



Prince Acheampong

📍 **Wa-Bole Street, Bamahu** : 00233, Wa, Ghana

✉ **Email:** acheampongprince77@gmail.com 📞 **Phone:** (+233) 542146652 📠 **Phone:** (+233) 596910828

🌐 **Website:** <https://archieprince.github.io> 🗨 **Whatsapp Messenger:** +233542146652

🌐 **LinkedIn:** [linkedin.com/in/prince-acheampong-85b495186](https://www.linkedin.com/in/prince-acheampong-85b495186)

Gender: Male **Nationality:** Ghanaian

ABOUT MYSELF

System & Application Security Engineer | System Administrator

Experienced cybersecurity specialist with a strong background in defending enterprises from online threats. Proficient in organizing and addressing technical concerns related to technology, processes, and user security. Skilled in identifying vulnerabilities, implementing robust security measures, and effectively managing incidents. Owns a dedicated cloud infrastructure and lab for continuous security testing and skill development.

EDUCATION AND TRAINING

[05/2023]

Cybersecurity and Digital Forensics - Advanced Short Course

Kwame Nkrumah University of Science and Technology <https://www.knust.edu.gh/>

City: Kumasi | **Country:** Ghana | **Field(s) of study:** Education

- Penetration Testing using Kali Linux
- Digital Forensics
- Best Ethical Hacking Practices

[09/2016 – 10/2020]

BSc. Information Technology

University of Cape Coast <https://ucc.edu.gh/>

City: Cape Coast | **Country:** Ghana | **Final grade:** 3.72 | **Thesis:** Re-engineered:
<https://gmdp.ucc.edu.gh/en/>

- System Security and Administration
- Network Computing
- Embedded System
- Software Engineering
- Information System Management
- Data Structures
- Algorithms
- Web Technology

[01/2024 – Current]

CRITAC ACM Professional

The Center for Research, Information, Technology and Advanced Computing (CRITAC) <https://critacghana.com/critac/>

City: Accra | **Country:** Ghana | **Field(s) of study:** Research in AI and Cybersecurity

- research assistantship in AI and Cybersecurity matters

WORK EXPERIENCE

[09/2021 – Current]

IT Specialist

- Supported in the implementation, and ongoing improvement of the ISMS at the project level, ensuring alignment with GIZ standards, needs and best practices.
- Led in the establishment and maintenance of the local asset register for all GIZ projects in Ghana.
- Coordinated in the reporting of information security incidents like loss and theft of official devices, and others, with relevant stakeholders at the country level with HQ in Germany.
- Provided ongoing information security awareness training and guidance to GIZ projects to promote secure practices and behaviors
- Facilitated and presented the new trends of attack vectors for developing and donor agencies to all projects in Ghana.
- Developed training materials as a monthly Information Security tit bits with ISO.
- Successfully collaborated with a diverse range of stakeholders, including management, IT teams, project managers, and headquarter's personnel, to achieve information security objectives in GIZ.
- Demonstrated excellent communication skills in presenting complex technical information to both technical and non-technical audiences.
- Collaborated with stakeholders across the organization like the Ernst & Young (EY), Competence Center, the InfSec team, the ISO HQ and others to ensure policies and procedures were clear, concise, and enforceable in the project's implementation of outsourcing of consultancy.
- Deployed a SIEM and XDR solution over two production servers, for project's implementation to partners, in the testing phase.
- Administered two major production servers (Linux Servers) ensuring compliance with the ISO 27001, and NIST security frameworks
- Ensured security controls for software development, collection of data (spatial) and server security hardening from the Software Development Lifecycle Policy and the NIST Framework
- Tested and deployed two major portals for the Metropolitan, Municipal, and District Assembly: e-library and e-learning
- Performed vulnerability assessment on the web applications APIs
- Developed a PowerShell script to automate the installation of over 400 new devices (Windows desktops and laptops)
- Developed Participant Information Management System for beneficiary and event tracking with Laravel, PHP, MySQL, JavaScript
- Facilitated the transformation of internal processes of units like Monitoring & Evaluation, Finance & Admin with M365 tools like MS List, MS Excel, etc.
- Trained over 40 staff of the GIZ/EU-REACH on digital working tools like M365 (MS Teams, Outlook, SharePoint, etc.)
- Trained service providers and consultants in GIZ organizational standards, operation and procedures around information security
- Develop and train over 250 GIZ colleagues on Security and Privacy Matters of Generative AI in the Workplace
- Created forms for (spatial) data collection for spatial planning ensuring the standards and procedures of GIZ
- Provided technical backstopping to different GIZ projects across countries

Project Leader: Spearheaded the implementation of E-Learning mechanism for project partners

[08/2022 – Current]

Vulnerability Assessment Consultancy

EU GAP Project

Conducted comprehensive penetration testing engagements:

Web Applications:

- Conducted hands-on testing for SQL injection, XSS, CSRF, and RCE vulnerabilities using Burp Suite and OWASP ZAP.
- Successfully exploited SQL injection to bypass authentication and access sensitive data in simulated environments.

- Identified and mitigated XSS vulnerabilities to prevent malicious script execution in user browsers.
- The hurdle here to jump was to bypass WAF.

APIs:

- Used Postman and Burp Suite to test API endpoints for security misconfigurations and broken authentication issues.
- Discovered and reported authorization flaws allowing unauthorized data access.
- Recommended and Implemented security controls and best practices to enhance API security based on identified issues.

Networks and Infrastructure:

- Conducted network scanning and vulnerability assessments using Nmap and Nessus.
- Performed penetration tests on network devices and firewalls to identify weaknesses in network segmentation.

Active Directory:

- Analyzed Active Directory setups to find misconfigurations and insecure password policies using tools like BloodHound.
- Demonstrated privilege escalation by exploiting weak permissions and improper configurations in simulated Active Directory environments.
- Provided detailed remediation steps to secure privileged accounts and enforce stricter password policies.

Reporting and Communication:

- Prepared detailed penetration testing reports that included findings, risks, proof-of-concepts, and actionable remediation strategies.
- Communicated complex technical issues effectively to both technical and non-technical stakeholders.
- Collaborated with peers on Pentesting community platform to discuss findings and share knowledge on emerging security threats and tools.

Ethical Hacking and Continuous Learning:

- Maintained a strong commitment to ethical hacking principles and best practices.
- Actively participated in TryHackMe challenges and labs to stay updated with the latest vulnerabilities and exploitation techniques.
- Engaged in continuous learning to enhance skills and adapt to the evolving threat landscape.

Exploited discovered vulnerabilities: Used advanced tools and techniques to demonstrate real-world impacts of vulnerabilities. Created detailed proof-of-concepts for various types of security flaws.

Reported findings: Prepared detailed penetration testing reports that documented findings, risks, proof-of-concepts, and recommended remediation strategies. Gained experience in articulating complex technical findings to both technical and non-technical audiences.

Collaborated with virtual teams: Worked with peers on TryHackMe's community platform to prioritize vulnerabilities, remediate issues, and enhance security controls. Participated in discussions and knowledge sharing to stay updated with emerging threats and offensive security tools.

Adhered to ethical hacking principles: Maintained a strong commitment to ethical hacking best practices throughout the training.

[03/2024 – 05/2024]

WordPress Vulnerability Assessment Consultant

TheAnointingBreaksTheYoke Inc, Maryland - USA

Conducted WordPress vulnerability assessments:

- **Comprehensive Security Scans:** Utilized WPScan to conduct thorough security scans on the client's WordPress site, identifying outdated plugins, themes, and core files.

- **Manual Testing:** Performed manual security testing to uncover vulnerabilities that automated tools might miss, including weak passwords and improper file permissions.
- **Exploit Demonstration:** Demonstrated exploitation techniques for vulnerabilities such as plugin/theme vulnerabilities, insecure configurations, and weak credentials, showing potential real-world impacts.

Advanced Techniques:

- **SQL Injection Testing:** Conducted SQL injection tests on WordPress plugins and themes using SQLmap and Burp Suite, successfully extracting sensitive data.
- **Cross-Site Scripting (XSS):** Identified and exploited XSS vulnerabilities to execute malicious scripts and gain unauthorized access to user sessions.
- **Cross-Site Request Forgery (CSRF):** Tested for CSRF vulnerabilities to demonstrate how attackers could perform unauthorized actions on behalf of authenticated users.

Security Recommendations:

- **Detailed Reporting:** Prepared comprehensive reports outlining identified vulnerabilities, associated risks, and proof-of-concepts. Included clear, actionable remediation steps tailored to the client's environment.
- **Security Hardening:** Advised on best practices for securing WordPress installations, including regular updates, strong password policies, and proper configuration of security plugins like Wordfence and iThemes Security.

Client Collaboration:

- **Remediation Support:** Worked closely with the client's development and IT teams to prioritize and implement remediation strategies. Provided guidance on fixing vulnerabilities and enhancing overall security posture.
- **Training and Awareness:** Conducted training sessions for the client's staff to raise awareness about common WordPress security issues and preventive measures.

Ongoing Monitoring and Support:

- **Continuous Monitoring:** Set up monitoring tools to continuously scan for new vulnerabilities and threats. Provided ongoing support to ensure the client's WordPress site remained secure.
- **Proactive Updates:** Advised on and assisted with regular updates and security patches for WordPress core, themes, and plugins to mitigate emerging threats.

[12/2020 – 08/2021] **Junior IT Specialist**

GIZ Ghana - (MOVE ComCashew Project) www.giz.de/ghana

City: East Legon | **Country:** Ghana | **Email:** prince.acheampong@giz.de

- Maintained accurate records, managing data entry, and adhering to data security protocols and GIZ standards and procedures for sensitive information
- Maintained accurate and up-to-date records, adhering to strict data security protocols.
- Provided technical support for project teams, ensuring efficient communication and project documentation management.
- Assisted with grant management tasks, maintaining data integrity and adhering to GIZ standards and procedures
- Support in the set up of computers for colleagues.
- Offered phone support for the project's helpdesk.
- Troubleshoot hardware and software problems, resolving issues in a timely and efficient manner.
- Assisted with troubleshooting hardware and software issues for end users with the IT Support
- Provided technical support and resolved IT-related problems.

[11/2019 – 09/2020] **Undergraduate Teaching Assistant**

University of Cape Coast <https://ucc.edu.gh>

City: Cape Coast | **Country:** Ghana | **Name of unit/department:** Computer Science and Information Technology | **Business/sector:** Education

Research Assistant

- Embedded Lab Assistant / Sys Admin
- Student Coach - UCC
- Teaching Assistant
- Data Analysis
- Re-engineered Ghana Music Documentation Project

RESEARCH SUPPORT

[07/2024 – Current]

ACM - CRITAC Chapter

Title: Strengthening Web Application Firewall (WAF) Security and Privacy: A Comprehensive Investigation and Mitigation Strategies

Objectives:

- a) To assess the effectiveness of WAFs in mitigating common web application attacks.
- b) To identify security vulnerabilities in WAFs that could be exploited by attackers.
- c) To investigate potential privacy risks arising from the use of WAFs in web application traffic inspection.
- d) To propose robust and privacy-preserving mitigation strategies to enhance the security and privacy of WAFs.

[03/2024 – Current]

ISMS-GIZ Headquarters, Germany - GIZ Ghana

Topic: The Strategy in the Implementation of Information Security Management by the ISMS GIZ in Ghana

The focus is on the ISMS-GIZ, Headquarters, within the context of GIZ Ghana. This implies a deep dive into the organization's structure, its role within the larger GIZ framework, and the specific challenges and opportunities it faces in information security management.

- To assess the effectiveness of the current ISMS implementation strategy within GIZ Ghana Headquarters.
- To identify the key factors influencing the success or failure of ISMS initiatives within the organization.
- To evaluate the alignment of the ISMS strategy with the overall organizational goals and objectives

[05/2020 – 07/2020]

Undergraduate Research Assistant - University of Cape Coast

Supported Dr Alimatu-Saadia Yussif (Supervisor) on this research.

Title: System Design and Usability Evaluation of Ghana Music Documentation System Using the System Usability Scale

Specific Objectives:

- Identify the lack of primary sources of information on Ghanaian music and the need for a centralized platform.
- Design and implement a database system to capture and store comprehensive information about Ghanaian music and its stakeholders.

- Develop features for browsing, searching, and mapping Ghanaian music information within the system.
- Assess the usability of the GMDS using appropriate evaluation methods (e.g., SUS).
- Analyze the system's effectiveness in documenting and mapping Ghanaian musical diversity.

Link: https://link.springer.com/chapter/10.1007/978-3-030-90235-3_22

BSc Information Technology - Thesis

Title: Reengineering Music Information Retrieval System

The following are the strategic objectives:

- To reengineer the music information retrieval system;
- To evaluate music information retrieval system;

Link: <https://gmdp.ucc.edu.gh/en/>

PROFESSIONAL CERTIFICATIONS

[07/2024]

CompTIA Security+ ce Certification

Skills verified:

- Assess the security posture of an enterprise environment and recommend and implement appropriate security solutions.
- Monitor and secure hybrid environments, including cloud, mobile, Internet of Things (IoT), and operational technology.
- Operate with an awareness of applicable regulations and policies, including principles of governance, risk, and compliance.
- Identify, analyze, and respond to security events and incidents.

Link: https://www.credly.com/badges/74c4046b-c0d9-495d-be2a-94cbd68448a9/public_url

[12/2023]

Certified In Cybersecurity - The International Information System Security Certification Consortium (ISC2)

Link: https://www.credly.com/badges/5c8b6147-1b95-4ea5-9092-eb6a3bf227e9/public_url

[04/2023 – Current]

Certified Governance Risk, and Compliance (GRC) Professional

OneTrust Certified Governance, Risk Management and Compliance Professional

Links: <https://www.credly.com/badges/cbee679f-00b1-4167-907f-fd16296c62b1> | <https://www.onetrust.com/trust/>

[10/2023 – 10/2024]

CRITAC ACM Professional Chapter

[06/2021 – Current]

Top 2% TryHackMe Training Platform

Digital Skills Acquired from TryHackMe CTFs:

- **Web Application Security Testing:** Conducted comprehensive security assessments for web applications using tools like WPScan, Burp Suite, and SQLmap.
- **Vulnerability Identification and Exploitation:** Identified and exploited vulnerabilities such as SQL injection, XSS, and CSRF to demonstrate potential impacts.

- **Automated and Manual Security Scanning:** Utilized automated tools and manual testing techniques to ensure thorough vulnerability coverage.
- **Security Reporting:** Prepared detailed reports with findings, risks, proof-of-concepts, and remediation steps.
- **Security Hardening and Best Practices:** Implemented best practices for securing web applications, including updates, strong password policies, and security plugin configurations.
- **Continuous Monitoring:** Set up monitoring tools for continuous security scanning and proactive threat mitigation.
- **Effective Communication:** Communicated complex technical findings to both technical and non-technical audiences clearly.

Link: <https://tryhackme.com/p/r0b0t4rch>

[03/2023 – Current] **AIZ Learning - Information Security Management System (GIZ)**

- Information Security Management
- Asset Management
- Information Security Risk Management
- Policies and Processes

[12/2020 – Current] **AIZ Learning - Information Security at GIZ**

[03/2023] **VTF Bootcamp for Security Analyst**

Continuous Security Testing

Security Analysis with Splunk

Threat Hunting with Atomic Read Team (ART)

Links: <https://verification.givemycertificate.com/v/4893990c-9413-42ec-bd26-6726ffc41644> | <https://verification.givemycertificate.com/v/30588f64-f86f-4428-b440-43c3dadb96fb> | <https://certificate.givemycertificate.com/c/4d2bc737-8067-4818-b490-7ff6ff64a6f6> | <https://vt.foundation>

[03/2023] **Security Information and Event Management (SIEM) Training with Splunk**

Link: <https://education.splunk.com/award/completion/bb58760d-ce4b-394c-be1b-4ea6c6e8141b>

[01/2023] **AttackIQ - Foundations of Operationalizing MITRE ATT&CK**

Link: https://www.academy.attackiq.com/certificate/6711?resource_id=4118&user_id=204634&type=course

[04/2023] **Active Countermeasures - Certificate of Attendance - Level 1 - Cyber Threat Hunting Training**

Link: https://issuer.gutenbergcerts.com/pdf/20230119-ACTI-kb00_ce880034-9e30-4e06-b02a-8a90577c595c.pdf

[10/2022] **Ethical Hacking for Beginners**

Link: <https://www.udemy.com/certificate/UC-313deaca-f213-48f8-aa87-69f49d83515e/>

DIGITAL SKILLS

My Digital Skills

Cybersecurity

Threat modelling | Network Security | Web Application Security | IT Security | Security Analysis | Threat Intelligence | Vulnerability Assessment | Incident Response | Endpoint Security | Scripts for automating tasks | SIEM Tools: Wazuh, OSSEC, Splunk | Python Programming Language

M365

Microsoft Suite (Outlook, Microsoft PowerPoint, Microsoft Excel, Microsoft Word) | Collaboration tools (Ms Teams, Ms Planner, Skype, Zoom)

Platforms

Installing and operation of Microsoft XP, Windows 7,8 & 10 MS-Office | Operating Systems Windows, Linux, macOS | Linux | Linux security hardening | Linux servers (CentOS, Kali Linux, Devuan, Ubuntu) | Active Directory / LDAP

IT Helpdesk

IT Software and Hardware Maintenance and Troubleshooting | IT Helpdesk Support | USER SUPPORT – helpdesk, product support and training to the staff

Software Development

Web Design & Web Development | Experience with PHP, SQL, HTML, CSS, JavaScript | Website content and management (WordPress and Joomla) | Design and management of a relational Database

Vulnerability Assessment and Penetration Testing

Nmap/Zenmap | Web Security Testing (OWASP ZAP) | ScoutSuite | Nessus Vulnerability Scanner | BloodHound | API Security

LANGUAGE SKILLS

Mother tongue(s): Akan (Asante Twi) , English

Other language(s):

French

LISTENING B1 **READING** B1 **WRITING** B1

SPOKEN PRODUCTION B1 **SPOKEN INTERACTION** B1

Levels: A1 and A2: Basic user - B1 and B2: Independent user - C1 and C2: Proficient user

HONOURS AND AWARDS

[24/07/2020]

First Class Honours (Bachelor of Science in Information Technology) Awarding institution: University of Cape Coast

The Best Graduating student - Department of Computer Science and Information Technology

Link: <https://ucc.edu.gh>

[11/2016]

Barclays Tertiary Scholarship Awarding institution: Barclays Bank

A full academic merit-based scholarship programme for BSc Information Technology for the 4-year programme at the University of Cape Coast

[10/2020]

Dean's Best Graduating Student Awarding institution: University of Cape Coast

Best Graduating Student - Department of Computer Science and Information Technology

[10/2019]

Dean's Overall Best Student - Level 300 Awarding institution: University of Cape Coast - School of Physical Science

2019 - Overall Best Student - Department of Computer Science and Information Technology for academic year 2018/2019

- [10/2018] **Dean's Overall Best Student - Level 200 Awarding institution:** University of Cape Coast
- School of Physical Science
2018 - Overall Best Student - Department of Computer Science and Information Technology for academic year 2017/2018
- [10/2017] **Dean's Overall Best Student - Level 100 Awarding institution:** University of Cape Coast
- School of Physical Science
2017 Overall Best Student - Department of Computer Science and Information Technology for the academic year 2016/2017

NETWORKS & MEMBER-SHIPS

- [Current] **The International Information System Security Certification Consortium (ISC2) - Member**
- [07/2024 – Current] **CompTIA Community Member**
- [04/2024 – Current] **Forum of Incident Response and Security Teams (FIRST) - Member**
- [01/2024 – Current] **Institute of ICT Professionals, Ghana - IIPGH** Accra
- [08/2023 – Current] **Gold Membership (Professional) - CRITAC**
- [2023 – Current] **Blacks In Cybersecurity (BIC)**
- [2023 – Current] **Member - AfricaHackon GH**

VOLUNTEERING

- [11/2023] **Cybersecurity Administrator and Analyst - CodersWhoTravel Inc - Remote**
Maryland: 6335 Green Field Rd. Unit 1712, Elkridge, MD 21075, USA
- Web Application Security Testing
 - Vulnerability Assessment
 - Threat Intelligence
 - Re-engineered 'TheAnointingBreaksTheYoke' website.
 - Regular updates monitoring and assessment of websites.
 - System Administration
 - Webmaster
- Links:** <https://www.coderswhotravel.org/> | <https://www.theanointingbreakstheyoke.com/>
- [08/2020 – 10/2022] **Cybersecurity Training Support - CyberGhana Institute** Accra
Link: <https://cyberghana.org/>
- [10/2022 – 07/2023] **Technical Advisor - Women in FinTech Ghana - Remote** Accra, Ghana
Providing technical advise and serving as the Cybersecurity Instructor
- [05/2021 – 06/2021] **Green Ghana Tree Planting Exercise - Competitive Cashew Initiative Project** Wa, Upper West Region - Ghana
Participate in a tree planting exercise organised every year at the Upper West region of Ghana

CONFERENCES & SEMINARS

[05/10/2023 – 07/10/2023]

Ghana Digital Innovation Week 2023 Accra International Conference Center, Accra

Link: <https://gdiw.com.gh/>

[06/04/2023]

Purple Hats Conference 2023 https://www.purplehats.org/2023/v/e?i=yUMrz1rCbGChFxDjrdwqLWAmWBErVXMt_1680793933

Purple Hats Conference — the industry destination for cybersecurity practitioners to collaborate, share ideas, and learn how to evolve from a reactive to proactive threat-informed defense!

Link: <https://www.purplehats.org/>

[24/10/2022 – 28/10/2022]

Ghana Digital Innovation Week 2022 Accra International Conference Center, Accra

A Platform to celebrate the accomplishments OF Ghana's Digital Innovation Ecosystem and build momentum towards a common vision for its future development

Link: <https://gdiw.com.gh/>

[29/09/2022]

Cyber Security Healthcare & Pharma Summit Online

Link: <https://cybersecuritysummit.com/>

HOBBIES AND INTERESTS

CTF Gamification

Playing Capture The Flag Games from TryHackMe (Top 2%), HackTheBox, LetsDefend, SANS, etc....

Link: <https://tryhackme.com/p/r0b0t4rch>

Music

RECOMMENDATIONS

Available upon request