SYNOPSIS ON

OPEN WEB APPLICATION SECURITY PROJECT

BY:

MERUGU AKSHAY KUMAR

SECTION:KE016

ROLL NO:67

OPEN WEB APPLICATION SECURITY PROJECT

Developing a secure Web application is very difficult task. Therefore developers need a guideline to help them to develop a secure Web application. Guideline can be used as a checklist for developer to achieve minimum standard of secure Web application. This study evaluates how good is OWASP guideline in helping developer to build secure Web application. The developed system is then tested using code auditing and penetration testing to identify the achievement of the system security for the application. After applying the testing techniques from Open Source Security Testing Methodology (OSSTMM) on the Top Ten Critical vulnerabilities as defined by OWASP, a standard measure score are calculated. The score is used to decide on the level of security of the developed web application. A high percentage score would indicate that the guideline helps in building a secured web application. Hence, the result proved that OWASP guideline is effective in ensuring the trustworthiness of the system and can be used as referral by other web developer especially in developing applications for a university.

Keywords: Web Application, Security

In the age of Internet and World Wide Web, system security has become an important issue in any global web based information systems. This can be seen from the strong commitments of system security professionals, the research community, and major application software vendors. Recently web technology has developed rapidly and affected people in many aspects of lives and working. Many daily activities, which required face-to-face interaction, can now be
conducted over the World Wide Web. Web applications are crucial components of our life. They cover critical activities such as economic transactions, e-commerce, e-government, e-business, e-procurement, e-education and many more. The processes of building a secure web application need one or more guidelines to make it a secure system. Without guideline, it is impossible to develop a secure system. Gritzales & Spinelis (1997) provide the best practice for addressing security issues and threats, which can be prevented using security services. Stuart et al. (2001) has been addressing a very comprehensive guideline including system, network, and software security. Ed (2002) provided a step-by-step guide to computer attacks and effective defences including web application. Darothy (1998) assert that the
best defence against security breaches is to make use of the tools and knowledge of good software engineering practice to prevent security attacks by developing and evolving secure system. This means that the requirements related to security issues must be identified and included early in the development and evolution of systems. Care must be taken to ensure that the security requirements are correct and complete.
The first OWASP (2003) issued the top 10 most critical web application security vulnerabilities. be considered inbuilding secure web application with an update on the latest vulnerabilities in 2004. OWASP issued the latest Top 10vulnerabilities (2007) which show that A1-Cross Site Scripting (XSS) has moved to the top of the list from 4th place andA2-Injection Flaws from 6th place to 2nd place. While A7-Broken Authentication and Session Management vulnerability
has moved down from 3rd place in the list to the 7th placement. Several new vulnerabilities have been identified in theTop 10 2007 list such as A3-Malicious File Execution, A4-Insecure Direct Object Reference, A5-Cross Site RequestForgery (CSRF) and A9-Insecure Communications.

In the article “Buzzing About Security“, Sandra (2002) explained why developer should have a framework as guideline to building secure web application. She recommends OWASP because it is an open source document where everybody can use it for developing, building, and testing secure system.