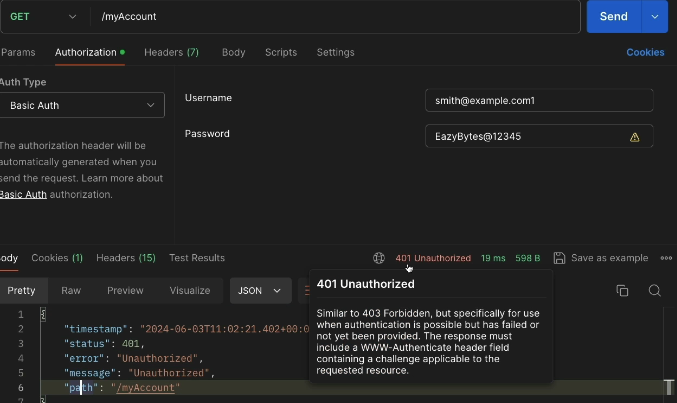
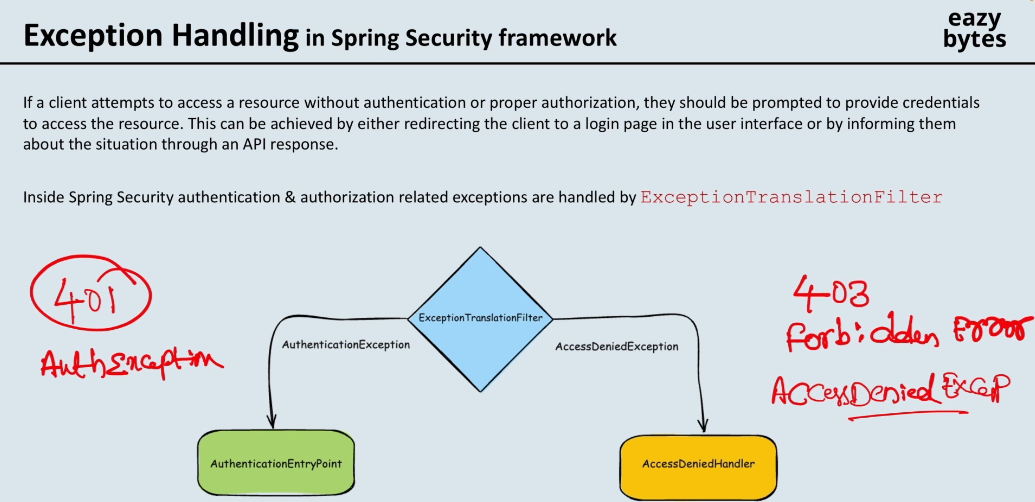
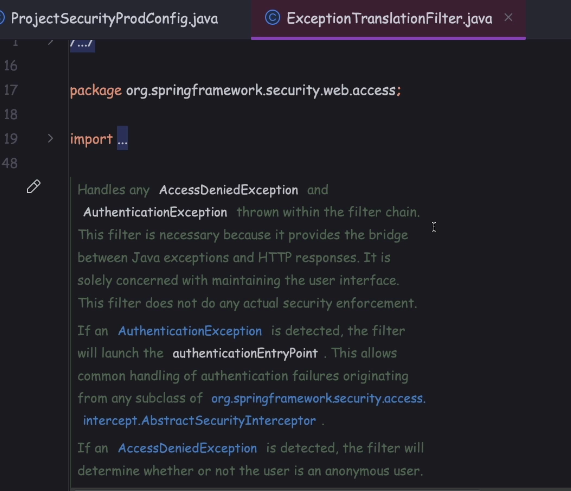
**6.spring security customization ; section 7**

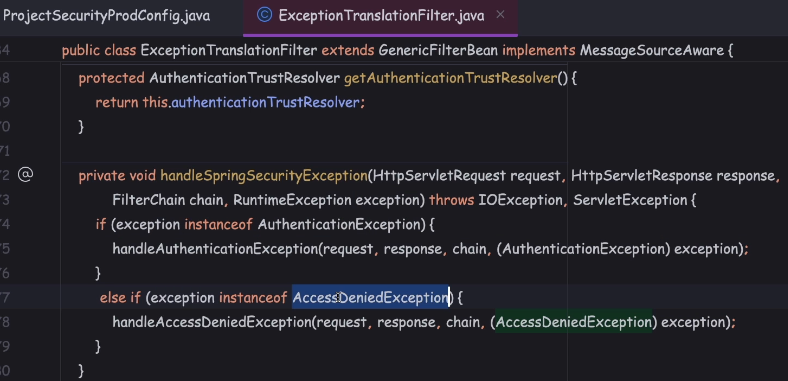
Accepting only HTTPS Traffic using Spring Security

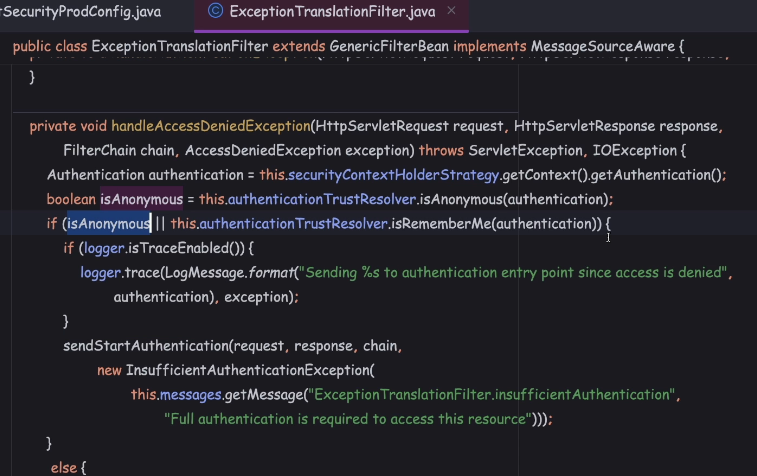
Exception Handling in Spring Security framework

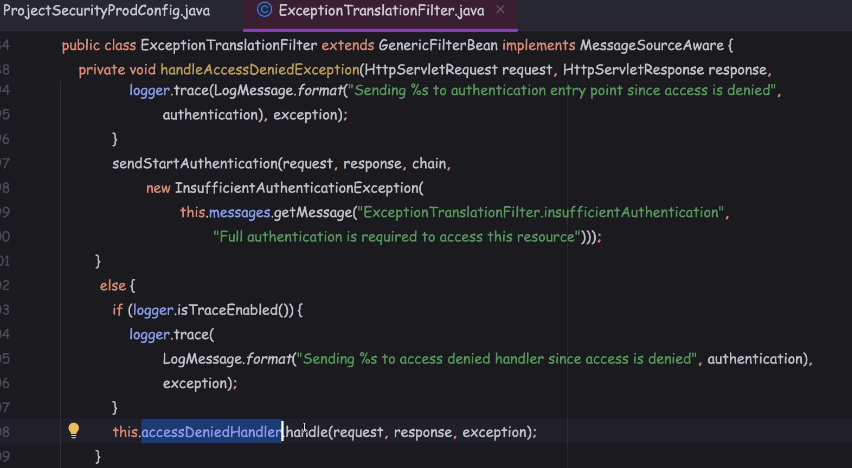
****

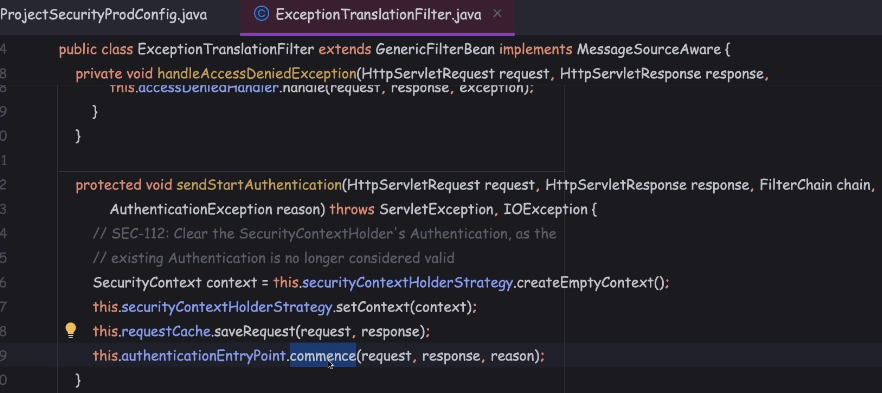
****

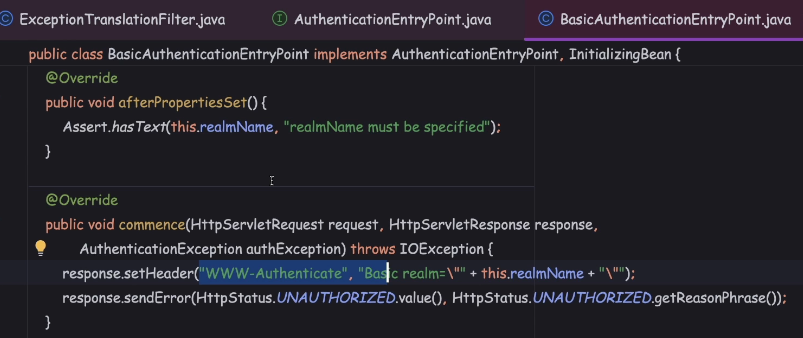
****

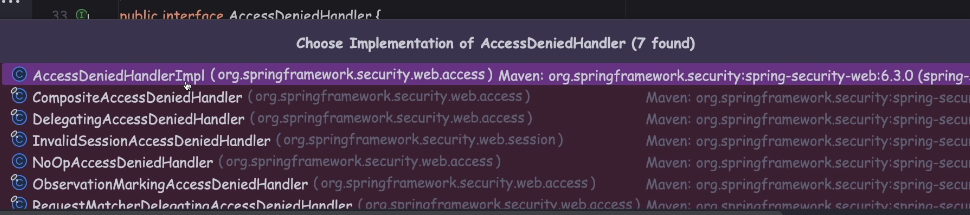
****

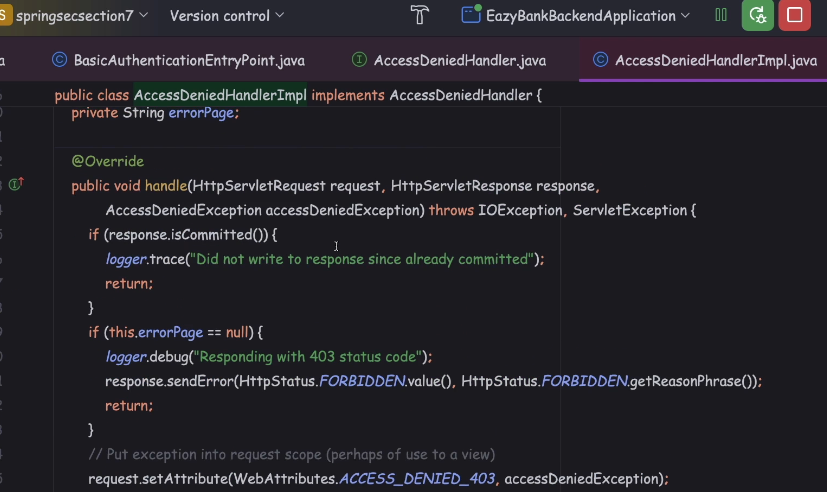
****

****

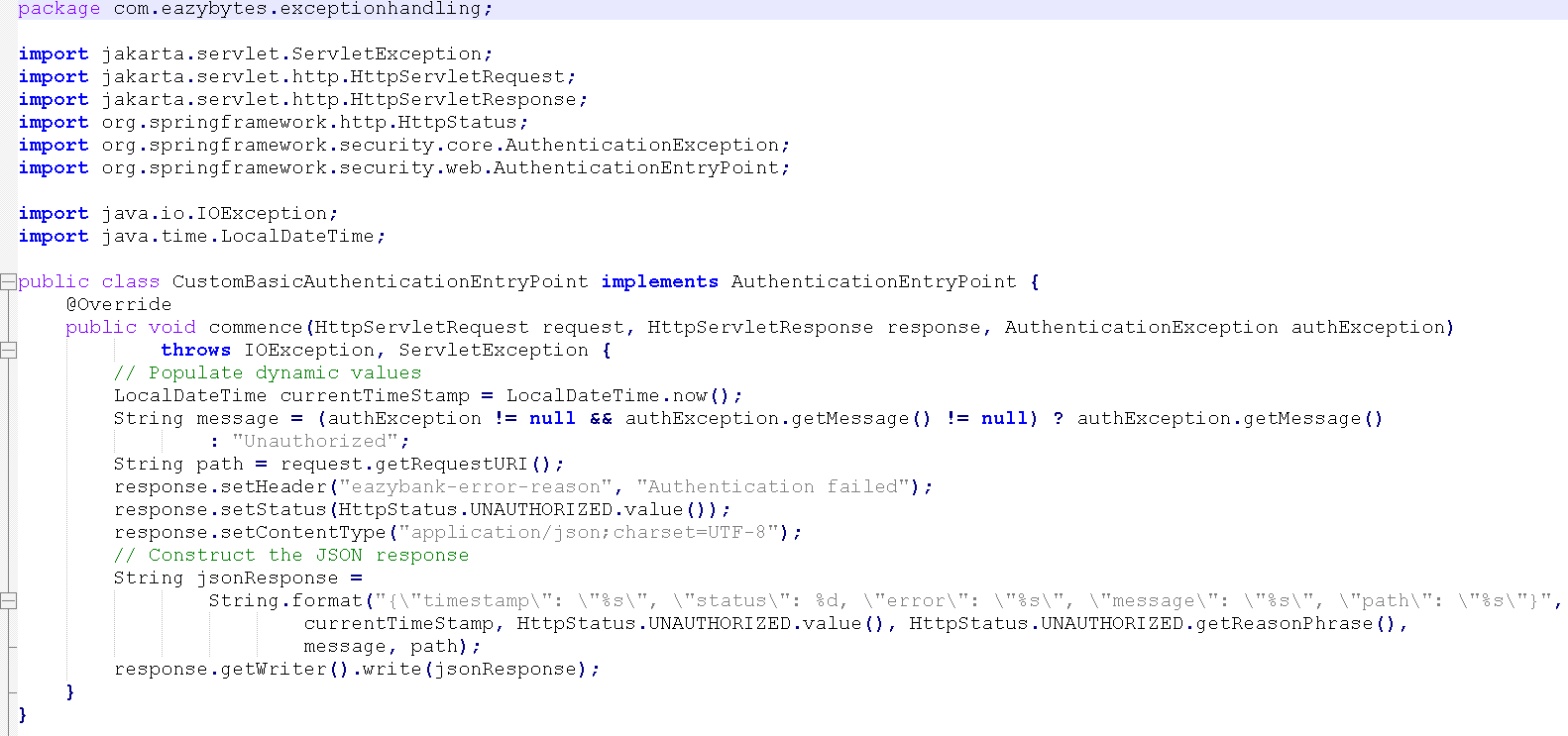
****

****





Defining Custom AuthenticationEntryPoint, Custom AccessDeniedHandler







what is the need of configuring these authenticationEntryPoint() at globally with the help of exceptionHandling?

If you try to configure the authenticationEntryPoint() only for the httpBasic(),

then these authenticationEntryPoint() is going to be executed or considered

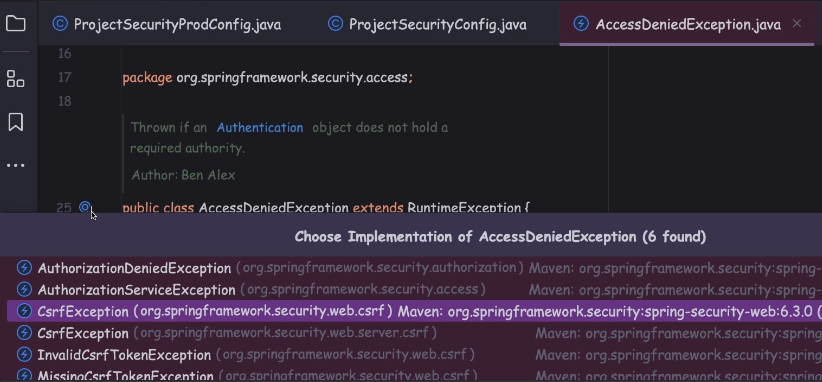
only during the httpBasic() flow, like during the login flow.

But apart from login flow, Spring Security may also throw 401

or AuthenticationException in many other places throughout the framework.

To handle all such possible scenarios, you can go with these global configuration.

Below are subclasses of access denied exceptions



Session Timeout & invalid session configurations

Default session timeout is 30 mins

server.servlet.session.timeout=${SESSION\_TIMEOUT:20m}

That's why Spring Boot never allow you to configure a timeout which is less than two minutes.

If I try to tamper this value by changing this eight to the six, then obviously this is an invalid session.

In this scenario, also though my session is not timed out, but I'm trying to access the API with an invalid session.

Even in these kind of scenarios also, the end user will be redirected

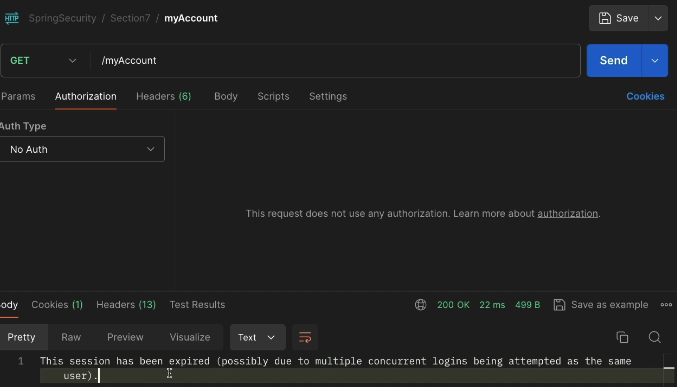
to the invalid session page instead of login page.

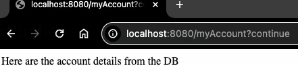
Regardless whether your session is getting invalidated due to some invalid tampered value or due to some timeout scenarios, in all these kind of scenarios,

the end user will be redirected to this page instead of the login page.

Concurrent Session Control configurations

http.sessionManagement(smc -> mc.invalidSessionUrl("/invalidSession").maximumSessions(1))





So the behavior right now we have is if the end user creates a new second session, the first session that the end user created is getting invalidate.

We can also change this behavior such a way that the end user can't create the second session, which means during the login of the second session itself,

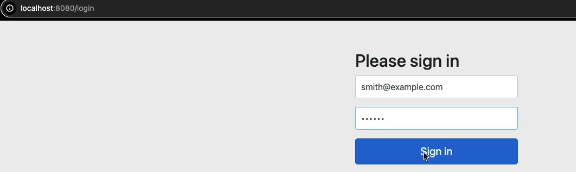
the end user will be stopped and the first session is always going to be retain.

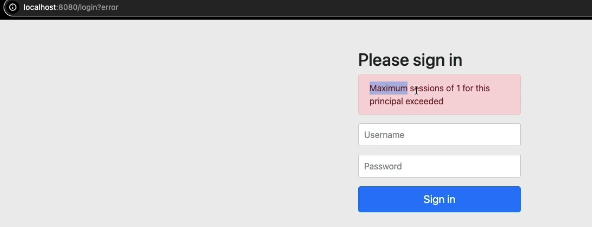
We can achieve this behavior by making a small configuration inside the Spring Security configurations. The configuration that we have to do here is we have

to invoke a method which is maximumSessionsPreventsLogin().

http.sessionManagement(smc -> smc.invalidSessionUrl("/invalidSession").maximumSessions(3).maxSessionsPreventsLogin(true))

access in browser after getting session in postman : localhost:8080//myAccount





if you want to have a fancy expired URL page, then feel free to leverage the expiredUrl() method.

But please note that whenever you are configuring the expiredUrl() with the path,

make sure that expiredUrl()path is also configured under the permitAll().

 Session Fixation Attack protection with Spring Security



To avoid Session Hijacking attack scenarios there are multiple approaches.

The very first approach the organizations they're going to use is, to use the history HTTPS protocol.

If they use the history HTTPS protocol for the communication, then hacker cannot steal the session ID during the network traffic or while your request is traveling throughout the internet.

And the next approach that typically organizations are going to follow is they're going to limit the session ID timeout for short time, like 10 minutes or 15 minutes.

At the same time, few organizations during the login operation,

they have a checkbox for the end user to check if they're using a public computer.

In such scenarios, the organizations are going to be very cautious in creating the cookies inside the browser.

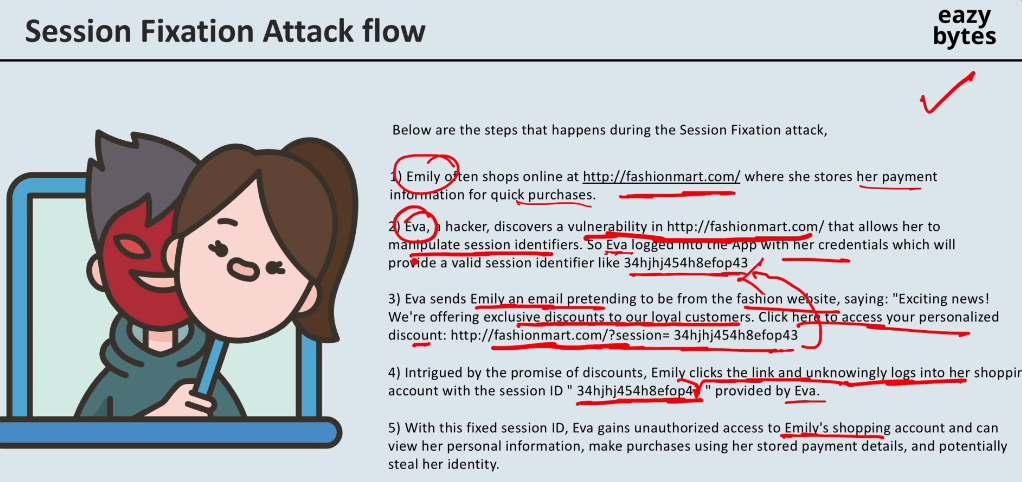
Instead of creating the cookies inside the user browser, they may switch to some other option.

So if you see here in the scenario of session hijacking, there is no role played by the Spring Security directly.

So the organization, they have to take multiple measurements like using the history HTTPS protocol, asking the end user if they're using the public computer

and having the session timeout with a very short time.

By using all these approaches, we can avoid the Session Hijacking scenario.



like how match fixation is going to happen inside the cricket matches and football matches. Very similarly here also the fixation is happening around the session ID.

Initially the hacker is going to generate a session ID and the hacker is going to provide the session ID to some other normal user and if the normal user use the same session ID to enter into the web application, then all the details of the normal user are going to be associated to the session ID which is originally shared by the hacker.

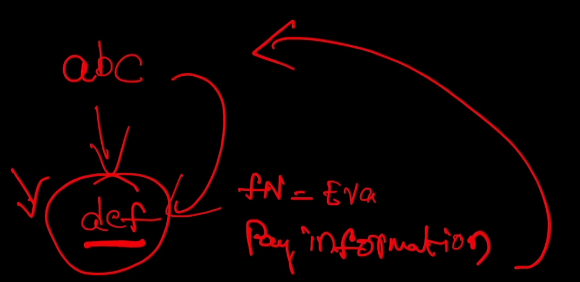
And with that hacker can happily use the session ID to know the normal user details.

This is happening because there is a vulnerability inside these Fashion Mart application. Ideally they should have some checks to avoid the Session Fixation Attack.

By default, if an application is using Spring Security as a dependency, Spring Security is going to take care of handling the Session Fixation Attack.



**changeSessionId** **strategy**



Let's assume the hacker initially performed the login operation and the hacker gave the session ID abc to normal person.

When the normal person trying to log in into the application with the **changeSessionId** **strategy**, the normal person is going to get the newSessionId

like def, but this session it is going to have all the details from the previous session.

For example, if the previous session has first name as Eva, the same details are going to be available inside this session as well with a different session ID which is def.

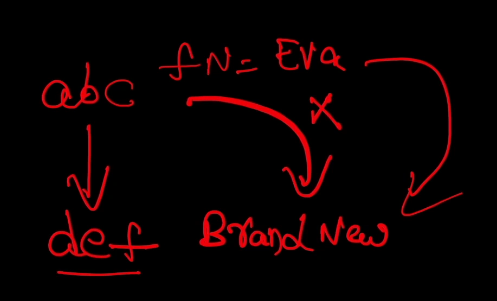
With this what is going to happen, the hacker will never know what is the new session ID that got generated on the normal person computer and with that he should not be able to see the extra details that are sailed inside this session.

Maybe payment information is stored after the login is completed.

So this extra information will never reach to the hacker because the hacker does not know the new session ID that got created.

So this is the default approach that is being used

by the Spring Security and Spring Boot framework as of now.



The next strategy available is new session.

In this newSession what is going to happen is, for example, first the hacker logged in

and the hacker got a session ID which is abc. The same is sent to the normal person.

And the normal person this time, even though he's trying to log in with the session ID abc but behind the scenes a new brand newSession is going to be created with the session ID like def.

So inside these brand newSession, the previous session details

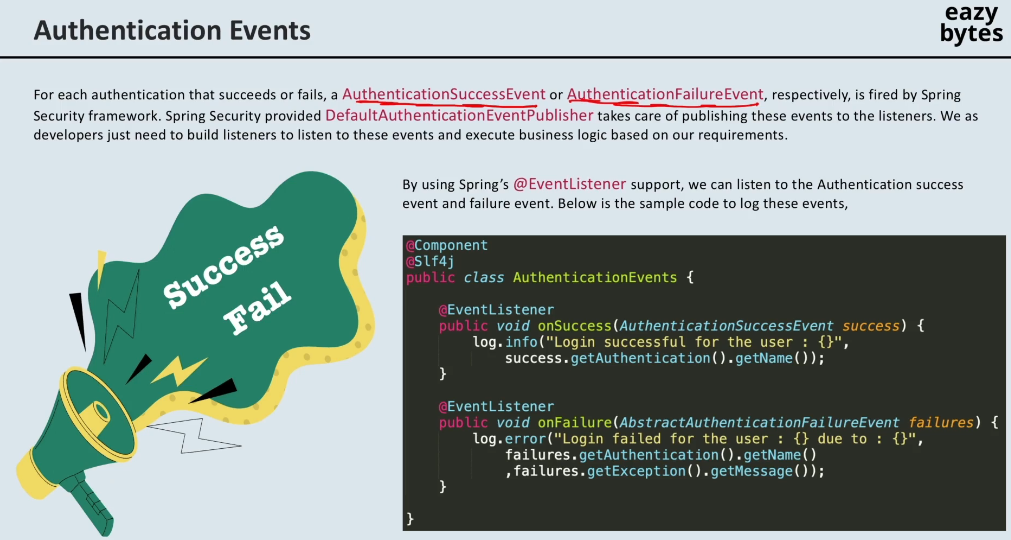
that are not going to be copied. For example, inside this session, if there is a variable which is first name as Eva, it is not going to be copied to the brand newSession

that is getting created here with the session ID def.

But please note that Spring Security related attributes, they're going to be copied into this brand new scenario.

So that is the only caveat that you need to be aware whenever you are using the newSession strategy.

 Listening Authentication Events



For example, on successful authentication, you may want to send an email to an end user saying that you have successfully authenticated, just informing the end user about the login operation.

This might be required for the super critical applications, and similarly, in the scenarios of authentication failure also, you may want to send an email

or you may want to make an entry inside the database that so and so failure attempts happened.

So, these kind of requirements are very common inside real applications.

To handle these kind of requirements, Spring Security is going to publish events

whenever an authentication is going to be successful and whenever the authentication is a failure.

