Oleh Olekshii

Application Security Analyst
oooleks@gmail.com
(408) 796-9122

PERSONAL PROFILE

A highly accomplished Security Tester with extensive experience in complete Software Development Life Cycle including requirements gathering, design, development, testing and implementation.

PROFESSIONAL SUMMARY

- 7+ years of IT experience in Information Security, Application Security, Mobile Security and SQA.
- Expertise in performing Application Security Risk assessments throughout SDLC.
- Excellent knowledge in OWASP Top 10 Vulnerabilities and CWE Threat Classification methodologies.
- Extensive experience in Vulnerability Assessment and Penetration Testing on Web and Mobile based Applications and Infrastructure using various tools like Burp Suite Pro, Acunetix, Metasploit, SQLmap, OWASP ZAP Proxy, Nessus, Nmap, etc.
- Expertise in identifying flaws like SQL Injection, Insecure Direct Object Reference, Security Misconfiguration, Sensitive Data Exposure, Cross Site Scripting (XSS), CSRF, Path Traversal and Unvalidated Redirects.
- Extensive experience in performing SAST (Static Application Security Testing/White-Box Testing), DAST (Dynamic Application Security Testing/Black-Box Testing), IAST (Interactive Application Security Testing) and SCA (Software Composition Analysis).
- Expertise in managing security programs comprising different security domains and teams.
- Ability to exploit recognized vulnerabilities and report the issues in the industry standard framework.
- Proficiency in SQL, Java, Python, Shell Scripting and HTML.
- Working knowledge of test automation (Selenium + Java) and build integration tools (maven, Jenkins).
- Able to work on own initiative or as part of a team, backed by excellent communication skills along with the capability to solve problems efficiently.
- Good team player and ability to learn the concepts effectively and efficiently.
- Diversified domain experience in Manufacturing, Banking, and Financial Services.

EDUCATION

- **BS, Economics and Finance**, Chernivtsi State University, Ukraine

TECHNICAL SKILLS

Vulnerability Testing	Tenable Nessus, Contrast Security, Nmap
Application Security	Burp Suite Pro, Contrast Security, Security AppScan, Acunetix, Fortify WebInspect, SQLmap, Metasploit, Kali Linux, Wireshark, Black Duck, Coverity
Methodologies	OWASP Top 10, CWE
Databases	Oracle, MS SQL Server
Query Tools	SQL Developer, SQL Server Management Studio
Languages	SQL, Java, Python, HTML, XML and Shell Scripting
Source Control	Azure DevOps Server (TFVC, Git), SVN and GitHub
Platforms	macOS, Linux, Windows, iOS, Android

EMPLOYMENT

State Compensation Insurance Fund, Pleasanton, CA
Application Security Testing Engineer **October 2015 – Present**

State Fund is California's provider of workers' compensation insurance and offers comprehensive products and services that provide a strong option for employers and injured employees with fast claims service and medical and indemnity benefits.

Responsibilities:

Web Application Vulnerabilities Assessment and Penetration Testing following the guidelines of OWASP to uncover security vulnerabilities in the internally developed and vendor's software products:

- Involved in Planning, Scheduling, Tracking, and Reporting on Manual/Automated Security testing on Internet and Intranet Applications.
- Performing penetration tests in the area of Cross-site scripting, Broken authentication and session Management, SQL injection, Cross site request forgery, Sensitive Data Exposure, Insecure Direct Object References etc.
- Running static and dynamic security scans with various security testing tools.
- Capturing Critical, High, Medium and Low vulnerabilities in the applications based on OWASP Top 10 and prioritized them based on the criticality.
- Inspecting security vulnerabilities associated with open-source and 3rd-party functional libraries.
- Developing a list of security test cases for each phase of application development.
- Providing the development team with detailed reports based on the findings obtained from manual and automated testing methodologies and remediation for individual findings.
- Handled baseline configurations, vulnerability exceptions and compliance exceptions.
- Running training programs to assist internal development personnel.

Environment: OWASP Top 10, Burp Suite Pro (DAST), Kali Linux, Contrast Security (IAST), Synopsys Coverity (SAST), HCL Security AppScan, Nmap, Tenable Nessus, OWASP Zed Attack Proxy.

RFSpot Inc, Los Altos, CA
Application Security Analyst **May 2015 – August 2015**

Cloud based indoor map, location, navigation and search – robotic solutions for Geo-spatial mapping of large facilities, real-time data capture and analysis, enhanced logistics for in store retail operations, and mobile customer experience enhancement.

Responsibilities:

- Performed security assessments to ensure compliance to firm's security standards (i.e., OWASP Top 10, SANS25). Specifically, security testing has been performed to identify Cross-Site Scripting, ClickJacking, Session Management/Hijacking, and SQL Injection related attacks within the code.
- Performed Dynamic Application Security Testing using tools such as Burp Suite Pro, OWASP ZAP.
- Analyzed network protocols using Wireshark tool by scanning network to capture its data.
- Executed security test cases.
- Wrote and used SQL queries for querying the MySQL database in UNIX environment to test the application for data integrity and verified the contents of the data table.
- Generated executive audit summary reports showing the security assessments results, recommendations and risk mitigation plans for senior management.
- Tested software and hardware of autonomous robotic, always connected product for mapping, navigation (SLAM – Simultaneous Localization and Mapping) and machine vision with GIS and Cloud (AWS) services.
- Developed Test Plans, Test cases, Test procedures for the Application.
- Automated test cases using Selenium WebDriver with Python.
- Played an active role in weekly meetings to improve the testing efforts.

Moka5, Redwood City, CA
Software QA Engineer **January 2014 – April 2015**

Moka5's core product is an enterprise solution that provides a secure corporate workspace to end-users – anytime, anywhere, on any device whether it is corporate or personally owned. SDLC is based on Agile methodology.

Responsibilities:

- Performed penetration tests of host security assessment feature by attacking software using malware to test security weaknesses, potentially gaining access to the data.
- Evaluated security of the tested system by manually auditing with vulnerability scans, reviewing application access controls with different sets of policies.
- Tested Virtual Desktop solution which works on top of VMware Hypervisor - client-server virtual container for Mac OS X, MS Windows platforms and bare metal hypervisor based on Linux. All types of testing of the complex virtual desktop management product.
- Took part in security infrastructure upgrades (e.g., firewall/VPN upgrades, intrusion detection, token-based authentication and remote management) for the company.
- Developed test documentation: Test plans, new feature specifications and test cases based on technical specifications and business requirements.
- Built robust QA lab and end-to-end tests simulating real customer environment to test application performance on different hardware setups, VoIP performance, network connectivity, security, software and hardware compatibility.
- Led QA efforts in mobile (iOS and Android) FileBrowser native app testing processes (manual and automation functional, UI testing using Appium (Java, Python)).
- Tested web-based console – Management Server. Performed Moka5 Desktop Administrator role to perform day-to-day operations, such as releasing and targeting images, managing users and OUs, changing policies, viewing reports and adjusting configurations.
- Identified, prioritized and submitted the bug reports and verified bug fixes in bug tracking system; triaging of existing reports for documenting known issues and providing workarounds.
- Actively participated in daily team meetings to discuss testing process and current issues.