Babak Amin Azad

Mobile (+98) 912-7902484
Email babak.aminazad@gmail.com

https://www.silverf0x00.com
https://ir.linkedin.com/in/babakaminazad

Education

Shahid Beheshti University, Tehran, Iran – Bachelor of Science - 2010-2014

Major: Software Engineering

GPA: 3.29/4

BSc Project: Trust Based Protection Against Malicious Javascript

In this project we first reviewed the attack vectors of javascript in web applications, went over some abuse cases and proposed a novel method to sandbox javascript APIs based on trust which is derived from factors like the origin where the script was loaded and the destinations if the script uses Ajax calls to send data elsewhere, we then showed how this method could potentially protect against some of the known web attack methods where javascript is engaged.

In this project, we also introduced a concept to verify resources (mainly javascript) fetched from CDNs to protect against cache poisoning attacks. Coincidentally this concept was later developed by Firefox and W3C named Subresource Integrity (SRI).

Conference Workshops

"Ransomware Threats and Mitigation Techniques" held at "5th Annual Conference on E-Banking and Payment Systems"

In this workshop we described the basics of ransomwares including infection vectors and monetization techniques, we then went over their business model and lastly the countermeasures we can put in place to prevent or alleviate their damage. The workshop was held at 5th Annual Conference on E-Banking and Payment Systems at Milad Tower Conference Building.

"Penetration Testing Methods for Android Applications" held at Khaje Nasir Toosi University - 2016

In this presentation, an overview of android applications were given and then common vulnerabilities for each section was discussed. After reviewing the penetration testing steps a live demo was given for a vulnerability that enables the attacker to bypass the in-app billing system of a top selling application from a 3rd-party market named Bazar which is Google Play Store's replacement in Iran.

Experience

Security Researcher, Offsec Research Team (offsec.ir) - 2016

Offsec is an independent Iranian research group with members ranging from BSc students to PhDs and the topics we work on are Web/Binary analysis, Exploit development, Stegano/Crypto analysis and Forensics.
At Offsec research team we publish an infosec e-magazine in Persian. We conduct research and write publications and also review the ones we get from people outside of the team proposed to be published.

Cyber Security Analyst, CSIRT Team, Kashef Banking Security Governance, Tehran, Iran - 2014-2016

Kashef was founded by Central Bank of Iran to monitor and govern the security status of national banks and financial institutions. At Kashef our CSIRT team also acted as an ISAC, we studied and designed projects ranging from honeynets to information sharing schemes. We conducted security tests for national banking systems & websites and also alerted our customers (banks & financial institutions) about new cyber threats and consulted them about possible mitigations, some notable projects were: Ransomware Advisory, APT Group detection tool, DNN (DotNetNuke CMS) Advisory, Reported vulnerabilities in websites and mobile banking applications. There was a great focus on reporting and documentation skills along with presentations during our projects.
I also handled the outsourced development of the company's report gathering website and cooperated in the implementation of hardware tokens (PKI) and WAF deployment and tuning.

Notable Projects and Reports at Kashef

- Website monitoring and Deface Detection Service

In this project an application was developed to monitor national banks' websites and alert the CSIRT team if a downtime or a deface takes place. During the preliminary research for this project, several tools, techniques and online monitoring services were studied, then a subset of techniques were chosen that matched our scenario (banks' websites clean state is known and they are limited in number), derived features for the system to be monitored were: "Script addition to the page, Redirect to another domain, containing a list of specified words, change in the source of website greater than a predefined threshold", we also monitored the DNS records status and also the whois records for the websites and changes were

reported. This system was integrated with Qualy's SSLLabs[1] system to produce an overall report about the status of uptime, attacks, SSL protocol configuration and domain expiration. The trend that was derived from these reports over the course of 1.5 years shed light on some common issues between organizations.

- Banking websites' SSL configuration report and hardening guide

This project spanned over 35 national banks' internet banking websites, SSL protocol configuration of these sites was studied, factors like immunity against SSL vulnerabilities (Heartbleed, POODLE, FREAK, LogJam etc.), certificate signature algorithm and cipher suites negotiated with clients were taken into consideration and a hardening report was delivered to their admins to address these issues. (During the course of one year, significant improvement was seen)

- Mobile banking software security status and secure android development guide

The android version of mobile banking applications of 35 national banks was studied, features like secure software distribution, frequent updates, tamper detection and integrity verification, secure communication channel to the server, cryptographic protocols, insecure data storage and presence of obfuscation was tested, during this study several high impact vulnerabilities were found and reported. Lastly, a secure android development guide was produced to address common pitfalls in applications tested during this study.

Freelance Web Developer, Ontechsolutions ltd., United Kingdom - 2013-2016

As remote workers our task at Ontech was to upgrade a legacy, windows based sector specific ERP software to a multiuser, web based application, this was a web development project but due to abundance of features it had, the design and implementation of it was quite a challenge.

Skills

Security Related

Networks & Security, Cryptography, Machine Learning, SSL/TLS, Pentest, C|EH, Android Security, Metasploit, WLAN Security

Software Development Related

Python, C#, ASP.Net MVC, C++, Javascript, Matlab, Bash
Agile, Scrum, RUP, UML, Design Patterns, ORMs

[1] https://ssllabs.com/

Professional Courses	Cryptography I (Stanford at Coursera)
	Machine Learning (Stanford at Coursera)
	Software Security & Usable Security (University Of Maryland at Coursera)
	Bitcoin and Cryptocurrency Technologies (Princeton at Coursera)
	SPSE (SecurityTube Python Scripting Expert)
	SMFE (SecurityTube Metasploit Framework Expert)
	Android Security for Pentesters (SecurityTube)
Languages	Farsi (Native)
	English (Fluent)