نام درس (فارسی)	توسعه امن نرم‌افزار
نام درس (انگلیسی)	Secure Software Development

شماره درس: ۴۰-؟؟؟	تعداد واحد: ۳	مقطع: تحصیلات تکمیلی
پیش‌نیازها: برنامه‌سازی پیشرفته (۴۰-۲۴۴) – مهندسی نرم‌افزار (۴۰-۴۷۴)		هم‌نیازها: امنیت داده و شبکه (۴۰-۴۴۲)
تهیه‌کننده: رسول جلیلی – محمدصادق دوستی		

هدف

این درس به معرفی فرایند توسعه امن نرم‌افزار می‌پردازد که شامل طراحی امن نرم‌افزار، پیاده‌سازی امن و مقاوم در برابر حملات، تست‌های امنیتی و بازرسی می‌باشد. تمرکز این درس روی نکات امنیتی از دیدگاه توسعه‌دهنده، آسیب‌پذیری‌های شایع امنیتی و ضعف‌ها و تهدیدهای امنیتی است. این درس اصول و استراتژی‌های امنیتی، تکنیک‌های کدزنی و ابزارهایی را معرفی و بیان می‌کند که کمک می‌کند تا نرم‌افزاری استوار در برابر حملات تولید گردد. دانشجویان در نهایت می‌توانند کدی تولید و یا تحلیل کنند که نشان دهنده مهارت آنها در توسعه امن نرم‌افزار باشد. اهداف این درس عبارتند از:

۱. آشنایی با اصول برنامه‌نویسی امن.
۲. آشنایی با خطاهای بسیار شایع برنامه‌نویسی که منجر به آسیب‌پذیری نرم‌افزار می‌شود.
۳. شناسایی و تحلیل مشکلات امنیتی در نرم‌افزار.
۴. آشنایی و محافظت در برابر تهدیدات امنیتی و آسیب‌پذیری‌های نرم‌افزار.
۵. اعمال عینی این آموخته‌ها برای ساخت سیستم‌های نرم‌افزاری امن.
۶. استفاده مؤثر از ابزارها برای ارزیابی امنیت نرم‌افزار.
۷. آشنایی با امکانات سطح پایین امنیتی در CPU، سیستم‌عامل و نرم‌افزار.
۸. توانایی مهندسی معکوس روی یک بخش از نرم‌افزار.

سرفصل مطالب

این درس به ۳ بخش تقسیم می‌شود: امنیت نرم‌افزار، مهندسی معکوس، برنامه‌نویسی امن.

۱. امنیت نرم‌افزار:

امنیت نرم‌افزار سعی دارد تا امنیت را در داخل نرم‌افزار بنا کند. برای رسیدن به این هدف، دانشجویان این مباحث را از مرجع [1] خواهند آموخت:

a. مقدمات و مبانی
b. ریسک و مدیریت ریسک
c. قدم‌های اصلی در امنیت نرم‌افزار
d. مرور کد
e. تحلیل ریسک بر پایه معماری
f. تست نفوذپذیری نرم‌افزار
g. تست امنیتی مبتنی بر ریسک

h. مورد کاربرد سوء
i. امنیت نرم‌افزار و عملیات امنیتی
j. تست امنیت نرم‌افزار در سطح سازمانی

۲. مهندسی معکوس:

مهندسی معکوس، فرایند کشف مبانی فناوری یک وسیله، شیء و یا سیستم از طریق تحلیل ساختار، کارکرد و عملیات آن می‌باشد. در حوزه نرم‌افزار، این کار معمولاً شامل باز کردن اجزای نرم‌افزار (توسط ابزارهای ترجمه معکوس زبان ماشین، ابزارهای اشکال‌زدایی و ...) و تحلیل دقیق طرز کار آن می‌باشد که به منظور نگه‌داری نرم‌افزار و یا ساخت یک نرم‌افزار جدید می‌باشد که همان کار نرم‌افزار اصلی را انجام می‌دهد ولی از هیچ یک از قطعات آن به طور مستقیم (و یا بدون درک کامل آن) استفاده نمی‌کند.

در این بخش از درس، ما به طور عمیق وارد جزئیات سطح پایین سیستم عامل و کد نرم‌افزار می‌شویم. پس از مروری سریع بر زبان اسمبلی ایکس ۸۶، دانشجو با بارگذاری یک فایل اجرایی در حافظه، نحوه نگه‌داری مقادیر در حافظه و مطالبی از این دست آشنا شده و در پایان روش‌های مقابله با مهندسی معکوس را می‌آموزد.

مرجع [2] مرجع اصلی این بخش می‌باشد ولی مطالب آنلاین (مانند [3, 4, 5]) نیز در این بخش استفاده می‌شود.

۳. برنامه‌نویسی امن:

این بخش به چهار قسمت اصلی تقسیم می‌شود:

a. نکات امنیتی در نرم‌افزارهای وب
b. نکات امنیتی در پیاده سازی نرم‌افزار
c. نکات امنیتی مرتبط با رمزنگاری
d. نکات امنیتی مرتبط با شبکه

این بخش سعی دارد تا حدوداً همه‌ی نکات امنیتی که یک توسعه‌دهنده در حین برنامه‌نویسی با آن روبرو می‌شود را پوشش دهد مانند تزریق کد SQL، سرریز بافر، حملات XSS و ... . منبع اصلی این بخش نیز [6] می‌باشد.

منابع

1. Gary McGraw, Software Security: Building Security In. Addison Wesley Professional, 2006.
2. Eldad Eilam, Reversing: Secrets of Reverse Engineering. Wiley Publishing, Inc., 2005.
3. http://www.reversing.be/
4. http://www.tuts4you.com/
5. http://crackmes.de/
6. Michael Howard, David LeBlanc, and John Viega, 24 Deadly Sins of Software Security: Programming Flaws and How to Fix Them. McGraw Hill, 2010.

نحوه ارزیابی

به دلیل ماهیت کاربردی درس، دانش عملیاتی دانشجویان باید ارزیابی گردد. نمره این درس بر اساس تقسیم‌بندی زیر محاسبه خواهد شد (تقریبی):

- تمرین ٪۴۰
- پروژه ٪۳۰
- امتحان ٪۳۰