Zachary Nicholas

October 9, 2024

CS 410 Software Reverse Engineering

Module Six Journal

* Define: What is a security vulnerability?

A security vulnerability has multiple definitions the most complete one I could find comes from the National Institute of Standards and Technology (NIST) and they say that a vulnerability is “ Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. Note: The term weakness is synonymous for deficiency. Weakness may result in security and/or privacy risks.” Another definition is flaws in a given computer system that weaken or otherwise make the security of the system less secure, these can include a range of different topics such as unpatched software, Missing or otherwise poor encryption, and a trust relationship.

* Identify: What kinds of vulnerabilities would be identifiable in C++ code?

Some of the top vulnerabilities can be things like a buffer overflow, Memory access or management errors, input that is not validated, and injection attacks like that of SQL injection.

* Purpose: Why would you be looking for vulnerabilities during legacy to C++ conversion rather than during testing?

When developing and working with legacy systems it is important to understand what the system or program was trying to accomplish and consider how security and privacy techniques have updated since the system was originally deployed or developed, A lot of infrastructure work on either old or outdated hardware such as was seen with the colonial pipeline hack, the US Voter database and, the office of personnel management.

* Solutions: How do you determine the appropriate fix to a security vulnerability?

There are multiple ways to consider or fix a vulnerability a lot of them relate back to the OWASP website which is a good starting point in identifying and remediating any issues that arise, given their extensive knowledge base it is easy to find and fix issues, use of these guidelines and resources can help when using both black and white-box testing as they will help to identify what is the most severe issues present in the code and offer solutions on how to fix them, They also offer the “Top 10” which can help to identify commonly came across issues. Another good site to use is the NIST website as it has different resources that can help you in staying in line with government guidelines such as HIPAA.

Refernces:

Editor, C. C. (n.d.). *Vulnerability - glossary: CSRC*. CSRC Content Editor. https://csrc.nist.gov/glossary/term/vulnerability

GuardRails. (2023, April 27). *The top C++ security vulnerabilities and how to mitigate them*. Security Boulevard. https://securityboulevard.com/2023/04/the-top-c-security-vulnerabilities-and-how-to-mitigate-them/

Kerner, S. M. (2022, April 26). *Colonial pipeline hack explained: Everything you need to know*. WhatIs. https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know

*The OPM data breach: How the government jeopardized our national security for more than a generation*. United States House Committee on Oversight and Accountability. (2016, September 8). https://oversight.house.gov/report/opm-data-breach-government-jeopardized-national-security-generation/

*Owasp Top Ten*. OWASP Top Ten | OWASP Foundation. (n.d.). https://owasp.org/www-project-top-ten/

Team, S. S. R. (2022, August 16). *Top 5 C++ security risks*. Snyk. https://snyk.io/blog/top-5-c-security-risks/

*What are vulnerabilities, exploits, and threats?*. Rapid7. (n.d.). https://www.rapid7.com/fundamentals/vulnerabilities-exploits-threats/