Week 8 WDD330

miércoles, 7 de junio de 2023 20:28

Ruth Cardona!

JSON Web Token (JWT)

IS AN OPEN STANDAR USED TO SHARE SECURITY INFO BETWEEN TWO PARTIES.

- INFO IS SHARE AS A JSON OBJECT
- IS DIGITALLY SIGNED (CAN USE PUBLIC OR PRIVATE KEY PAIR OR A SECRET)

- IT CAN BE:
  - COMPACT => - BECAUSE OF ITS SIZE
    - IT CAN BE SENT THROUGH URL, POST, HTTP HEADER
    - ITS TRANSMISSION IS FAST
  - SELF-CONTAINED - PAYLOAD CONTAINS ALL REQUIRED INFO ABOUT USER

WHEN TO USE THEM?

- AUTHENTICATION: - ONCE USER IS LOGGED IN, EACH SUBSEQUENT REQUEST WILL INCLUDE THE JWT
  - THIS ALLOWS USER TO ACCESS ROUTES, SERVICES AND RESOURCES THAT ARE PERMITTED WITH THAT TOKEN.

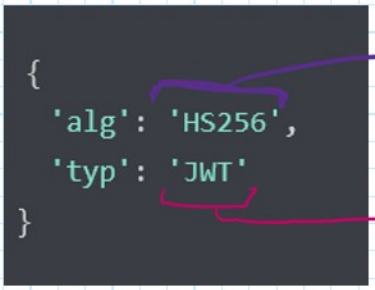
- INFORMATION EXCHANGE: - SECURE AND SIGNED
  - YOU CAN VERIFY THE CONTENT, SENDER, HEADER, PAYLOAD

STRUCTURE:

HEADER — PAYLOAD — SIGNATURE

xxxxx.yyyyy.zzzzz

- HEADER => IT HAS TWO PARTS



- THIS JSON IS BASE64URL ENCODED TO FORM THE FIRST PART OF JWT

. PAYLOAD ⇒ IT CONTAINS THE CLAIMS (STATEMENTS ABOUT AN ENTITY AND ADDITIONAL METADATA). THERE ARE THREE.

- RECERVED CLAIMS PREDEFINED CLAIMS, RECOMMENDED TO PROVIDE A SET OF USEFUL INTEROPERABLE CLAIMS
  EXAMPLES: iss (ISSUER), EXP (EXPIRATION TIME), SUB (SUBJECT) AUD (AUDIENCE), ETC

- PUBLIC CLAIMS TO AVOID COLLISIONS THEY SHOULD BE DEFINED IN IANA JSON WEB TOKEN REGISTRY OR AS A URL THAT CONTAINS A COLLISION RESISTANT NAMESPACE.

- PRIVATE CLAIMS THE CUSTOM CLAIMS CREATED TO SHARE INFO BETWEEN PARTIES THAT AGREE ON USING THEM

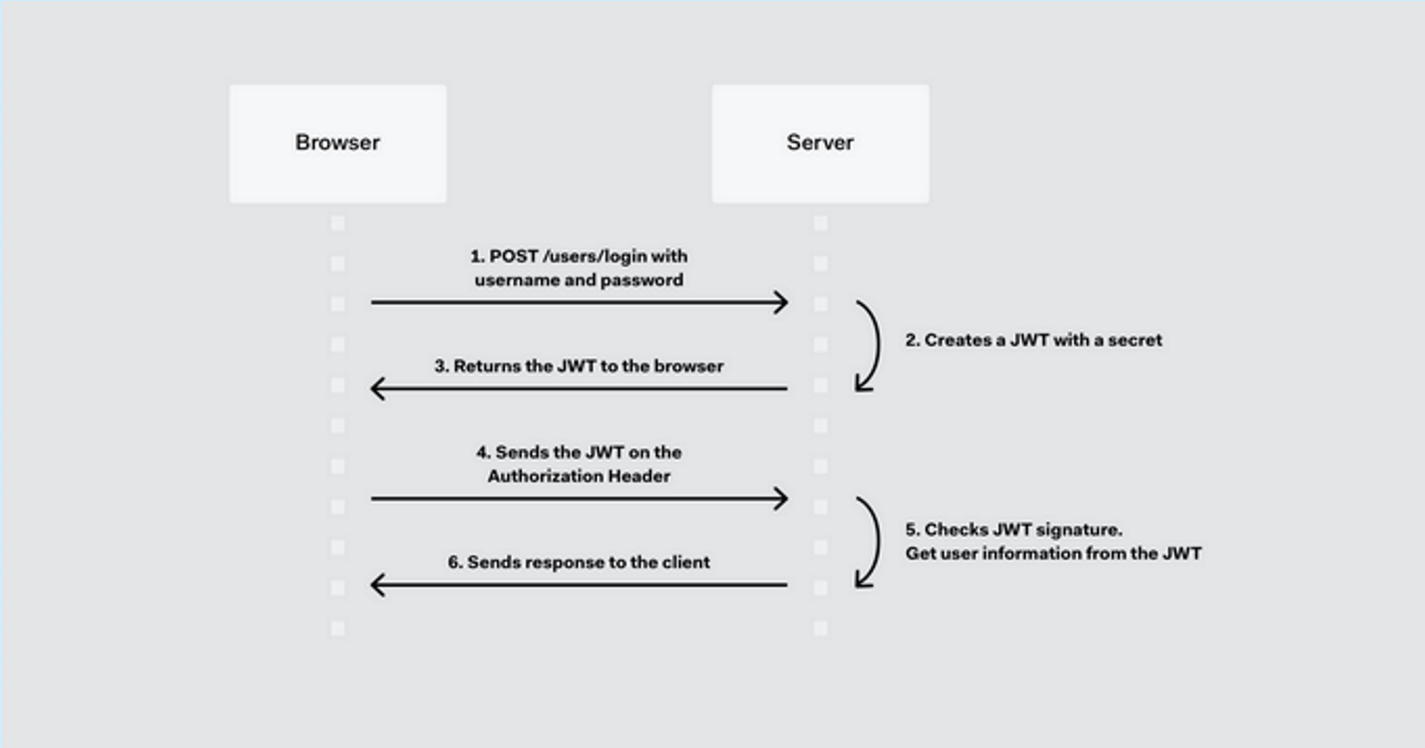
. SIGNATURE IS USED TO VERIFY THAT THE SENDER OF THE JWT IS WHO SAYS IT IS AND THE MESSAGE WASN'T CHANGED.

```
HMACSHA256(
  base64UrlEncode(header) + '.' +
  base64UrlEncode(payload),
  secret)
```

FULL EXAMPLE =>

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4
gRG9lIiwiaXNTb2NpYWwiOnRydWV9.
4pcPyMD09olPSyXnrXCjTwXyr4BsezdI1AVTmud2fU4
```

How they work ?



- WHEN THE USER SUCCESFULLY LOGS IN USING THEIR CREDENTIALS A JSON WEB TOKEN WILL BE RETURNED.

YOU SHOULD NOT STORE SENSITIVE SESSION DATA IN BROWSER STORAGE

DO NOT TRUST ANYTHING COMMING FROM THE BROWSER.

WHEN USER WANTS TO ACCESS A PROTECTED ROUTE IT SHOULD SENT THE JWT.

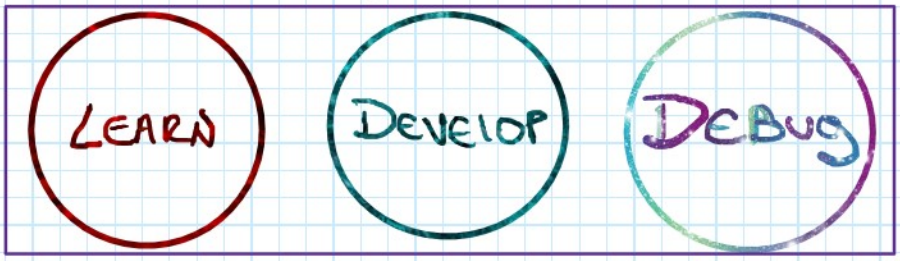
- USING THE BEARER SCHEMA: `Authorization: Bearer <token>`, THE USER STATE IS NEVER SAVED IN THE SERVER MEMORY
- THE SERVER'S PROTECTED ROUTES WILL CHECK FOR VALID JWT TO ALLOW THE USER GET THE INFO
- IT ALLOWS FULLY RELY ON DATA APIs THAT ARE STATELESS.

WHY TO USE THEM?

- IT'S COMPACT, MORE THAN SAML
- SECURITY-WISE. (SECRET, PUBLIC/PRIVATE KEY PAIR)
- IS USED AT AN INTERNET SCALE

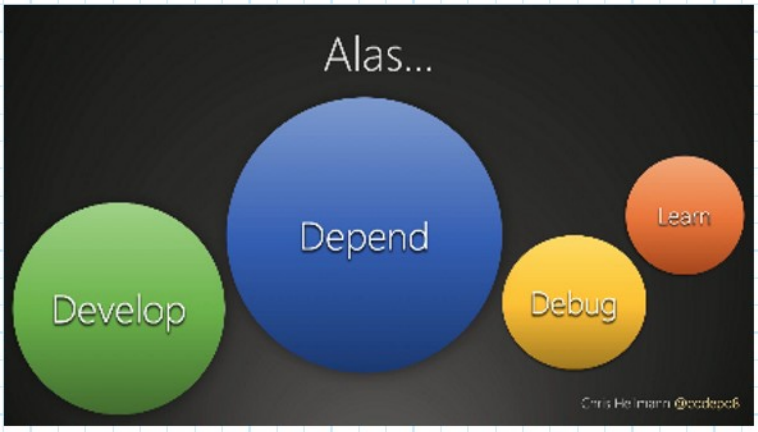
Develop, Debug, Learn? - Chris Heilmann (dotJS 2019 - Chris Heilmann - Develop, Debug, Learn?)

- WE LEARNED JS (THROUGHT THE YEARS) AS A LOGICAL ORDER...



- WE COULD DO THIS IN THE BROWSER
- LATER IT CAME ABSTRACTION AND LIBRARIES, THIRD-PARTIES, ETC

- IN OUR DAYS WE DEPEND MOSTLY ON OTHER THINGS WHEN DEVELOPING (OTHER PEOPLES CODE), AND THIS BECOME MORE DIFFICULT TO DEBUG



- WE CAUGHT IN A RUSH OF BECOMING THINGS BETTER AND BETTER

BUT WE LOSE THE FOCUS OF OUR END USER

- IT'S NOT ABOUT US, IS ABOUT THE END USER
  ↳ WHAT ARE THE NEEDS OF OUR END USER?

- "THIS IS NOT ABOUT US. THIS IS ABOUT TECH LEGACY"
  ↳ TECH DOES NOT HAVE GOOD REPUTATION IN OUR DAYS:
  - BECAUSE OF LACK OF MANTAINANCE OF OLD CODE USE BY MANY PEOPLE

- AS DEVELOPERS WE HAVE AN OVERLOAD! (TO MUCH DEMANDS ON KNOWING EVERYTHING!) THAT MAKE USE OVERWHELME

"WE WORK ON FAITH" (HOPING THAT THE PARTIES WE USE HAS EVERYTHING WE NEED)

- "YOU ARE NOT A REAL (OR GOOD) DEVELOPER" IF YOU DON'T KNOW EVERYTHING YOU SUPOSE TO... (THAT'S WHAT OTHER WANTS YOU BELIEVE)

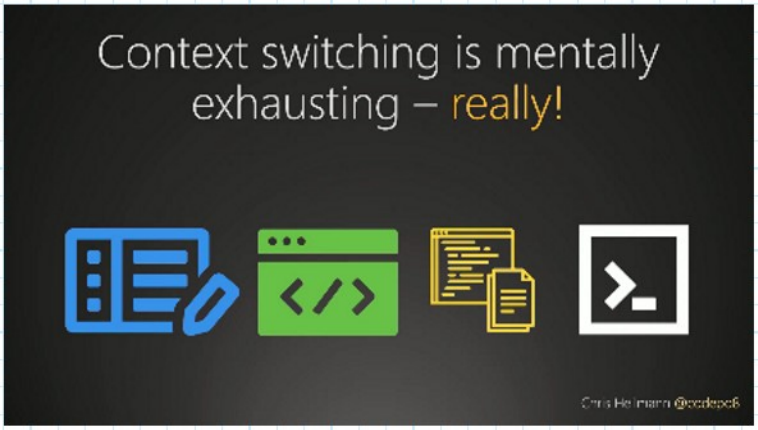
WE ARE FULL-STACKOVERFLOW DEVELOPERS (COPY-PASTE-WORKS-WOHOO?)

WHAT IS THE PROBLEM?:

- WE ONLY USE LIKE 10% OF THE DEVELOPERS TOOLS. WE HAVE THE

- WE ONLY USE LIKE 10% OF THE DEVELOPERS TOOLS. WE HAVE THE AMAZING DEBUGGING TOOLS BUT WE ARE STILL USING CONSOLE.LOG()

- SWITCHING IS MENTALLY EXHAUSTING



- AND WHEN WE SPEND TO MUCH TIME CUSTOMIZING EACH ENVIROMENT...

RETHINKING TOOLING => PREVENT US FROM DOING THINGS WRONG INSTEAD OF PATCHING UP WHAT WE CREATED.

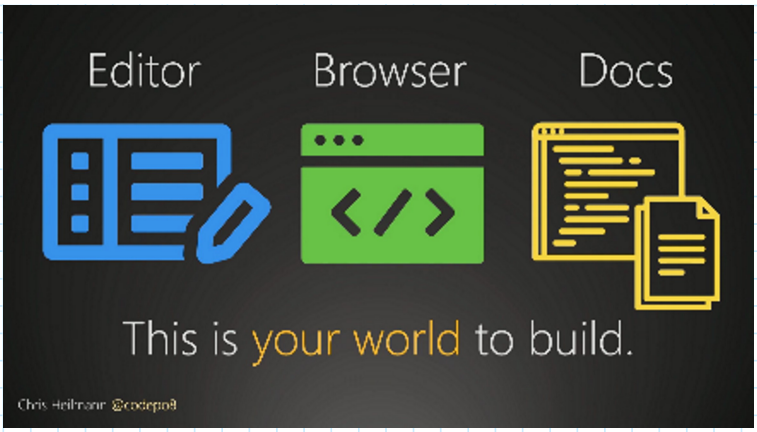
- "WHY ARE OUR DEVELOPMENT ENVIROMENT NOT ALSO ON THE WEB?"

TO HELP PEOPLE LEARN WHILE THEY ARE DEVELOPING.

"OPEN SOURCE CODE IS A RESOURCE"

↳ FOR EX = AUTOCOMPLETE

THIS IS A GOOD TIME TO MAKE EASIER FOR PEOPLE TO BECOME A DEVELOPER BY USING THESE SYSTEMS (ENVIROMENT, OPEN SOURCES, LEARN WHILE DEVELOPING)


Editor
Browser
Docs
This is your world to build.
Chris Heilmann @codepo8