



MASTS

Product Walkthrough

Trial Edition



Security Solution by



VARUTRATM

Disclaimer

Varutra Consulting has made every sincere possible effort to ensure the accuracy and completeness of this guide. However its staff and development team will not be liable for any errors or omissions and use of the software is subject to the customer's licence with Varutra Consulting Private Limited.

This guide should not be relied upon as a detailed specification of the software. Varutra Consulting may make changes to this guide from time to time without prior notice or intimation.

Copyright

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system or translated into any language in any form by any means without the written permission of Varutra Consulting Private Limited.

Products or corporate names may be trademarks or registered trademarks of other companies and are used only for the explanation and to the owner's benefit, without intent to infringe.

The content mentioned is informational and all the modules of this software program are owned by Varutra Consulting Private Limited (Varutra).

Trademark Rights

All rights reserved. MASTS name and MASTS logo is a registered trademark of Varutra Consulting Private Limited.

All other trademarks are the property of their respective owners.

Congratulations on downloading Trial Edition of MASTS!

This quick guide will act as a walkthrough to various modules available in MASTS Trial Edition.

For a detailed instruction set, please refer our knowledge base section [here](#).

Registration

Visit MASTS website at <http://www.varutra.com/masts> via any standard browser (preferably Firefox)

Request Trial Edition by submitting required details in the form under Support section/tab

You will receive request confirmation email from MASTS team to download the setup

Download HID Generator utility via the link provided in the email

Run the utility and respond to MASTS team with the generated HID code

You will receive an email with setup download information/link and license file

Download the setup and install it on your workstation

Prerequisites

Prerequisites for target test environment to execute MASTS Trial Edition:

1. Rooted Android Device OR Android OS Virtual Machine
2. MASTS Agent APK installed on target test device
Download MASTS Agent APK from [MASTS website](#) OR [Google Playstore](#)
3. Hardware: Intel i5 processor (i7 recommended), 8 GB RAM (12 GB recommended)
4. Software: Java - JRE 8, Microsoft Windows OS - 7, 8, 8.1, 10
5. Web Browser: Internet Explorer, Google Chrome, Mozilla Firefox (recommended)

Note: If you are facing difficulties in rooting Android device, we can ship rooted device to you.

Installation

MASTS installation is facilitated with an easy to use and intuitive installer

1. Locate MASTS Trial Edition setup executable from your downloads folder
2. Right click on it and select **Run as administrator**

Note: Let the installer do its task and wait until the installation completes.

Licensing

Download the license file which is received from MASTS team via email

On executing MASTS for the first time, you must upload the license file to activate the product

After successful activation and for configuration updates your system needs a reboot

It is advised to close all programs and save your work and perform a reboot

Note: Trial Edition will be valid only for 30 days having limited number of scans and test cases.

Scanning

MASTS facilitates multiple types of scanning as per industry best practices for testing:

A. **Static Analysis** - performs static APK level testing without the need of tester to capture traffic (URL's) via the target application and check for vulnerabilities/security issues.

B. **Dynamic Analysis** - performs runtime testing by allowing user to navigate through the application screen/modules and check for vulnerabilities/security issues.

B1. **Black Box Scanning** - performs scanning without user/tester to log into the application. This scanning approach imitates an unknown user/hacker accessing the application without any valid credentials of the application and check for the vulnerabilities/security issues. Black box scanning can be performed in two ways i.e. without navigating through the application screens as well as by navigating through the application screens.

B2. **Gray Box Scanning** - performs scanning by first asking user/tester to log into the application via the target test device and navigate through the application modules/screens and check for vulnerabilities/security issues.

Note: For more information and tutorials visit MASTS YouTube channel [here](#).

SAND a unique feature, captures the state of the device and is abbreviated as **Snapshot** for **Android**.

SAND module comes in two forms:

1. **Capturing SAND** - facilitates the tester to capture a new snapshot of the device
2. **Comparing SAND** - facilitates the tester to compare snapshots already taken. Tester can compare any two (2) captured snapshots at any given time from below available options:
 - A. Before Installing the application
 - B. After Installing the application
 - C. After logging in the application
 - D. After logging out of the application
 - E. After Uninstalling the application

SAND

MASTS provides following set of additional utilities for mobile application pentesting needs:

1. **APK Reverse Engineering Decompiler** - facilitates the tester to decompile the target application APK for source code level analysis. *Available only in Pro Edition!*

Q. How to run reverse engineering decompiler?

A. Select any target application APK from the list to get it decompiled.
2. **APK Reverse Engineering Recompiler** - facilitates the tester to recompile into a binary (APK file). The APK can be any file decompiled earlier. *Available only in Pro Edition!*

Q. How to run reverse engineering recompiler?

A. Browse for the .zip archive and upload it. After successful operation click Push APK to transfer the APK to the device. To download the rebuilt APK click Download APK to download it on local workstation.
3. **Traffic Sniffer** - facilitates the tester to capture traffic flowing from the target application to its web server.

Q. How to capture traffic?

A. Run the target application, click on Start Sniffer to begin the capture, click on Stop sniffer to stop the capture. Click on Download to download the captured packets.
4. **Screen Capture** - facilitates the tester to capture the current screen on the mobile device to maintain it as a Proof of Concept.

Q. How to capture screen?

A. Run the target application and navigate to the module for which the screen is to be captured. Click Get Screen shot to capture the active screen. Click Download to download it as an image.
5. **Logcat** - facilitates the tester to capture logs from all the processes in the target device under execution.

Q. How to work with Logcat?

A. Click Start Logcat to start capturing the events and logs from the target test device. Click Stop Logcat to stop the capture. Click Download to download the captured logs.
6. **File Explorer** - facilitates the tester to view the internals of the target test device, file system, structure, etc.
7. **Database Explorer** - facilitates the tester to perform various operations on database including adding custom values to tables, deleting table values to deleting the entire database or table.

Android Utilities

MASTS administrator is facilitated with following account management functions,

1. Change administrator password
2. Change pattern lock
3. View last login history
4. View MASTS license details

MASTS has a unique reporting structure with all necessary information for a tester as well as the client’s development team to understand the vulnerability, its business impact and recommendations.

1. **Completed Scan Reports** - facilitates the tester to view the reports of all successful scans which are completed.
2. **Failed Scan Reports** - facilitates the tester to view the reports for scans which got failed.

Note: Tester can only view the reports in trial edition. Downloading report is only facilitated in Pro Edition. Supported formats are PDF and HTML.

3. **Completed Snapshots** - facilitates the tester to view the reports for all successful completed snapshots.
4. **Compared Snapshots** - facilitates the tester to view the reports of any two (2) given snapshots compared earlier.

Note: Tester can only view the reports in trial edition. Downloading report is only facilitated in Pro Edition. Report can be exported in PDF format.



For any queries or any technical assistance, please feel free to contact MASTS technical support team on masts@varutra.com

Talk to our experts on (+91) 8554 811 911 between Monday to Friday, 10:00 AM to 06:00 PM (IST)

It was pleasure to serve you!

Thank you for choosing MASTS for your mobile application security testing needs.