برای کتاب "امنیت نرم‌افزار در جاوا"، سرفصل‌ها می‌توانند به شکل زیر تنظیم شوند:

**فصل 1: مقدمه‌ای بر امنیت نرم‌افزار**

* اهمیت امنیت در نرم‌افزارهای امروزی
* تهدیدات رایج در دنیای نرم‌افزار
* معرفی مفهوم امنیت در نرم‌افزارهای جاوا
* اصول پایه امنیت نرم‌افزار

**فصل 2: تهدیدات و آسیب‌پذیری‌ها در نرم‌افزارهای جاوا**

* **SQL Injection:** خطرات و روش‌های پیشگیری
* **Cross-Site Scripting (XSS):** شناسایی و جلوگیری از حملات XSS
* **Cross-Site Request Forgery (CSRF):** نحوه محافظت در برابر CSRF
* **Insecure Deserialization:** آسیب‌پذیری‌ها و راهکارهای پیشگیری
* **Command Injection:** معرفی و روش‌های ایمن‌سازی
* **Directory Traversal:** شناسایی و مقابله با این نوع حملات

**فصل 3: امنیت در معماری و طراحی نرم‌افزار**

* مفهوم طراحی امن در نرم‌افزار
* اصول معماری امنیتی برای سیستم‌های جاوا
* الگوهای طراحی امن (Secure Design Patterns)
* بررسی سیستم‌های احراز هویت و مجوزدهی امن
* ایمن‌سازی ارتباطات در شبکه (SSL/TLS)

**فصل 4: رمزنگاری در جاوا**

* **رمزنگاری متقارن و نامتقارن:** تفاوت‌ها و کاربردها
* **کتابخانه‌های رمزنگاری در جاوا (Java Cryptography API)**
* پیاده‌سازی الگوریتم‌های استاندارد مانند AES و RSA
* استفاده از امضای دیجیتال و توکن‌های امنیتی
* تکنیک‌های هشیاری (Hashing) و بررسی الگوریتم‌های رایج

**فصل 5: امنیت در پایگاه‌داده‌ها و ذخیره‌سازی داده‌ها**

* ایمن‌سازی پایگاه‌داده‌ها در جاوا
* جلوگیری از SQL Injection در دستورات پایگاه‌داده
* ذخیره‌سازی ایمن اطلاعات حساس مانند پسوردها
* استفاده از تکنیک‌های رمزنگاری در ذخیره‌سازی داده‌ها
* پشتیبانی از امنیت در پایگاه‌داده‌های NoSQL

**فصل 6: امنیت در احراز هویت و مجوزدهی**

* پیاده‌سازی روش‌های احراز هویت امن در جاوا (JWT, OAuth)
* مدیریت سشن‌های ایمن
* امنیت در مدیریت دسترسی و مجوزها (Role-based access control)
* احراز هویت دو مرحله‌ای (2FA) و پیاده‌سازی آن در جاوا

**فصل 7: تست امنیت در نرم‌افزارهای جاوا**

* **تست‌های نفوذ (Penetration Testing):** اصول و ابزارها
* **Static Code Analysis:** تحلیل کد برای شناسایی آسیب‌پذیری‌ها
* **Dynamic Analysis:** تست امنیتی زمان اجرا
* استفاده از ابزارهای امنیتی برای اسکن و تست آسیب‌پذیری‌ها

**فصل 8: امنیت در فریم‌ورک‌ها و کتابخانه‌های جاوا**

* ایمن‌سازی فریم‌ورک‌های وب مانند Spring و Hibernate
* امنیت در APIها و سرویس‌های RESTful
* استفاده از کتابخانه‌های ایمن برای رمزنگاری و احراز هویت
* بررسی ابزارهای امنیتی در محیط جاوا (مانند OWASP Dependency-Check)

**فصل 9: بهترین شیوه‌ها و توصیه‌های امنیتی برای توسعه‌دهندگان جاوا**

* اصول برنامه‌نویسی امن
* نحوه برخورد با خطاها و استثناها در امنیت نرم‌افزار
* مدیریت امنیت در چرخه حیات نرم‌افزار
* آموزش و آگاهی‌رسانی به تیم‌های توسعه

**فصل 10: جمع‌بندی و آینده امنیت نرم‌افزار در جاوا**

* روندهای جدید در امنیت نرم‌افزار
* تکنیک‌ها و ابزارهای آینده‌نگر در امنیت نرم‌افزارهای جاوا
* چالش‌ها و فرصت‌ها در امنیت نرم‌افزارهای پیچیده و مقیاس‌پذیر

این سرفصل‌ها به شما کمک می‌کنند تا کتابی جامع در حوزه امنیت نرم‌افزار با تمرکز بر جاوا بنویسید. اگر نیاز به جزئیات بیشتر یا تغییرات در بخش‌ها دارید، می‌توانیم آن‌ها را اضافه یا اصلاح کنیم!