Travis Plugin for Contrast Security Guide

Contrast Travis Plugin – Solution Overview

The Travis plugin allows you to fail a job based on the number of existing vulnerabilities in Contrast Security Team Server. Vulnerability thresholds are configurable for the each of the 5 severities of vulnerabilities. The plugin will retrieve all vulnerabilities at the end of the travis job, compare it against the configured thresholds and fail the build automatically, if any of the thresholds are breached.

Some things to keep in mind when using the plugin:

- The plugin should be used with Travis **jobs which run integration/regression tests** on an application for best results. Contrast Security is an interactive security tool which instruments applications with its agent and finds vulnerabilities only when instrumented applications are exercised.
- The **plugin will NOT find vulnerabilities** in your application. You will first need to deploy a Contrast Security agent with your application to report the vulnerabilities. This plugin only queries for the number of existing vulnerabilities from Contrast Security. This plugin executes during the "after script" phase of the Travis build process.

To properly instrument your application with the Contrast Security agent please find the documentation available online at the links below.

- Java : https://docs.contrastsecurity.com/installation-javastandard.html
- Node : https://docs.contrastsecurity.com/installation-nodeinstall.html

Contrast Travis Plugin – Solution Assets

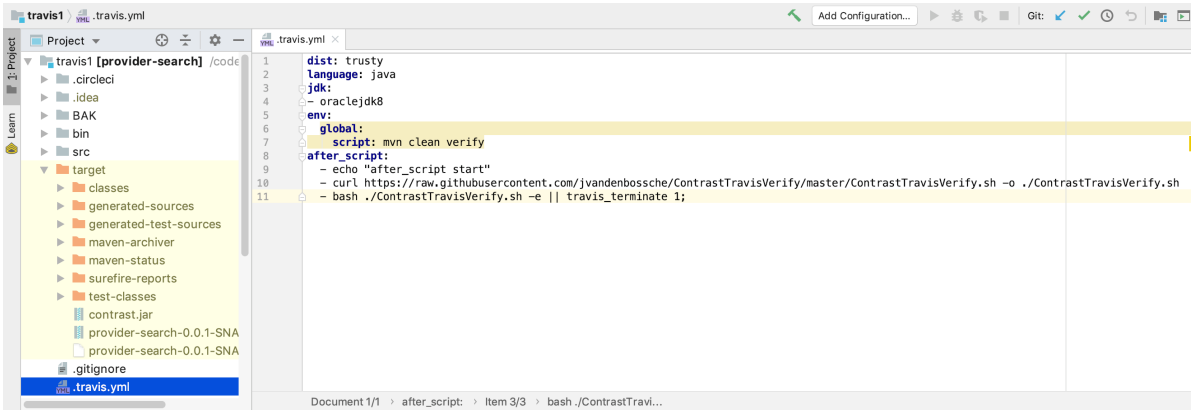
These can be downloaded from https://github.com/jvandenbossche/ContrastTravisVerify.git

Filename	Description
Travis Plugin for Contrast Security Guide v4.pdf	This guide in PDF format
.travis.yml	Sample Travis YAML file
ContrastTravis.conf	Configuration file containing vulnerability thresholds expected by "ContrastTravisVerify.sh"
ContrastTravisVerify.sh	Bash Script executed by Travis at end of build to Pass or Fail build. This script can be downloaded from GitHub in the URL in the travis.yml

Installation / Configuration

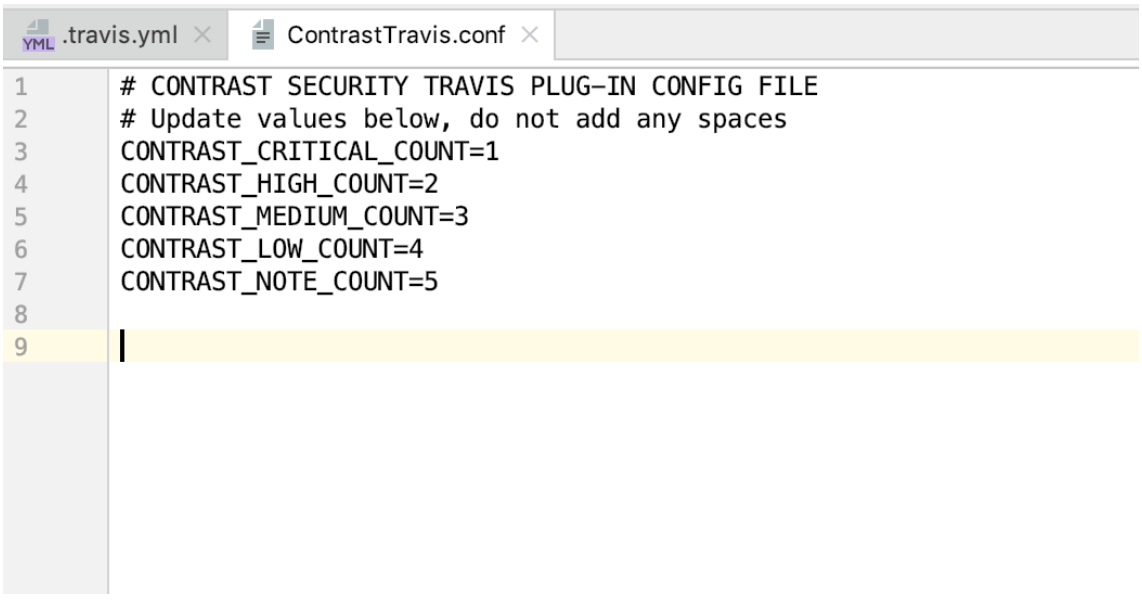
1. Update '.travis.yml'

   In your travis.yml file add the lines from the provided Sample YAML file from the "after_script" section. The provided sample will download the latest script from a Git repo. If you opt to just include the file inside your build, download it, put it in place and comment out the "curl" line.



2. Add "ContrastTravis.conf " to your project

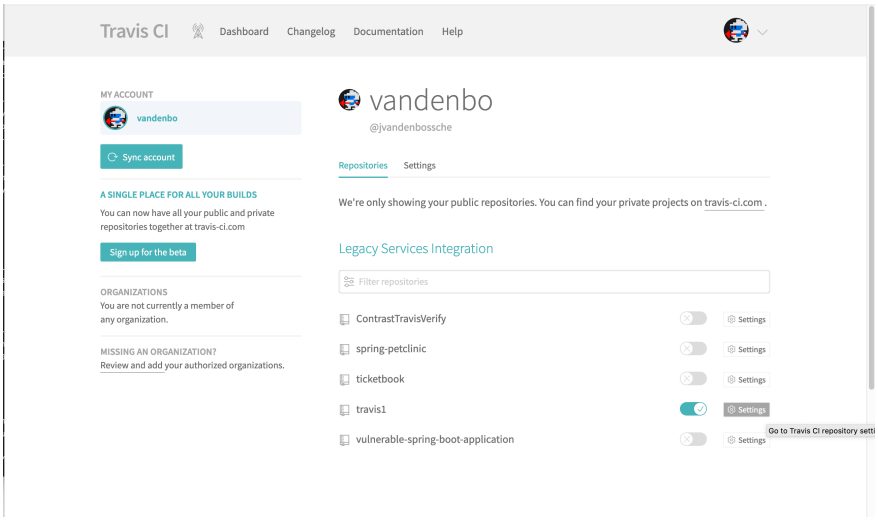
   Copy the file named "ContrastTravis.conf " to your application's root directory. You can edit the contents with your own thresholds. Do not add lines, spaces or other characters. Only update the numbers to preserve the necessary format.



2.1. Thresholds to fail the build on. If the counts for any category **exceed** the value set here, the build will fail.
   - **CONTRAST_CRITICAL_COUNT** – Number of **Critical** vulnerabilities
   - **CONTRAST_HIGH_COUNT** – Number of **High** vulnerabilities
   - **CONTRAST_MEDIUM_COUNT** – Number of **Medium** vulnerabilities
   - **CONTRAST_LOW_COUNT** – Number of **Low** vulnerabilities
   - **CONTRAST_NOTE_COUNT** – Number of **Note** vulnerabilities

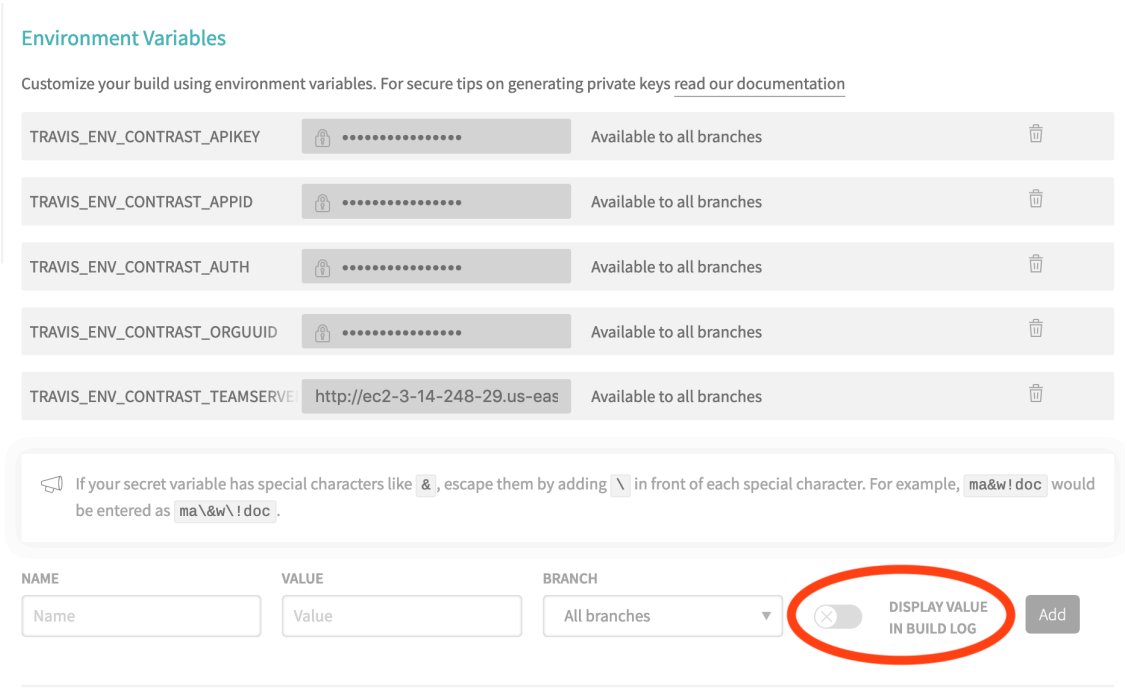
3. OPTIONAL - ContrastTravisVerify.sh
   3.1. This file can be downloaded from GitHub and used within your project, and not downloaded from a GitHub repo every time.
   3.2. You can put it in your own Git repo, then update the travis.yml file URL
   3.3. You can also just download this file and put it in your application's root folder

4. Travis Plugin – Create Travis Environment Variables
   4.1. Open up your project settings to set necessary environment variables.



   4.2. Each of the following Environment Variables will need to be created. Create all of the following as secure variables. These values will not be readable in Travis or written to any of the logs. The values of your Contrast Security keys must be secured, because anyone with these keys can easily exercise the Contrast API on your behalf with your full access permissions. To accomplish this disable "DISPLAY VALUE IN BUILD LOG" as shown below… circled in red.

Environment Variable	Where to retrieve value
TRAVIS_ENV_CONTRAST_TEAMSERVERURL	4.2.5
TRAVIS_ENV_CONTRAST_APIKEY	4.2.5
TRAVIS_ENV_CONTRAST_ORGUUID	4.2.5
TRAVIS_ENV_CONTRAST_AUTH	4.2.5
TRAVIS_ENV_CONTRAST_APPID	4.2.7

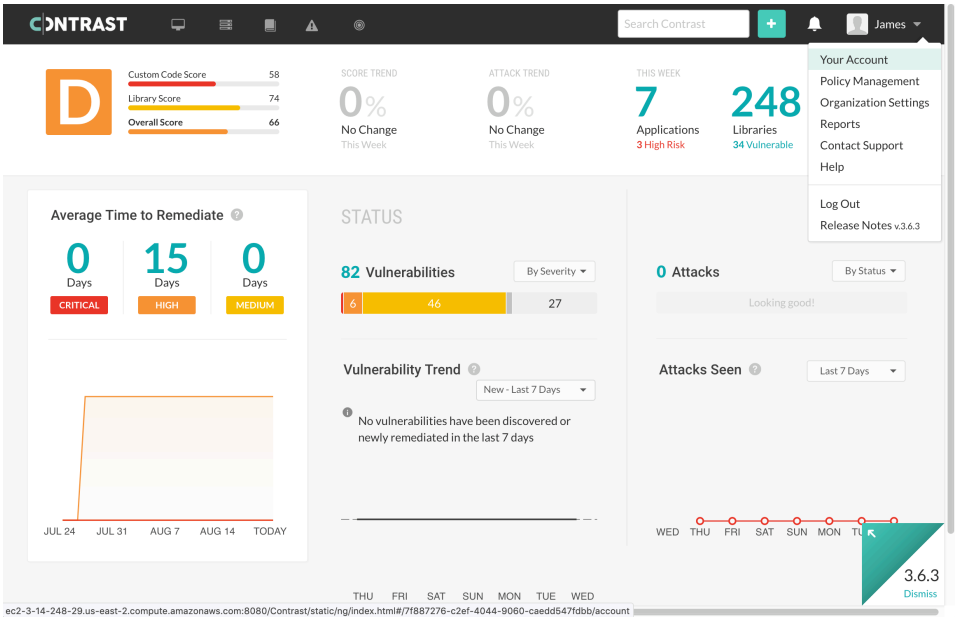


4.2.1. You will need to retrieve the values for these from the Contrast Security Team Server. Here are the steps to retrieve this information.

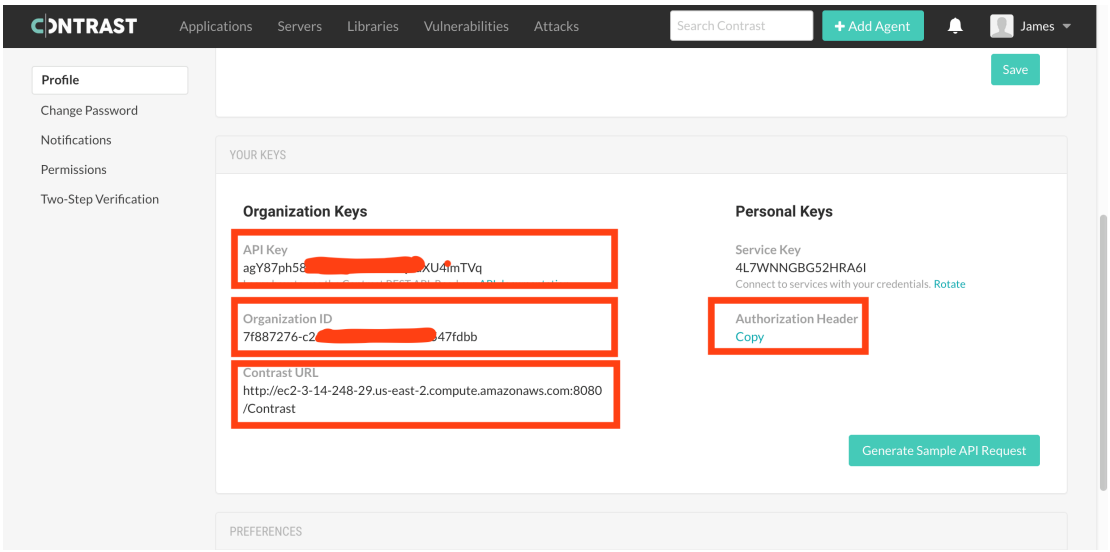
4.2.2. Login to Contrast

4.2.3. Click on your name on the top right

4.2.4. Click on “Your Account” menu item

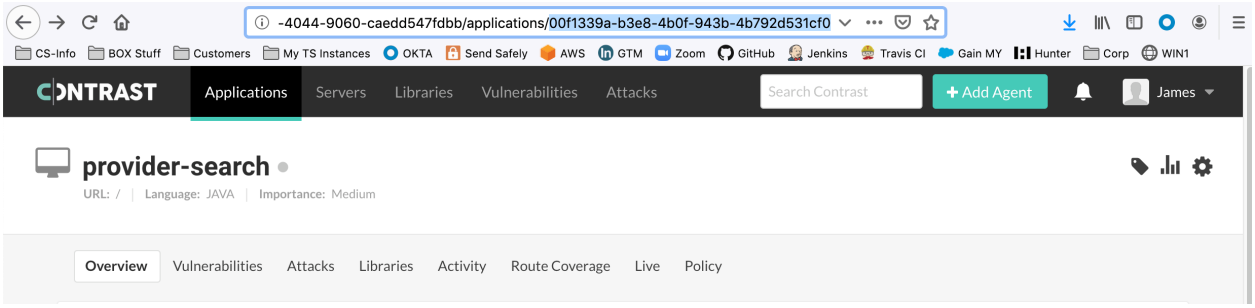


4.2.5. In the Profile section 4 of the 5 needed values are found here. To extract the Auth Header, just click the "Copy" link provided to have it loaded in your computer's clipboard.

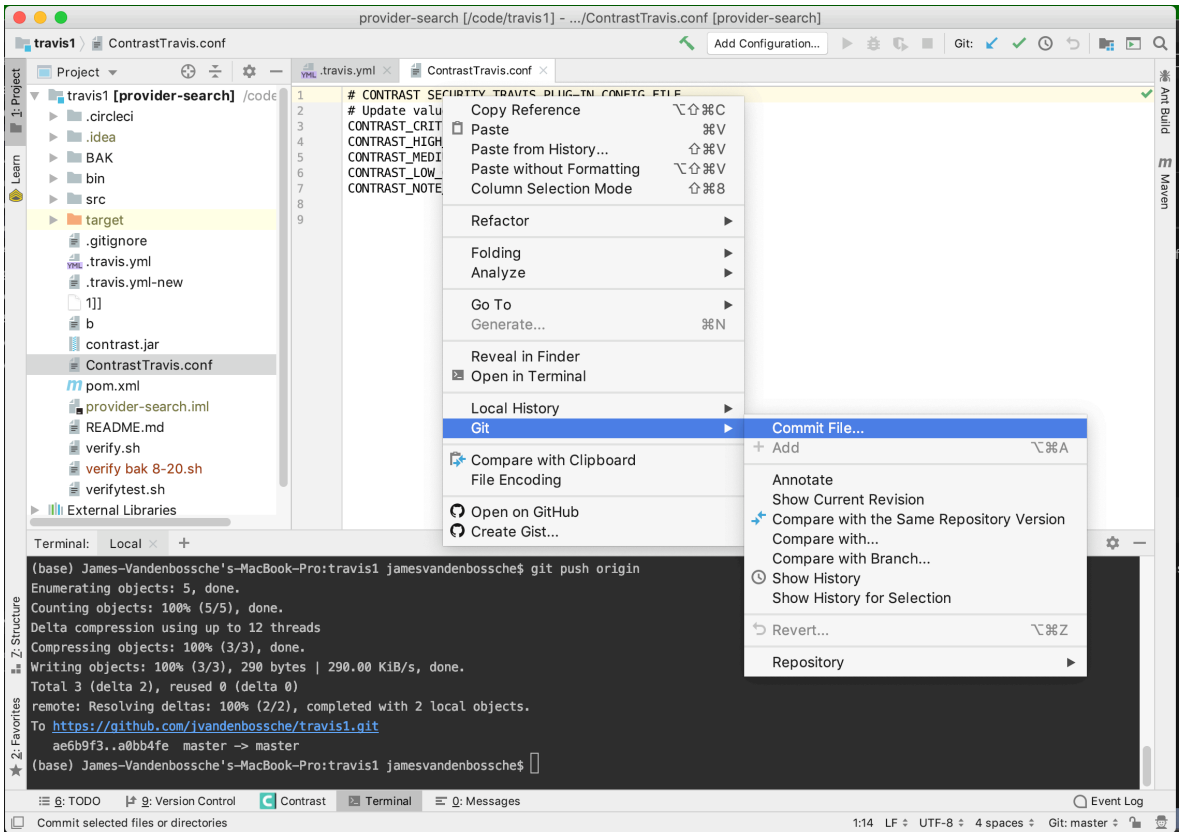


4.2.6. Click on Applications at the top

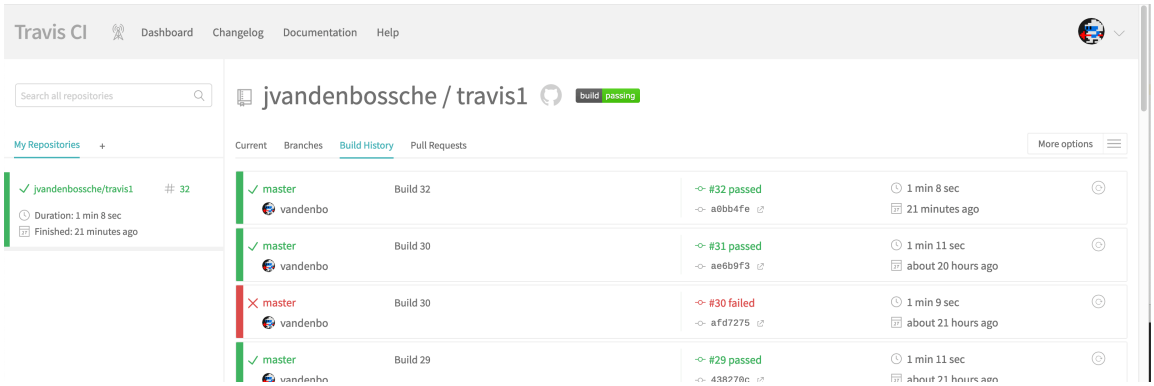
4.2.7. Click on your application Copy the **<APP ID>** for the environment variable. In the URL shown in the browser below, the format will be:
https://app.contrastsecurity.com/Contrast/static/ng/index.html#/<ORG ID>/applications/**<APP ID>**



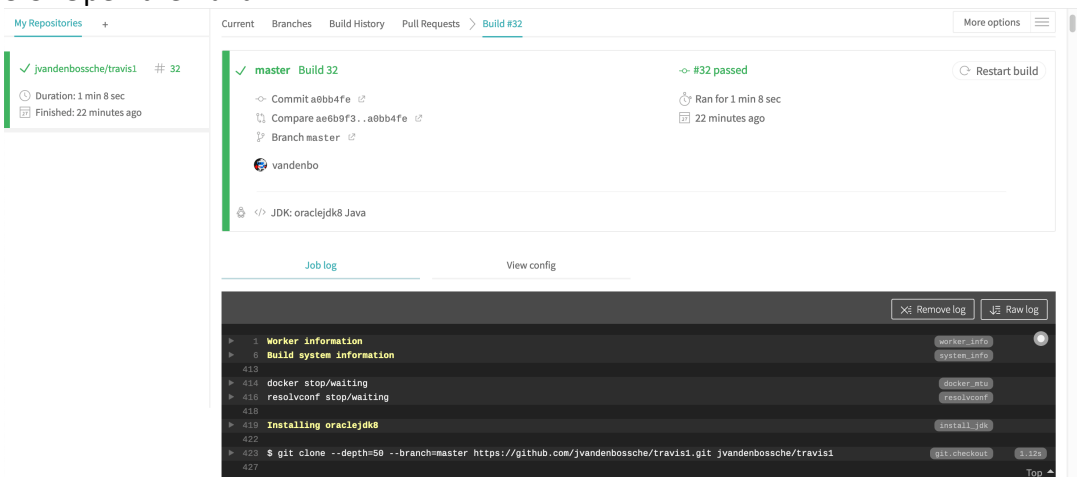
5. Verifying the solution
   5.1. Check in a file to trigger the Travis Build. As shown here in IntelliJ, a Git>Commit File was followed by the “git push origin” command in the terminal



5.2. In Travis the build will be automatically run, and the output from the Travis Contrast Plugin script will be found initially collapsed at the bottom.



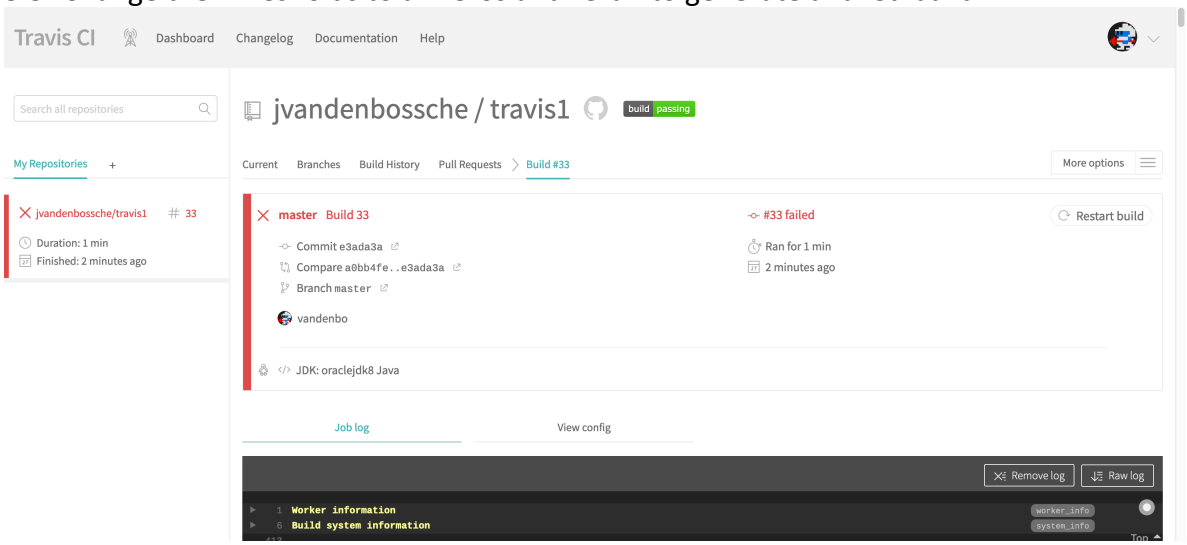
5.3. Open the Build



5.4. Scroll Down to bottom of “Job Log” and expand log for details. This build passed, as the application has only 1 Medium and 3 Note level vulnerabilities open. The thresholds set for the build are also displayed above.

```
1979
1980 $ echo "after_script start"                                                    after_script.1  0.00
1982 $ curl https://raw.githubusercontent.com/jvandenbossche/ContrastTravisVerify/master/ContrastTravisVerify.sh -o  after_script.2  0.19s
1983 $ bash ./ContrastTravisVerify.sh -e || travis_terminate 1;                    after_script.3  0.18s
1984
1985 -=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
1986 Contrast Security - Travis Build Verification
1987 PlugIn Integration - Version 2019_08_20
1988 -=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-+
1989 Team Server URL: http://ec2-3-14-248-29.us-east-2.compute.amazonaws.com:8080/Contrast/api
1990 -=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
1991 Travis Build Vulnerability Threshold Settings
1992 If current open vulnerabilities exceeds thresholds, the build will be failed
1993 Critical > 1
1994 High     > 2
1995 Medium   > 3
1996 Low      > 4
1997 Note     > 5
1998 CONTRAST API CALL : http://ec2-3-14-248-29.us-east-2.compute.amazonaws.com:8080/Contrast/api/ng/[secure]/orgtraces/filter/severity
     /listing?expand=skip_links&quickFilter=OPEN&modules=[secure]&tracked=false&untracked=false&metadataFilters=%5B%5D
1999   % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
2000                                  Dload  Upload   Total   Spent    Left  Speed
2001 100   592    0   592    0     0   4124      0 --:--:-- --:--:-- --:--:--  4139
2002 -=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
2003 Current Open Vulnerabilities for this application in Contrast Security
2004 Critical count: 0
2005 High count: 0
2006 Medium count: 1
2007 Low count: 0
2008 Note count: 3
2009
2010 Done. Your build exited with 0.
                                                                                  Top
```

5.5. Change the Thresholds to all zeros and rerun to generate a failed build.



```
$ echo "after_script start"                                                        after_script.1   0.00s
$ curl https://raw.githubusercontent.com/jvandenbossche/ContrastTravisVerify/master/ContrastTravisVerify.sh -o     after_script.2   0.21s
$ bash ./ContrastTravisVerify.sh -e || travis_terminate 1;

-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
Contrast Security - Travis Build Verification
PlugIn Integration - Version 2019_08_20
-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-+
Team Server URL: http://ec2-3-14-248-29.us-east-2.compute.amazonaws.com:8080/Contrast/api
-=-=-=-=-=-=-=-=-=-=-=-=-=-
Travis Build Vulnerability Threshold Settings
If current open vulnerabilities exceeds thresholds, the build will be failed
Critical > 0
High     > 0
Medium   > 0
Low      > 0
Note     > 0
CONTRAST API CALL : http://ec2-3-14-248-29.us-east-2.compute.amazonaws.com:8080/Contrast/api/ng/[secure]/orgtraces/filter/severity
/listing?expand=skip_links&quickFilter=OPEN&modules=[secure]&tracked=false&untracked=false&metadataFilters=%5B%5D
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   592    0   592    0     0   5280      0 --:--:-- --:--:-- --:--:--  5285
-=-=-=-=-=-=-=-=-=-=-=-=-=-
Current Open Vulnerabilities for this application in Contrast Security
Critical count: 0
High count: 0
Medium count: 1
Low count: 0
Note count: 3
1 is greater than the threshold of  0
Failing job because Medium vulnerability threshold was violated
Please check the Contrast UI for the vulnerability details and how to fix them.
Refer to https://docs.contrastsecurity.com/user-vulns.html#analyze for steps to set the vulnerability status to closed (Remediated or Not a Problem)
                                                                                                   Top
```