COMP307 Assignment 7

Research based on different documents by OWASP

Instructions

Work in teams of maximum four students. Read the resources shared in folder OWASP on e-centennial.

SAMM

In the Welcome to OWASP section of the page, **click** the **SAMM** (Software Assurance Maturity Model) **link.** OpenSAMM uses a 0 to 3 grading structure across four critical business functions, each containing three security practices to rate software development activities. From this page you can download the OpenSAMM framework, but the document is also available on the ecentennial.

focus: the rating, what it means

Read the document and review the SAMM framework.

OWASP Application Security Verification Standard Project

This standard describes best practices for testing Web application technical security controls. **Click** the **Download link to** open the download page and access the standard, but the document is also available on the e-centennial. Read the **forward**, review the **Standard** and close the document **OWASP_Application_Security_Verification_Standard_3.0.1 .pdf**

focus: the standard, how to implement it

The **About_OWASP_ASVS_Web_Edition.ppt** is the OWASP ASVS Project presentation which describes the process for integrating ASVS into software development. The document is also available on the ASVS Download page. Review the presentation and close the file.

Development Guide

whitelist -> accept known good
backlist -> reject known bad

In the Welcome to OWASP section of the page, **click** the **Development Guide link.** The Development Guide describes secure software development practices. The document is also available on the e-centennial as **OWASPGuide2.0.1.pdf.**

Read the **Data Validation Strategies** and **Authentication-Best Practices** and **close** the **chapters.**

page 161, 164

The OWASP development guide has a lot of very useful information. For example, it covers best practices for handling credit cards, including: Process the card immediately and do not store credit card numbers; If you must store the card number, follow PCI DSS (Payment Card Industry Data Security Standard ,transaction authorization number for reference; do not, part of the credit display any guidelines; store the number back to the user unless absolutely necessary and following PCI guidelines; never store the card CCV (credit card verification), CCV2, or PIN (personal identification number) numbers. In addition, any system processing credit cards should include antivirus software and be patched within one month after a security patch becomes available.

PCI DSS have auditors who check to ensure that ppl who use the 5 cc services follow the stds. to ensure that customers can have faith in their brands

OWASP Code Review Guide

Click the **OWASP_Code_Review_Guide-V1_1.doc** link , which is also available on the centennial . The Code Review Guide describes the importance of code review in software development and suggests best practices. Read the introduction and close the document.

page 11-13

checklist, page 15

https://www.owasp.org/index.php/Error_Handling

Use the browser's scrollbar to locate the Pages in **category "OWASP Code Review Project "section** of the page, and click the **Error Handling link**. This page suggests best practices for handling errors in Web applications. **Read** the **Error, Exception handling & Logging** and **Generic error messages sections** of the page.

Testing Guide V 4.0 ./Owasp/OTGv4.pdf

In the Welcome to OWASP section of the page, **click** the **Testing Guide link** to open the project page, click the **Project About tab,** and **click** the **Testing Guide V 4.0 link** in the Last review Release section of the page. . **Read** the **Principles of Testing** and **How to Write the Report of the Testing sections** of the document and **close** the **Acrobat Reader (OTGv4.pdf)** when done.