Christopher Tarquini

Marlton, NJ, United States
resume@tarq.io
https://tarq.io

Skilled system administrator and developer with experience with a diverse range of technologies and infrastructures. I pride myself on my dedication to learning how technologies work under the hood and applying this knowledge to ensure the security and stability of the platforms I create, maintain, and support.

Technical Skills

Likes: node.js c++ c mysql ansible linux perl

Experience

Professional Services Technical Lead – Linode *May 2016 → Current*
linux, mysql, galera, percona, nginx, apache, node.js, reactjs, ansible, coldfusion, perl

- Plan infrastructures for Clients based on their requirements and goals.
- Define standard configurations and technology stacks for our team to use in customer projects. Assist team with any blocking problems with projects.
- Create training materials and tools to help streamline our process
- Execute system administration projects for Clients
- Provide system administration for our On-Going System Administration Clients

Security Committee Member – Linode *Aug 2015 → Current*

- Evaluate bug/vulnerability reports
- Find and report potential vulnerabilities in our applications and infrastructure
- Work with the Development and Ops Teams to create and deploy patches

Implementation Specialist – Linode *Jul 2015 → May 2016*
linux, mysql, galera, high-availability, apache, node.js, ruby-on-rails, reactjs

- Plan infrastructures for Clients based on their requirements and goals.
- Execute system administration projects for Clients (deployments, investigations, optimization)

Lead Developer – Whitefire Media LLC *Jun 2012 → May 2013*
cakephp, node.js, rds, heroku, amazon-ec2

- Custom affiliate control panel written with CakePHP
- Found and reported security flaws in third party backend
- Administrated several Amazon EC2 instances
- Custom backend server to handle affiliate traffic with lower costs written in Node.JS

Projects & Interests

Stack Overflow – http://stackoverflow.com/users/148766/christopher-tarquini *2009/07 → Current*

Written 61 answers. Active in javascript, node.js, php and c#.

Slim Signals – https://github.com/ilsken/slimsig *Apr 2015 → Jul 2015*
c++11, c++

Faster signal library for written for C++11

Schematic – https://github.com/schematic *Aug 2013 → Jul 2015*
node.js

Type validation and casting for Javascript designed for both the frontend and backend. Meant to be the building blocks for an ORM

Javascript Private Name Polyfill – https://github.com/ilsken/name *Jul 2013 → Aug 2013*
javascript

Polyfill for the ES6 Private Name specification

DIP Dependency Injector – https://github.com/ilsken/dip *Jun 2013 → Aug 2013*
javascript, promise

Promise based dependency injection in Javascript

Public Artifacts

Root Privilege Escalation using Wordpress, W3TC and Nginx – https://blog.tarq.io/root-your-box-with-w3tc-and- *Mar 2017*
nginx/

Commonly suggested configuration allows an attacker to change the ownership of arbitrary files on server.

Galera Remote Command Execution Vulnerability – https://blog.tarq.io/cve-2016-5483-galera-remote-command- *Mar 2017*
execution-via-crafted-database-name/

Using an evil database name, an attacker can gain remote command execution on all nodes in the cluster with only `CREATE DATABASE` privileges.

Backdooring MySQL Backups – https://blog.tarq.io/cve-2016-5483-backdooring-mysqldump-backups/ *Mar 2017*

By crafting malicious table name, an attacker can execute arbitrary SQL queries and shell commands if the dump file is imported.

Insecure Defaults - Exploiting LOAD DATA LOCAL INFILE – https://blog.tarq.io/insecure-defaults-exploiting-load- *Oct 2016*
data-local-infile/

Using an evil server, arbitrary files can be stolen from MySQL clients and shipped off to an attacker

Node.js Request Smuggling – https://blog.tarq.io/node-js-request-smuggling/ *Sep 2016*

Relaxed security checks on in the Node HTTP Client allow an attacker to create arbitrary requests with a specially crafted path variable

Others

Identified and Reported Bug in MaxScale – Bug Reports *Jun 2016*

During the course of a Client deployment, I discovered a bug in the Read/Write Split Router for MaxScale. After looking through the source code, I was able to identify the source of the bug and report it to MariaDB

Tumblr Bug Bounties – Bug Bounty *May 2015*

Reported and collected 7 bug bounties from Tumblr via HackerOne.

Tools

First Computer:	Built from parts of computers people threw away
Favorite Editor:	Emacs in Evil Mode