RAJA HAYAT [raja.hayat@hotmail.com](mailto:raja.hayat@hotmail.com)

**SUMMARY OF QUALIFICATIONS**

* Application Security Specialist for the Library of Congress in Washington, DC
* Information Security Specialist for the Citigroup (Multinational Investment Banking & Financial Services)
* SAST Analyst for Citibank (Secure Coding / Code Review)
* Security Analyst for the largest U.S. health insurance company (UnitedHealth Group)
* Penetration Tester for General Service Administration
* Systems Security Engineer for The University of Pittsburgh Medical Center
* Application Security Specialist for Saint Jude Medical
* Security Analyst for the U.S. Marine Corps Headquarters Network Operations and Security Center
* Bachelor’s degree in Information Systems Management with a concentration in information security
* Certified Information Systems Security Professional (CISSP) - ISC² (IAM Level III)
* Certified Ethical Hacker (CEH) - EC-Council member (DOD CNDSP Auditor)
* Web Application Penetration Tester (GWAPT) - Global Information Assurance Certification (GIAC)
* OWASP DevOps Training - The Open Web Application Security Project
* BLACK HAT Certification: The Web Application Hacker’s Handbook Live Edition
* SANS SEC542: Web Application Penetration Testing and Ethical Hacking
* Project Management for IT Professionals certificate, University of Maryland University College
* CompTIA Security+ & CompTIA Network+ (DOD 8570.01-M IA Security Engineer IAT)
* Customer focus and leadership experience in working with diverse and multicultural personnel.
* Expert in time management, multi-tasking, and prioritization under pressure in fast paced environments.
* Recognized for team building, motivating others, problem solving and goal oriented initiatives.

**PROFESSIONAL EXPERIENCE**

**Tools proficiency:** Burp Suite, HP fortify SCA / SSC, HP WebInspect, IBM Security AppScan, Whitehat, Nessus & Nexpose, Metasploit Framework/Pro, SQLMap, BeEF, BackTrack/ Kali Linux, Saint, Paros, Acunetix, ZAP, Nmap, Wireshark, Core Security Core Impact, Nikto, W3af, Brutus, Cain & Able, Social Engineering Toolkit, Putty/ SSH, Eclipse, otool, iAuditor and Androwarn for Android, iOS Snoop-it and iNalyzer Framework. SIEM (Splunk, Nitro and HP ArcSight), McAfee ePolicy Orchestrator (McAfee ePO), IDS/IPS - intrusion detection/prevention technologies (NSM Intrushield and HBSS), Symantec Enterprise Anti-Virus, BlueCoat, Check Point, and Fortinet technologies including firewalls, packet analyzers, proxies, and filters.

**Information Security Specialist (SDLC / DevOps)**

Citigroup, 10/2016 – Present

Implementing PCI/ application security program: Working with stakeholders to develop security requirements and secure design documentation. Performing Architectural Risk Assessment (ARA) and generating threat models. Performing various risk assessments throughout DevOpsSec/ SSDLC including SAST (HP Fortify), DAST (Burp Suite), manual penetration tests and code reviews. Developing & delivering assessment presentations, secure coding training, corresponding remediation guidelines and documentation.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_09/2015 – 12/2016**

**Security Analyst (Application Security)**

UnitedHealth Group, PenSecure LLC – Remote

* Performing and managing full scope application risk assessments throughout the Secure Software Development Life Cycle (SSDLC).
* Working with stakeholders to develop security requirements and secure design documentation.
* Performing Architectural Risk Assessment (ARA) and generating threat models.
* working with development teams to provide security requirements and training for design improvements.
* Developing & delivering full scope SDLC security training in addition to generating detailed secure coding guidelines and remediation documentation for Governance, Risk and Compliance (GRC).
* Managing security projects and working in cooperation with GRC teams to develop policies / procedures and incorporate application security into the organizational information security program.
* Performing Dynamic Application Security Testing (DAST) & Static Application Security Testing (SAST) as well as manual source code reviews.
* Penetration testing a variety of systems including mobile / web applications and services, operating systems and databases (hybrid, automated and manual penetration testing).
* Conducting mobile device vulnerability analysis including forensics and reverse engineering.
* Researching and developing policies, procedures and security plans for evaluating nonstandard & new medical technologies using industry best practices / compliance guidelines. (HIPAA, OWASP, ESAPI, CWE, CVSS, NVD-CVE, PCI DSS, SOX, NIST, etc.)
* Testing a variety of systems including Medical systems with a broad range of technologies: Java/J2EE, ASP.NET, C#, VB.NET, PHP, SQL, MSSQL, MySQL, Oracle, HTML5, JavaScript, JSON, AJAX, XML, SOAP, REST, Apache Webserver, MS IIS, Websphere and others.
* Security testing various environments (QA / Production) and authentication types (OAuth, SAML, etc.)
* Security testing: Input and Access handling, SQLi - SQL Injection, XSS - Cross Site Scripting, CSRF - Cross-Site Request Forgery, Session / Cookie Manipulation, Logic Flaws, Buffer Overflows, & etc.
* Determining and ranking security vulnerabilities using threat categorization methodologies such as STRIDE.
* Generating and presenting detailed / management level reports that include methods, findings, conclusions and recommendations for remediation and secure coding practices.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_06/2014- 07/2015**

**Systems Security Engineer**

University of Pittsburgh Medical Center, PenSecure LLC - Pittsburgh, PA

* Performing system risk assessments throughout the System Development Life Cycle (Agile SDLC).
* Generating security controls for user requirements and developing secure architecture / design documentation for multitier applications.
* Performing Architectural Risk Assessment (ARA), threat modeling and source code reviews.
* Determining and ranking security vulnerabilities using threat categorization methodologies such as STRIDE.
* Performing Dynamic Application Security Testing (DAST) & Static Application Security Testing (SAST) as well as penetration testing (hybrid, automated and manual penetration testing).
* Researching and developing security plans for evaluating new technologies using industry best practices / compliance guidelines. (PCI DSS, SOX, COBIT, COSO, HIPAA, OWASP, ESAPI, CWE, CVSS, NVD-CVE)
* Penetration testing web applications, web services and mobile applications.
* Conducting host vulnerability analysis including forensics and reverse engineering.
* Security testing: Input and Access handling, SQLi - SQL Injection, XSS - Cross Site Scripting, CSRF - Cross-Site Request Forgery, Session / Cookie Manipulation, Logic Flaws, Buffer Overflows, & etc.
* Testing a variety of systems that include financial (PCI / SOX) & Medical systems with a broad range of technologies: Java/J2EE, ASP.NET, C#, VB.NET, PHP, SQL, MSSQL, MySQL, Oracle, HTML5, JavaScript, JSON, AJAX, XML, SOAP, REST, Apache Webserver, MS IIS, Websphere and others.
* Security testing various environments (QA / Production), non-standard networks and communication electronics from internal and external locations with different types of authentications (OAuth, SAML, etc.)
* Managing system security plans and working with information owners to ensure that adequate security questionnaires are developed and also appropriate vulnerability remediation occurs.
* Developing & delivering full scope SDLC security training in addition to generating detailed remediation guidelines and documentation for secure coding practices.
* Generating and presenting detailed / management level reports that include methods, findings, conclusions and recommendations for information security polices and industry best practices for secure coding.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_02/2014- 05/2014**

**Information Security Analyst**

ETM Inc., contract – Green Bay, WI

* Analyzing the complete application environment for security risks through design reviews, code reviews and dynamic application security testing.
* Recommending security measures to safeguard applications and information assets using threat modeling, OWASP, CWE, CVSS and NVD-CVE.
* Providing consulting and compliance guidance to project teams and developers regarding industry regulations and best practices for secure coding.
* Performing and managing system vulnerability assessments and application security tests.
* Performing dynamic application security analysis & static application security analysis for a wide range of vulnerabilities in mobile / web applications and services, operating systems and databases.
* Testing vulnerabilities include: SQL Injections, Cross Site Scripting, Cross-Site Request Forgery, Cookie Manipulation, Logic Flaws, Buffer Overflows, & etc.
* Testing technologies include: databases (MSSQL, MySQL, Oracle, DB2), server side technologies such as Java/J2EE, ASP.NET (C# & VB.NET), PHP, Apache Webserver, MS IIS, Websphere and other technologies like HTML5, JavaScript, JSON, AJAX, XML, SOAP & etc.
* Analyzing business impact and exposure based on emerging security threats, vulnerabilities, and risks.
* Conducting risk assessments to ensure security posture, security breach management, research and remediation.
* Presenting the final reports that include methods used, findings, conclusions, and recommendations.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_06/2013- 12/2013**

**Security Analyst (Penetration / Intrusion analysis and testing)***U.S. Marine Corps Headquarters Network Operation and Security Center – Northrop Grumman subcontract*

* Analyzing security architecture and design controls for web applications, web services, mobile applications, operating systems, databases and recommending secure coding practices.
* Reviewing code and evaluating applications for vulnerabilities such as SQL Injection, Cross Site Scripting, Cross-Site Request Forgery, & etc.
* Testing Application / network security and providing appropriate course of actions for remediation.
* Mitigating identified risks through incident handling and forensics (including emergency response).
* Ensuring all vulnerabilities & mitigations are accurately documented and presented in the final report.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_11/2012- 05/2013**

**Application Security Specialist***The Library of Congress, GBTI contract – Washington, DC*

* ­­Performing and managing application risk assessments throughout the Software Development Life Cycle.
* Generating security requirements and evaluating architecture to develop threat models.
* Reviewing design documentation and prioritizing remediation based on threat modeling (STRIDE).
* Performing Dynamic Application Security Testing (DAST) & Static Application Security Testing (SAST) as well as manual source code reviews for cloud based applications, Amazon Web services (AWS).
* Identifying application security vulnerabilities and developing mitigation plans to meet business security needs.
* Developing system security plans, security assessment plans and security assessment reports consistent with the National Institute of Standards and Technology (NIST) Risk Management Framework. (800-53 & 800-30)
* Performing automated vulnerability assessments and manual penetration tests.
* Using black-box techniques, hybrid / manual code review and a variety of tools including python scripts and self-developed manual tools to test for vulnerabilities in web applications, web services, mobile applications, databases and operating systems.
* Testing access control and code injection flaws, SQL Injection, Cross Site Scripting, Cross-Site Request Forgery, Session / Cookie Manipulation, Logic Flaws, Buffer Overflows, & etc.
* Providing remediation guidance to system engineers, administrators, end users and developers.
* Researching and Developing (R&D) guidelines for information security policies and secure coding practices using industry best practices. (ISO27001/2, ESAPI, PCI DSS, HIPAA, COBIT, COSO, SOX, CMMI, ITIL, ISACA)
* Presenting the final reports that include methods used, findings, conclusions, and recommendations.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_06/2009- 11/2012**

**Communications and Security Specialist (Security - Engineer)**

*The U.S. Army – Aberdeen Proving Ground*

* Developing & delivering application security training.
* Planning and assessing security controls for enterprise application platforms such as Java/J2EE & .Net.
* Using code reviews and OWASP guidelines to identify, analyze & report application security vulnerabilities such as code injections and access controls flaws.
* Generating detailed security test reports & recommending risk mitigation solutions based on OWASP, CWE, CVSS and NVD-CVE.
* Presenting reports that including findings and remediation recommendations.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_02/2006- 05/2009**

**IT integrator - Software Developer***IT integrity contract – Glen Burnie, MD*

* Working in Agile (Scrum) team to develop enterprise level applications (Java, SQL, few .NET/C#).
* Analyzing requirements and developing secure design patterns (UML) to meet security and usability standards for multitier applications.
* Analyzing coding errors and refactoring using object oriented design.
* Performing code reviews and debugging applications to resolve errors and vulnerabilities such as SQL Injection, Cross Site Scripting, and Cross-Site Request Forgery, etc.
* Generating summery reports for manager and detailed report for technical customers.

**EDUCATION AND TRAINING**

* **Bachelor of Science in Information Systems Management**, University of Maryland University College
* **Certified Information Systems Security Professional (CISSP)** - ISC² (IAM Level III)
* **Certified Ethical Hacker (CEH) -** EC-Council member (DOD CNDSP Auditor)
* **Web Application Penetration Tester (GWAPT)** - Global Information Assurance Certification (GIAC)
* **OWASP DevOps Training -** The Open Web Application Security Project
* **BLACK HAT Certification:** The Web Application Hacker’s Handbook Live Edition
* **SANS SEC542:** Web Application Penetration Testing and Ethical Hacking
* **Project Management for IT Professionals certificate,** University of Maryland University College
* **CompTIA Security+** & **CompTIA Network+** (DOD 8570.01-M IA Security Engineer IAT)
* **Penetration / Intrusion Analysis & Testing,** Northrop Grumman Corporation
* **Certified Satellite Systems** **Specialist (Security - Engineer)**,U.S. Army
* **U.S. Army leadership development training**, U.S. Army

**HONORS & AWARDS**

* (ISC)² Member, OWASP member, EC-Council member, CompTIA member
* U.S. Army letter of recognition for academic excellence

**OTHER QUALIFICATIONS**

(ISC)² Certified Secure Software Lifecycle Professional (CSSLP) Course, *United States Army e-learning*

Cisco Certified Network Associate Course (CCNA course), *University of Maryland University College*

Advance proficiency in speaking Hindi

**INFORMATION SYSTEMS MANAGEMENT COURSEWORK**

Bachelor’s program includes instructions, case studies, and applications in the broad range of Information technology including Information Security, Network Engineering, Database Administration, Systems Analysis, Programming and Project Management.

**Information Security:** Identifying risk and participating in risk mitigation activities by selecting and employing comprehensive safeguards such as PKI, intrusion detection systems and intrusion prevention systems (IDS/ IPS) to protect organizational assets. Applying infrastructure, applications and operational security controls to maintain confidentiality, integrity and availability. Working with threat data and analyzing anomalous or malicious activity using anti-virus. Providing corrective actions such as patching and writing reports. Designing operational security in a business environment. Working with various forensics platforms and tools including commercial or open source used in forensics lab to conduct legal and cyber investigations.

**Network Engineer**: Implementing secure and defined network architectures. Configuring, maintaining and troubleshooting network devices using appropriate network tools. Training on network devices. (routers, switches, hubs, bridges, gateways, laptop computers/PC workstation, peripheral devices, telephones, Printer / Copier, fax machines, scanners, audio visual equipment, media types and interfaces. Training on software technologies. (Microsoft Windows XP and Windows 7 operating system, active Roles and active Directory, Adobe and IBM Enterprise software. Training on network and web technologies (TCP, IP addressing, ICMP, UDP, SMTP, FTP, HTTP, HTTPS, SOAP, HTML, JavaScript, XML, AJAX, JSON, REST, & etc.) Interconnecting, installing and configuring Cisco switches, routers and other hardware according to the specification and compatibility. Familiarization with MAC hardware, MACOSX, IOS, UNIX (Solaris environment), Red Hat Linux and Android. Familiarization with network monitoring tools such as Traverse, NetVigil, TACACS logs, Computerized Maintenance Management Systems (CMMS) and Enterprise Asset Management (EAM) systems. Familiarization with Remedy, Dell/ HP servers and storage, virtualization (VMware), imaging and data migration. Familiarization with Video Teleconferencing (VTC) equipment, VoIP telephones, Cisco data/ Voice, remote support tools (Citrix, VNC, JAMF Casper suite) and SCCM/SCOM. Willing to learn more about paging, swapping.

**Database Administrator**: Creating relational databases using SQL and managing RDBMS. Constructing entity/relationship diagram, data modeling and performing normalization process through the third normal form. Defining and comparing desktop, workgroup, enterprise and database environments as well as various database models and architectures. Creating audit databases for analysis, monitoring and trending data errors. Creating, quarrying and maintaining databases and archives as required for analytics. Using statistical and analytical methods to identify patterns and integrate data.

**Systems Analyst**: Planning, building, and maintaining systems that meet organizational strategic goals by applying enterprise architecture and enterprise governance principles and practices. Developing and implementing successful system designs by effectively applying the role of systems engineers and functional analysts. Integrating systems with project management. Using effective organizational planning and excellent communication skills to determine, manage, and document business requirements throughout the system development life cycle. Using advance oral and written communication skills to translate business requirements into systems by applying appropriate SDLC methodologies and incorporating industry best practices.

**Programmer**: Developing robust enterprise applications by secure coding in PHP, Java, .Net, C/C++, Assembly, Objective-C and other platforms. Also, using web content management systems. Analyzing requirements and defining software program design to meet customer requirements and usability standards. Creating custom scripts in languages such as python and JavaScript for security testing purposes. Performing code reviews and debugging applications to resolve vulnerabilities and errors. Familiarization with Perl, Ruby on rails, ETL and SHELL.

**Project Manager**: Managing and controlling IT projects that align with organizational strategic goals using Microsoft software suit including MS exchange, outlook email, Microsoft Project, and Microsoft Office applications such as Word, Power point, Access, Visio and Excel (Pivot tables, calculations, statistic tools and charts/ graphs, etc.). Planning, implementing, and executing quality IT projects with resource constraints. Managing high-performing project teams to plan and implement technological solutions. Familiarization with ITIL.