Application

Identifying and Fixing Security Weaknesses

--------------------------------------------------------------------------------

Because modern applications are complex, it is not practical to think about finding and fixing vulnerabilities by simply inspecting the code. Instead, a wide variety of sources—ranging from the government and professional software developers to the hacker community—provide information about potential application vulnerabilities. That information is reported from all of those sources to automated bug-tracking services like Bugzilla and it can be used to guide the application development and maintenance process.

Thus, the CISO has asked you to use Bugzilla to identify and guide the patching of the Firefox application for your company.

Go to **Bugzilla** and search for "injection." Sort the list by severity. Take a screenshot of your search.

Select one vulnerability of your choice from your result lists and write a 2- to 3-page paper in which you use the information provided for that vulnerability to analyze the specific problem and its causes. Then evaluate the recommended mitigations Bugzilla suggests. (Hint: you will find these by clicking on the ID number in the far left column.)

Your evaluation should address the following questions:

•What are the severity and priority rankings for your chosen vulnerability?

•What are the code level concerns for the vulnerability?

•What security issues will this vulnerability raise for the application?

•What are the precise steps required to fix the vulnerability you selected?

•How effective are the recommended mitigations for this vulnerability? (You may need to conduct some research to answer this question.)

•What other mitigations would you recommend? Why?

•Why should you, as a developer, and your organization be concerned about fixing this vulnerability?

Remember to include the screenshot of your Bugzilla search as appendices to your paper.