- Session puzzling is an application level vulnerability that occurs when the app session variable is using more than one purpose.

- Session variable overloading

- Attacker try to access application entry point.

- Session objects creation assigned

Impact:

session puzzle enable the attacker to bypass authentication, impersonate legitmate users, elevate priviledge, bypass flow restrictions, and execute additional attacks

How to hunt:

1. reset your password, application will generate session key.
2. you reset your password, same session continue and you are loged in.

How to detect:

session puzzle can be detected and exploited by enumerating all the session variables used by the application and in which context they are valid.