@SheHackPurple

API Security Best Practices

APIs still need just as much security attention as web applications; not having a front end does not make them invisible to attackers. Below is a list of high-level best practices for APIs.

- Create a complete inventory of all APIs
- All external APIs are connected to via an API gateway
- Throttling and Resource Quotas on ALL APIs
- Logging, monitoring and alerting, same as for web apps
- Block all unused HTTP methods/verbs
- Use a service mesh for communication management
- Implement standards for your org, enforce them
- Strict linting of all calls
- Authenticate THEN authorize
- Avoid verbose error messages
- All the same secure coding practices you normally do; input validation using approved lists, parameterized queries, bounds checking, etc.

@WeHackPurple