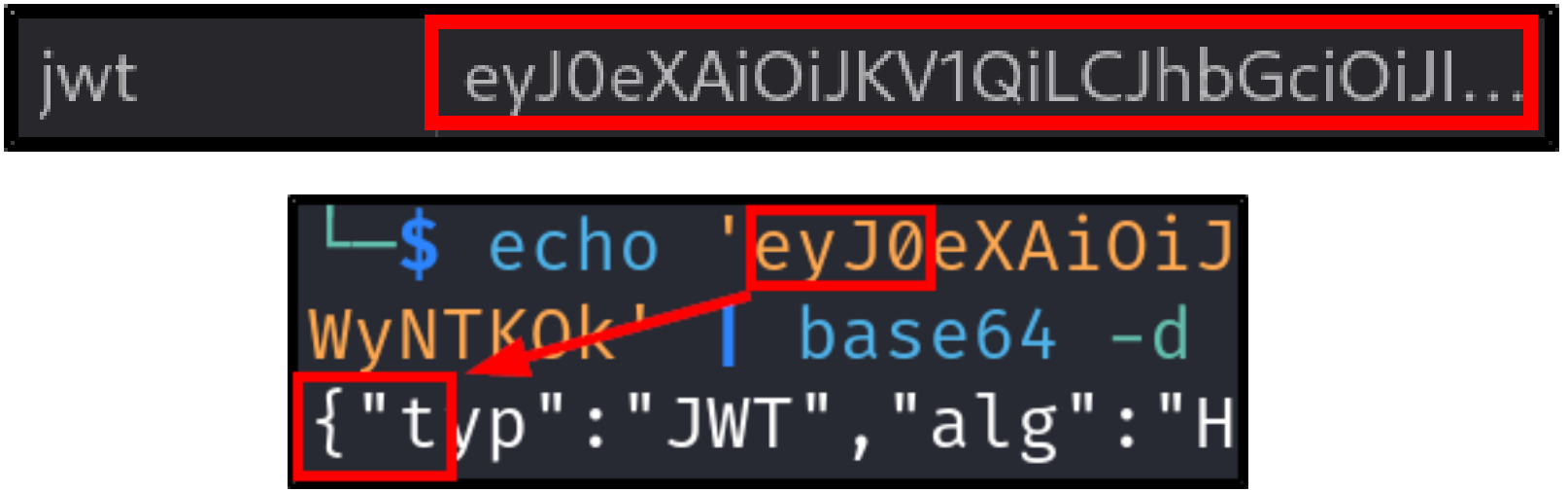
JWTs (JSON Web Token)

JSON Web Tokens, common called JWTs, are a common technology that web apps use to handle user sessions, and they're passed to web browsers as cookies

Identifying JWTs

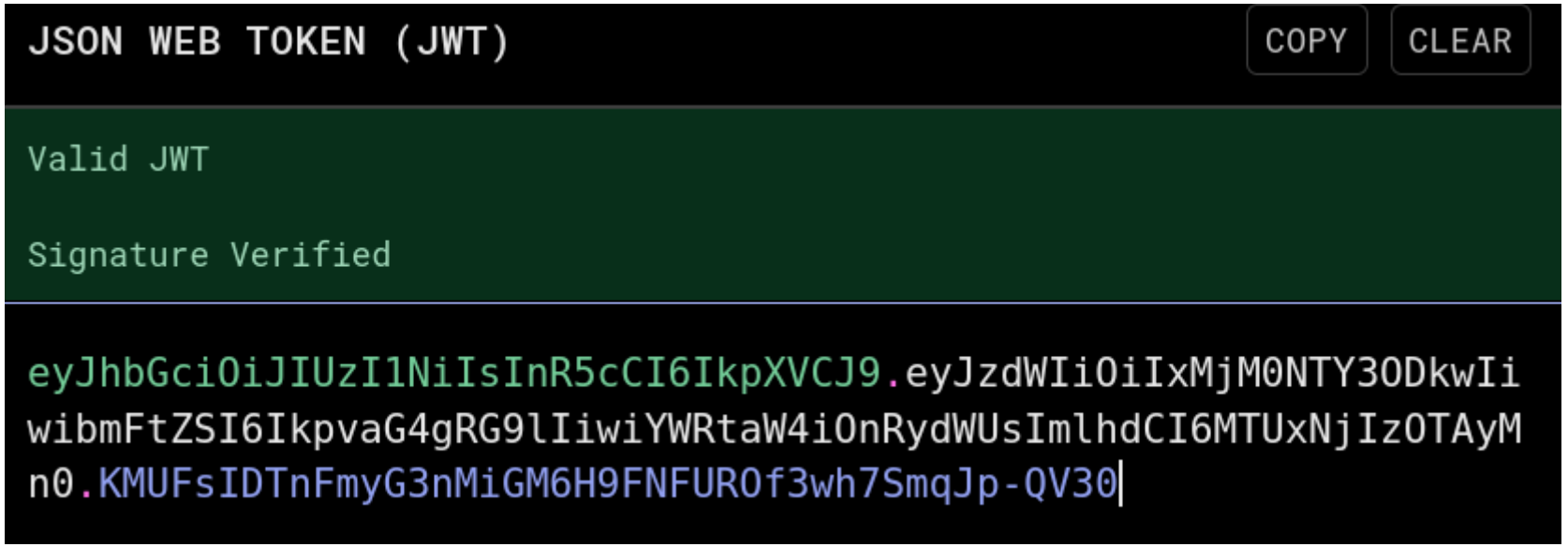
JWTs can be easily identified as a cookie value that begins with the characters `eyJ0`., that's because the first part of the JWT is encoded as a base64 string

Identifying JWTs



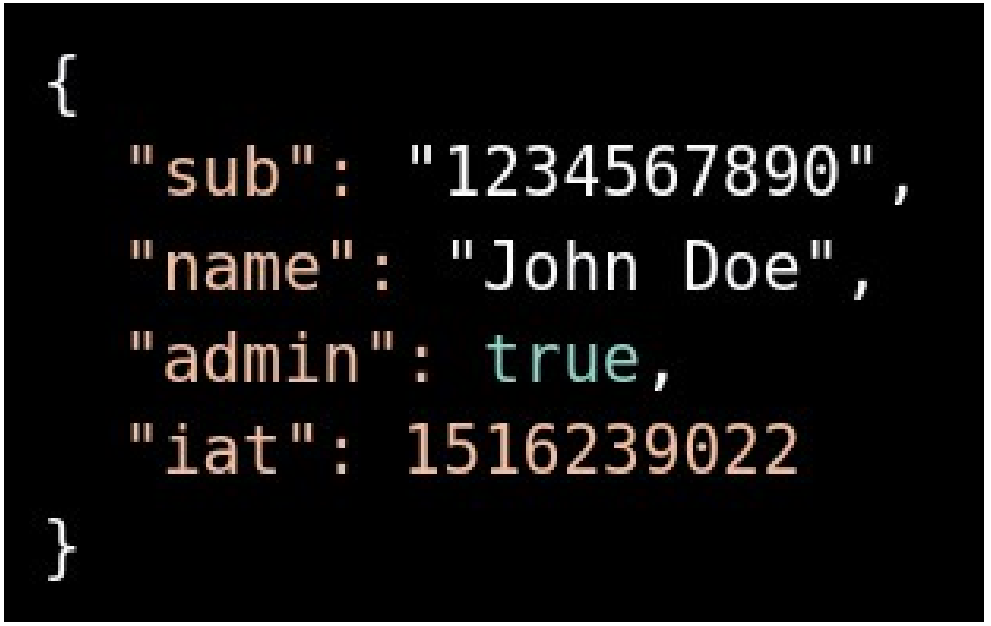
All decoded JWT values begin with `{"typ"`, so we can ID their encoded values easily

Reading / Writing JWTs



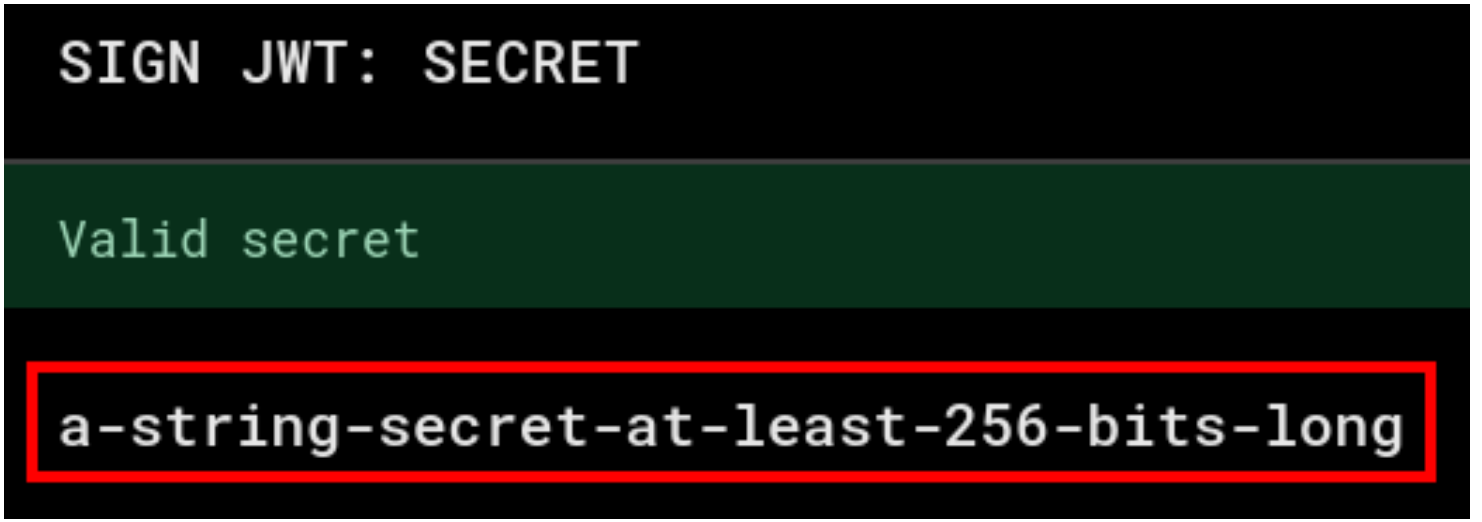
There are many different tools we can use to read and write JWTs, such as the the **jwt.io** web app

Reading / Writing JWTs



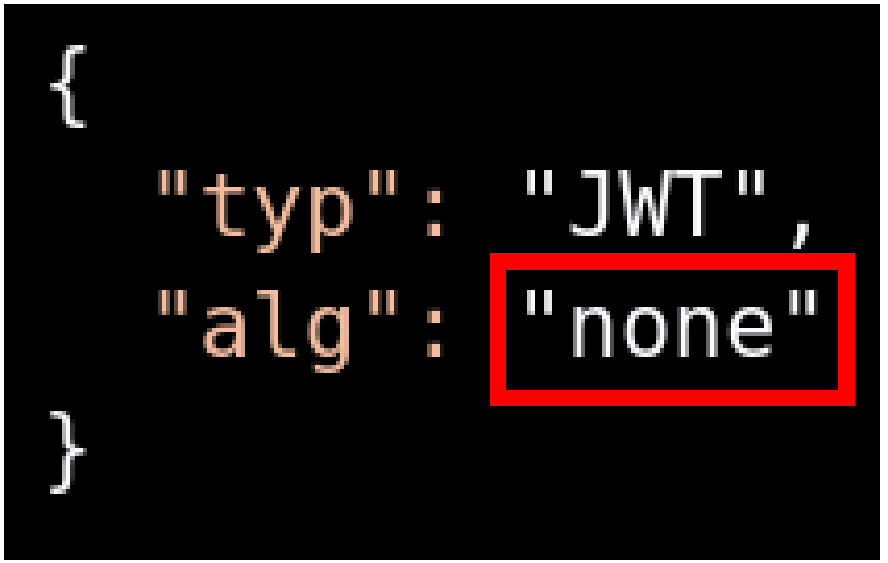
The same web app can be used to modify JWT data, which could be used to get access to different user accounts

JWT Signing Keys (Secrets)



The last detail about JWTs is that they must be signed using a key word (secret) to be considered valid by the web app

The Alg:none Vulnerability



There is a well-known vulnerability for JWTs where some web apps will accept JWTs that have not been signed (Alg:none), bypassing the need for a valid secret