1. 推荐的防御SQL注入的最佳方式是

A. 限制外部输入的长度

B. 使用存储过程

C. 使用预编译语句--java.sql.PreparedStatement

D. 对外部输入进行转义

2. 下列错误使用异常的做法是

A. 在程序中使用异常处理还是使用错误返回码处理，根据是否有利于程序结构来确定，并且异常和错误码不应该混合使用，推荐使用异常

B. 一个方法不应抛出太多类型的异常。throws/exception子句标明的异常最好不要超过三个

C. 异常捕获尽量不要直接 catch (Exception ex)，应该把异常细分处理

D. 程序内抛出的异常本身就可说明异常的类型、抛出条件，可不填写详细的描述信息。捕获异常后用exception.toString()取到详细信息后保存

3. 下面说法或者语句不符合公司编程规范的排版要求的是

A. 逗号、分号只在后面加空格; 比较操作符, 赋值操作符"="、 "+="，算术操作符"+"、"%"，逻辑操作符"&&"、"&"，位域操作符"<<"、"^"等双目操作符的前后加空格; "!"、"~"、"++"、"--"、"&"（地址运算符）等单目操作符前后不加空格

B. 如果语句已足够清晰则括号内侧(即左括号后面和右括号前面)不需要加空格，多重括号间不必加空格，因为在Java语言中括号已是最清晰的标志了

C. 较长的语句、表达式或参数（>80字符）要分成多行书写，长表达式要在低优先级操作符处划分新行，操作符放在新行之首，划分出的新行要进行适当的缩进，使排版整齐，语句可读

D. if, for, do, while等语句的执行语句如果只有一行的话，不需要要加括号{}

4. JAAS授权类中，不包含以下哪一类

A. Policy

B. AuthPermission

C. PrivateCredentialPermission

D. LoginContext

5. 一段使用ZipInputStream对压缩文件进行解压的代码，在[1]处填入适合的关键字是

public RandomAccessFile openFile(java.io.File f) {

[1] java.io.File copy = new java.io.File(f.getPath());

askUserPermission(copy.getPath());

// ...

return (RandomAccessFile)AccessController.doPrivileged(new PrivilegedAction

A. final

B. static

C. volatile

D. private

6. 对于下面的代码片段，假设PasswordManager的实例可以被非信任代码所访问，且changePassword()方法调用属于敏感操作，则下列说法中不正确是的

public class PasswordManager

{

public final Object lock = new Object();

public void changePassword() throws FileNotFoundException

{

synchronized (lock)

{

// . . .

}

}

}

A. changePassword()方法中应该包含安全管理器检查，以确认调用代码是否具有该操作权限

B. 应该将lock成员变量的可见性声明为private

C. 可以省去changePassword()方法中的同步块，直接将changePassword()方法声明为synchronized修饰的同步方法

D. changePassword()方法不应该抛出FileNotFoundException异常

7. 下面哪个是推荐使用的对称密码算法

A. DES

B. AES

C. SHA

D. RSA

8. 若程序中需要获取操作系统登录用户名，应采取下列哪种方法来获取

A. 提示用户输入

B. 由环境变量获取:System.getenv("USER")

C. 由JVM属性获取:System.getProperty("user.name")

D. 启动程序的时候由程序参数传入

9. 关于线程以下说法错误的有

A. 新起一个线程，都要使用Thread.setName(“…”)设置线程名

B. 在JDK1.5或更新的版本中，若字符串拼接发生在单线程环境，使用StringBuffer

C. 对多线程访问的变量、方法，必须加锁保护，避免出现多线程并发访问引起的问题

D. 线程使用时，要在代码框架中使用线程池，避免创建不可复用的线程；禁止在循环中创建新线程，否则会引起JVM资源耗尽

10. 以下说法正确的是

A. 尽量使用Java 5.0新循环写法

B. 判断一个变量是否等于null、或者一个常量，应把变量放在操作符的左边

C. 方法参数不能超过7个

D. 用“==”比较两个字符串内容相等

11. 关于命名规范，以下说法错误的有

A. 属性名使用意义完整的英文描述，第一个单词的字母使用小写，剩余单词首字母大写其余字母小写的大小写混合法。属性名不能与方法名相同

B. 方法名使用类意义完整的英文描述：第一个单词的字母使用小写、剩余单词首字母大写其余字母小写的大小写混合法

C. 方法中，存取属性的方法采用setter 和 getter方法，动作方法采用动词和动宾结构

D. 常量名使用全大写的英文描述，英文单词之间用下划线分隔开，并且使用 static 修饰

12. 下列JDK中的API调用中若使用不当易遭致OS命令注入的是

A. java.lang.System.load()

B. java.lang.Runtime.exec()

C. java.lang.Thread.start()

D. java.lang.Process.waitFor()

13. 安全编程规范中，下面说法错误的是

A. 对外部输入进行校验

B. 禁止不受信任的代码直接终止JVM

C. 创建文件时指定合理的访问权限

D. 记录日志时可以抛异常

14. 下列不符合编码规范的是

A. 数据库、IO操作等需要使用结束close()的对象必须在try-catch-finally 的finally中close()

B. 数组声明的时候使用 int[] index ，而不要使用 int index[]

C. 所有的类必须重载toString()方法，返回该类有意义的内容

D. 自己抛出的异常必须要填写详细的描述信息

15. 如下描述不正确的是

A. 除了构建器外，不要使用和类名相同的方法名

B. 使用 equals() 比较两个类的值是否相同

C. 不要使用嵌套赋值，即在一个表达式中使用多个 =

D. 重载 equals() 方法时，不必要重载 hashCode() 方法

16. 以下说法正确的有

A. 程序中的一些状态多直接用数字表示，如函数执行成功return 1

B. 对于表示函数执行错误，多用约定的错误码来标识

C. 用有意义的静态变量或者枚举来代替数字型的程序状态，如函数执行成功return SUCCESS

D. 程序中的魔鬼数字并不可怕，需要所有开发人员努力理解这些数字的含义

17. 对于注释的描述错误的是

A. 公有和保护方法注释内容：列出方法的一句话功能简述、功能详细描述、输入参数、输出参数、返回值、异常等

B. 对重载父类的方法必须进行@Override声明

C. 对关键变量的定义必须编写注释，分支语句（条件分支、循环语句等），可以根据实际情况，可以增加注释，也可以不加，根据注释量确定

D. 对于方法内部用throw语句抛出的异常，必须在方法的注释中标明，对于所调用的其他方法所抛出的异常，选择主要的在注释中说明。 对于非RuntimeException，即throws子句声明会抛出的异常，必须在方法的注释中标明

18. 如下关于集合类的描述错误的是

A. 含有集合意义的属性命名，尽量包含其复数的意义

B. 集合中的数据不需要释放，垃圾回收器会自动回收

C. 集合必须指定模板类型

D. 使用集合类时要设置初始化容量

19. 下列哪个场景可以使用java.util.Random类产生的随机数

A. 挑战算法中的随机数生成

B. 验证码的随机数生成

C. 随机选取路由

D. Web应用会话标识符

20. 在下列哪个场景中，不需要加密和数字签名机制保证数据安全

A. 序列化传输敏感数据

B. 无SSL传输通道或者代价太高

C. 敏感数据需要持久化长久保存

D. 同一信任域内组件间传递

21. 当与非信任代码（非产品包中的代码）交互时，说法正确是

A. 通过硬编码方式（即不通过参数输入数据）或者是在进行特权操作之前进行输入数据校验

B. 先对不受信任的对象或者参数做防御性拷贝，建议使用clone()方法进行拷贝

C. 敏感操作必须由 SecurityManager来检查控制

D. 对敏感数据访问的接口需要控制访问权限

22. 下列说法描述正确的是

A. public方法参数的合法性检查应由方法本身负责，每一个public方法必须保证自己的健壮性

B. 调用方法获取返回结果后必须进行有效性校验，以确保后续代码在运行过程中不会抛出异常或产生逻辑错误

C. 访问数组、List等容器内的元素时，必须首先检查下标是否越界，杜绝下标越界异常的发生

D. 对于if ? else if ?(后续可能有多个else if …)这种类型的条件判断，最后必须包含一个else分支，避免出现分支遗漏造成错误；每个switch-case语句都必须保证有default，避免出现分支遗漏，造成错误

23. 关于异常，以下说法正确的有

A. 运行时异常使用RuntimeException的子类来表示，不用在可能抛出异常的方法声明上加throws子句

B. 运行时异常使用RuntimeException的子类来表示，必须在可能抛出异常的方法声明上加throws子句

C. 非运行期异常是从Exception继承而来的，必须在方法声明上加throws子句

D. 非运行期异常是从Exception继承而来的，不需要在方法声明上加throws子句

24. 以下哪些方式是被禁止的

A. ${JDK\_PATH}/bin/java -agentlib:libname=options ApplicationName

B. ${JDK\_PATH}/bin/java -agentlib:libname=options -Djava.security.manager ApplicationName

C. ${JDK\_PATH}/bin/Java -Dcom.sun.management.jmxremote.port=8000 ApplicationName

D. ${JDK\_PATH}/bin/java -Djava.security.manager ApplicationName

25. 当外部输入用于以下哪些场景的情况下需要进行合法性验证

A. 输入改变系统状态

B. 输入作为数组下标

C. 输入作为格式化字符串

D. 输入作为内存分配的尺寸参数

26. 以下哪些场景可能会导致攻击者绕过安全检查

A. 只检查当前调用者

B. 检查整个调用栈

C. Java applets 允许给自己授权执行任意代码

D. 覆写安全检查执行的方法

27. 下列关于编码相关说法，错误的是

A. 在连接数据库的时候，可以将连接字符串硬编码在程序中

B. 连接字符串中的敏感信息，如口令、初始密钥等需要加密保存

C. 程序中一些没有用到的变量或者值因为它们不影响程序的正常逻辑功能，可以不用删除

D. 程序中一些即使执行也不会产生任何效果的代码因为他们不影响程序的正常逻辑功能，可以不用删除

28. 为防止敏感数据传输过程中被窃听和非法篡改。在以下哪些场景中，需要加密和数字签名的机制保证数据安全

A. 序列化或传输敏感数据

B. 无SSL传输通道或者代价太高

C. 敏感数据需要长久保存

D. 安全通过传输（如HTTPS、SSL）

29. 关于局部变量说法，符合编程规范的说法是

A. 不要定义不会被用到的局部变量，类私有属性，类私有方法和方法参数

B. 几乎每一个局部变量的声明都应该包含一个初始化表达式

C. 变量定义的“就近原则”

D. 属性名可以和公有方法参数相同，也可以和局部变量相同

30. 下面关于存取控制符号的描述，符合编程规范的有

A. 只是该类内部调用的函数使用 private 属性

B. 继承类可以使用的使用protected属性

C. 对外公开的函数使用public属性

D. 类的成员变量的尽量采用protected修饰，其他类可以通过类的成员方法来访问和修改变量

31. 如下哪些地方应该加上空行

A. import语句与类定义之间

B. 注释与其上面的无关的代码之间

C. 注释和被注释的代码之间

D. 变量说明之后

32. 目录遍历攻击可以直接带来哪些危害

A. 攻击者可以访问受限目录和文件

B. 攻击者可以改变程序的运行逻辑

C. 攻击者可以执行恶意的命令或程序

D. 攻击者以窃取内存中数据

33. 安全规范中，如下描述正确的有

A. Web Service接口（包含RESTfulWeb Service）的调用必须进行认证，同时对提交的数据进行输入校验，涉及传递敏感数据时，必须保障其机密性

B. Web Service调用不需要进行日志记录

C. DWR接口的调用必须进行认证，同时对提交的数据进行输入校验

D. DWR调试功能需要关闭

34. 循环嵌套的时候，下面哪些情况需要尽量避免

A. 实例化对象

B. try/catch

C. 开启IO

D. 连接数据库

35. 以下说法正确的有

A. 一个系统或者模块应该统一规划异常类型和返回码的含义

B. 异常的处理效率比条件分支低

C. 异常的跳转流程难以预测

D. 系统非正常运行产生的异常捕获后，如果不对该异常进行处理，则应该记录日志

36. 下述排版代码中，符合编码规范的是

A. if (i>j) doStart();

B. Object o = new Object(); Object b = null;

C. 类定义 { 类的公有属性定义 类的保护属性定义 类的私有属性定义 类的公有方法定义 类的保护方法定义 类的私有方法定义 }

D. typeCounter \*= 2;

37. 下列关于类和接口的注释，正确的说法有

A. 放在class或者interface关键字之前

B. 放在import关键字之后

C. 注释主要是一句话功能简述与功能详细描述

D. 类注释使用“/\*\*\*\*/”注释方式

38. 如下类名符合公司规范的有

A. FtpDownload\_Util

B. DEBUGLOG

C. OrderResponse

D. UserManager

39. 对于文件IO操作，下列哪些说法是正确的

A. 临时文件使用完毕应该及时删除

B. 禁止在单个输入流上创建多份buffered wrapper

C. 避免在共享目录操作文件

D. 创建文件时指定合理的访问权限

40. 下列异常中，哪些易引起信息泄露从而给攻击者攻击系统提供帮助

A. java.io.FileNotFoundException

B. java.sql.SQLException

C. java.net.BindException

D. java.lang.OutOfMemoryError

41. 敏感对象发送出信任域前应该先加密然后再签名

正确

错误

42. 应明确规定对接口方法参数的合法性检查应由方法的调用者负责还是由接口方法本身负责，缺省是由方法调用者负责

正确

错误

43. 不要使用循环将集合转为数组，可以使用集合的toArray()方法

正确

错误

44. 带有敏感数据的表单必须使用 HTTP-GET 方法提交

正确

错误

45. 不能直接将来自不可信源的字符串作为格式化字符串的一部分

正确

错误

46. 对于JSP语言，所有servlet必须进行静态映射，不允许通过绝对路径访问

正确

错误

47. 对外部字符串输入做校验之前需要先对其进行归一化，推荐使用的归一化格式是NFKC

正确

错误

48. 异常中的文本描述信息可能会产生信息泄露，异常本身的类型信息也可能会导致信息泄露

正确

错误

49. interface 中定义的常量不要写public、static、final的修饰词，方法需要写public修饰词

正确

错误

50. 代码提交前，需要消除相应的错误、告警，并将findbug清零

正确

错误

51. 一个文件不要定义两个类(并非指内部类)

正确

错误

52. 安全编程规范中，所有安全相关的敏感代码不应该放在一个jar包中

正确

错误

53. 在对外部输入进行校验过滤时，在“白名单”与“黑名单”两种方式中应该优先考虑选用“黑名单”方式

正确

错误

54. 类属性和类方法可以交叉放置

正确

错误

55. 判断语句可以使用”\* == true”来判断为真

正确

错误

56. 实现Serializable接口的可序列化类应该显式private static final声明 serialVersionUID

正确

错误

57. 对于switch语句下的case语句，必须在每个case分支结束前加上break语句

正确

错误

58. 将字符串转换为数字时必须处理NumberFormatException异常

正确

错误

59. 对于java.io.FileNotFoundException异常，捕获并抛出另一种非敏感类型的异常再抛出到信任边界之外

正确

错误

60. 由于序列化将对象输出为二进制数据流而非可读的明文形式，所以在传输或保存序列化的敏感数据时不需要加密

正确

错误