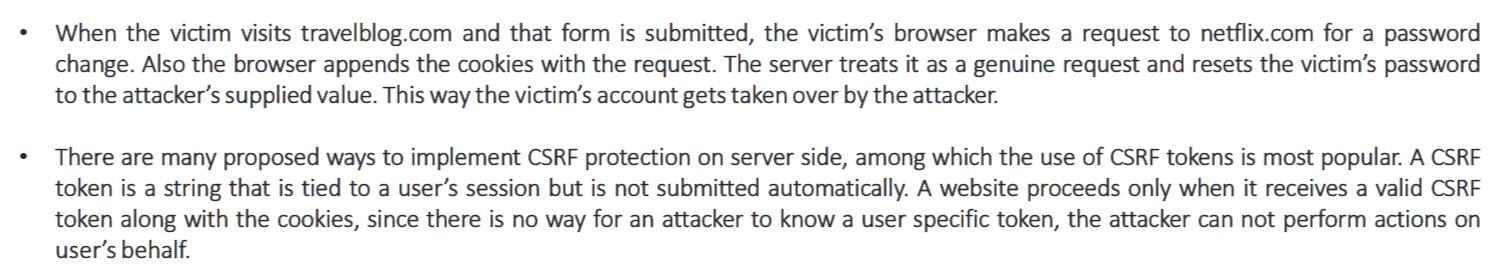
1. ID Token – to get the basic Details

2. Access Token – to get the Authorization Details



Limitation with only using Session is there may be a CSRF (Cross Site Request Forgery) attacks

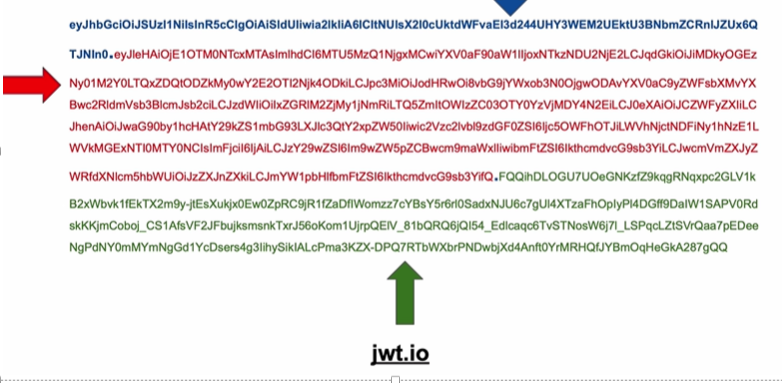




We can address this by using a xsrf token like along with jsession id



2. **Second way is to use self contained type**



Where we have Header , payload and Signatures for more security.

