Application Security Engineer

Description

- ### 🔲🔲 Why This Role is Exciting

  Help build security-first products that protect cloud infrastructure used by millions. As an Application Security Engineer at Salesforce, you'll be embedded with engineering teams to prevent vulnerabilities before they're shipped. You'll influence secure development practices, perform risk assessments, and make sure the apps you touch are locked down — while still being scalable, usable, and high performing.

  ### 🔲🔲 At a Glance

  Detail
  Info

  Estimated Salary Range
  Example: $130,000 – $200,000 / year (varies by location & seniority)

  Location
  San Francisco, CA / Remote options / Hybrid – depending on product & team

  Key Tools & Technologies
  SAST, DAST, Code Review tools, API security, Web application security, TLS/SSL, secure authentication (OAuth, SAML)

  What You'll Bring
  Strong coding skills, secure SDLC experience, vulnerability remediation, threat modeling experience, collaboration with dev teams

  Certifications That Help
  CSSLP, OWASP, Certified Application Security Engineer (CASE), CISSP, etc.

  ### 🔲🔲 Official Description (Salesforce)

  (Paste the current official Application Security Engineer job description here from Salesforce's site.)

  ### 🔲🔲 Your Role & Responsibilities

  - Perform security design and code reviews of applications and APIs.

  - Conduct vulnerability assessments and help with remediation plans.

  - Integrate security into the SDLC – catch gaps early.

  - Work closely with developers to ensure secure coding practices.

  - Do threat modeling and risk assessments for new features/products.

Employment Type
Full-time

Employment Type
Full-time

Hiring organization
Salesforce

Job Location
Remote work from: USA

Base Salary
$ 130,000 - $ 200,000

- Use or build tooling to automate security checks where possible.

- Stay current on web-application threats (e.g., OWASP Top 10, CWE) and raise awareness.

- Assist in incident investigations involving application-level issues, when necessary.

🔲🔲 Skills & Experience You Need

- Several years of experience in application security, secure coding, or related engineering roles.

- Strong knowledge of web apps, APIs, authentication/authorization, and encryption.

- Hands-on with security tools (SAST / DAST / code-scanning / dynamic analysis).

- Comfortable reading and reviewing source code in one or more languages (e.g. Java, Python, JavaScript, etc.).

- Ability to model threats and assess risk.

- Good communication skills: explain security issues to technical and non-technical people.

- Bonus: cloud security experience, container security, secure deployment pipelines.

🔲🔲 Why Salesforce?

- Work on large scale cloud systems you use every day.

- Collaborate with top engineers in security, dev and product.

- Strong culture of innovation + security baked in.

- Opportunities for growth, learning, tools development, and impact.

🔲 Think You're a Fit? Next Steps

- Make sure your resume shows relevant examples: secure code reviews, threat modeling, vulnerability remediation.

- Be ready to talk through real vulnerabilities you've found and how you handled them.

- Apply via Salesforce's careers page or via this listing on DamnJobs.

- If you like, also check out related roles like **Product Security Engineer**, **Security Architect (Applications)**, or **DevSecOps Engineer** in Salesforce.