一、单选(共35题，每题2.0分)

以下关于信息劫持与泄露，描述不正确的是（）

A. 使用pendingIntent时候，如果使用了一个空Intent，会导致恶意用户劫持Intent的内容。

B. 针对PendingIntent误用风险，应禁止使用空intent去构造pendingIntent，且构造PendingIntent的Intent一定要设置ComponentName或者action；

C. APP创建Intent传递数据到其他Activity，如果创建的Activity不是在同一个Task中打开，就很可能被其他的Activity劫持读取到Intent内容，跨Task的Activity通过Intent传递敏感信息是不安全的。

D. 针对Intent敏感数据泄露风险，应使用包含FLAG\_ACTIVITY\_NEW\_TASK标志的Intent来传递敏感信息。

STRUTS2开启开发者模式，可造成（）

A. SQL注入

B. 跨站攻击伪造

C. 查看和调用系统提供的所有DWR接

D. 将导致严重远程代码执行漏洞。如果WebService启动权限为最高权限时，可远程执行任意命令，包括关机、建立新用户、以及删除服务器上所有文件等等。

以下关于FASTJSON命令执行漏洞，描述不正确的是（）

A. fastjson在1.2.24及之前版本存在远程代码执行高危安全漏洞。攻击者可以通过此漏洞远程执行恶意代码来入侵服务器;

B. 需要升级到1.2.24以后的版本；

C. 升级到1.2.28/1.2.29或者更新版本来保证系统安全；

D. 大于1.2.24但是小于1.2.28的版本虽然为fastjson的过渡版本，但是不受此漏洞影响，但是还是建议直接升级到官网最新版本；

下列关于MD5加密说法不正确的是（）

A. MD5以512位分组来处理输入的信息，且每一分组又被划分为16个32位子分组，经过了一系列的处理后，算法的输出由四个32位分组组成，将这四个32位分组级联后将生成一个128位散列值。

B. MD5是不可以逆向破解的

C. 敏感信息使用MD5加密后存放数据库中，即使用户得到密文也无法还原出明文

D. 可以使用加“salt”的方式来防止类似彩虹表之类的破解

Service作为组成Apk的四个组件之一，一般作为后台运行的服务进程，如果设置了导出权限，可能被系统或者第三方的App直接调出并使用。Service导出可能导致拒绝服务攻击，程序功能被第三方恶意调用等风险。。因此我们需要做正确的安全配置，以下说法不正确的是（）

A. 如果组件不需要与其他app共享数据或交互，请将AndroidManifest.xml 配置文件中设置该组件为exported = “False”

B. 如果组件必须要提供给外部应用使用，建议对组件进行权限控制

C. 检测到Service无intent-filter标签，则其属性默认为false

D. 若Service有intent-filter标签，且需将android:exported属性设置为true;

对特殊字符进行过滤是防护XSS攻击的常用方式，那么我们要对以下哪些对象做防护过滤（）

A. Get参数

B. POST参数

C. 消息头参数

D. 以上都是

War、bak等一些与应用正常运行无关的文件放在web目录下面，可造成什么风险（）

A. 源码、配置文件等信息泄露

B. SQL注入

C. 文件上传漏洞

D. XML注入

如下攻击报文获取到passwd文件： <?xml version="1.0"?><!DOCTYPE foo [<!ENTITY test SYSTEM "file:///etc/passwd"> ]><Function name="findByOrgTmpXml" serviceName="com.zterc.uos.oaas.service.postmanager.PositionManagerWeb" userTransaction="false" generatedTime="2018-06-27 12:25:13"><Param type="s">&test;</Param></Function> 则这里存在什么漏洞（）

A. XML注入

B. XXE

C. 任意文件读取漏洞

D. 任意文件下载漏洞

关于XSS的正确防御，针对“URL中输出”的场景，应采用什么办法（）

A. 对变量使用html编码

B. 对变量使用javascript编码

C. 对变量使用url编码

D. 先检查变量是否以http开头，如果不是则自动添加，然后再对变量进行URLencode

在“智能营销助手”的场景中，点击“推荐”按钮可给对应用户发送推荐信息，截取该请求报文，发现某参数值为“尊敬的客户：点击http://a.10086.cn下载MM商城客户端。安全免费的应用、游戏，在线听歌、看书，精彩无限，马上体验吧！中国移动”，则该场景可能存在什么漏洞（）

A. 对任意用户形成短信轰炸

B. 对任意用户形成任意内容的短信轰炸

C. 可加载电话号码字典对批量用户发送任意内容的短信

D. 以上都是

为了保证系统日志可靠有效，以下哪一项不是日志必须具备的特征（）

A. 统一而精确的时间

B. 全面覆盖系统资产

C. 包括访问源、访问目标和访问活动等重要信息

D. 可以让系统的所有用户方便的读取

查看个人信息的请求http://10.46.34.230/bop/userinfo.jsp?userid=1001331，将userid改为1001332发现可以返回他人信息，并且报文中包含密码字段的信息，以下描述不正确的是（）

A. 存在水平越权漏洞

B. 可以遍历任意人的资料，包括密码

C. 密码字段在界面上做模糊化处理可以解决“遍历任意人密码”漏洞

D. 存在敏感信息泄露漏洞，因禁止将无关的敏感字段返回给前端

以下关于文件上传漏洞攻击描述正确的是（）

A. 上传的文件能够被web容器解析执行

B. 用户能够从web上访问该文件

C. 如果容器存在解析漏洞，则应用程序的防护过滤策略可能被绕过

D. 以上描述都正确

以下哪项是防御 “多步骤越权”攻击的最大误区（）

A. 不可预测性原则可以有效抵御多步骤越权攻击

B. 任何在客户端执行但服务器并不采用的控件均可以被避开

C. 可以通过客户端控件来实行有效的访问控制

D. 任何到达验证过程后续阶段的用户一定已经拥有相关权限，因为前面阶段已经验证了这些权限

如下配置会引发什么漏洞（） <servlet> <servlet-name>dwr-invoker</servlet-name> <servlet-class>uk.ltd.getahead.dwr.DWRServlet</servlet-class > <init-param> <param-name>debug</param-name> <param-value>true</param- value> </init-param> <load-on-startup>100</load-on-startup> </servlet>

A. DWR接口泄露

B. 目录遍历

C. struts2开启开发者模式

D. host head attack

以下哪个选项属于垂直越权（）

A. 某系统只有超级管理员才拥有“用户管理”权限，一普通用户登录后可通过直接访问usermanage.jsp链接进行用户管理操作

B. 一学籍系统，某学生登录后可以通过修改userid，获取其他同学的学籍信息

C. 在多步骤重置密码的步骤中，出现逻辑断层，在最后步骤通过篡改username重置任意人密码

D. 某重要信息，下载重要文件需要短信验证码，但是短信验证码属于异步校验，导致短信验证码校验可被绕过

在“智能营销助手”的场景中，点击“推荐”按钮可给对应用户发送推荐信息，截取该请求报文，发现某参数值为“尊敬的客户：点击http://a.10086.cn下载MM商城客户端。安全免费的应用、游戏，在线听歌、看书，精彩无限，马上体验吧！中国移动”，为了避免出现短信内容被篡改，以下防御方法正确的是（）

A. 增加无缺陷的图形验证码

B. 增加频率限制

C. 通过传递应用场景ID值，从数据库中捞出对应的短信内容进行发送

D. 前端做禁止编辑限制

下列关于日志记录，说法不正确的是（）

A. 业务系统日常正常登陆后的日志应包含准确的账户登陆与退出时间、账户登陆的IP、账户登陆的类型、账户登陆后的操作信息、账户登陆的方式以及涉及其他数据安全相关的访问记录。

B. 用户访问日志和系统错误日志可以一起记录并存储

C. 系统应用操作日志应详细记录操作的详细内容。系统自身检测到时攻击的日志需单独记录

D. 日志信息存储于文件中时，应对该文件权限进行安全策略的控制，涉及到敏感信息需要进行模糊化

为了防止文件上传漏洞，某系统在服务端使用白名单做了文件扩展名校验，但是攻击者发现直接上传test.jsp.jpg，被服务端重命名为test\_20180818086701.jsp，则以下关于该漏洞描述不正确的是（）

A. 重命名过程中带入了用户可控参数test

B. 服务端的文件扩展名白名单校验，是选择最后一个点号的后缀

C. 服务端重命名时，文件扩展名是选择第一个点号的作为后缀

D. 文件进行完全随机的重命名不带入用户可控参数可以解决文件上传漏洞。

SQL注入的本质描述最正确的一项是（）

A. 数据库版本太低

B. 未对尖括号进行过滤

C. 用户的输入直接进行拼接变成代码的一部分执行，违反数据与代码分离原则

D. 未对换行字符进行过滤

http://10.1.0.217:3033/BossWeb/aop/opr\_portal/common/file\_down\_full\_path.jsp?full\_path=/bossapp1/webapp/BossWeb.war/aop/opr\_portal/file/temp\_file/temp\_file\_20160913040536\_1.xls&nick\_name=test.xls，无需进一步测试，可以判断该链接有什么漏洞（）

A. 任意文件下载

B. 物理路径泄露

C. 路径遍历

D. 文件上传漏洞

关于以下代码的描述，正确的是（） string name = request.getParameter("name"); if (null != name) name = name.replaceAll("<script>", ""); … out.println(name);

A. 由于对<SCRIPT>进行了过滤，所以不存在安全漏洞

B. 构造name的值为<sc<script>ript>alert(2222）</script>，就会发生XSS攻击

C. 对输入进行过滤是防御XSS的一种方式，因此对<SCRIPT>进行过滤虽不是最佳方式，但也可行

D. 应该对<script>使用转义更好

以下关于XSS防御描述最正确的是（）

A. 对输入进行格式化检查

B. 在客户端与服务端均进行输入过滤

C. 选择一种编码进行输出转义

D. 对不同的的发生场景使用不同的编码处理

以下哪个选项与短信/邮箱凭证泄露无关（）

A. 凭证本地生成

B. 凭证本地校验

C. 凭证服务端校验，但在获取凭证时将凭证返回到前端

D. 凭证无错误尝试次数限制

下面关于跨站与跨站请求伪造描述正确的是（）

A. 两者都是针对服务端的攻击

B. 前者是对服务端的攻击，后者是对前端的攻击

C. 前者是发生在前端输出的时候，后者是发生在更改服务端数据的时候

D. 两者都是XSS攻击

凭证校验若存在逻辑漏洞，会导致攻击者不需要正确凭证甚至不需要输入凭证，直接打破系统的认证逻辑，以下哪种是属于这类攻击（）

A. 未做凭证和账号的匹配校验

B. 多步骤绕过，如篡改服务端的响应结果使客户端进入下一步

C. 多步骤绕过，如直接操控后续步骤或最后一个步骤的报文

D. 以上都是

消息头注入是指（）

A. 在重定向或生成cookie等基于外部传入的参数输出到HTTP响应头时所产生的安全隐患。

B. LDAP注入

C. XML注入

D. SQL盲注

在“密码修改”的场景，如果旧密码校验使用异步提交，将造成（）

A. 旧密码校验被绕过，可能存在修改任意人密码的风险

B. 通过删除旧密码参数名与参数值，绕过校验

C. 跨站请求伪造攻击

D. 密码泄露

以下代码存在什么漏洞（） PrintWriter pw = new PrintWriter(new BufferedWriter(new FileWriter( request.getRealPath("/")+getFIlename(request)))); ServletInputStream in = request.getInputStream(); int i = in.read(); while (i != -1) { pw.print((char) i); i = in.read(); } pw.close();

A. 任意文件下载

B. 文件包含

C. 命令注入

D. 文件上传漏洞

对输入字符进行过滤防止XSS的一种解决办法，那么一级过滤至少要过滤哪些字符（）

A. & < > ( ) ;

B. < > ’ ” \ ;

C. < > ’ ( )

D. ” ’ + / ( )

Web系统，在登录、修改密码、重置密码等场景中做强密码校验可以避免系统引入弱密码，以下所述的密码强度最保险的是（）

A. 字母与数字的组合

B. 至少8位，且要包含字母与数字组合

C. 大写、小写、数字的组合

D. 至少8位，且必须包含大写、小写、数字

消息头注入发生在（）

A. 外部传入的参数在HTTP响应头输出

B. 登录

C. 注销

D. 获取客户端IP

当服务器设置cookie 时，secure标签的意义是（）

A. secure 标签用于向浏览器发出以下指示：只应通过HTTPS 连接、绝不能通过未加密的 HTTP连接重新提交cookie。

B. secure标签用于向浏览器发出以下指示：可通过HTTPS 连接或 HTTP 连接重新提交 cookie。

C. secure标签用于向浏览器发出以下指示：只应通过HTTP连接重新提交 cookie。

D. 无特殊意义

以下关于撞库的防护，不正确的是（）

A. 只要同一账号连续输错5次密码就进行锁定，即可以防御撞库攻击

B. 无缺陷的图形验证码可作为防撞库攻击的重要辅助手段

C. 重要的系统，还需要采用多重验证，如增加短信验证码

D. 账号枚举会极大降低撞库的攻击成本

以下代码存在什么漏洞（） String path = request.getParameter("path"); java.io.OutputStream os = response.getOutputStream(); java.io.FileInputStream fis = new java.io.FileInputStream(path); byte[] b = new byte[1024]; int i = 0; while ((i = fis.read（）) > 0 ){ os.write(b, 0, i); } fis.close(); os.flush(); os.close();

A. 任意文件下载

B. 文件包含

C. 命令注入

D. 文件上传漏洞

二、多选(共10题，每题3.0分)

以下关于Content Provider目录遍历描述正确的是（ABCD）

A. 该漏洞由于Content Provider组件暴露，没有对Content Provider组件访问权限进行限制且对Uri路径没有进行过滤，攻击者通过Content Provider实现的OpenFile接口进行攻击，如通过”../”的方式访问任意的目录文件，造成隐私泄露；

B. 如果必须给合作方的APP提供Provider的访问权限，而合作方的APP签名证书又于自己公司的不同，可将合作方的APP的签名哈希值预埋在提供Provider的APP中，提供Provider的APP要检查请求访问此Provider的APP的签名，签名匹配通过才让访问。

C. 公开的content provider确保不存储敏感数据，并去除没有必要的openFile()接口；

D. 过滤限制跨域访问，对访问的目标文件的Uri进行有效判断（使用Uri.decode()先对Content Query Uri进行解码后，再过滤如可通过“../”实现任意可读文件的访问的Uri字符串）；

我们可以从以下哪几个方面来加固中间件控制台（ABC）

A. 禁止使用默认密码，设置强密码

B. 移除中间件控制台

C. 移除docs、examples、首页等与应用正常运行无关的界面

D. 根据最小化原则，通过本机的IPTABLE做白名单限制

以下哪些信息是属于系统需要保护隐藏或移除，避免泄露信息泄露（ABD）

A. 源码

B. 数据库、系统错误信息

C. War等冗余文件

D. SQL语句

http://10.46.34.230/bop/getresouse.jsp?resouseid=187534&userid=1001331，这是某应用获取资源的请求链接，服务端会根据根据该链接中传递的resouseid 与userid 做权限判断并根据判断结果进行响应，则针对该防御方案以下说法不正确的是（ACD）

A. 服务端做了userid与resouseid权限匹配校验，因此不会产生资源越权访问

B. 将userid写在cookie中，将权限校验机制修改为“将cookie中的userid该链接传递过来的resouseid做权限匹配校验” ，才是安全的校验机制

C. 该场景中，如果userid是从会话中获取，则不会形成越权访问

D. 用户可以提交任意输入，通过篡改各种关键参数打破服务端权限校验机制，是常见的越权攻击手段。

以下关于账号枚举说法不正确的是（BCD）

A. 账号枚举，极大降低了暴力破解的成本

B. 由于图形验证码校验的存在，账号枚举不会形成风险

C. 由于账号/IP锁定机制的存在，账号枚举不会形成风险

D. 由于密码校验的存在，账号枚举不会形成风险

使用编码，是绕过XSS过滤器的常见攻击手法，以下哪些是XSS攻击中常见的编码（ABD）

A. URL编码

B. JS编码

C. Base64编码

D. HTML编码

以下关于日志的访问控制，描述正确的是（ABD）

A. 只有Web应用程序的管理员才能查询数据库表形式或文件形式的安全日志

B. 除数据库超级管理员外，只有应用程序连接数据库的帐号可以查询（select）及插入（insert）安全日志表

C. 除操作系统超级管理员外，只有应用程序的运行帐户才能读、写文件形式的安全日志（但不允许删除）

D. 禁止通过http可直接访问读取日志文件

以下配置不正确的是（）

A. struts.xml文件配置：<constant name="struts.devMode" value="true" />

B. dwr配置 <servlet> <servlet-name>dwr-invoker</servlet-name> <servlet-class>uk.ltd.getahead.dwr.DWRServlet</servlet-class > <init-param> <param-name>debug</param-name> <param-value>true</param- value> </init-param> <load-on-startup>100</load-on-startup> </servlet>

C. <init-param> <param-name>listings</param-name> <param-value>false</param-value> </init-param>

D. <security-constraint> <web-resource-collection> <url-pattern>/\*</url-pattern> <http-method>PUT</http-method> <http-method>DELETE</http-method> <http-method>HEAD</http-method> <http-method>TRACE</http-method> </web-resource-collection> <auth-constraint></auth-constraint> </security-constraint>

在“找回密码”的场景中，需要防范哪些漏洞（ACD）

A. 账号枚举

B. 账号密码明文传输

C. 重置任意人密码

D. 短信/邮箱炸弹

XSS可以划分为哪几种类型（ABD）

A. 反射型

B. 存储型

C. XXE

D. DOM