# Application Security Engineer

**Hiring organization**
Vimeo

**Job Location**
Bengaluru, Karnataka, India

**Base Salary**
$ 65000 - $ 125000

**Date posted**
June 16, 2024

Apply Now

## Description

As a Sr. Application Security Engineer at Vimeo, you will engage in a variety of activities, either offensive, defensive, or some combination thereof, ultimately aimed at safeguarding our users who entrust Vimeo with their content every day. Youâ??ll plan, carry out, and lead security initiatives to monitor and protect sensitive data and systems from infiltration and cyber-attacks. You will likely collaborate frequently with and support developers, as well as members of the infrastructure security team, the compliance team, IT, Product, and other teams throughout the organization. You love to solve puzzles and are a great team player. This role is remote. What youâ??ll do: Depending on your preferences and the current needs of the team, you may either focus on just one or two of the following areas, or you may choose to become involved with many of them. Penetration testing â?? either hunt for security issues on our production or staged applications during an open-box internal pen test or help coordinate an engagement with an external firm Writing code for internal automated security tools â?? write some code, usually in Python, Bash, or Go, to support any of our team's various initiatives. Often, we strive to facilitate a culture of â??paved roadsâ?? for our developers, such that it is easy for any developer to incorporate security into their designs and implementations Threat modeling â?? consider how malicious attackers may compromise our systems, and advise developers and product managers on what defenses are needed Code reviews â?? discover weaknesses in our source code before it reaches production Bug bounty program â?? help triage new incoming reports on a daily basis, plus launch creative initiatives to increase researcher engagement in our programs Web Application Firewall and Rate Limiting â?? expand coverage and tune new rules while coordinating with developers, support team members, and the site reliability team Remediation â?? enable and encourage developers to correctly fix recently discovered security issues in a timely manner, ultimately reducing our Mean Time To Remediate Secure Software Development Lifecycle â?? configure automated tooling (eg. static and dynamic code analysis, IAST) in our SDLC to detect security issues in our source code before it reaches production Developer Education, Security Culture â?? create fun ways to spread technical security awareness throughout the engineering department Incident response â?? lead or assist in running the various phases of incident response, including initial detection, triage, containment, recovery, root cause analysis, retrospective, etc. Collaboration with the infrastructure security team â?? pair with members of the infrastructure security team on various projects to secure our cloud instances and employee workstations Collaboration with the compliance and privacy team â?? help ensure that our company complies with industry best practices and standards Process improvements â?? help strengthen our own internal processes and procedures A typical day will look like: Engage with one or more product development teams and guide them through a threat model and data flow analysis. Review the code for major new functionality to ensure security best practices are followed. Review new tickets in our bug bounty program (http://hackerone.com/vimeo) and use your system design and threat modeling knowledge to reproduce, define risk and mitigating controls and propose a fix. A call or two with Development, Product Management teams to discuss security-related issues Pen test a new feature in a staging environment with Burp Pro Assist the compliance team on a privacy-related project Provide technical advice in response to occasional questions from developers and other members of the security team Skills and knowledge you should possess: Required: 4+ years of prior experience in either software development, devops, or site reliability engineering with hands-on coding experience. Preferred: prior experience in Application Security 6+ total years of relevant experience in Engineering, Application Security,

or a similar technical field. Strong knowledge of modern web, mobile, and network security Strong programming skills with at least one of the following languages, and the ability to read all of them: Python, Go, PHP, Javascript, and Ruby Expertise with application pen testing, using tools like Burp or Zap Confident working in and across cloud environments like AWS and GCP. Detailed knowledge of at least one cloud environment. Confident with shell scripting Confident with common SDLC components, like git, Jira, Jenkins, etc Confident ability to communicate technical security concepts to developers At least an upper-intermediate level of English Bonus points (nice skills to have, but not needed): Link to a Github repo with security tools/scripts youâ??ve developed or help maintain Full-stack web development experience creating RESTful applications (in any language) is a big plus Open-source vulnerability research or blog posts is a big plus Experience with system security hardening guidelines and SDLC principles Please mention the word **WARM** and tag RMjYwMDoxOTAwOjIwMDA6OTI6OjE6ODAw when applying to show you read the job post completely (#RMjYwMDoxOTAwOjIwMDA6OTI6OjE6ODAw). This is a beta feature to avoid spam applicants. Companies can search these words to find applicants that read this and see they’re human.

**Contacts**
Job listing via RemoteOK.com