Assignment 6

by Krishna Pinnaboyina

Submission date: 03-Oct-2017 02:54PM (UTC-0700)
Submission ID: 856729455
File name: 12487_Krishna_Pinnaboyina_Assignment_6_769028_1067656330.doc (45K)
Word count: 726
Character count: 3984

Assignment 6

Krishna Teja Pinnaboyina

Student ID: 544885

Campbellsville University

Prof: Dr. Jimmie Flores

Computer Science

Much has been made of the new Web 2.0 phenomenon, including social networking sites and user-created mash-ups. How does Web 2.0 change security for the Internet?

Web 2.0 as an online technology allows for the greater collaboration among the internet users, enhances the internet connectivity and enhances the channels of communication due to its great user interactivity. It can be said to be advanced because it is enabled by applications such as Ajax, eclipse, and RSS among others. Web 2.0 changes the internet security due to the many possible security threats. One of the possible security threats is the Ajax-related threats. In this, Ajax is used together with other web services which make it to be more prone to the attacks because the attackers can be in a position to easily gain access to confidential information and steal it and they may also insert codes that are malicious (Vossen, & Hagemann, 2007).

Describe the relationship of the requirements phase, testing phase, and use cases concerning software engineering development and secure code.

The requirements phase, testing and use case phases in software engineering development and secure code are related in that; it is in the requirement phase that the gathering of the business requirements is done. After the gathering, the requirements are usually analyzed so that they can be checked for validity and their possibility of incorporating the requirements in the system that is being developed. The testing phase is related to the requirements phase in that after the code is developed, it is usually tested against the set requirements to ensure that the product is solving the needs that have been addressed and gathered in the implementation phase. The use is also related to the other two phases because after the product is successfully tested, it is delivered to the clients for use (Conklin, White, Williams, Davis, & Cothren, 2016).

Develop a list of five security-related issues to be put into a requirements document as part of a secure coding initiative.

1. Validation of input from all the untrusted sources of data.
2. Heed to the complier warnings through the use of static and dynamic analysis tools in the detection and elimination of additional security flaws.
3. Architect and design for security policies- software architecture should be created and software designed for enforcing and implementing security issues.
4. Defaults deny- Access decision should be based on permission instead of exclusion.
5. Sanitize the data that is sent to other systems.

Choose two requirements from the previous question and describe use cases that would validate them in the testing phase.

One of the requirements is the validation of the input from all the sources of data that are untrusted. This is imperative in the elimination of the vast majority software vulnerabilities. Some of the use cases that would validate them in the testing phase are command line arguments, files that are controlled by the users, environmental variables and network interfaces. The second requirement is sanitizing the data that is sent from the other systems. In this, all the data that is passed to the complex subsystems should be sanitized including the command shells, commercial off-the-shelf components, and relational databases. Attackers can invoke the unused functionality in the components by using the command, SQL, and other injection attacks. Data should always be sanitized before the subsystem is invoked.

You have been asked by your manager to develop a worksheet for code walkthroughs, another name for structured code reviews. This worksheet should include a list of common errors to look for during the examination, acting as a memory aid. You want to leave a lasting impression on the team as a new college grad. Outline what you would include on the worksheet related to security.

1. Introduction
2. Common errors
    a. Requirements-related testing problems
    b. Test tools and environments problems
    c. Test process problems
    d. Management-related testing problems
    e. Test planning and scheduling problems
3. Code analysis resources and tools
    a. Threat modeling
    b. Static code analysis
    c. The application security professional
4. Conclusion

2

References

Conklin, W., White, G., Williams, D., Davis, R. & Cothren, C. (2016). *Principles of computer security*. New York: McGraw-Hill Education.

Vossen, G. & Hagemann, S. (2007). *Unleashing Web 2.0 : from concepts to creativity*. Amsterdam Boston: Elsevier/Morgan Kaufmann.

Assignment 6

ORIGINALITY REPORT

36%	9%	1%	36%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Campbellsville University Student Paper	19%
2	Submitted to Colorado Technical University Online Student Paper	4%
3	Submitted to University of South Africa Student Paper	3%
4	Submitted to American Intercontinental University Online Student Paper	3%
5	wiki.answers.com Internet Source	3%
6	Submitted to American Public University System Student Paper	3%
7	pgc.ac.in Internet Source	1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	Off		