Ankit Gaur

560037, IN

↗ https://www.linkedin.com/in/ankitgaur/ ✉ ankitgaur3@acm.org 📱 +91-9740465237

PROJECTS (15)

MSL 4: Low Latency Live Streaming January 2015- Current
https://www.akamai.com/us/en/products/media-delivery/media-services-live.jsp

Worked as SDET on various modules for the Akamai's new solution for Low Latency Streaming called MSL4. Handled features involving archiving of data, support for various media protocols (like DASH, HDS, HLS etc), and other system features.

MSL 4: Live to VOD January 2018- Current
https://learn.akamai.com/en-us/webhelp/media-services-live/media-services-live-ingest-users-guide-v4/GUID-4B33E5B0-2C73-4795-B49A-83E68CA540D7.html

The MSL4 Live-to-VoD feature enables customers to convert live streams to video-on-demand assets for HLS and DASH. I worked as SDET engineer for the core features which involved indexing the HLS and DASH playlists and saving it on interval key-value store. I wrote parsing utilities for these protocols (by utilizing open source libraries) as well as implemented a key-value store simulator using Python PickleDB library.

Automated Capacity Determination using Dynamic Load Control January 2018- June 2018

Developed a generic Python based framework to automatically discover the software capacity by adjusting the load on the machine (on basis of monitored metrics) given the limiting values for various parameters like CPU, RSS, request latency etc.

Pre-Submit Checks with Perforce and Jenkins August 2016- October 2016

Developed a Pre-checkin system (OATS) to test the code before being committed to the trunk branch. (something similar to Chrome CQ - https://dev.chromium.org/developers/testing/commit-queue/design) . Used Perforce shelve functionality, Jenkins pipeline, Jenkins Blue Ocean and Consul as key-value store. This also served as introduction to Jenkins 2.0 for the team, and I helped out in Jenkins 2.0 pipeline adoption.

CI Crash Reporting January 2016- January 2016

Added crash reporting functionality to the Jenkins based Continous Integration system which gives information about crashes happening in CI along with relevant information to help in debug and fix the issue. Developed this using linux kernel's 'core_pattern' functionality in combination with a data collector script.

GCOV/LCOV based code coverage for C++ Server software January 2015- Current

Generated and reported code coverage for C++ based software with lcov instrumentation and gcov frontend. Worked with Akamai's internal build system to instrument the binary and solved various challenges associated with proper instrumented compilation and reporting of coverage. Developed better understanding of linkers and loaders as part of this project.

SDET Owner for USS VOD Translator January 2015- Current
https://developer.akamai.com/legacy/learn/Content_Delivery/HD_On_Demand_Content.html

Took SDET ownership of USS VOD Translator product, a C++ based server, which supported content transmuxing (from and to Akamai HD Flash, Adobe HDS, and Apple HLS) format for Akamai's HTTP based Video On demand workflow. Supported product features like SSL support, captioning support for WebVTT and did capacity testing .

Continuous Integration Setup Co-Ownership January 2015- January 2018

Co-owned the Jenkins and Ansible based CI setup for the project, which involved adding new projects, enhancing the ansible playbooks etc. Developed understanding and skills in this area. Also helped in reducing the number of machines required for testing by merging two machine roles into one. Helped other teams in the org to ramp-up on advanced aspects of CI.

SSL support for VOD Translator server September 2014- November 2014
https://developer.akamai.com/legacy/learn/Content_Delivery/HD_On_Demand_Content.html

This was the first feature I worked on, in my role as SDET in Akamai's Media Division. I was involved in test planning and automation (in a Perl based framework) to enable secure end-to-end video delivery over HTTPS for Mid-Tier components. This involved interaction with KMI (Key Management Infrastructure) to obtain the certs and other secrets. I developed fine grained understanding of how automated key management infrastructure is run at the global scale. Technology: HTTPS, SSL, KMI, KDC

Protocol Robustness Testing using Codenomicon Fuzz Testing January 2011- March 2011
https://www.synopsys.com/software-integrity/security-testing/fuzz-testing.html

The Defensics Codenomicon tool provides automated solution to test the protocol implementation for robustness against malformed packets (like one which would trigger buffer overflow, format string, memory allocation issues). I took initiative to start protocol robustness testing on IronPort Web Security Appliance. Trained and engaged team on effort, Developed strategy and best practices for the tool usage. This helped us identify many of memory leaks and crashes.

Firewall NAT Functionality January 2011- January 2014

Qualified IPv6 support for Network Address Translation on Cisco Adaptive Security Appliance. Also worked on adding TCL based automation and qualifying the stabilization efforts for the functionality.

SaaS Access Control January 2010- March 2010
https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-0/user_guide/b_WSA_UserGuide/b_WSA_UserGuide_chapter_01010.html

SaaS Access control centralizes the management of access to multiple SaaS applications (like SalesForce, Webex, Google Apps) by integrating the the SaaS application authentication with the already existing authentication mechanism in organization (like NTML/LDAP etc). The Web Security appliance uses the Security Assertion Markup Language (SAML) to authorize access to SaaS applications. My role was as test engineer to create test plan, execute the test cases and qualify the feature.

Build Qualification Automation using Selenium IDE January 2009- June 2010

Maintained Python + Selenium IDE based build qualification suite to smoke test the build before taking up further testing. This helped us to discover any basic defects at the start itself, so as to not waste further efforts.

HTTP/HTTPS Proxy Authentication January 2009- January 2011

WSA supported NTLM and LDAP authentication to establish identity of the users going via the proxy. I acted as co-owner of the Authentication module from the QA side and qualified various features such as Per Identity Auth, Transparent HTTPS Authentication etc.

QA Qualification for Data Loss Prevention October 2008- December 2008
https://www.cisco.com/c/en/us/products/collateral/security/web-security-appliance/solution-overview-c22-738537.html

IronPort Data Security Filters provide administrator with visibility and control over data leaving the network via the web (HTTP/HTTPS) and FTP. This feature allows admin to create policies and take actions based on relevant parameters like the source (user), destination (URL categories and web reputation), and file metadata (file name, file type, and file size). I was involved in doing qa qualification for the feature.