**Web Application Security**

### **Professional Summary**

* Web Application Security professional with 8+ years of experience designing, implementing, and managing enterprise-grade security solutions for web applications across multiple clients.
* Expertise in application vulnerability assessments, penetration testing, secure coding practices, and threat modeling to safeguard critical business applications.
* Designed and implemented runtime protection and threat detection systems for high-traffic enterprise applications, leveraging modern cloud-native architectures.
* Architected and deployed secure CI/CD pipelines with integrated security scanning for Java, .NET, Node.js, and Python applications.
* Developed automated security monitoring and alerting frameworks using SIEM tools and log orchestration to detect anomalies in real time.
* Integrated security-as-code principles into DevOps workflows, reducing manual intervention and improving compliance alignment.
* Migrated legacy web applications to cloud environments (AWS, Azure) while embedding security best practices in authentication, authorization, and data protection layers.
* Built security dashboards and reports to provide visibility into application risk posture for executive and development teams.
* Implemented threat modeling and attack surface analysis to guide secure architecture and application lifecycle decisions.
* Conducted in-depth vulnerability scanning using OWASP ZAP, Burp Suite, and Nessus to identify and remediate security gaps.
* Optimized web application security protocols including TLS/SSL configuration, CSP, HSTS, and secure cookie management.
* Integrated automated SAST/DAST tools into Agile and DevOps processes, ensuring early detection of vulnerabilities.
* Led cross-functional workshops on secure coding and application security standards for development and QA teams.
* Collaborated with cloud architects to enforce IAM policies, encryption strategies, and network segmentation for web applications.
* Provided enterprise guidance on regulatory compliance (PCI-DSS, HIPAA, GDPR) impacting web application security practices.

## **Technical Skills**

| **Category** | **Key Technologies & Expertise** |
| --- | --- |
| **Security Engineering** | DevSecOps, SAST/DAST Integration, Threat Modeling, Penetration Testing, RASP Implementation, Secure CI/CD Pipelines |
| **Cloud & Infrastructure** | AWS (WAF, KMS, IAM), Azure (AD, RBAC), Kubernetes, Docker, Terraform (Security-as-Code) |
| **Tools & Platforms** | Burp Suite, OWASP ZAP, Nessus, Splunk, ELK Stack, GitHub Actions, Jenkins, Trivy, Clair |
| **Web & App Stacks** | Java (Spring Boot), .NET Core, Node.js, React/Angular, PostgreSQL, SQL Server |
| **Protocols & Hardening** | OAuth 2.0, JWT, MFA, TLS 1.3, CSP, HSTS, WAF Rule Customization |
| **Compliance & Governance** | PCI-DSS, HIPAA, GDPR, Security Policy Development, Incident Response |

### **Professional Experience**

#### **Client:**

#### **Web Application Security**

#### **Environment:** AWS, Java, Spring Boot, Angular, PostgreSQL, Terraform, Jenkins, Docker, Kubernetes, Burp Suite, OWASP ZAP, Splunk, GitHub Actions, Agile, DevSecOps

**Responsibilities:**

* Led the design and deployment of a cloud-native web application security architecture for enterprise-scale applications.
* Implemented automated SAST/DAST scans in CI/CD pipelines, integrating Burp Suite Enterprise and OWASP ZAP into GitHub Actions workflows.
* Developed runtime application self-protection (RASP) mechanisms to detect and mitigate SQL injection, XSS, and CSRF attacks in real-time.
* Designed and implemented secure authentication mechanisms using OAuth 2.0, JWT, and multi-factor authentication for web applications.
* Conducted comprehensive threat modeling and attack surface analysis to guide secure architecture decisions across microservices.
* Deployed Web Application Firewalls (AWS WAF) with custom rules to mitigate advanced application layer attacks.
* Automated vulnerability reporting and remediation dashboards using Splunk and custom Python scripts, providing executive-level visibility.
* Integrated DevSecOps practices into Agile pipelines to embed security checks at every stage of development.
* Orchestrated container security scanning using Trivy and Clair for Docker and Kubernetes environments.
* Developed encryption strategies for sensitive data at rest and in transit using AWS KMS and TLS 1.3.
* Implemented CSP, HSTS, and secure cookie policies to harden front-end applications.
* Collaborated with cross-functional teams to remediate vulnerabilities discovered during penetration testing cycles.
* Developed and delivered secure coding guidelines, workshops, and training sessions for developers and QA teams.
* Monitored security incidents and performed root-cause analysis for recurring application vulnerabilities.

#### **Client:**

#### **Senior Web Application Security Engineer**

#### **Environment:** Azure, .NET Core, React, SQL Server, Jenkins, Terraform, Docker, Kubernetes, OWASP ZAP, Qualys, Splunk, Agile, DevSecOps

**Responsibilities:**

* Architected secure cloud web application frameworks, implementing identity management via Azure AD and RBAC policies.
* Conducted in-depth vulnerability assessments and penetration tests on enterprise applications to ensure regulatory compliance.
* Built automated pipelines for SAST/DAST security scans integrated with Jenkins and Terraform deployments.
* Designed multi-layered web application defenses, including WAF, API security policies, and intrusion detection alerts.
* Implemented data encryption strategies across databases and APIs to protect sensitive information.
* Developed dashboards for real-time monitoring of application security events, integrating Splunk and custom ETL pipelines.
* Migrated legacy applications to containerized microservices while ensuring security controls in Kubernetes clusters.
* Led incident response simulations and developed playbooks for web application threats and breaches.
* Automated compliance reporting using integrated security monitoring tools.
* Implemented tokenization and key management practices for sensitive data exchanges.
* Integrated secure coding and application security requirements into Agile user stories and acceptance criteria.
* Coordinated vulnerability remediation efforts with development and operations teams to ensure timely fixes.
* Conducted security reviews of third-party libraries and APIs to prevent supply chain risks.
* Developed custom scripts to detect anomalous user behaviors and potential web attacks in real time.

#### **Client:**

#### **Web Security Engineer**

#### **Environment:** AWS, Node.js, React, MySQL, Jenkins, Docker, Kubernetes, Burp Suite, Nessus, ELK Stack, Agile, DevOps

**Responsibilities:**

* Designed and implemented security controls for web applications to protect sensitive customer and internal data.
* Conducted penetration tests and automated scans using Burp Suite and Nessus to identify vulnerabilities.
* Developed security automation scripts in Python to streamline vulnerability detection and reporting.
* Integrated CI/CD pipelines with automated security testing for Node.js microservices deployed in AWS and Kubernetes.
* Configured AWS WAF and security groups to protect web applications from OWASP Top 10 attacks.
* Implemented secure authentication and authorization frameworks using OAuth 2.0 and JWT tokens.
* Conducted threat modeling sessions to guide secure architecture decisions and risk mitigation strategies.
* Developed monitoring dashboards using ELK Stack to track security incidents and anomalous behaviors.
* Automated remediation workflows for vulnerabilities discovered during security scans.
* Collaborated with DevOps teams to ensure container security and image scanning using Trivy.
* Delivered developer workshops on secure coding practices, including XSS, CSRF, and injection prevention.
* Implemented logging and alerting for real-time detection of security incidents.
* Reviewed third-party libraries for vulnerabilities and coordinated safe upgrades across applications.
* Integrated secure API gateways and SSL/TLS configurations to protect client-server communications.

#### **Client:**

#### **Web Application Security Analyst**

#### **Environment:** On-premises and AWS hybrid, Java, Spring MVC, AngularJS, Oracle DB, Jenkins, Docker, Burp Suite, OWASP ZAP, ITIL, Agile

**Responsibilities:**

* Conducted full lifecycle web application security assessments for enterprise applications.
* Designed and implemented security standards, policies, and best practices for development teams.
* Executed penetration testing and vulnerability scans using Burp Suite and OWASP ZAP to identify application flaws.
* Implemented access control and authentication mechanisms to secure web applications.
* Developed security dashboards for incident tracking and regulatory reporting purposes.
* Collaborated with developers to remediate vulnerabilities in legacy Java and AngularJS applications.
* Integrated static and dynamic security testing into Jenkins pipelines to automate security validation.
* Developed encryption and tokenization strategies for sensitive data.
* Conducted secure code reviews to ensure adherence to enterprise security standards and OWASP guidelines.
* Implemented monitoring and alerting systems to detect unauthorized access and anomalous activity.
* Provided consulting for migration projects from on-premises to AWS cloud infrastructure.
* Developed training materials and conducted workshops to raise developer awareness of application security threats.
* Worked with QA teams to implement security-focused test cases for regression and functional testing.
* Created detailed documentation of security incidents, mitigation strategies, and compliance measures.