API SECURITY REQUIREMENTS

Project Team: Group 2

INTRODUCTION

Organisations and businesses increasingly use APIs to access data and services; the significance of API security cannot be overstated (axway, 2023). Insecure APIs are an attractive target for cybercriminals looking to steal data and carry out software attacks, as they are often the most exposed components of a network (Cobb, 2022). We will present below a security brief for an API based on the information we have about an API. The gaps in the information we have will be filled with the requirements that an API must meet in order to be secure.

BUSINESS NEED

We are specifying the API security requirements for a common business case to gather Gross Domestic Product data. Gross Domestic Product (GDP) measures the value of goods and services produced in a country over a year. It's a key indicator of a country's economic performance and is used by companies to assess business conditions. Our team created a Python API to make it easier for organisations to access GDP data.

API PROVIDER

The FEDERAL RESERVE BANK of ST. LOUIS is providing economic research data. We are using the API **fredapi,** a Python API that provides a function in Python that connects to the data services. An API key is needed to access the services provided by the API (FRED® API, N.D.).

PYTHON CODE

This example code below shows the package import and simple data retrieval; full documentation can be found on GitHub (Mehyar, 2022).

```
from fredapi import Fred
fred = Fred(api_key='insert api key here')
data = fred.get_series('SP500')
```

SECURITY REQUIREMENTS SPECIFICATION

Authentication

The **fredapi** uses API keys to support secure authentication mechanisms. There is a requirement for setting up an account and providing a valid reason for the data retrieval.

Authorisation

FredAPI uses a role-based access control (RBAC) based on the account profile, allowing different users different access levels (Cobb, 2022). FredAPI's team verifies credentials of eg. a University researcher and grants them a wider access than the one granted to an individual without valid reason.

Encryption

The API uses the secure communications protocol (HTTPS); this protocol includes standard protection (Cobb, 2022) for server requests ("GET", "POST" etc.). The data does not have to be too carefully encrypted as it is public information and does not contain any PII.

Rate limiting

The API limits the number of requests per, for example, IP address in order to prevent abuse (Cobb, 2022).

Input validation

The API does allow for the data to be read only, there is no possibility to write into an API which prevents eg. SQL injections attacks.

Error handling

There should be unit testing in place that tests that correct errors are thrown and also that no sensitive information is being displayed as a part of the error thrown.

Logging and monitoring

The API logs all of the requests sent through the API in order to prevent malicious actors from abusing the API (Cobb, 2022). This helps to set up a monitoring and alerting system should any breach be detected and so the cyber security team can respond in a timely manner (axway, 2023).

Security Testing

Regular security testing, such as penetration testing and vulnerability assessment, must be conducted to identify and fix any vulnerabilities in the API. The API must implement appropriate data management controls, including access controls, backup and recovery, and retention policies, to ensure the security and integrity of data (Koshy, 2021).

Update process

There should be defined a process for updating the API in order to fix known vulnerabilities and ensure that the system remains secure as the technology develops.

Compliance

This API does not need to adhere to any major data privacy regulation (like GDPR, HIPAA or PCI-DSS) because it is not handling the type of data that would be covered by either of these regulations. However, any API should consider adherence to privacy regulations in order to make sure that the data is safely encrypted, masked where needed and that only authorised individuals can access any type of sensitive information.

REFERENCES

1. axway (2023) API security: 12 essential best practices. Available from: https://blog.axway.com/learning-center/digital-security/keys-oauth/api-security-best-practices [Accessed 8 April 2023].

2. Koshy, I. A (2021) API Security Testing: Importance, Risks and Best Practices. Available from: https://beaglesecurity.com/blog/article/api-security-testing.html [Accessed 8 April 2023].

3. Cobb, M. (2022) 12 API security best practices to protect your business. Available from:https://www.techtarget.com/searchapparchitecture/tip/10-API-security-guidelines-and-best-practices [Accessed 8 April 2023].

4. FRED® API (N.D.) FRED ECONOMIC DATA | ST. LOUIS FED. Available from: https://fred.stlouisfed.org/docs/api/fred/ [Accessed 8 April 2023].

5. Mehyar, M. (2022) fredapi: Python API for FRED (Federal Reserve Economic Data). Available from: https://github.com/mortada/fredapi [Accessed 8 April 2023].

6. IBM QRADAR - Kaif Integration (no date) www.intellas.biz. Available at: https://www.intellas.biz/case-studies/ibm-qradar-kaif-integration (Accessed: April 10, 2023).