PGS SOFTWARE

The Art of Web API Design

How to keep sanity while creating noisy applications

PAWEŁ ZAJĄCZKOWSKI · @gvaireth

Author

Paweł Zajączkowski

@gvaireth

- Made in Poland in the eighties
- Javaloper since 2009, for telecom, logistics, banking, automotive…
- …and PGS Software
- Likes beautiful code, agility and open minds
- …also Aikido, Lego, Dota2 and scribbling stuff

Agenda

The Scout - Intro

The Wizard - Theory

The Warrior - Core

The Cleric - Support

Intro

- Why?
- What?
- How?

Made with ♡ by PGS Software ·

Why

- Data is precious
- Evolution of web applications
- Everything talks to everything

Made with ♡ by PGS Software ·

What

- Server-side web API
  - Programatic Interface
  - Public Endpoints
  - Request - Response

How

- People vs Machines Balance
- API Design: UX for programmers
- Laziness
- Intuition - POLA

Made with ♡ by PGS Software ·

Theory

- Morville
- Fielding
- Richardson

Morville’s UX Honeycomb

- Useful
- Usable
- Desirable
- Findable
- Accessible
- Credible

- **Value**

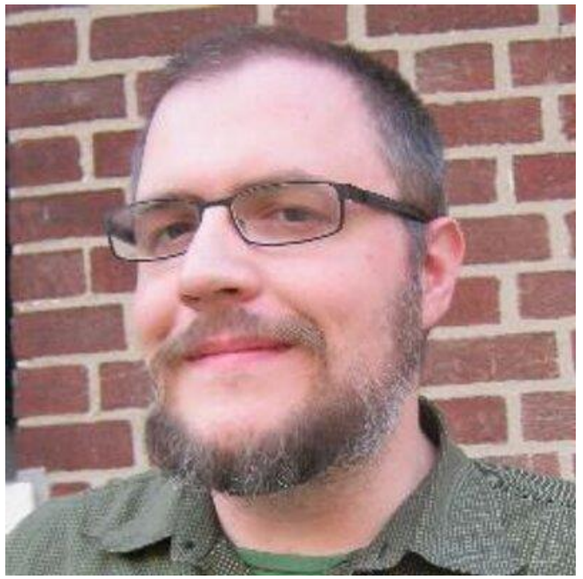
Made with ♡ by PGS Software ·

Fielding’s REST

- Client-Server
- Stateless
- Cacheable
- Layered System
- Uniform Interfaces
- Code on Demand

Richardson’s Maturity Model

- Level 0: The Swamp of POX
- Level 1: Resources
- Level 2: HTTP Verbs
- Level 3: Hypermedia Controls



Made with ♡ by PGS Software ·

Core

- Resources
- Relations
- Behavior
- Functions
- Parameters
- Naming
- Searching
- Sorting
- Pagination
- Status

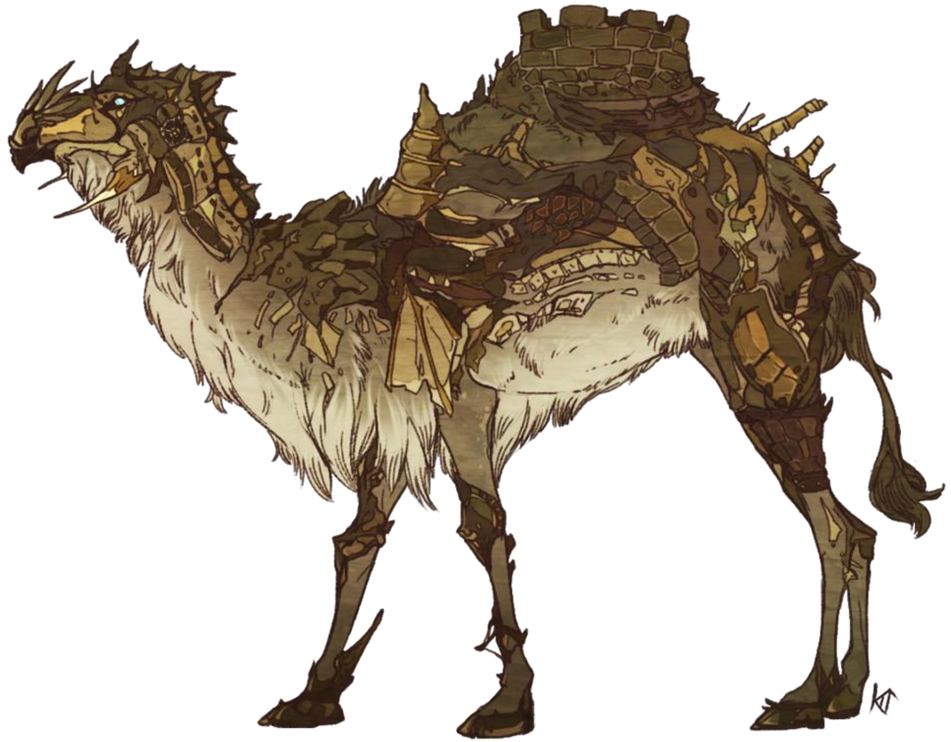
Resources

- Resources and Representations
- Nouns
- Plural forms
- Hide details

Made with ♡ by PGS Software ·

Camels vs Snakes

- JavaScript convention of **camelCase**
- Readability of **snake_case**
- Elegance of **hyphen-case**
- Anyway: Be consistent



Made with ♡ by PGS Software ·

Relations

- Many to many relations: top-level resource
- Can be added / deleted
- /**groupMemberships**/123
- Sub-resources if there is dependence
- /buildings/123/**rooms**/456

Made with ♡ by PGS Software ·

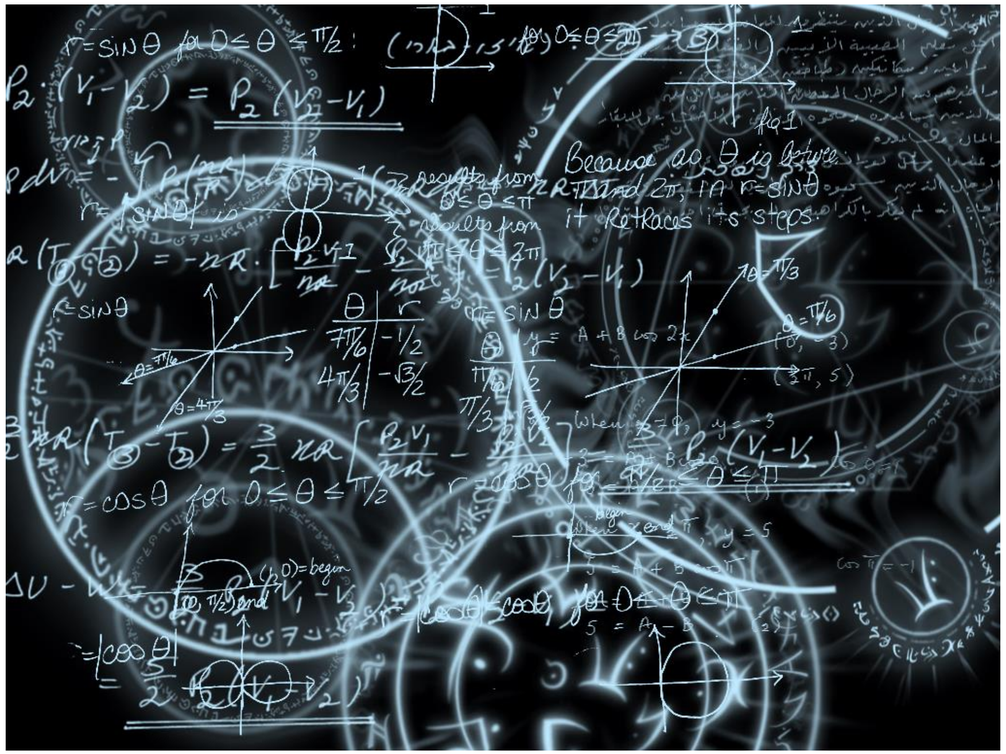
Behavior

- HTTP verbs on list / item
- GET: get list / get item
- POST: create without id / error or partial update
- PUT: update batch / create with id or full update
- DELETE: delete batch or error / delete item
- PATCH: error / update part of item

Made with ♡ by PGS Software ·

Functions

- What if it’s not resource?
- Mask it as resource
- Star and unstar: /gists/123/**star**
- Otherwise document it
- Don’t be dogmatic



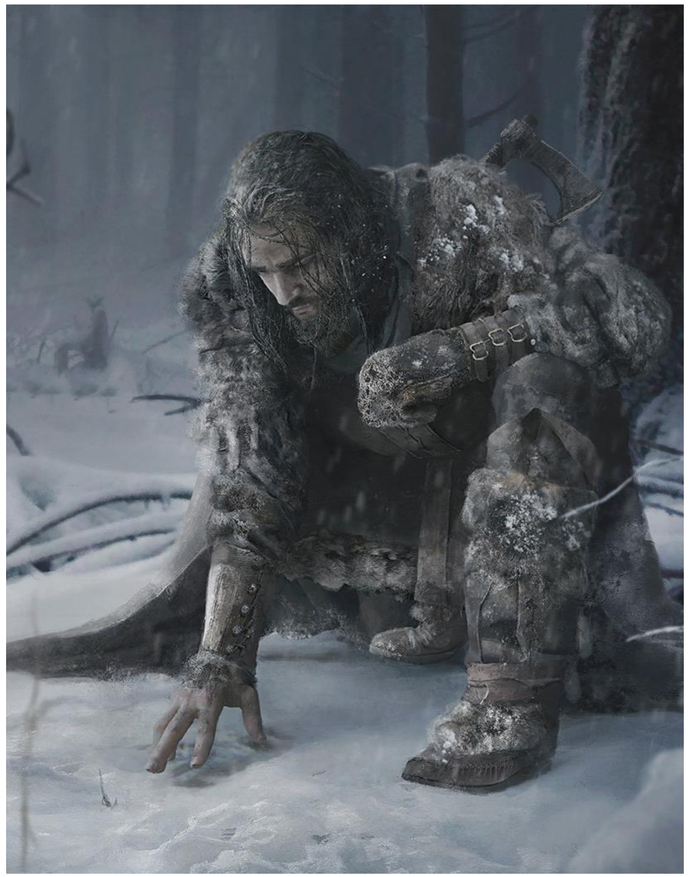
Parameters

- Path – resource identifiers, mandatory
- Query – optional
- Header – global
- Custom Header – specific global
- Body – resource specific
- _underscored – meta / control

Made with ♡ by PGS Software ·

Searching / Filtering

- Query parameters: /…?**age**=27
- SQL-like language: /…?**nameLike**=Schw%gger
- Fields included: /…?**fields**=name,title
- Exclusions: /…?**exclude**=resume,biography
- Profiles: /…?**style**=compact



Made with ♡ by PGS Software ·

Sorting

- /…?**sort**=title
- /…?**sort**=title+**DESC**,author+**ASC**
- /…?**asc**=title,author&**desc**=year
- /…?**sort**=title,author,year&**asc**=title,author&**desc**=year
- /…?**sort**=**+**title,**+**author,**-**year
- /…?**sort**=title&title.**dir**=**ASC**

Made with ♡ by PGS Software ·

Pagination

- **Offset** / **page** and **limit**
- Problem with insertion: /…?**page**=17
- Cursor helps: /…?**cursor**=FD5H7H
- Semantic param: /…?page=**recentlyClosed**
- Accept-range / Link headers
- Navigation links: **next**, **previous**, **last**

Made with ♡ by PGS Software ·

Status

- HTTP codes
- Error body object
- Additional internal codes, 4xx**YY**
- Descriptive messages
- Links to details
- Don’t expose internals

Made with ♡ by PGS Software ·

2xx Success

- 200: OK
- 201: Created
- 202: Accepted
- 204: No Content
- 206: Partial Content

3xx Redirection

- 300: Multiple Choices
- 301: Moved Permanently
- ~~302: Found~~
- 303: See Other
- 307: Temporary Redirect

Made with ♡ by PGS Software ·

4xx Client Error

- 401 Unauthorized
- 403 Forbidden
- 404 Not Found
- 405 Method Not Allowed
- 409 Conflict
- 410 Gone
- 422 Unprocessable Entity

Made with ♡ by PGS Software ·

5xx Server Error

- 500 Internal Server Error
- 501 Not Implemented
- 502 Bad Gateway
- 503 Service Unavailable
- 504 Gateway Timeout

Made with ♡ by PGS Software ·

Support

- Security
- Versioning
- Cache
- Throttling
- HATEOAS
- Documentation
- Management
- Platforms
- Miscs

Security

- Basic auth over **SSL** only
- Don’t **redirect** from non-SSL to SSL
- Don’t do **in-house** cryptography
- **API keys** instead of username / pass
- OWASP
- API Gateway pattern

Versioning

- URL: /**v2**/users
- Parameter: /users?**v=2**
- Accept header: application/vnd.github.**2**+json
- Custom header: x-ms-version:**2**
- API and Resource versioning

Made with ♡ by PGS Software ·

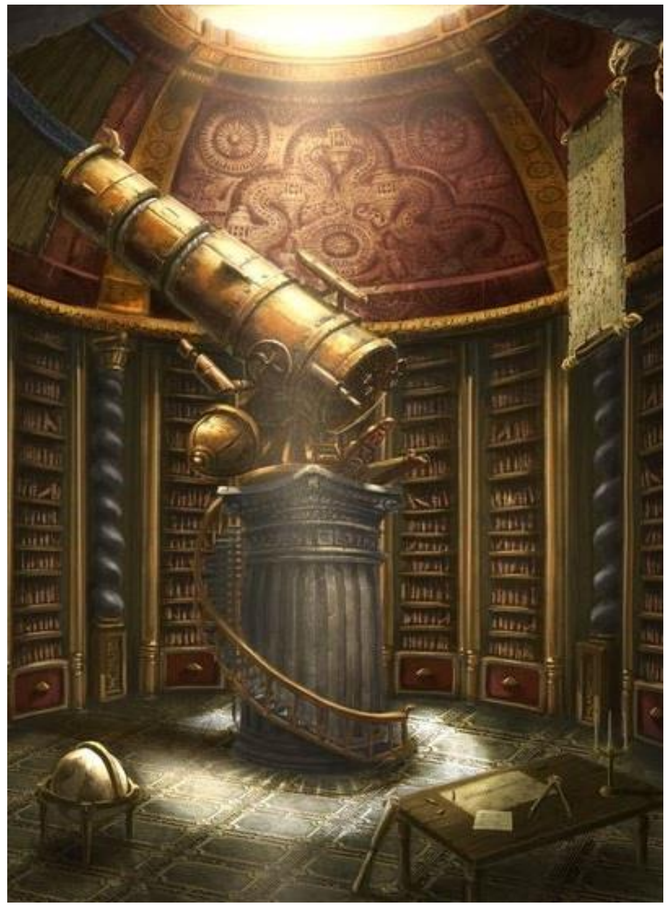
Cache Control

- **Public**: Anyone
- **Private**: No intermediate (default)
- **No-Cache**: Needs validation
- **No-Store**: Not reusable
- **No-Transform**: No changes
- **Max-Age**: Expiration date

Made with ♡ by PGS Software ·

Cache Validation

- **ETag** header
- Weak: semantically equal, Strong: binary equal
- GET: **If-none-match** header - get / 304 Not Modified
- PUT: **If-match** header - put or / 412 Precondition Failed
- Last-Modified / If-Modified-Since headers



Made with ♡ by PGS Software ·

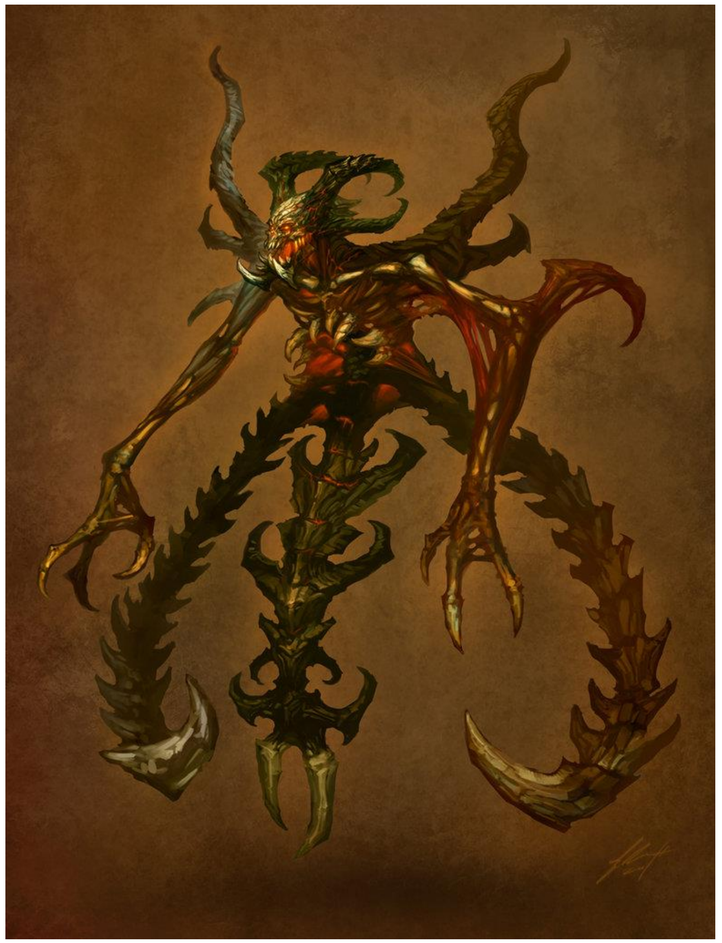
Throttling

- HTTP 429 Too Many Requests
- X-Rate-Limit-Limit
- X-Rate-Limit-Remaining
- X-Rate-Limit-Reset
- API Gateway again

Made with ♡ by PGS Software ·

HATEOAS

- Self-describing API dogma
- Generic clients vs performance
- HAL
- Collections+JSON
- JSON-LD
- SIREN



Made with ♡ by PGS Software ·

Documentation

- Public and easy to find
- Pastable examples
- Exhaustive reference
- Engaging tutorial
- Concise quickstart

Management

- Lifecycle
- Productivity
- Traffic
- Analytics
- Monetization

Made with ♡ by PGS Software ·

Platform

- Agent / Proxy
- Security, Alerts
- Message mediation, Prototyping
- Load balancing, Throttling
- Catalogue, Billing
- Userbase management

Made with ♡ by PGS Software ·

Miscs

- Update and creation returns **resource**
- Autolading: /…?**embed**=customer
- **X-HTTP-Method-Override**
- Pretty print: /?**_pretty**=true
- Compression: **Content-Encoding**

Made with ♡ by PGS Software ·

More Miscs

- **Resource UID** instead of counters
- **Request UID** as param
- **No** REST client vs browser **differentiation**
- Time: **ISO 8601**
- Metadata: Enveloping vs Link Header

Made with ♡ by PGS Software ·

Even More Miscs

- **IANA** registry for formats and link names
- Health and application info endpoint
- Top urls: **api**.company.com
- Ugly things: /__server_kaboom
- External API is a big deal

Made with ♡ by PGS Software ·

Summary

- Good API takes effort
- APIX: balance people vs machines
- Verbs + HTTP semantics
- Follow REST principles…
- …but not blindly

Want more?

- **HowToTrainYourJava.com**
- API category [episodes]:
  - [47] API Management Tools
  - [86] Tech and UX
  - [87] The Origins of REST
  - [88] Core Concepts
  - [89] …

Let’s get in touch

Paweł Zajączkowski

pzajaczkowski@gmail.com

@gvaireth

HowToTrainYourJava.com