

User Guide: qkbcc

INTRODUCTION

Qkbcc (QuickBCC) tries to detect vulnerable code clones in given binary executables.

Qkbcc analyzes binary files and identifies vulnerable functions by comparing them with a vulnerability database.

The vulnerability database is experimental and currently contains a limited number of signatures for well-known vulnerabilities.

USEAGE

Step 1. Getting Started

To use QKBCC, access the IoTcube platform: <https://iotqv.korea.ac.kr/sast/qkbcc>

No installation is required for web-based analysis.

Step 2. Prepare Input File

To use QKBCC, access the IoTcube platform: <https://iotqv.korea.ac.kr/sast/qkbcc>

No installation is required for web-based analysis.

QKBCC requires binary executables compressed into a .zip file.

QKBCC does not accept a single raw binary file directly.

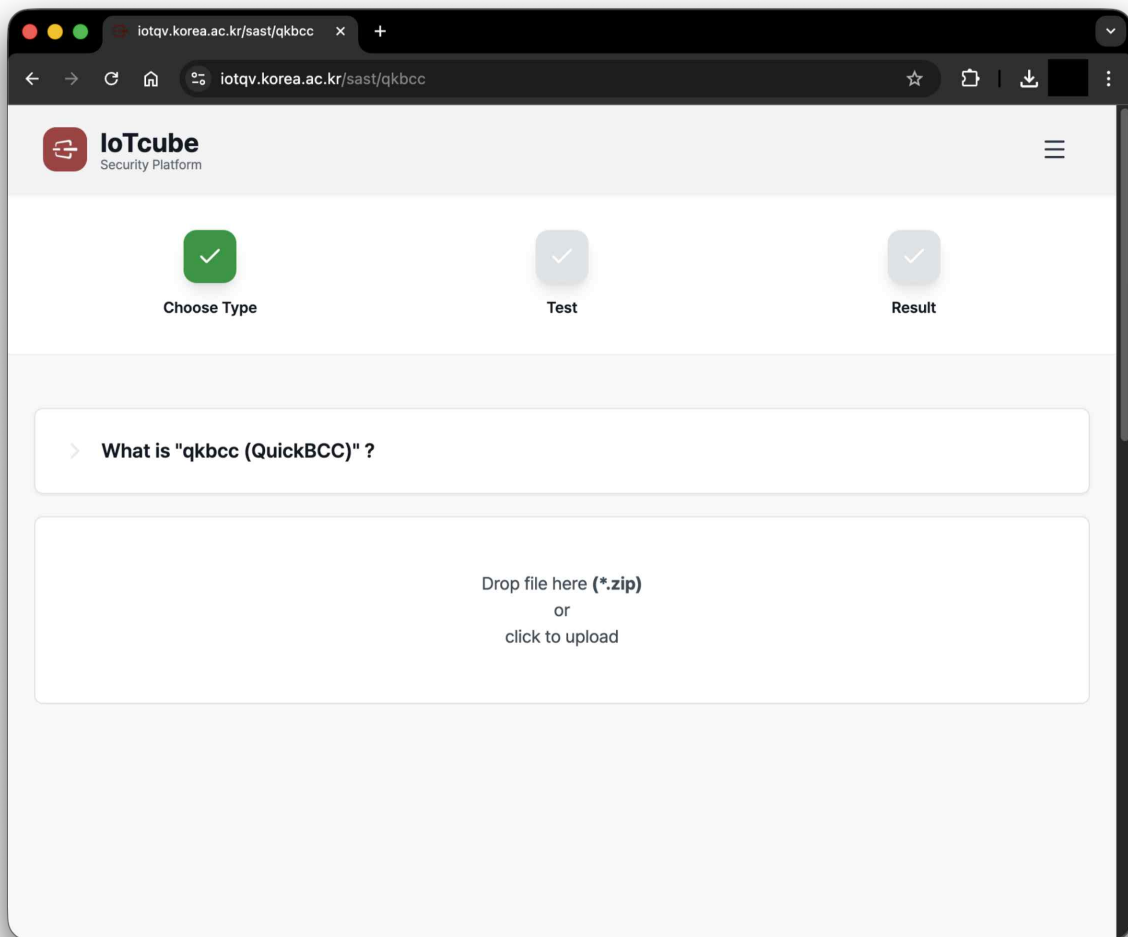
You must compress the executable(s) before uploading.

Input Requirements

- A .zip file containing:
- One binary executable, or
- Multiple binary executables

Step 3. Upload File (Testing)

On the Qkbcc page you will see the upload area:



Upload the prepared .zip file by:

- Dragging and dropping the file into the upload area, or
- Clicking the area to select the file manually.

After uploading, Qkbcc automatically starts the analysis.

Step 4. Running Analysis

After the .zip file is uploaded:

1. QKBCC extracts the compressed files.
2. Binary executables are parsed.
3. Function-level features are extracted.
4. Extracted functions are compared with the vulnerability database.
5. Potential vulnerable code clones are identified.

The analysis may take several minutes depending on the file size.

Step 5. Inspect Results

After analysis is completed, move to the **Result** stage.

The result page shows:

- Detected vulnerable functions
- Matched vulnerability signatures
- Related vulnerability information

Each result corresponds to a matched vulnerable code clone detected in the uploaded binary.

(figure: After Drag & Drop result zip file)

The screenshot displays the IoTcube Security Platform interface. At the top, the browser address bar shows the URL `iotqv.korea.ac.kr/sast/qkbcc?requestId=6dbc7edc-74ae-4975-92c4-2b1dc4d42148`. The IoTcube logo and 'Security Platform' text are visible in the top left. A navigation menu icon is in the top right. Below the header, three green checkmark icons indicate successful steps: 'Choose Type', 'Test', and 'Result'. The main content area is titled 'Result of Whitebox Testing' and contains two summary tables.

Result of Whitebox Testing

Target Overview	
Target Name	/tmp/anonymous
# of Files	1
Architecture	ARMv7

Scan Overview	
Processing Time	00:00:14.2621778
Total number of function	418,646
# of vulnerability signatures found	4
# of unique vulnerable functions	3

iotqv.korea.ac.kr/sast/qkbcc x +

iotqv.korea.ac.kr/sast/qkbcc?requestId=6dbc7edc-74ae-4975-92c4-2b1dc4d42148

0 of vulnerability signatures found

IoTcube
Security Platform

Vulnerable functions

Vulnerable functions ratio

Safe: 100.00% Vulnerable: 0.00%

■ Safe ■ Vulnerable

List of Vulnerable code

#	filename	name of vulnerability	function	similarity
1		CVE-2014-0160	tls1_process_heartbeat	92.5%
2		CVE-2014-0160	dtls1_process_heartbeat	88.5%
3	libssl_454.so	CVE-2015-1791	SSL_SESSION_new	90.9%
4		CVE-2014-0160	tls1_process_heartbeat	92.5%
5		CVE-2014-0160	dtls1_process_heartbeat	88.5%
6		CVE-2015-1791	SSL_SESSION_new	90.9%

restart main