Road Map for Chameleon Security T3 2023

Company Misson:

Chameleon's objective is to research, develop, test, record, and deploy IoT-based solutions to improve everyday life for individuals through the use of smart city technologies, such as smarter cities, homes, transportation, and energy management systems.

Weeks 1-2: Research and Upskilling (Research Phase):

- Researching the latest security trends, tools, and technologies.
- New members to educate themselves on the handover of the project and from T2 and the progress of the websites and company goals.
- Upskill team members on new security applications and methodologies and relevant software being used for the project tasks.
- Schedule training sessions and workshops to enhance expertise and plan for ongoing meetings with team members and leaders.

Weeks 3-5: Project Tasks and Collaboration (Execution Phase):

- Conduct code reviews on the Chameleon and MOP websites from a security perspective to ensure all aspects of the web pages have good digital security.
- Perform various security tests, including SSL testing and DDoS attacks. Simulate attacks to evaluate the website's strength.
- Execute SQL injection attacks on MOP websites to assess the susceptibility of the databases to manipulation. Identify and patch SQL injection vulnerabilities to prevent unauthorized access or tampering with the database.
- Collaborate on implementing secure coding practices, input validation, and other preventive measures to strengthen the overall security posture of web applications.
- Regularly perform port scans on both the Chameleon and MOP websites to identify any open ports that could be potential entry points for attackers.
- Document findings throughout the testing process as well as provide clear and actionable recommendations for each identified issue, outlining steps for remediation and prevention.
- Work with the MOP team to address vulnerabilities and ensure coordinated security measures.

Week 6: Review and Handover Preparation (Review and Finalization Phase):

- Review all security testing and assessment results, by examining vulnerabilities, strengths, and areas requiring improvement, ensuring a comprehensive understanding of the digital landscape's security posture.

- Compile and finalize summarising documentation, including a detailed report. This documentation will include an analysis of vulnerabilities discovered, approaches used during testing, and strategic recommendations for building digital security.
- Conduct a final review meeting with the Chameleon Security Project team and stakeholders to foster a shared understanding of the security testing outcomes and allow for collective decision-making on prioritizing and implementing security measures.
- Prepare for the handover by organizing documentation and insights for a smooth transition and ensuring a clear unanimous understanding of the project's current state and future needs.

Throughout the 6 Weeks:

- The security team will continually collaborate with the Chameleon Web Development team for real-time feedback and adjustments.
- Regularly review code to identify and address any security vulnerabilities and simulate attacks on the MOP and Chameleon sites to ensure the page continues to strengthen its security.
- Continuous monitoring and assessment of security measures to ensure the team aligns with the project's progress and contributes effectively to the overall enhancement of the company.
- Iterative adjustments to security policies and procedures based on emerging threats and continually reviewing the cybersecurity environment, allowing for adequate responses to new risks.