JWT Tokens

- the jwt token always have the start with (ey)
- jtw token bugs can lead to privilage escalation and account takeover
- it contains 3 parts : headers , payload ,signature
- we use the token.dev website to analyze the token or we use jwt.io
- another edit that can be done to this is the cookies expiration where it can extended .

scenarios :

---

1. what we do to try and edit on the token because the signature may be not verified in the server so we can change the user to admin or administrator and get admin privilege and we edit it within the payload .(first lab in port swagger) where the signature is not verified
2. the developer may check for the signature if its valid or not but if we send the signature value with null we may get access because the server lack validation and we will get access(**we can change the signature to non using the jwt editor in burp suite**)
3. third scenario is that the signature is weak and can be cracked using craking tools like hascat or john the repear and then using the jwt editor we start adding a new key and just change the K field inside of it with the key we got from the crack tool then we get back to the repeater and change the sub in the payload to admin or administrator and attack using the key we just generated and by that we got admin access .
4. we can also try to add a jwk algorithm where the server will check for the first algorithm only and this will bypass the jwt verification
5.