**Rest API Best Practices**

**By name:**

* Url should not indicate any kind of CRUD function (link getUser, postStudent)

Ex: /user/{:id} instead of /getUser

* Using noun not verb
* Using ( , ) for multiple same data

Ex: /user/{:id}, {:id}

* Always use lower-case & dash ( - )

Ex: /pending-order instead of /Pending\_Order

* No file extension
* No ( / ) provide in lest

**Response**:

* Provide Status code
* Provide File type
* Provide cash status
* Provide Authentication token
* Provide String (req, res)
* Provide Length
* Provide Date & time

**Response Body:**

* Avoid response status, massage
* Doesn’t use json for single data

**Request**:

* Structure json Array & Object
* Multipart form data for Image/audio/video
* Should not hold any authentication data

**Request Header:**

* Carry all security information
* Provide Key:value
* Provide User-agent

**Controller**:

* Clean as possible & shouldn’t place any business logic
* Consider API version

**Middleware**:

* Use to implement API key, user-agent, restriction, CSRF, security, API authentication
* Rate limit
* log/ document store
* Redirecting
* Inspect Request

**Security**:

* API key verification
* User-agent verification (for type of device access control)
* CSRF (cross site scripting protection)
* Rate limit
* HTTP security Header
* Parameter pollution
* Data sanitization (SQL injection / schema)
* Authentication

**Json Best Practice**

* Easy to read
* Lightweight
* Language independent
* Always enclose the key:value pair within double quotes

Ex: {“name”: “Riad”}

* Never use hyphens (\_) & dash (-) in key field

Es: {“firstName”: “Riad”}

* Always a Root element

Ex: { **main**: [

{

“name”: “riad”

}

]

}