

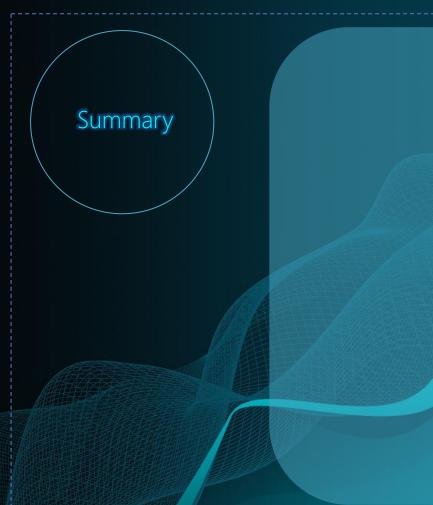




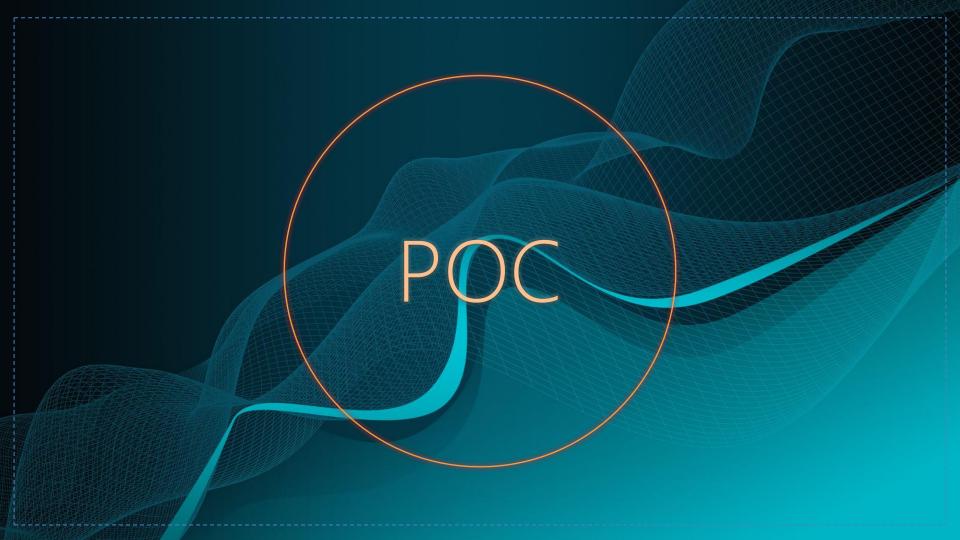
API: A programming interface for communication with external services and executing various operations in applications.

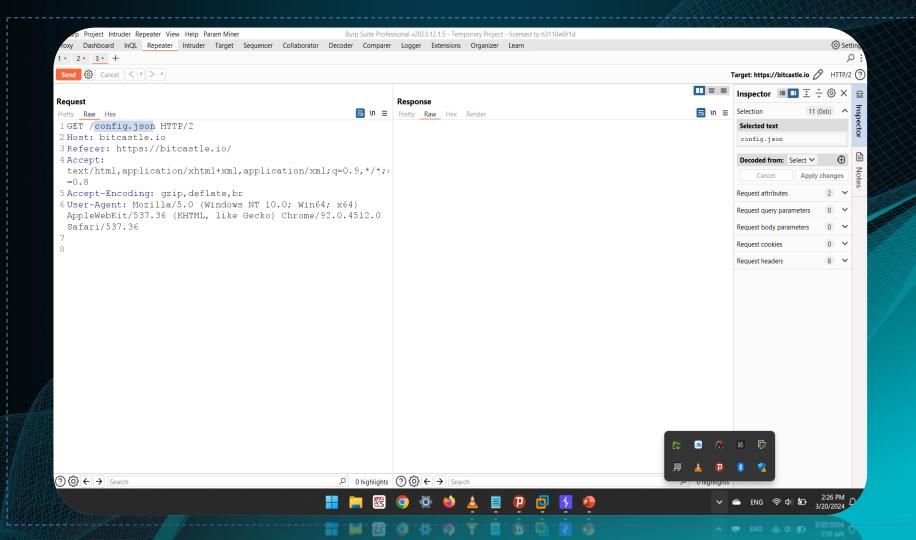
RECAPTCHA_KEY: An authentication key required for utilizing the reCAPTCHA human verification service.

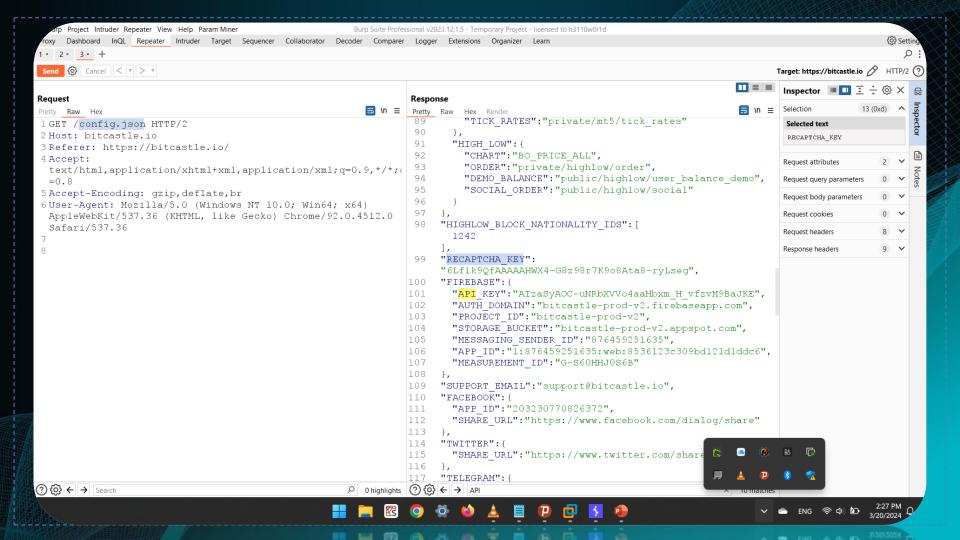
Confige.json: A configuration file containing various settings including API keys and other configurations for the program.

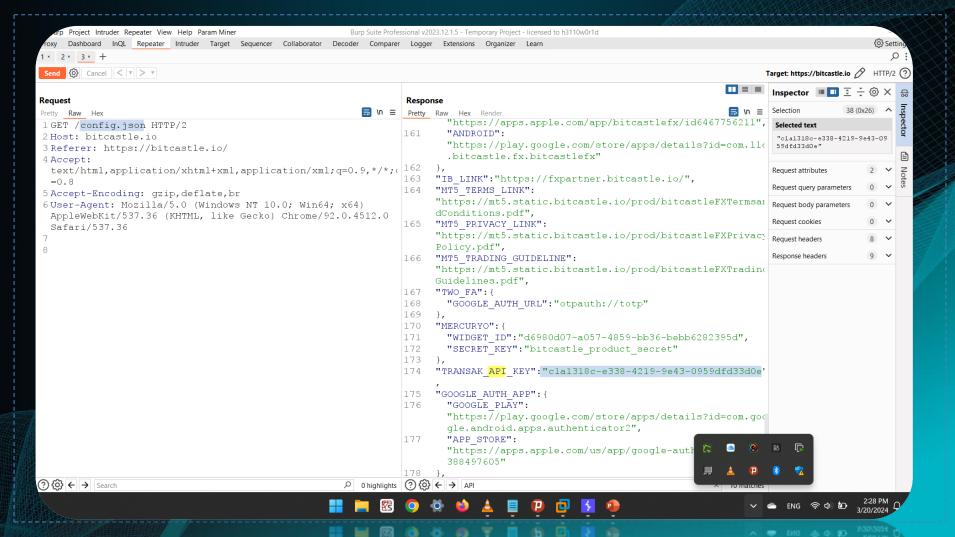


underscores a critical security vulnerability. It highlights the potential exposure of sensitive information, posing significant risks such as data breaches and unauthorized access. Immediate steps are necessary to mitigate these risks, including changing all exposed keys and implementing robust security measures for data storage. Additionally, a comprehensive investigation is essential to identify the root cause of the leak and prevent similar incidents in the future. Failure to address this issue promptly could ead to severe consequences, including financial losses and damage to the organization's









GET /config.json HTTP/2

Host: bitcastle.io

Referer: https://bitcastle.io/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)

Chrome/92.0.4512.0 Safari/537.36

CWE-200

Base Score: 6.0 - CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N

RECAPTCHA_KEY: "6Lf1k9QfAAAAAHWX4-G8z98r7K9o8Ata8-ryLseg"

API_KEY": "AIzaSyAOC-uNRbXVVo4aaHbxm_H_vfzvM9BaJKE

TRANSAK_API_KEY: "c1a1318c-e338-4219-9e43-0959dfd33d0e

About bug

- 1. Sensitive and private information is exposed to public access
- 2.Exposing reCAPTCHA keys enables brute-force attacks.
- 3.If relevant information is disclosed, the security mechanism can be bypassed
- 4.In case of information disclosure, unauthorized access to different parts may occur.

Impact

How To Fix it

- 1. Change critical keys and replacing them with new secure ones.
- 2. Setting up an authentication system to prevent unauthorized access to sensitive files
- 3. Reviewing configuration files to detect and prevent the presence of sensitive information, enhancing system security and preventing data leaks
- 4. Using environment variables to store sensitive data securely and separate from application code, enhancing confidentiality and security measures

