Bofin Babu

BM 137
BITS-Pilani HYD Campus
Telengana, India

(Ph)+91 7097691400
bofinbabu@gmail.com
https://www.bofinbabu.com

EDUCATION

BITS-Pilani Hyderabad Campus, Hyderabad, India — June 2013 - Present
(Integrated) Master of Engineering, Computer Science
Specialization: Information Security

Mahatma Gandhi University, Kottayam, Kerala, India — June 2010 - April 2013
Bachelor of Science, Physics

EXPERIENCE

Intern — NVIDIA
January 2016 - Present — Pune
Full-time Software Engineering Intern in ShadowPlay team of GeForce Experience(GFE) group.

Teaching Assistant — BITS-Pilani
January 2015 - May 2015 — Hyderabad
CS/IS C313 - Object Oriented Programming and Design.
Assignment preparations, question-paper preparations and evaluations.

Teaching Assistant — BITS-Pilani
July 2015 - December 2015 — Hyderabad
CS/SS G518 - Database Design and Applications.
Lab notes preparations and evaluations.

SKILLS

Languages: C, C++, Python.
WebTech: HTML+CSS+JavaScript, Node+Oracle, OpenShift, CloudFlare.
Applications & Tools: Vi/Vim, Eclipse, Visual Studio, Git, VMWare, VirtualBox, Metasploit, Nmap, w3af, Zap, Scapy, Wireshark, Netcat, OpenVas, John, Burp, afl-fuzz, WEKA, Scikit-learn, Click modular routing.
Operating Systems: Ubuntu, Debian, Windows family, Android.

SELECTED PROJECTS

A Network Fuzzer with Evolutionary fuzzing capabilities. Fuzzing or Black-box testing is a way to test an application for security vulnerabilities. The application under test will be subject to a large number of automatically generated test cases and will be observed for special behaviors for every input. Normal fuzzing is like blind brute forcing, but by using Genetic Algorithms the the test case generation is much more effective by automating the approach of exploratory testing.

PyARP: (https://github.com/bofinbabu/PyARP) An ARP(Address Resolution Protocol) Spoofer based on ScaPy. ARP Spoofing or ARP cache poisoning is a technique by which an attacker can alter routing on a network, effectively allowing for a man-in-the-middle attack. This python program I wrote has the capabilities of scanning an IP range and performing the ARP attack.

Detection of malicious domain names using Machine Learning: Various families of malware use Domain Generating Algorithms (DGAs) to periodically generate a large number of domains names for malicious purposes. With one million top websites dataset from Alexa and about 10K DGA-domains generated with a couple of DGA's, I came up with a model that detect algorithmically generated domains. The Random forest classifier was used for the classification and evaluation gave an accuracy of 97.8%. The project made use of Scikit-learn for classification.

FilterPlus: A real-time content filtering extension for Google Chrome: Built an extension for Google Chrome which allows users to have easy control over what they wish to receive from a web page. Also build this extension in such a way that

it remembers the choice of options made by the user for every URLs, thereby letting users create rules for websites they visit.

Automatic TV Show Highlighting : Wrote a Python program which outputs an excerpt of TV shows consisting of the highlighted parts of it.The main idea behind this program is, usually when something interesting happens during the show, the audio levels increase (up to a short period of time)from it's normal pattern due to the combined response of (live)audience. I measured those differences and cut the video properly (with transitions) to form the excerpt. Libraries used for this project include (but was not limited to) MoviePy, ffmpeg and NumPy.

A SaaS Testing approach based on crowdsourcing(Research Project): In recent years the Software as a Service (SaaS) model of software flourished as organizations of different size and types are extremely interested in readily available business applications. Traditional SaaS testing methodologies in restricted environment is not sufficient to overcome SaaS challenges. In this research, I propose an efficient and cost effective SaaS testing approach using crowdsourcing followed by some techniques of effective management of crowd, based on a case study.

Spectral Analysis using IRAF: The optical spectra is obtained from Sloan Digital Sky Survey(sdss server dr7), a project make a large part of the universe. IRAF(image reduction and analysis facility) is a product of the National Optical Astronomy Observatories (NOAO) and was developed for the astronomical community. I took fresh spectral data of galaxy clusters from sdss, plotted and analyzed them using IRAF.

Updated on 1-21-2015
Contact me for more information.
My Linkedin profile: **https://in.linkedin.com/in/bofinbabu**