Recently, almost all websites or web applications have been divided into front-end and back-end, which are connected through an application programming interface (API). This communication between the interfaces must be secured to transfer messages and data and protect against any form of cyber attack. The security of an API is passed through a set of rules for transferring messages. Amongst other data-exchanging rules, REST is a common architecture discussed in this brief (Kornienko, et al., 2021).

A screenshot of a computer

Description automatically generated

Figure 1 Common REST API vulnerabilities and mitigations (Emeka, Hidaka & Liu, 2021)

Despite being an architectural style, REST is still flexible in its approach, and it lets developers add, replace, and change elements easily. This can be a challenge when securing the API. Figure 1 shows several security vulnerabilities that API security might encounter. These vulnerabilities should all be analysed and mitigated with the mitigations suggested in Figure 1 (Emeka, Hidaka & Liu, 2021). Having said this, Kornienko et al. (2021) state that developers must prioritise input control when it comes to security. Some formal best practices for input data control are the client’s and server’s side validation of data; when validating, use built-in functions of the framework or programming language. Other methods include checking query length, type and size, use of parametrised queries, error log storage, and data entry attempt storage.

**References**

Emeka, B., Hidaka, S. & Liu, S. (2021) ‘A Formal Approach to Secure Design of RESTful Web APIs Using SOFL’, in: Xue, J., Nagoya, F., Liu, S. & Duan, Z. (eds) *Structure Object-Oriented Formal Language and Method*. Cham: Springer International Publishing. 105-125.

Kornienko, D. V., Mishina, S. V., Shcherbatykh, S. V. & Melnikov, M. O. (2021) Principles of securing RESTful API web services developed with Python frameworks. Journal of Physics: Conference Series 2094(3): 32016-. DOI: <https://doi.org/10.1088/1742-6596/2094/3/032016>