Kai Ueno Junior Application Security Engineer

San Francisco, CA · kai.ueno@gmail.com · +1 415-555-0136 · linkedin.com/in/kaiueno

PROFILE SUMMARY

- **Junior Application Security Engineer** with **3 years** in QA and AppSec, now on the product security team of a **bug bounty platform**, triaging **scanner findings** and bounty reports against the company's own **Rails and React** apps.
- Works daily in **Ruby** and **TypeScript** code, scans with **Semgrep** and Snyk, tests with **Burp Suite Professional**, and writes **Python** scripts that pull new reports into Jira with the right owner and severity.
- Building depth in **GraphQL authorization testing**, **IDOR and SSRF triage** and **CVSS scoring**, and checks every fix against OWASP ASVS Level 1 before a ticket gets closed.
- Works with **product engineers**, the **platform team** and senior AppSec engineers, joins the weekly triage review and STRIDE sessions, and writes fix notes a developer can act on without a meeting.
- Keeps the team's **Semgrep rule notes** and **ZAP onboarding runbook** current, answers questions in the engineering security channel, holds **CompTIA Security+**, and is studying for **BSCP**.

TECHNICAL SKILLS

Languages & Frameworks:	Ruby on Rails, TypeScript, React, GraphQL, Python (scripting)
SAST & Code Scanning:	Semgrep, GitHub code scanning, Brakeman, Gitleaks
DAST & Pentest Tools:	Burp Suite Professional, OWASP ZAP, Postman
SCA & Supply Chain:	Snyk Open Source, Dependabot, npm audit
Threat Modeling & Standards:	OWASP Top 10, OWASP ASVS (Level 1), STRIDE (basics), CVSS 3.1
Auth, API & Crypto:	OAuth 2.0, JWT, GraphQL field authorization, session handling
CI/CD, Cloud & Bug Bounty:	GitHub Actions, Docker, HackerOne, Jira

EDUCATION

San José State University — **B.S. in Software Engineering** — San Jose, CA · Aug 2019 to May 2023

CompTIA — **Security+ certification** — San Francisco, CA · Mar 2024

WORK EXPERIENCE

HackerOne — **Junior Application Security Engineer** — San Francisco, CA · Oct 2024 to Present

- Triaged **310+ reports** on HackerOne's own bug bounty program, reproducing each one, scoring it with **CVSS 3.1** and routing valid bugs to the owning team in Jira.
- Wrote **18 Semgrep rules** for Rails patterns the default rulesets missed, like unscoped record lookups and open redirects, and added them to the **GitHub Actions** checks on the main app.
- Reviewed pull requests that changed **GraphQL** resolvers or permission checks, catching **9 authorization bugs** before release, including one that showed private report titles to other programs.
- Wrote up the threats from **11 STRIDE sessions** on new features, then tracked each agreed design change in Jira until the owning team shipped it.
- Cleared a backlog of **Dependabot** and Snyk alerts on the React front end by batching upgrades per package, taking open critical dependency alerts from 23 to **2**.

Lever — **QA Engineer (Security focus)** — San Francisco, CA · Jun 2023 to Sep 2024

- Built **Cypress** tests for role-based access and session timeouts on the recruiting app, catching **3 permission regressions** before they reached customers.
- Tested login, SSO and password reset flows on release branches with **Burp Suite**, filing **7 security bugs**, including an account enumeration issue the AppSec team fixed that week.
- Ran a monthly lunch session on common **OWASP Top 10** bugs for **20+ testers**, then moved into AppSec after earning Security+.