

To whom it may concern

Reference letter for Shahriyar MAMMADOV

Shahriyar MAMMADOV has been working for six months as of August 8th, 2016 as an intern in the SAP Product Security Research group at SAP Labs France, under my supervision. SAP is known for being the market leader in business solutions for all types of industries and for each major market.

For the duration of his internship, Shahriyar has been working at SAP Labs France, in the context of an internal project in the field of Intrusion Deception. This project consisted in defining and testing a framework allowing applications to detect proof of intrusion by usage of decoy database tables, records and other types of honeypots, as well as redirect the identified malicious traffic to a honeypot system where from attackers' actions and motives could be further analyzed.

During his internship, Shahriyar had to understand the value and usage of honeypots and of honeypot systems, implement diverse prototypes based on a previously designed architecture concept, overcome the technical limitations and make it ready for productive usage. His main challenges were to adapt a theoretical architecture to a real environment, to define an effective means to route rogue sessions to honeypots in a fully transparent manner, and to re-think the concept in a way that is both requiring minimal changes to existing code and full customization of the solution once deployed, in order to adapt to the observed behaviour. After these six months, Shahriyar was able to develop a fully functional application, and to enhance the initial concept greatly, namely by proposing and implementing a dashboard application where from operators can fully control the deployment and monitoring of honeypots, and a solution to transparently route traffic which does not require any code change in the router of technologies such as Cloud Foundry, a limitation of the original idea.

Some of the tasks achieved by Shahriyar include:

- Developing a prototype in PHP / MySQL, consisting in a vulnerable web application and in a component (named 'trap') for honeypot creation, deployment and monitoring
- Developing a second version of the prototype, on Node.js / MongoDB, able to be deployed on cloud environment(s), including creation of honeypot clones and solving the reverse proxy connection issue
- Developing a third and final version of the prototype, which generalizes the approach of the second prototype for an existing node.js internal application and which adds some extra features such as the possibility to unlock trapped sessions from the trap dashboard
- Write the technical documentation, a how-to guide for developers wishing to 'tokenize' their application, record demo videos and write presentations for several audiences.

Shahriyar performed quite well during his work under my supervision. He showed a genuine interest for the topic and for information security in general, up to the point that he'd like now to work in the field. He was able to work autonomously, proposing alternatives and new ideas regularly – most of them ending up into the prototype, and he always took my suggestions into consideration. He was a very pleasant intern to have in the team, always cheerful and motivated, and who belonged very well with the other interns and team members.

To conclude, I am fully satisfied with Shahriyar's work and attitude during these six months, and I am convinced he will perform well in a similar position in a full-time job.

SAP Labs France SAS
805, Avenue du Docteur Maurice DONAT
BP 1216 - 06254 MOUGINS Cedex
Tél. +33/4 92 28 62 00
Fax +33/4 92 28 62 01
SIRET 419 855 127 00033 - Code APE 6201Z

Cédric Hébert, OSCP, CISSP.
cedric.hebert@sap.com
SAP Research Project Manager