OPEN SECURITY SUMMIT Supported by OWASP

OUTCOMES MOBILE SECURITY TEAM

Jeroen Willemsen – Open Security Summit

OWASP Open Web Application Security Project | Standard

Mobile AppSec Verification

Version 1.1

Project leaders: Sven Schleier and Jeroen Willemsen

Creative Commons (CC) Attribution Share-Alike
Free version at http://www.owasp.org

OWASP Open Web Application Security Project

MSTG

MOBILE
SECURITY
TESTING
GUIDE

Bernhard Mueller
Sven Schleier
Jeroen Willemsen
The OWASP mobile team

OWASP
Open Web Application
Security Project

FRIDA
FLORIDA

FOCUS:
GET IT DONE, GET IT DONE
GET IT DONE

Want to join? Have the same ***FOCUS***

There are 99 worries in Infosec/DevSecOps
BUT THERE IS ONLY ONE MSTG

FOCUS!

FOCUS! FOCUS EVERYWHERE!

OWASP Open Web Application Security Project | Standard

Mobile AppSec Verification

Version 1.1

Project leaders: Sven Schleier and Jeroen Willemsen

Creative Commons (CC) Attribution Share-Alike
Free version at http://www.owasp.org

GOAL 1.1.4: Improve Quality & Ease

And prepare for bigger changes with a focus on content,
not the format

Outcomes – quality improvements

OWASP | Standard

Mobile AppSec Verification

Version 1.1

Project leaders: Sven Schleier and Jeroen Willemsen

Creative Commons (CC) Attribution Share-Alike

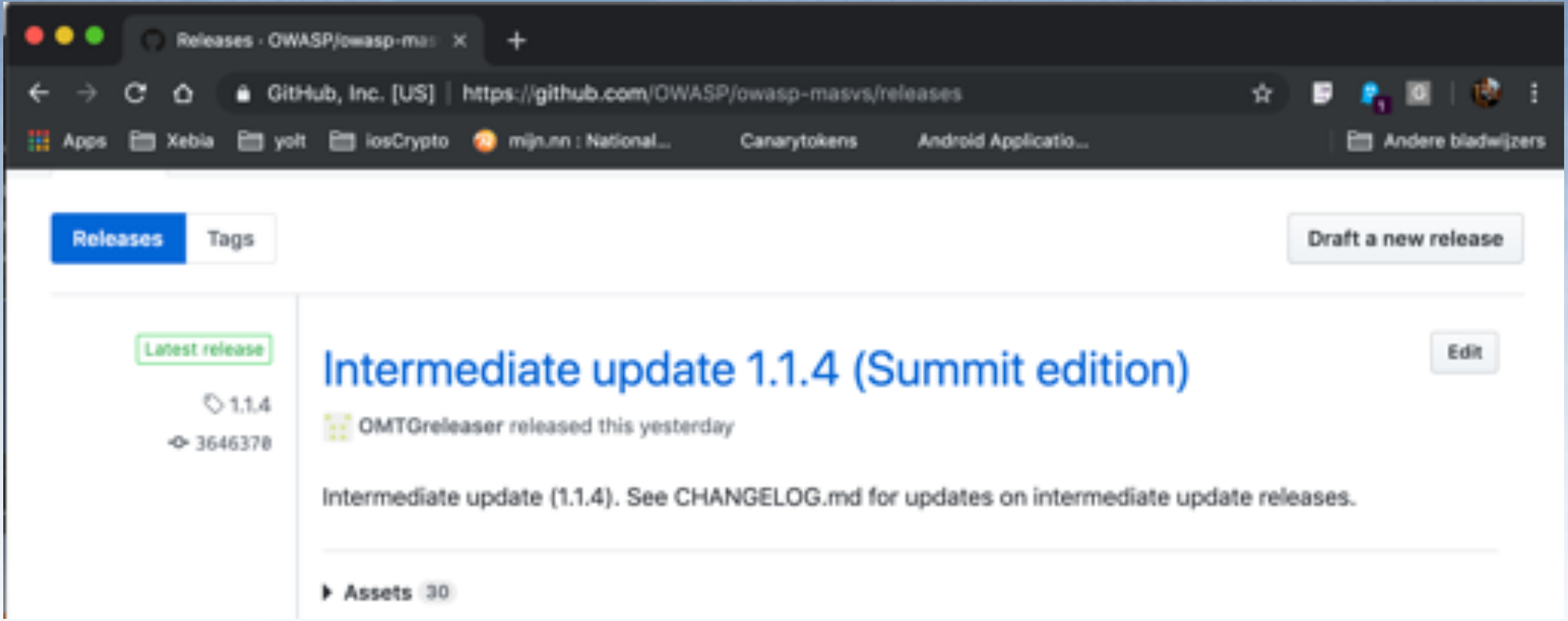
Free version at http://www.owasp.org

- Fix all markdown issues.
- Updates in the French and Spanish translations.
- Translated changelog to Chines (ZHTW) & Japanese.
- Automated verification of the the markdown syntax and reachability of the URLs.
- Added identification codes to the requirements.

Outcomes – quality improvements

OWASP
Standard
Mobile AppSec Verification
Version 1.1
Project leaders: Sven Schleier and Jeroen Willemsen
Creative Commons (CC) Attribution Share-Alike
Free version at http://www.owasp.org

- Reduced the repo size
- Added a Code of Conduct & Contributing guidelines.
- Added a Pull-Request template.
- Improved Gitbook sync speed.
- Updated the scripts to generate XML/JSON/CSV for all the translations.
- Translated the Foreword to Chinese (ZHTW).

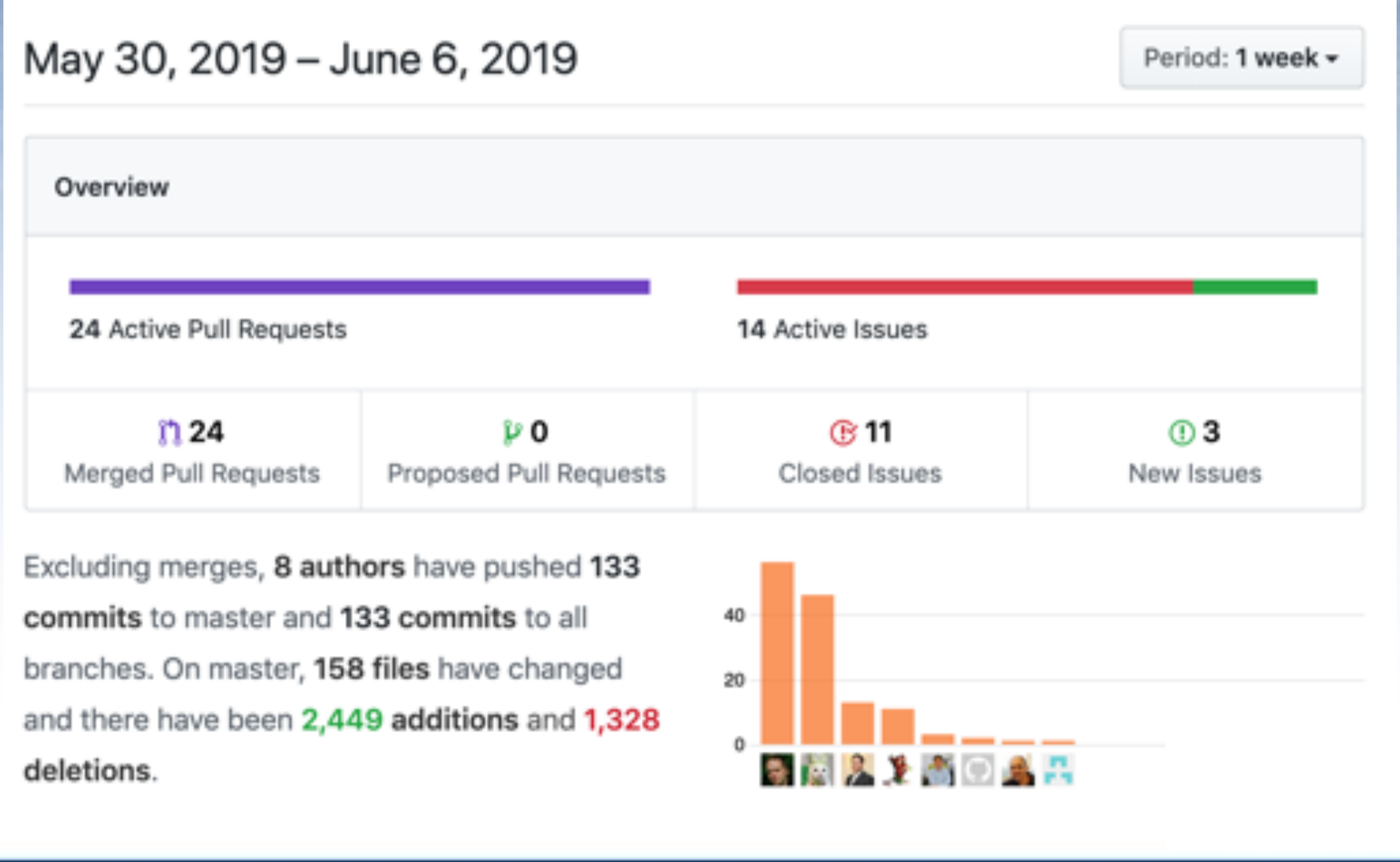


Intermediate update 1.1.4 (Summit edition)

OMTGreleaser released this yesterday

Intermediate update (1.1.4). See CHANGELOG.md for updates on intermediate update releases.

- Format: EPUB, MOBI, PDF, DOCX
- Languages: Chinese (ZHTW), English, German, Japanese, Russian & Spanish
- Generated on "*git push --tags*"



May 30, 2019 – June 6, 2019

Period: **1 week** ▾

Overview

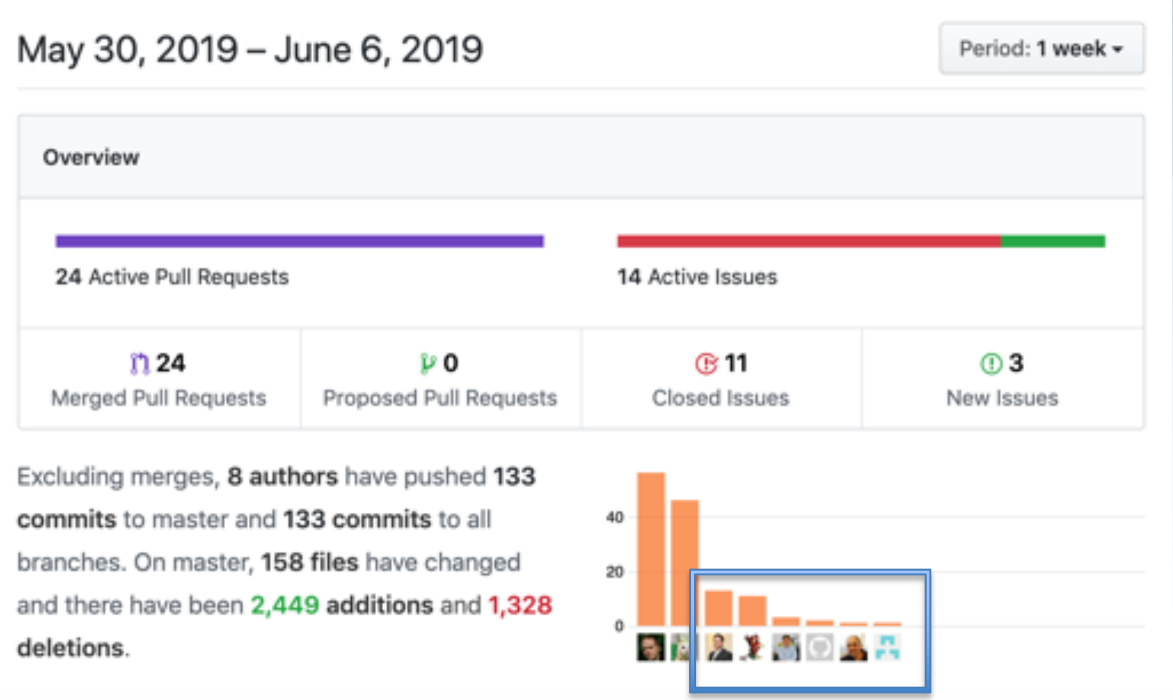
24 Active Pull Requests

14 Active Issues

24 Merged Pull Requests	**0** Proposed Pull Requests	**11** Closed Issues	**3** New Issues

Excluding merges, **8 authors** have pushed **133 commits** to master and **133 commits** to all branches. On master, **158 files** have changed and there have been 2,449 **additions** and 1,328 **deletions**.

Remote heroes!



May 30, 2019 – June 6, 2019

Period: 1 week ▾

Overview

24 Active Pull Requests

14 Active Issues

24 Merged Pull Requests	0 Proposed Pull Requests	11 Closed Issues	3 New Issues

Excluding merges, **8 authors** have pushed **133 commits** to master and **133 commits** to all branches. On master, **158 files** have changed and there have been **2,449 additions** and **1,328 deletions**.

Special thanks to:

- Henry Hu -
- Riotaro Okada -
- Koki Takeyama -

For their swift response and Great remote help

OWASP

MSTG

MOBILE
SECURITY
TESTING
GUIDE

Bernhard Mueller
Sven Schleier
Jeroen Willemsen
The OWASP mobile team

GOAL 1.1.3: Restructure, Update & Expand

And prepare for the final sprint for 1.2

CHALLENGE 1: Technical challenges

1. iOS 12 jailbroken & Android Pie rooted are not as mature as their predecessors. Meaning: tools will not work immediately.
2. iOS & Android pentesting tools vary in quality and ease of use.
3. How can we make sure that they still work?

IF YOU LET EVERY TEAM-MEMBER FIND OUT HIMSELF THEN IT WILL TAKE FOREVER. → Enter the technician

CHALLENGE 2: Depth of content

1. Mobile security goes deep
2. There is a lot to think about

IF YOU LET EVERY TEAM-MEMBER TRY TO FIND THE DEPTHS/BREADTHS OF A SUBJECT AND WHAT TO TAKE CARE OF: HE WILL BE BUSY FOREVER. → Enter the content guide/mentor

CHALLENGE 3: Spelling, grammar & Style

1. English is hard
2. Most of us are non-native speakers

IF EVERY TEAM-MEMBER…. → enter the reviewer!

Work together!

1. Review a PR first (content guiding / grammar & spell review)!
2. Make sure that stuff works first!
3. Asked for help? Help them first!
4. Work on your write-up.

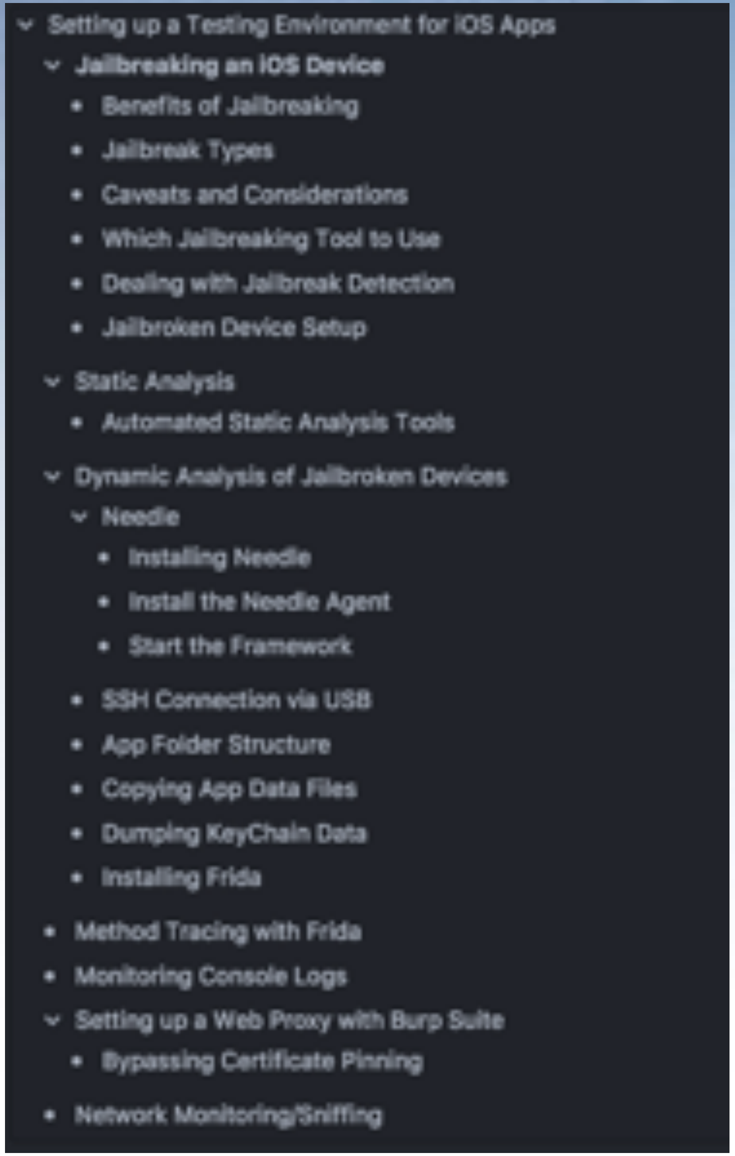
So: fix hurdles as a team, THEN move forward.

Be prepared!

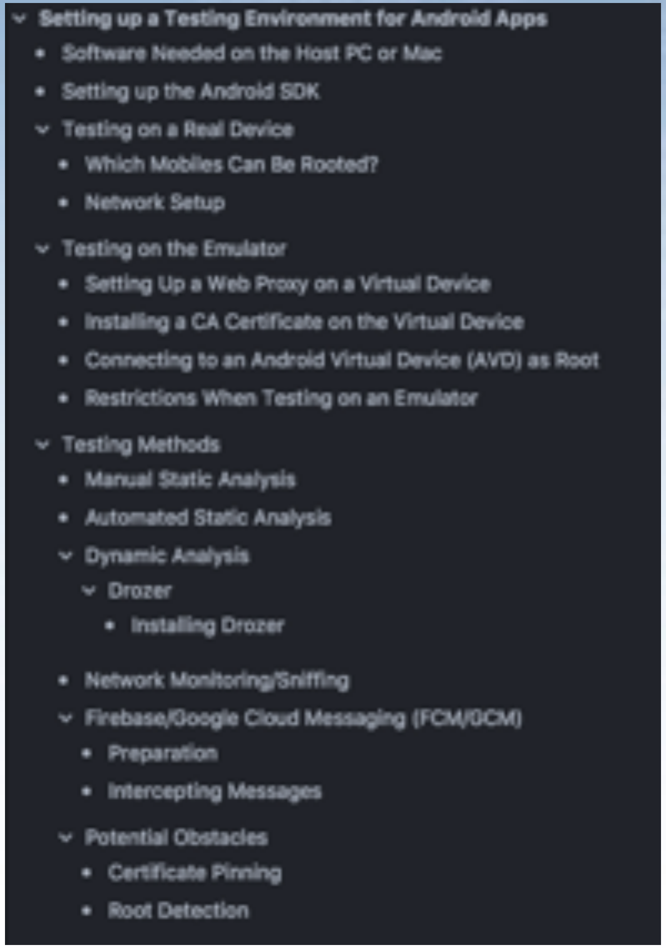
1. Preparation is key: have clear goals, baby steps and move forward
2. Align BEFORE you start: so the team can function
3. Focus on the team before, during and after

Outcome: Restructure, Update & Expand

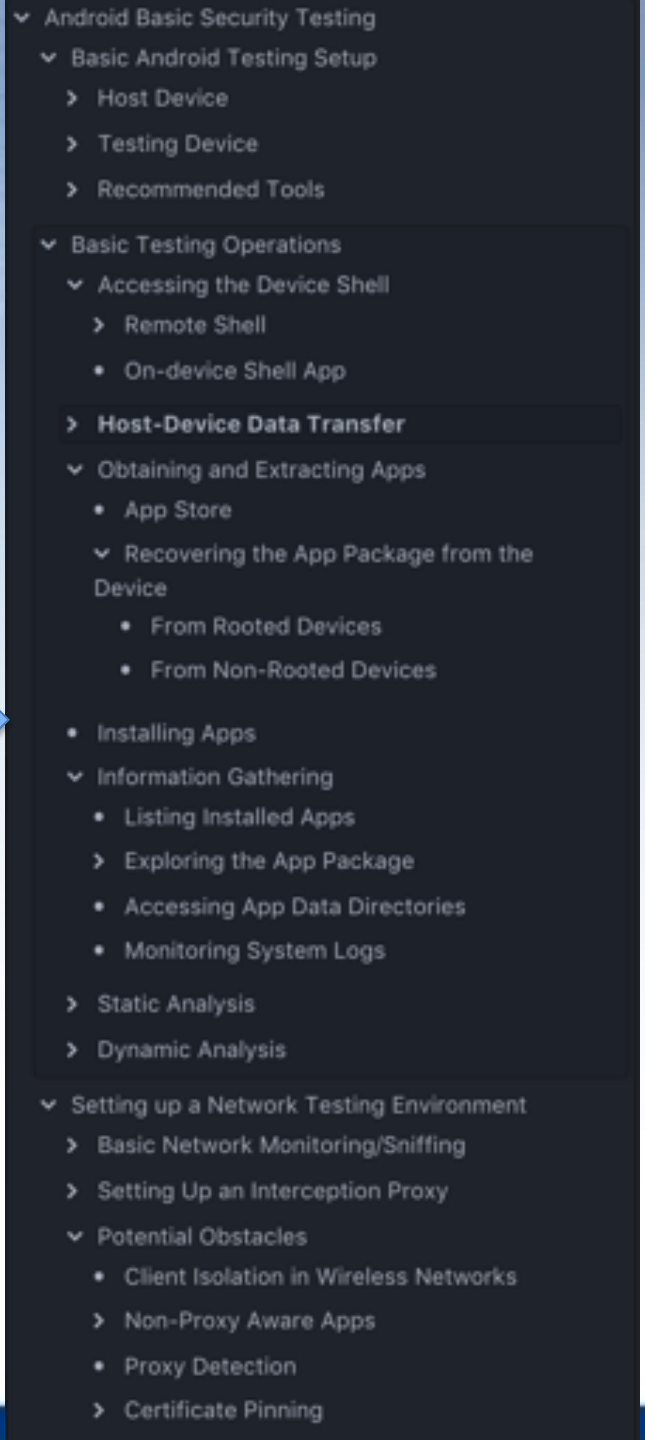
- Restructured!
- Many tools updated!
- Automation!
- Clean Markdown!
- Many other smaller things ;-)
- Preparation for better app-products (many repo’s & a planning to get there)



- Setting up a Testing Environment for iOS Apps
  - **Jailbreaking an iOS Device**
    - Benefits of Jailbreaking
    - Jailbreak Types
    - Caveats and Considerations
    - Which Jailbreaking Tool to Use
    - Dealing with Jailbreak Detection
    - Jailbroken Device Setup
  - Static Analysis
    - Automated Static Analysis Tools
  - Dynamic Analysis of Jailbroken Devices
    - Needle
      - Installing Needle
      - Install the Needle Agent
      - Start the Framework
    - SSH Connection via USB
    - App Folder Structure
    - Copying App Data Files
    - Dumping KeyChain Data
    - Installing Frida
  - Method Tracing with Frida
  - Monitoring Console Logs
  - Setting up a Web Proxy with Burp Suite
    - Bypassing Certificate Pinning
  - Network Monitoring/Sniffing



- **Setting up a Testing Environment for Android Apps**
  - Software Needed on the Host PC or Mac
  - Setting up the Android SDK
  - Testing on a Real Device
    - Which Mobiles Can Be Rooted?
    - Network Setup
  - Testing on the Emulator
    - Setting Up a Web Proxy on a Virtual Device
    - Installing a CA Certificate on the Virtual Device
    - Connecting to an Android Virtual Device (AVD) as Root
    - Restrictions When Testing on an Emulator
  - Testing Methods
    - Manual Static Analysis
    - Automated Static Analysis
    - Dynamic Analysis
      - Drozer
        - Installing Drozer
    - Network Monitoring/Sniffing
    - Firebase/Google Cloud Messaging (FCM/GCM)
      - Preparation
      - Intercepting Messages
    - Potential Obstacles
      - Certificate Pinning
      - Root Detection



- Android Basic Security Testing
  - Basic Android Testing Setup
    - Host Device
    - Testing Device
    - Recommended Tools
  - Basic Testing Operations
    - Accessing the Device Shell
      - Remote Shell
      - On-device Shell App
    - **Host-Device Data Transfer**
    - Obtaining and Extracting Apps
      - App Store
      - Recovering the App Package from the Device
        - From Rooted Devices
        - From Non-Rooted Devices
    - Installing Apps
    - Information Gathering
      - Listing Installed Apps
      - Exploring the App Package
      - Accessing App Data Directories
      - Monitoring System Logs
    - Static Analysis
    - Dynamic Analysis
  - Setting up a Network Testing Environment
    - Basic Network Monitoring/Sniffing
    - Setting Up an Interception Proxy
    - Potential Obstacles
      - Client Isolation in Wireless Networks
      - Non-Proxy Aware Apps
      - Proxy Detection
      - Certificate Pinning

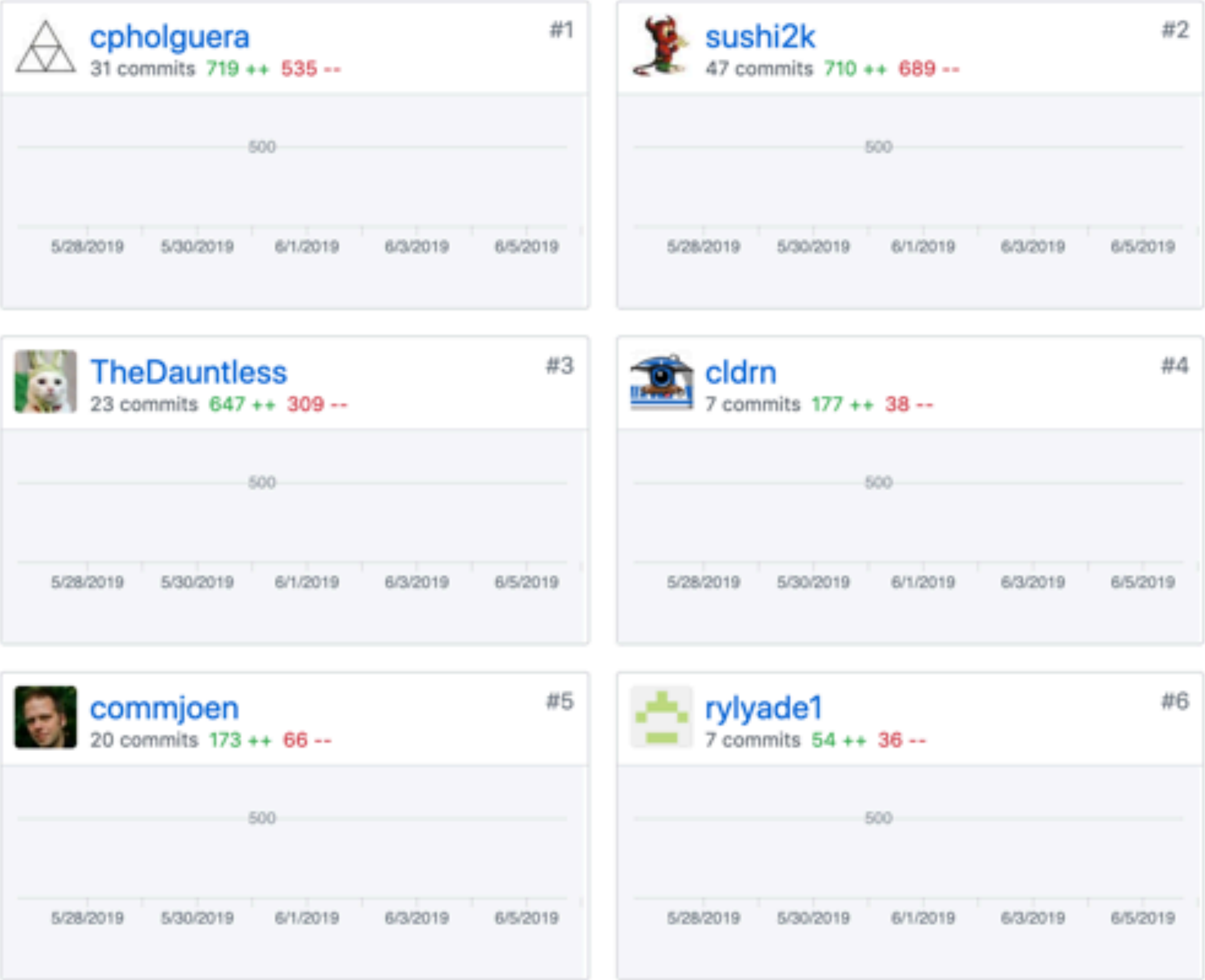
Let’s go to Github Pulse!!

https://github.com/OWASP/owasp-mstg/pulse

No release yet…

- There are quiet some TODO’s left (10 actually) in the document. Once these are fixed. We will create a release…

REMEMBER THE BOOK CHALLENGE?



cpholguera #1
31 commits 719 ++ 535 --

sushi2k #2
47 commits 710 ++ 689 --

TheDauntless #3
23 commits 647 ++ 309 --

cldrn #4
7 commits 177 ++ 38 --

commjoen #5
20 commits 173 ++ 66 --

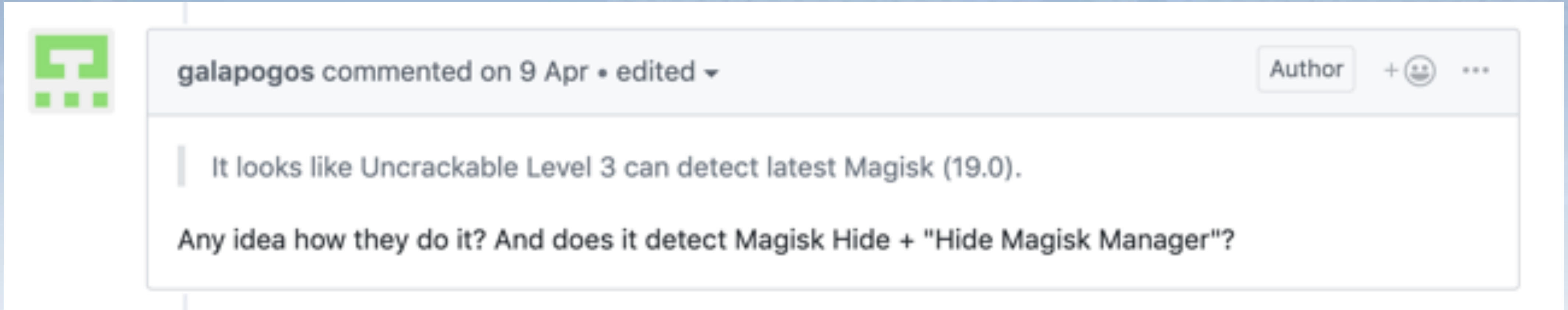
rylyade1 #6
7 commits 54 ++ 36 --

FЯ
MSTG
MOBILE SECURITY TESTING GUIDE

ONE SPECIAL PRICE….

- Although Carlos had the MOST contributions
- Paulino took the MOST effort to get here From Mexico and join in the game late
- GIVE HIM A WARM APPLAUSE!

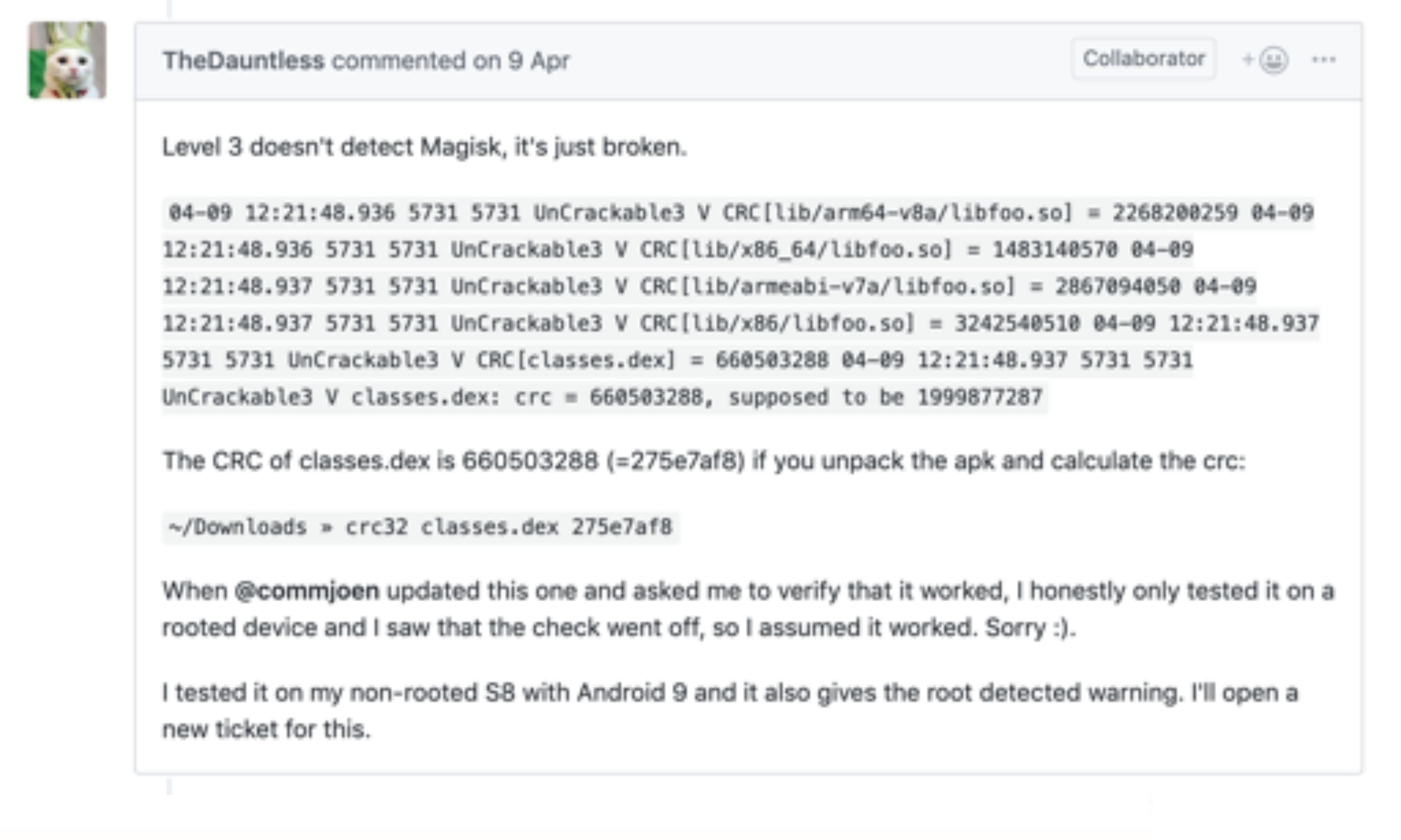
OWASP
Open Web Application
Security Project



galapogos commented on 9 Apr • edited

> It looks like Uncrackable Level 3 can detect latest Magisk (19.0).

Any idea how they do it? And does it detect Magisk Hide + "Hide Magisk Manager"?



TheDauntless commented on 9 Apr

Level 3 doesn't detect Magisk, it's just broken.

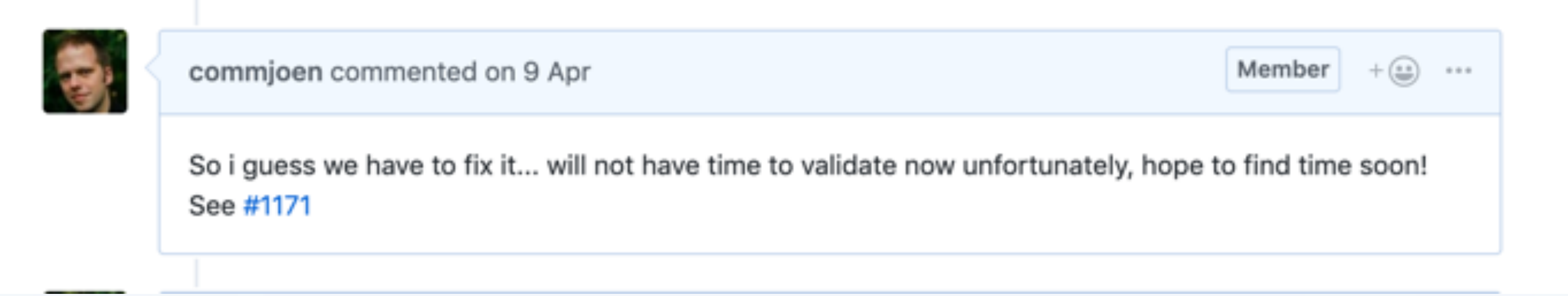
```
04-09 12:21:48.936 5731 5731 UnCrackable3 V CRC[lib/arm64-v8a/libfoo.so] = 2268200259 04-09
12:21:48.936 5731 5731 UnCrackable3 V CRC[lib/x86_64/libfoo.so] = 1483140570 04-09
12:21:48.937 5731 5731 UnCrackable3 V CRC[lib/armeabi-v7a/libfoo.so] = 2867094050 04-09
12:21:48.937 5731 5731 UnCrackable3 V CRC[lib/x86/libfoo.so] = 3242540510 04-09 12:21:48.937
5731 5731 UnCrackable3 V CRC[classes.dex] = 660503288 04-09 12:21:48.937 5731 5731
UnCrackable3 V classes.dex: crc = 660503288, supposed to be 1999877287
```

The CRC of classes.dex is 660503288 (=275e7af8) if you unpack the apk and calculate the crc:

```
~/Downloads » crc32 classes.dex 275e7af8
```

When @commjoen updated this one and asked me to verify that it worked, I honestly only tested it on a rooted device and I saw that the check went off, so I assumed it worked. Sorry :).

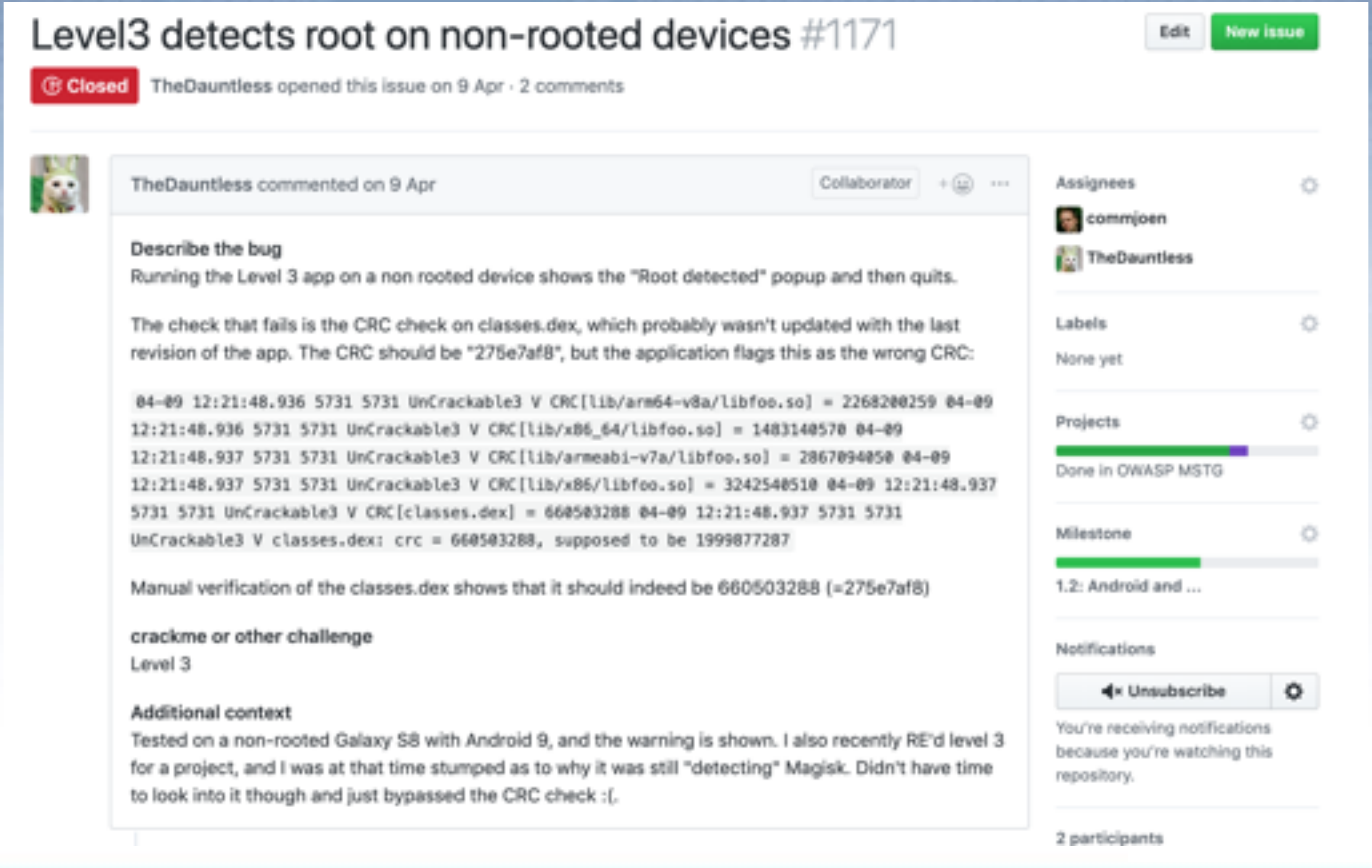
I tested it on my non-rooted S8 with Android 9 and it also gives the root detected warning. I'll open a new ticket for this.



commjoen commented on 9 Apr

Member

So i guess we have to fix it... will not have time to validate now unfortunately, hope to find time soon!
See #1171



Level3 detects root on non-rooted devices #1171

TheDauntless opened this issue on 9 Apr · 2 comments

TheDauntless commented on 9 Apr

Describe the bug
Running the Level 3 app on a non rooted device shows the "Root detected" popup and then quits.

The check that fails is the CRC check on classes.dex, which probably wasn't updated with the last revision of the app. The CRC should be "275e7af8", but the application flags this as the wrong CRC:

```
04-09 12:21:48.936 5731 5731 UnCrackable3 V CRC[lib/arm64-v8a/libfoo.so] = 2268200259 04-09
12:21:48.936 5731 5731 UnCrackable3 V CRC[lib/x86_64/libfoo.so] = 1483140570 04-09
12:21:48.937 5731 5731 UnCrackable3 V CRC[lib/armeabi-v7a/libfoo.so] = 2867094050 04-09
12:21:48.937 5731 5731 UnCrackable3 V CRC[lib/x86/libfoo.so] = 3242540510 04-09 12:21:48.937
5731 5731 UnCrackable3 V CRC[classes.dex] = 660503288 04-09 12:21:48.937 5731 5731
UnCrackable3 V classes.dex: crc = 660503288, supposed to be 1999877287
```

Manual verification of the classes.dex shows that it should indeed be 660503288 (=275e7af8)

crackme or other challenge
Level 3

Additional context
Tested on a non-rooted Galaxy S8 with Android 9, and the warning is shown. I also recently RE'd level 3 for a project, and I was at that time stumped as to why it was still "detecting" Magisk. Didn't have time to look into it though and just bypassed the CRC check :(.

Assignees
commjoen
TheDauntless

Labels
None yet

Projects
Done in OWASP MSTG

Milestone
1.2: Android and ...

Notifications

You're receiving notifications because you're watching this repository.

2 participants

Thank you

- Organizers, for making this possible
- Team, for rocking it
- Attendees, for respecting our “different” behavior
- Cu next year ;-).
- Want to stay in touch?
  - See you at the OWASP Slack
  - Follow @OWASP_MSTG
  - Star https://github.com/OWASP/owasp-mstg
  - Star https://github.com/OWASP/owasp-masvs

THE END…

@OWASP_MSTG

https://github.com/OWASP/owasp-mstg

https://github.com/OWASP/owasp-masvs