Episode 3

Hacking Sunday

JWT

Twitter- @trouble1_raunak

WHAT IS JWT?

In simple words JWT is a web token which contains a some information and a key which is verified only in the back-end.

Its main purpose is the provide data to valid users only

You can say like it helps to prevent IDOR's/Access control

HOW DOES JWT LOOKS LIKE?

Token looks like this which is Base64 encoded separated by 3 dots

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.SflKxwRJSMeKKF2QT4fwpMeJf36POk6yJV_adQssw5c

HOW DOES JWT LOOKS LIKE?

If we decode it

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.SflKxwRJSMeKKF2QT4fwpMeJf36POk6yJV_adQssw5c

{"alg":"HS256","typ":"JWT"}.{"sub":"1234567890","name":"JohnDoe","iat":1516239022fQ.lùJÇIHÇ(□Ob□¤Ç□
~:□N²JV_iÔ,³\

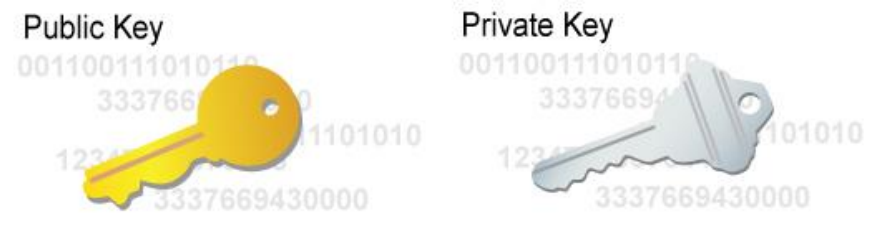
HOW DOES JWT LOOKS LIKE?

```
{
  "alg": "HS256",            ==>      Header
  "typ": "JWT"
}
{
  "sub": "1234567890",       ==>       Payload
  "name": "John Doe",
  "iat": 1516239022
}
HMACSHA256(
  base64UrlEncode(header) + "." +          ==> signature
  base64UrlEncode(payload), secret
)
```

SIGNATURES

Asymmetric

Works with private and public key



Symmetric

Works private key only

ATTACKS

Most common attack
Changing "alg": "HS256" => "alg": "none"

None means that there is no algorithm is use and due to which you can access information without a signature
LoL.

But now a days this is a very rare case

ATTACKS

Most common attack
Changing "alg": "HS256"   => "alg": "none"

None means that there is no algorithm is use and due to which you can access information without a signature
LoL.

But now a days this is a very rare case

LET'S JUMP RIGHT INTO OUR LAB

THANK YOU

Motivated by - @m0nkeyshell