Subhoj Kumar

**Email:** [**subhojkumar1@gmail.com**](mailto:subhojkumar1@gmail.com)

**Contact:201-885-0190**

**Professional Summary:**

* Over 5 years of Experience as an Application Security Analyst, involved in **OWASP Top 10 based Vulnerability Assessment** of various internet facing point of sale web applications and Web services.
* Skilled in identifying the business requirements for information security as well as regulations of information security.
* Extensive experience in Application Security testing - Expertise in detecting various vulnerabilities (including OWASP top 10) comprised over **authentication, authorization, input validation, session management, server configuration, cryptography, information leakage** areas.
* Experience on vulnerability assessment and penetration testing using various tools **like Burp Suite, OWASP ZAP Proxy, NMap, Nessus, Kali Linux, Metasploit, Microfocus Fortify on Demand, IBM AppScan, Visual Code Grepper.**
* Developed, implemented and enforced security policies through experience, in-depth knowledge of security software, and asking customer the right questions.
* An enthusiastic team player who embodies a strong work ethic and a leader who utilizes complex problem solving skills for incident analysis.
* Basic Understanding of Programming languages like Java, Python, C# and SQL.
* Excellent communication, analytical, troubleshooting, customer service and problem solving skills; excel in mission-critical environments requiring advanced decision-making.
* Experience in automation tools development for **penetration testing.**

**Technical Skills:**

|  |  |
| --- | --- |
| **Tools:** | IBM AppScan Standard Edition, HP Web Inspect, Parosproxy, Wireshark, Metasploit, Burp Suite, SQLmap, OWASP ZAP Proxy, Microfocus Fortify on Demand, DIR-Buster, Acunetix Web Scanner, SQL Injection Tools, CSRFTester AND Kali Linux, Webgoat SSL implementation, RSA implementation, PKI (Public key infrastructure) Encryption algorithms |
| **Platforms:** | Windows 98/2000/XP/Vista/Windows 7,10 Windows Server 2000/2003/2008, Linux |
| **Virtual Machines** | VMWARE Workstation, VM Virtual box |
| **Database** | My SQL 5.0 |
| **Packages:** | MSOffice |
| **Network Tools:** | NMap, Wire Shark, Nessus, QualysGuard |
| **Programming Languages** | Java, Python, C#, SQL |
| **Front End Technologies** | HTML, CSS, Javascript |
| **IDE** | Visual Studio, Eclipse oxygen |

**Education:**

* NYIT, NY, USA | Masters in Computer Science.

**Certification:**

* **CEH** - Certified Ethical Hacker

**Professional Experience:**

**Client: LA County Probation Department, Los Angeles, CA Feb 2019 - Till Date**

**Role: Application Security Analyst**

Los Angeles County Probation department is the largest probation services agency in the United States. Has around 50 fully staffed facilities that serves around 80,000 people in probation. Endeavors to build a foundation of trust with community groups, stakeholders and agencies in order to carry out the mission of this department of ongoing public safety initiatives for juvenile and adult probation services in the county.

**Responsibilities:**

* Expertise in identifying OWASP top 10 and SANS 25 vulnerabilities.
* Performing manual penetration testing to exploit and mitigate security threats such as XSS, CSRF, SQL Injection, Buffer Overflows and DOS Attacks etc
* Communicating with client/customer after identifying vulnerabilities in order to imply appropriate mitigations.
* Assessing and risk classification of identified vulnerabilities based on the security impact, likelihood and business risks.
* Determining the scope of Security testing for Web Applications.
* Collaborating with development team to remediate the vulnerabilities identified in web or mobile based applications.
* Performing Dynamic Application Security Testing using Burp Suite professional and generated reports with mitigation plans.
* Working with Risk group to ensure security risks are properly aligned with business
* Developing and implementing best security standards, and researched on latest security trends
* Understand security requirements: areas of the application which deal with PII information in consultation with the business user/client and baseline the requirements
* Preparation of Test Setup, Security Test Area Coverage definition, Test Plan and Test Cases for new features/implementation
* Periodically review and update overall security strategy for the modernization program
* Involved in training the development team on the most common vulnerabilities and common code review issues and explaining the remediation.
* Understand network protocols TCP/IP, SSH, SSL HTTP and HTTPS.

**Client: Sutter Health, Rancho Cordova, CA March 16 – Dec 18**

**Role: Application Security Engineer**

Sutter Health is a health care provider for more than 3 million Californians. It’s integrated network

invests heavily in research programs to advance its patients care.

**Responsibilities:**

* Performed validation and verification. Recommend process improvements.
* Assisting client in understanding risk and threat level associated with vulnerability so that customer may or may not accept risk with respect to business criticality
* Assisting in review of business solution architectures from security point of view which helps avoiding security related issues/threats at the early stage of project.
* Assisted team Lead with day to day issues and finding way to mitigate high scale vulnerabilities.
* Manually validating vulnerability findings by identifying false positives.
* Developed and managed vulnerability assessments including development of risk mitigation strategies.
* Responsible for identifying gaps in the tool capability and providing solutions to address the gaps.
* Manually mapped the web applications for full coverage during a dynamic scan.
* Implemented automated DAST solutions by deriving the information from QA tests.
* Worked with Agile teams to streamline the security related activities and prioritize security activities for business-critical applications.
* Generated scan reports prioritizing the Critical, High and Medium alerts and distributed to Development and Executive team members
* Documented information security guidance in step by step operational procedures.
* Performed static code reviews with the help of automation tools.
* Conducted vulnerability assessment of internal/external facing web application using automated tools such as Fortify on Demand and Burp Suite Professional.

**Client: Jefferies Group LLC, NYC, NY Jan 15 – Feb 16**

**Role: Security Engineer**

Jefferies Group is an Independent investment bank and financial services company in NYC. It provides clients with capital markets, financial advisory services, securities research and asset management.

**Responsibilities:**

* Analyze, log, track and complex software and hardware matters of significance pertaining **to network connectivity issues, printer, server, and application** to meet business needs.
* Handled the tasks of designing and planning LAN network expansion of the organization.
* Responsible for upgrading and configuring Microsoft Window servers.
* Worked on Password Recovery and troubleshooting network issues.
* Installed **network routers, firewall and cabling**.
* Responsible for **preparing, loading, documenting and testing desktop** and network developed applications for deployment.
* Managed computer/user accounts in Active Directory.
* Supported users in multiple branches with computer, network and desktop application software.
* Assisted in user login and connectivity issues.