

Report

K6D0L


for

LOL

Security Team

bitcastle

*Data: 2024-3-21*

The background is a solid teal color with abstract, wavy, wireframe-like patterns in a slightly darker shade of teal. A large, thin white circle is centered on the page, containing the text.

# 2API Key Exposure with Config File Leakage





## Introduction

**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.

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

## Summary

The discovery of two APIs along with a configuration file containing sensitive keys 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 lead to severe consequences, including financial losses and damage to the organization's reputation. Therefore, swift action and diligent security measures are imperative to safeguard sensitive data and maintain trust with stakeholders.



The background features a dark teal gradient with several wavy, translucent lines in a lighter teal color. A thin, bright orange circle is centered on the page, framing the text. The overall aesthetic is modern and digital.

POC

Project Intruder Repeater View Help Param Miner  
Burp Suite Professional v2023.12.15 - Temporary Project - licensed to h3110w0r1d

Proxy Dashboard InQL Repeater Intruder Target Sequencer Collaborator Decoder Comparer Logger Extensions Organizer Learn

1 x 2 x 3 x +

Send Cancel < >

### Request

Pretty Raw Hex

```
1 GET /config.json HTTP/2
2 Host: bitcastle.io
3 Referer: https://bitcastle.io/
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Encoding: gzip,deflate,br
6 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
7
8
```

### Response

Pretty Raw Hex Render

### Inspector

Target: https://bitcastle.io HTTP/2

Selection 11 (0xb)

**Selected text**  
config.json

Decoded from: Select +

Cancel Apply changes

Request attributes 2

Request query parameters 0

Request body parameters 0

Request cookies 0

Request headers 8

0 highlights

0 highlights

2:26 PM  
3/20/2024

ProjectIntruderRepeaterViewHelpParam Miner

DashboardInQLRepeaterIntruderTargetSequencerCollaboratorDecoderComparerLoggerExtensionsOrganizerLearn

1 ×2 ×3 ×+

SendCancel<>

Target: https://bitcastle.ioHTTP/2

Inspector

Selection13 (0xd)

Selected text

RECAPTCHA\_KEY

Request attributes2

Request query parameters0

Request body parameters0

Request cookies0

Request headers8

Response headers9

Notes

Request

PrettyRawHex

1 GET /config.json HTTP/2

2 Host: bitcastle.io

3 Referer: https://bitcastle.io/

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

5 Accept-Encoding: gzip, deflate, br

6 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

7

8

Response

PrettyRawHexRender

89 "TICK\_RATES": "private/mt5/tick\_rates"

90 },

91 "HIGH\_LOW": {

92 "CHART": "BO\_PRICE\_ALL",

93 "ORDER": "private/highlow/order",

94 "DEMO\_BALANCE": "public/highlow/user\_balance\_demo",

95 "SOCIAL\_ORDER": "public/highlow/social"

96 }

97 },

98 "HIGHLOW\_BLOCK\_NATIONALITY\_IDS": [

1242

99 ],

100 "RECAPTCHA\_KEY":

101 "6Lf1k9QfAAAAAHWX4-G8z98r7K9o8Ata8-ryLseg",

102 "FIREBASE": {

103 "API\_KEY": "AIzaSyAOC-uNRbXVVo4aaHbXm\_H\_vfzvM9BaJKE",

104 "AUTH\_DOMAIN": "bitcastle-prod-v2.firebaseio.com",

105 "PROJECT\_ID": "bitcastle-prod-v2",

106 "STORAGE\_BUCKET": "bitcastle-prod-v2.appspot.com",

107 "MESSAGING\_SENDER\_ID": "876459251635",

108 "APP\_ID": "1:876459251635:web:8536123c309bd121d1ddc6",

109 "MEASUREMENT\_ID": "G-S60HHJ0S6B"

110 },

111 "SUPPORT\_EMAIL": "support@bitcastle.io",

112 "FACEBOOK": {

113 "APP\_ID": "203230770826372",

114 "SHARE\_URL": "https://www.facebook.com/dialog/share"

115 },

116 "TWITTER": {

117 "SHARE\_URL": "https://www.twitter.com/share"

118 },

119 "TELEGRAM": {

0 highlights

API

Project Intruder Repeater View Help Param Miner  
Proxy Dashboard InQL Repeater Intruder Target Sequencer Collaborator Decoder Comparer Logger Extensions Organizer Learn

1 x 2 x 3 x +  
Send Cancel < >

Target: https://bitcastle.io HTTP/2

### Request

Pretty Raw Hex

```
1 GET /config.json HTTP/2
2 Host: bitcastle.io
3 Referer: https://bitcastle.io/
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Encoding: gzip,deflate,br
6 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
7
8
```

### Response

Pretty Raw Hex Render

```
161 "https://apps.apple.com/app/bitcastlefx/id6467756211",
  "ANDROID":
  "https://play.google.com/store/apps/details?id=com.llc
    .bitcastle.fx.bitcastlefx"
162 },
163 "IB_LINK":"https://fxpartner.bitcastle.io/",
164 "MT5_TERMS_LINK":
  "https://mt5.static.bitcastle.io/prod/bitcastleFXTermsa
    dConditions.pdf",
165 "MT5_PRIVACY_LINK":
  "https://mt5.static.bitcastle.io/prod/bitcastleFXPrivac
    yPolicy.pdf",
166 "MT5_TRADING_GUIDELINE":
  "https://mt5.static.bitcastle.io/prod/bitcastleFXTradin
    Guidelines.pdf",
167 "TWO_FA":{
168   "GOOGLE_AUTH_URL":"otpauth://totp"
169 },
170 "MERCURYO":{
171   "WIDGET_ID":"d6980d07-a057-4859-bb36-bebb6282395d",
172   "SECRET_KEY":"bitcastle_product_secret"
173 },
174 "TRANSAX_API_KEY":"c1a1318c-e338-4219-9e43-0959dfd33d0e"
  ,
175 "GOOGLE_AUTH_APP":{
176   "GOOGLE_PLAY":
  "https://play.google.com/store/apps/details?id=com.goo
    gle.android.apps.authenticator2",
177   "APP_STORE":
  "https://apps.apple.com/us/app/google-auth
    388497605"
178 },
```

### Inspector

Selection 38 (0x26)

Selected text  
"c1a1318c-e338-4219-9e43-0959dfd33d0e"

Request attributes	2
Request query parameters	0
Request body parameters	0
Request cookies	0
Request headers	8
Response headers	9



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

TRANSAX\_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



*bug hunter*  
*security researcher*

icandohat010@gmail.com

*Aiden*



*snowfall*