Road Map for Chameleon Security T1 2024

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 1-3/March 4th- March 22nd: Research and Upskilling (Research Phase):

- Researching the latest security trends, tools, and technologies particularly in the to with Electric Vehicles, Smart Cities, and Smart Data.
- New members to educate themselves on the handover of the project and from T3 and the progress of the websites and company goals.
- Team members to upskill on new security applications and methodologies and relevant software being used for the project tasks.
- Schedule and plan for ongoing meetings with team members and leaders.
- Independent upskilling and research on the Chameleon site, and our common resources, GitHub and Trello.

Weeks 4-8/ March 25th – May 3rd: 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 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.
- Developing governance and policies for best practices in cyber safety. As well as security and compliance auditing for all Chameleon team.

Week 9/6 May – 13: 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.

Week 10/ May 13th- May 17th: portfolio preparation and review:

- Students independently ensure their task submissions are up to the standard of the grade they have applied for. All tasks are wrapped up and ready for handover including and communications with other teams.

Throughout the 10 Weeks:

- The security team will maintain ongoing collaboration with the Chameleon Web Development team, ensuring immediate feedback and modifications.
- Conduct periodic code inspections to detect and rectify any security flaws, and perform simulated attacks on both the MOP and Chameleon sites to consistently improve their security defenses.
- Persistently monitor and evaluate security protocols to guarantee that the team's efforts are in sync with the project's advancement, thereby significantly enhancing the company's security posture.
- Make regular updates to security strategies and practices in response to new threats, continuously examining the cybersecurity landscape to enable prompt reactions to emerging risks.