Inspiratron.org - Natural language processing, machine learning and cybersecurity

Educational framework added to OWASP Seraphimdroid

by Nikola Miloševi? - Sunday, August 28, 2016

https://inspiratron.org/blog/2016/08/28/educational-framework-added-to-owasp-seraphimdroid/

OWASP Seraphimdroid is back after Google Summer of Code with a new version, this time, it will be 2.5 and some exciting changes, we thought that may help users protect their security and privacy. I would like to briefly write about our new features. The app is available on old good place: Google play (https://play.google.com/store/apps/details?id=org.owasp.seraphimdroid)

What is new?

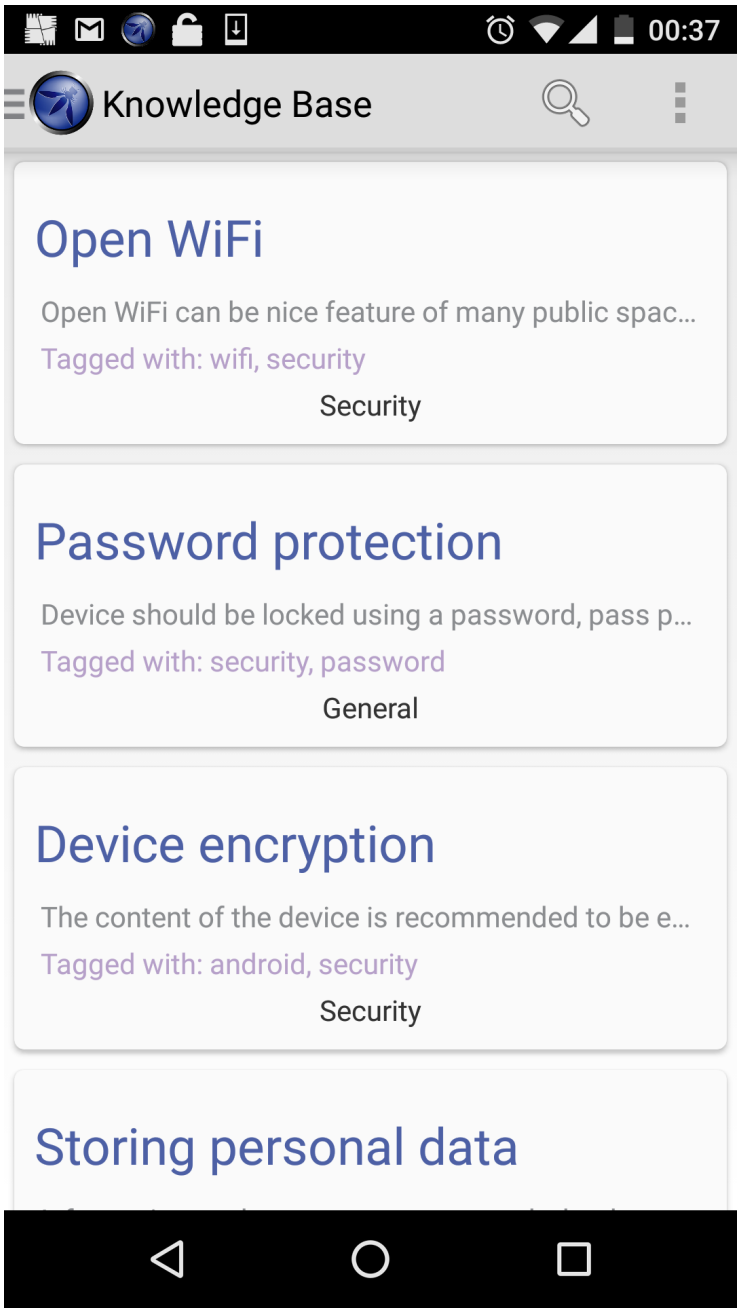
Educational component

From the very beginning of OWASP Seraphimdroid project, as a project leader, I saw in it a project that contains an educational component. However, until now we aimed to develop a number of features that will on technical level protect users. I have been writing about the development previously:

OWASP SERAPHIMDROID ANDROID SECURITY PUBLISHED

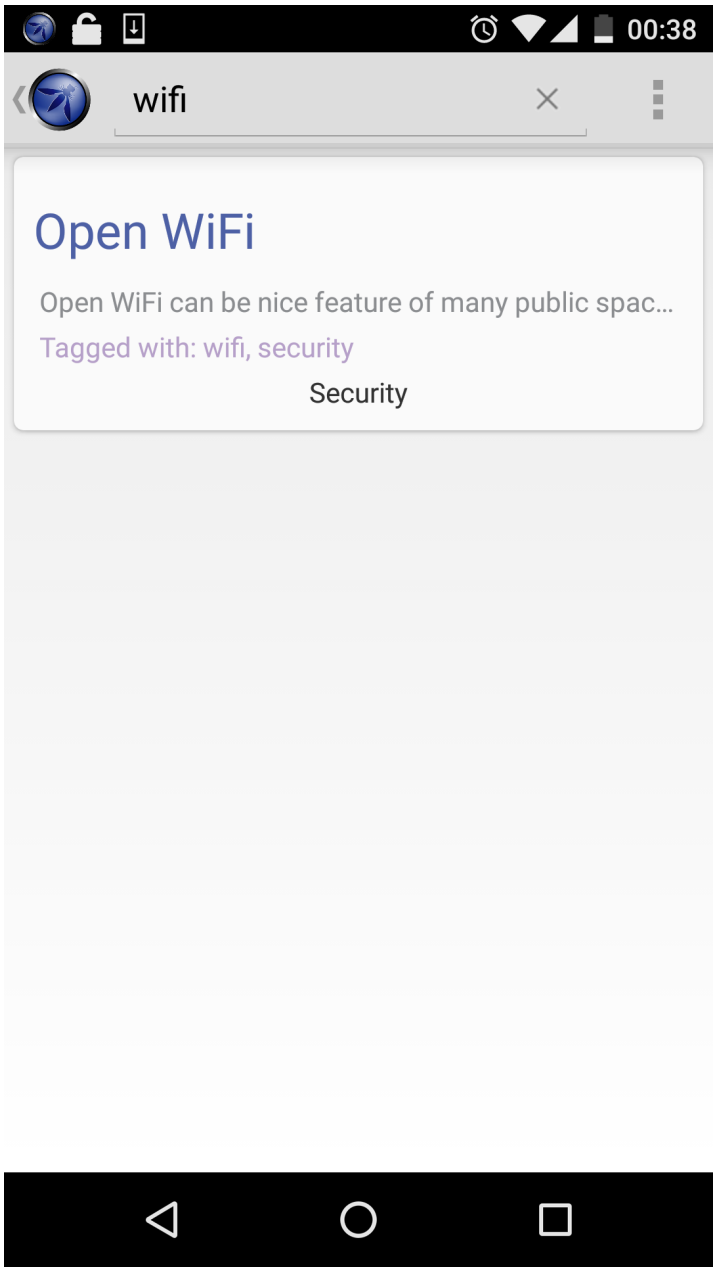
NEW VERSION OF OWASP SERAPHIMDROID (V2.0) IS PUBLISHED

Now, we are coming back with a version 2.5 that contains the long-awaited educational component. Why is this component necessary? Because, as it has been stated in many researchers in computer security area, most of the intrusions, hacking, theft of information is due to the human error or not applying best practices. This means also that majority of these things happen because people are uninformed, uneducated and ignorant. However, it is not that hard to read a couple of articles about mobile security and apply them. We are now bringing them into the OWASP Seraphimdroid app. So apart from being security tool that protects your device, now OWASP Seraphimdroid will be able to educate users about important topics in mobile security. We tried to develop this educational component as simple as it was possible. Users have a screen with a number of articles and a Search function where he can search for these articles. We tried really hard to make search functional and not only string match the entries in the database, but to use state-of-the-art information retrieval techniques. Namely, we used TF-IDF (term frequency+inverse document frequency) algorithm in combination with cosine similarity. We modified, for our purposes and for the sake of working under Android, Apache Lucene - a framework for creating information retrieval engines. Below is an image showing how our knowledge base looks like.



Educational component of OWASP Seraphimdroid - Knowledge base main screen

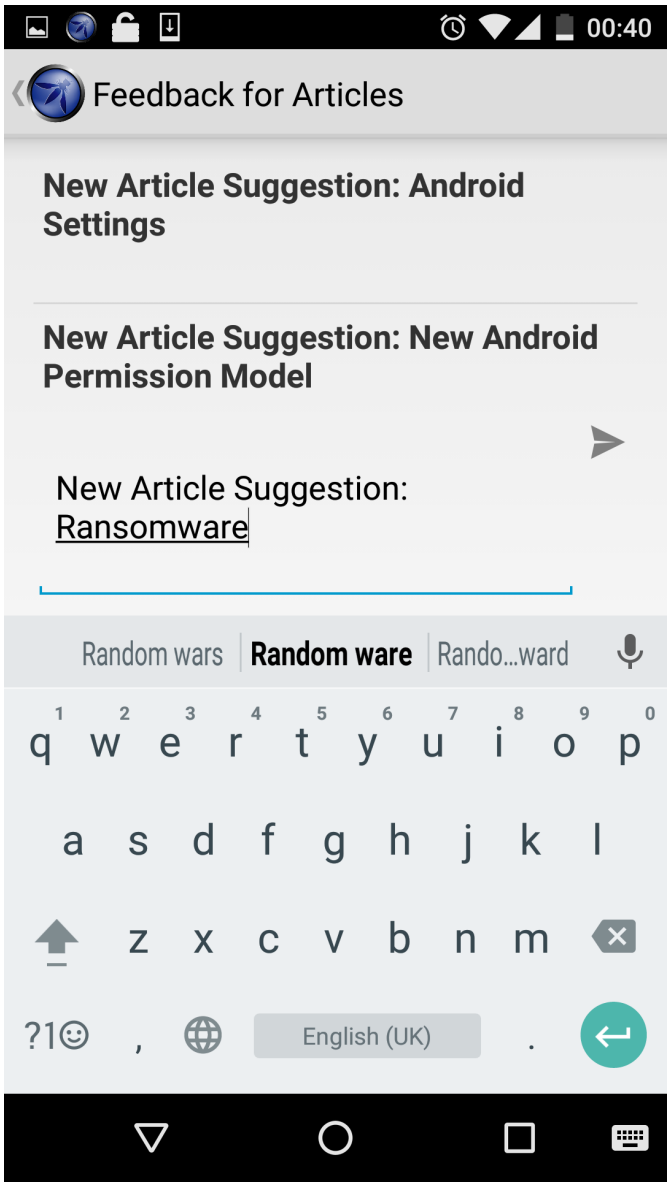
On the next picture, it is presented how search shows data. Click on the article opens the article with its text and potential images.



Search function in knowledge base

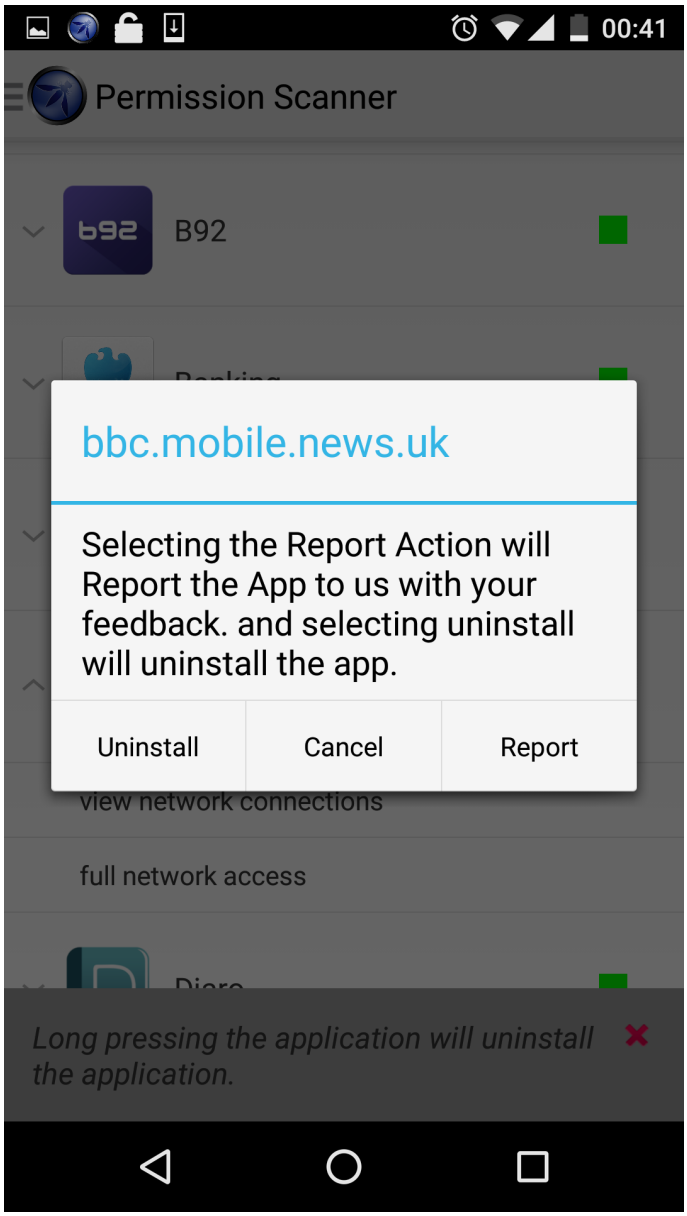
Feedback function

In the past, our team did not interact too much with the users. However, users are important to us and we would like to know what they think and how would they suggest us to improve OWASP Seraphimdroid. Also, we would like to hear what new features and articles they would like us to add. For this purpose, we built in the application a feedback function that allows users to tell us about these things. we tried as well to keep it simple, where a user can only add a text.



Feedback function

Apart from this raw text feedback functionality, we built-in a function to give us feedback on permission scanner classifications. Permission scanner function is using machine learning in order to predict whether some application is potentially dangerous and malicious. In case it is it will show a red square. However, I wrote previously about the feature and that it is accurate in about 87% of cases. Taking into account that it will make mistakes in classification, we also assumed that more savvy users will know that something on their device is malicious or it is not. If it is misclassified, they can report it to us and we will analyze the app and probably in the next version develop a feature that will take these reports into account in some way. The function is accessible from the permission scanner by pressing for a long tine (long click) on misclassified app. The pop-up menu will ask the user whether he wants to cancel, report misclassification or uninstall the application.



Report permission scanner misclassification

Better and built-in documentation

We finally did some work with making our documentation better and more user approachable. Actually, we split our previous documentation that contained technical documentation and user guide to two different documents - one for a user guide, while the other was technical documentation for developers. We included a user guide into the app and it can be accessed from the about screen.

Knowledge base dashboard

Also, we added server-side of the application, which currently serves only to push new articles to the users. It contains a dashboard for easy access and writing articles in markup language similar to the one used by GitHub. Currently, there are 7 articles about securing device and privacy. We are planning to add much more, but also we would like help in terms of suggestions and even already written articles. So we highly encourage people who have a knowledge about mobile and Android security to join our mailing list and let us know about them and their knowledge. Also, if anyone has already written articles or is willing to write, please let us know as well, so we can include them in the app.

The whole server-side platform was developed in Ruby and for GUI, Bootstrap was used. We gave some attention to user-friendliness, so it can be used by a wider range of article authors.

Acknowledgments

The improvements and new features were developed by Aditya Dua, who did it as part of his Google Summer of Code project, where he was mentored by myself. OWASP Seraphimdroid can be downloaded from Google Play on the following link: https://play.google.com/store/apps/details?id=org.owasp.seraphimdroid

More information about OWASP Seraphimdroid can be found here.
