Exploitation of Json Web Tokens

By Mohit Vohra

What is JSON?

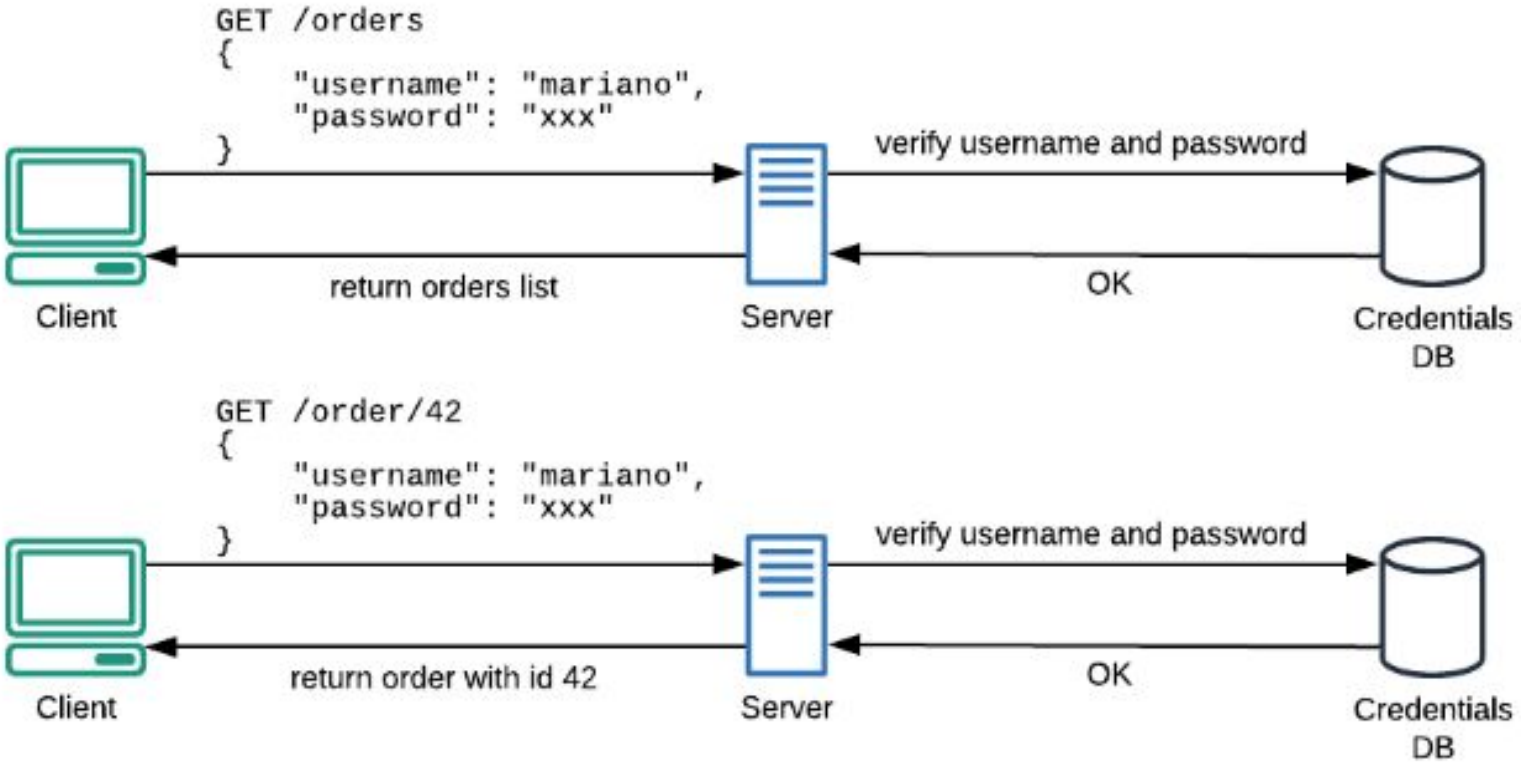
JSON (JavaScript Object Notation) is a lightweight format that is used for data interchanging.

```
{
    "firstName": "John",
    "lastName": "Smith",
    "address": {
        "streetAddress": "21 2nd Street",
        "city": "New York",
        "state": "NY",
        "postalCode": 10021
    },
    "phoneNumbers": [
        "212 555-1234",
        "646 555-4567"
    ]
}
```

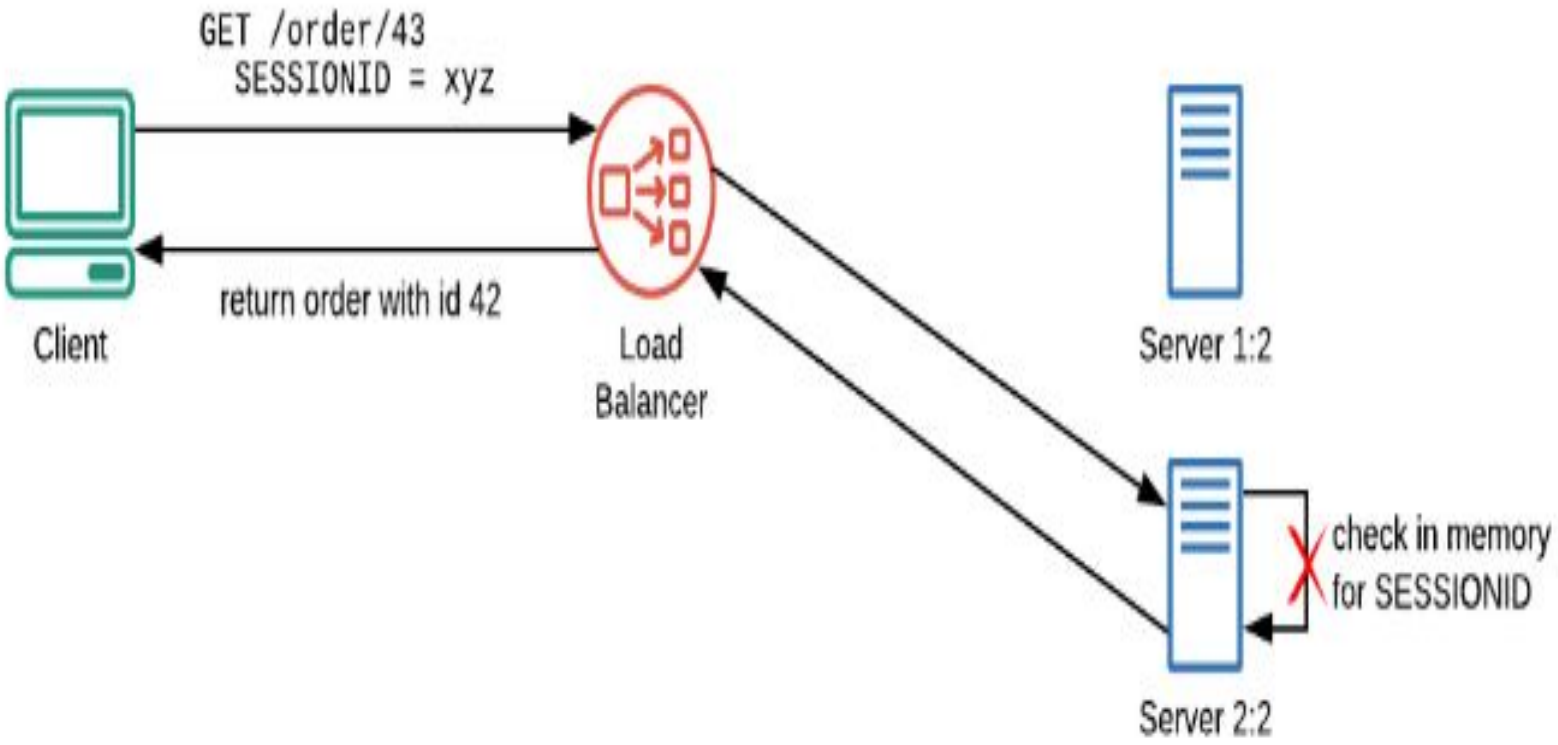
What is JWT?

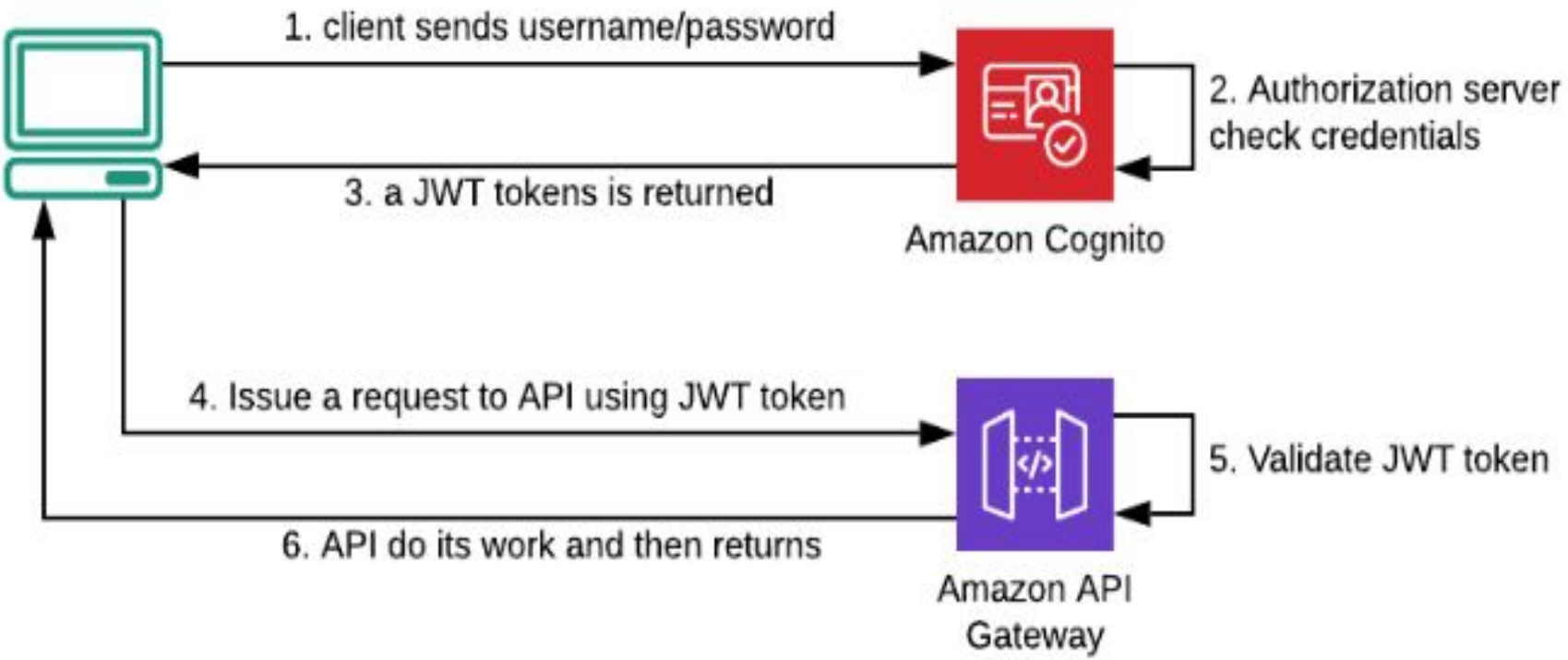
JSON Web Token (JWT) is an open standard that defines a compact and self-contained way for securely transmitting information between parties as a JSON object. This information can be verified and trusted because it is digitally signed. JWTs can be signed using a secret (with the HMAC algorithm).

Why need for it in industry?



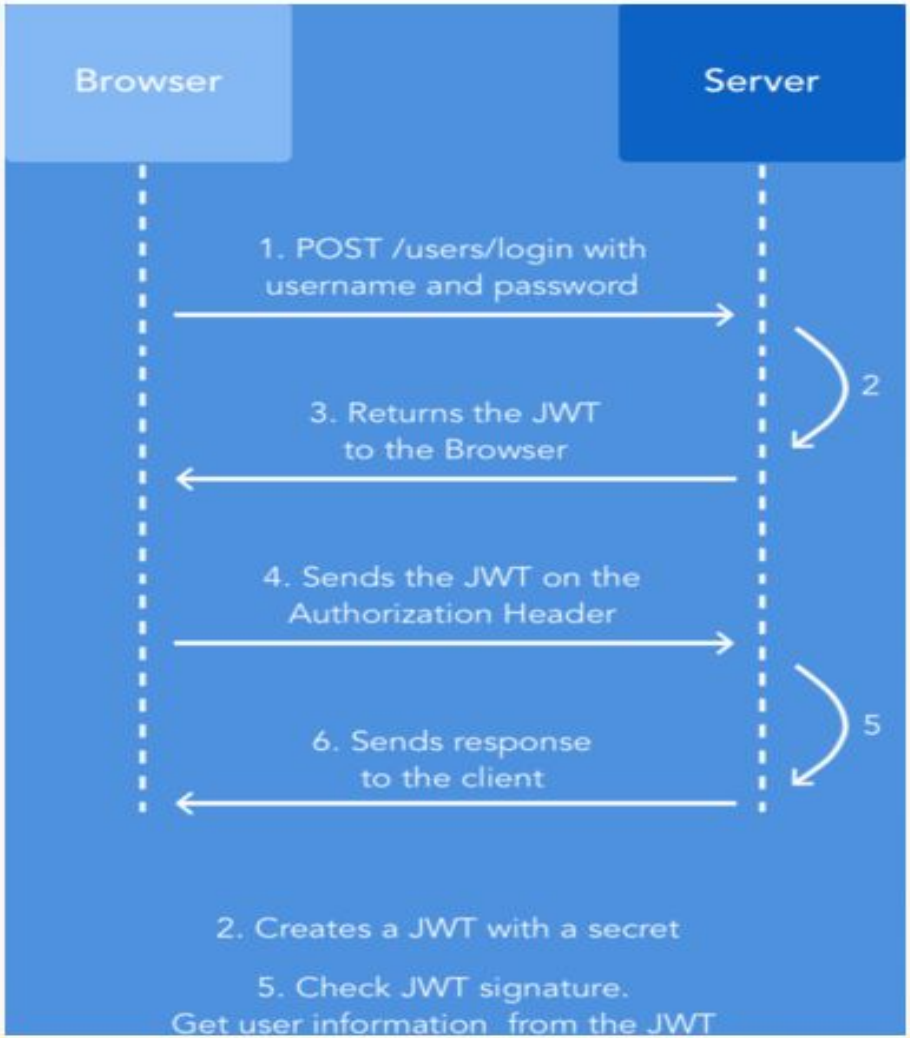
HTTP connection


GET /order/43
SESSIONID = xyz
return order with id 42
Client
Load
Balancer
Server 1:2
Server 2:2
check in memory
for SESSIONID



JWT workflow

Architecture of JWT



How the token look like?

```
Base64(Header).Base64(Data).Base64(Signature)
```

Multiple signature methods used for JWT integrity

- RSA Based
- Elliptic curves
- HMAC
- None

Exploitation of JWT

Bang ..!!! Bang ..!!!

Thank You