



- 📞 (555) 234-5678
- ✉ michael.anderson@email.com
- 📍 San Francisco, CA
- 🌐 www.michaelanderson.com

## SKILLS

- Web Application Security
- Penetration Testing
- SQL Injection
- Security Assessment
- Burp Suite
- Secure Coding
- Threat Analysis
- Vulnerability Management

## EDUCATION

**BACHELOR OF SCIENCE IN INFORMATION SECURITY, STATE UNIVERSITY**

## LANGUAGE

- English
- Spanish
- German

## ACHIEVEMENTS

- Contributed to a 15% reduction in vulnerabilities across client web applications.
- Received commendation for excellence in performance during internship.
- Developed a security awareness program that was adopted by the organization.

# Michael Anderson

## WEB APPLICATION PENETRATION TESTER

Motivated Penetration Tester with 3 years of experience specializing in web application security assessments. I am adept at identifying vulnerabilities in web applications using a variety of testing methodologies and tools. My background includes hands-on experience with SQL injection, cross-site scripting, and session management vulnerabilities. I have collaborated with development teams to ensure that security practices are integrated throughout the software development lifecycle.

## EXPERIENCE

### WEB APPLICATION PENETRATION TESTER

SecureWeb Inc.  
2016 - Present

- Conducted penetration tests on web applications, identifying vulnerabilities such as SQL injection.
- Worked closely with development teams to implement security fixes.
- Utilized automated tools to streamline testing processes, improving efficiency by 20%.
- Developed comprehensive reports detailing vulnerabilities and recommendations.
- Engaged in continuous learning to stay updated with the latest web security trends.
- Participated in security awareness training for non-technical staff.

### SECURITY INTERN

TechSecure Solutions  
2014 - 2016

- Assisted in security assessments for various web applications.
- Learned about common vulnerabilities and mitigation techniques.
- Documented findings and assisted in preparing reports for stakeholders.
- Participated in team meetings to discuss security strategies.
- Gained hands-on experience with tools such as Burp Suite.
- Supported the development of security training materials.