Overview As a cybersecurity professional, you don’t need to be a programmer to contribute a security mindset to a development team. Having a proactive security mindset can help your team minimize security issues at the onset of application development; this will save you time and resources in later stages of development. In this activity, you will analyze the OWASP Top Ten risks and the OWASP Top Ten Proactive Controls to provide a better perspective on how a security professional can interact with an application development team and be a valuable contributing member. This activity will help prepare you for Project Two, which will be submitted in Module Seven. Scenario In a previous development, during the final security testing, a number of risks were identified prior to the app being released, including the following risks from the OWASP Top Ten risks: • A-1: Injection • A-2: Broken authentication • A-3: Sensitive data exposure • A-5: Broken access control • A-7: Cross-site scripting (XSS) Prompt As you prepare for your consulting role in a future development, your supervisor has asked you to prepare a preliminary report on what preventative measures could have been put into place to mitigate the security risks experienced earlier in the development life cycle. Using the OWASP Top Ten risks and the OWASP Top Ten Proactive Controls, select two of the risks uncovered during the security testing and discuss what controls would have been beneficial to address in the early stages of development to prevent the last-minute revisions necessary in the previous development. You must address the critical elements listed below. I. Risk One A. Based on the list provided in the scenario, summarize an OWASP Top Ten risk identified during the security testing. B. Using the OWASP Top Ten Proactive Controls, describe the strategy you would employ to minimize the risk in future developments. Note: Your strategy may include more than one of the OWASP Top Ten Proactive Controls. II. Risk Two A. Based on the list provided in the scenario, summarize an OWASP Top Ten risk identified during the security testing. B. Using the OWASP Top Ten Proactive Controls, describe the strategy you would employ to minimize the risk in future developments. Note: Your strategy may include more than one of the OWASP Top Ten Proactive Controls. Project Two Stepping Stone Rubric Guidelines for Submission: Your submission should be 1 to 3 pages in length. Use double spacing, 12-point Times New Roman font, and one-inch margins. References should be cited according to APA style. Use a file name that includes the course code, the assignment title, and your name—for example, CYB\_123\_Assignment\_Firstname\_Lastname.docx.