

Random Hacks of Kindness, September 2013

On the weekend of the 6th through the 8th of September 2013, ScotlandHacks and Geeks Without Bounds paired up to present a special cybersecurity focused hackathon event, part of the Random Hacks of Kindness series of hackathons. At the event, participants worked in teams of two projects to improve the security of existing humanitarian software, two projects to improve cybersecurity education, one challenge to explore the problem of security in mobile assessment platforms for academic qualifications and one security study of an open source distributed database. The event was made possible through the financial support of SQA, Basho the people behind the Riak distributed database, the security consulting firm encryption, Cyber Security Challenge UK and Scottish Informatics & Computer Science Alliance and by in-kind support from code repository host GitHub, Glasgow's makerspace MAKLab, Police Scotland, and the IET Glasgow Teacher Building.

THE SPEAKERS

Paul Mason, ScotlandHacks

Delivered the introduction to the event.

Lisha Sterling, Geeks Without Bounds

Spoke about the need for secure code in humanitarian software projects.

Graeme West, Open Rights Group

Spoke about privacy in the digital age and the work of ORG.

Brian Moore, encryption

Spoke about cybersecurity consulting at encryption and what he looks for in a pentester.

Eamonn Keane, Police Scotland

Spoke about what the e-crime unit of Police Scotland does and described the current need for skilled cyber forensics experts to deal with the reality that all crime today has a digital aspect to it.

Dr. Michelle Govan, Glasgow Caledonian University

One of our three judge panel at the end of the event. She described the integrated Digital Security, Forensics and Ethical Hacking course at Glasgow Caledonian University and spoke about the value of events like the Random Hacks of Kindness Cybersecurity Event in providing an environment for students to practice their skills.

Councilor Dr. Martin Bartos, Glasgow City Council

Also on the judges panel, gave a short talk about computing in general, spiced with some xkcd cartoons about operating systems and people's approach to security.

Dr. Martin Beaton, Scottish Informatics and Computer Science Alliance

Another one of our judges, he told the group about the work of SICSA and the need for improved cybersecurity capacity in Scotland.

THE PROJECTS

Securing Taarifa

Taarifa is an open source web application for information collection, visualization and interactive mapping. It allows people to collect and share their own stories using various mediums such as SMS, Web Forms, Email or Twitter, placing these reports into a workflow. Where these reports can be followed up and acted upon, while engaging citizens and communities.

Previous to RHoKsec, Taarifa had no authentication or built-in security of any kind. Two developers spent the weekend adding authentication into the Taarifa system, allowing for the development of varied roles and permissions for use of or editing specific types of data.

The code was contributed into the repository at https://github.com/taarifa/taarifa_backend.

Security in Bachchao

Bachchao is a panic button application for Android phones that sends messages to pre-selected trusted friends, contacts the police, and starts a streaming recording of video and audio in the event of a mugging or other physical attack. The challenge for this application was to do a code review and report findings back to the project group.

The team working on Bachchao found several bugs, including incompatibility issues with certain Android devices. They prepared a report which was sent to project manager Chinmayi SK.

A Curriculum for Ethical Hacking

There was previously a curriculum for Ethical Hacking available in the SQA database which, as far as we know, was not used. The curriculum had a number of problems, including the fact that it didn't mention ethics anywhere in the course. We presented a challenge to create a new curriculum.

This challenge was taken up by Team Pi, who presented their weekend's work through a new proposed curriculum which is available at <http://scotlandhacks.org.uk/content/rhoksec-proposed-higher-national-uni...>

SQA Secure Mobile Assessment

The Scottish Qualifications Authority offers formative assessments and qualifications exams in many countries. As their reach extends to many locales where it may be difficult if not impossible to provide physical testing facilities with invigilators on hand, they have been looking into the possibility of providing secure assessments online and through mobile devices. Our challenge was to

A large group sat together to discuss the problems of security, identity and privacy in regards to mobile assessment platforms. They wrote up their notes on Hackpad. Those notes have been copied to a permanent page on ScotlandHacks Website at <http://scotlandhacks.org.uk/content/rhoksec-sqa-secure-assessment-team-n...>

Ciphers for Learning

The UK Cyber Security Challenge has a small HTML, CSS & Javascript application that allows them to offer small cipher challenges at events like the Cheltenham Science Festival. The application allows for participant information (name and email) along with the results of their attempts to crack the ciphers to be saved onto a USB thumb drive so that any available computer can be used to set up the challenges. The challenge put to RHoKsec was to create new levels for the program, helping to create a larger, tiered puzzle from the original code.

The team that worked on this developed code and a storyline for the full challenge. Notes for the story can be found at <http://scotlandhacks.org.uk/content/rhoksec-cipher-challenge>. Code for the project can be found at <https://github.com/pdm126/RHoK-Cipher>.

Breaking Riak

One of the projects that was much anticipated at this event was the set up of a pentesting lab with a Riak install across four computers. A team of participants had discussed in advance several potential attacks that they would attempt against Riak in order to get it to provide information to an unauthorized user or to corrupt the data held.

Unfortunately, while it was possible to set up a small “development environment” on a single computer, the team was never able to install a Riak cluster that spanned multiple devices. Since the planned attacks were based on vulnerabilities in communication between nodes in a cluster, the planned penetration testing never happened.

The team has unanimously agreed that they would like to set aside time to solve the problem of the initial install in the future so that they can do the security research as intended. This may be a project for a planned future “Defcon Glasgow” chapter.