**2017年信息安全工程师考试下午试题加答案（五）**

新开的**信息安全工程师考试**分属该考试“信息系统”专业，位处中级资格。大家在找试题做练习的时候是否苦恼没有资源？希赛软考学院为大家整理了一些下午试题的练习，供大家参考，希望能有所帮助。

阅读下列说明，回答问题1至问题4，将解答填入答题纸的对应栏内。

【说明】

在Internet技术飞速演变、电子商务蓬勃发展的今天，开发的银多应用程序都是Web应用程序，随着微信、微博、网上银行等一系列的新型的Web应用程序的诞生，Web应用越来越广泛。然而Web应用程序及Web站点往往很容易遭受各种各样的入侵，Web数据在网络传输过程中也银容易被窃取或盗用。如何能够使Web及数据传输更加安全，就显得尤为重要。

如今，Web业务平台己经在电子商务、企业信息化中得到广泛应用，很多企业部将应用架设在Web平台上，Web业务的迅速发展也引起了黑客们的强烈关注，他们将注意力从以往对传统网络服务器的攻击逐步转移到了对Web业务的攻击上。黑客利用网站操作系统的漏洞和Web服务程序的SQL注入漏洞等得到Web服务器的控制权限，轻则篡改网页内容，重则窃取重要内部数据，更为严重的则是在网页中植入恶意代码，使得网站访问者受到侵害。

国际权威机构Forrester的统计数据表明，67%的攻击是通过应用层的攻击。即是，最简单的网页浏览也有可能造成威胁，比如，单击含有病毒的网址、隐秘的图片，或者，单击下载某些免费的软件、文件等，由于下载的软件或者文件中含有未知的恶意代码，当用户在运行程序或者打开这些文件时，恶意代码被启动就有可能造成用户个人信息丢失，甚至后台服务器系统出现漏洞给恶意攻击者窃取信息提供方便的大门。

【问题1】（5分）

开源Web应用安全项目（OWASP）是一个开放的社区组织。专注于讨论应用程序，代码开发的威胁讨论。TOP 10项目的目标是通过找出企业组织所面临的最严重的十大风险来提高人们对应用程序安全的关注度。以下是其中罗列的十大最有可能发生的应用漏洞，将选项A-J正确对应到其括号内。

1、注入（）

2、失效的身份认证和会话管理（）

3、跨站脚本（XSS）（）

4、不安全的直接对象引用（）

5、安全配置错误（）

6、敏感信息泄露（）

7、功能级访问控制缺失（）

8、跨站请求伪造（CSRF）（）

9、使用更含有已知漏洞的组件（）

10、未验证的重定向和转发（）

A、如果一个带有漏洞的组件被利用，这种攻击可以造成更为严重的数据丢失或服务器接管，在应用程序中使用会破坏应用程序防御系统。

B、攻击者可能会窃取或篡改这些弱保护的数据以进行信用卡诈骗、身份窃取，或其他犯罪。

C、Web应用程序经常将用户重定向和转发到其他网页和网站，并且利用不可信的数据去判定目的页面。

D、迫使登录用户的浏览器将伪造的HTTP请求，包括该用户的会话cookie和其他认证信息，发送到一个存在漏洞的Web应用程序。

E、应用程序需要在每个功能被访问时在服务器端执行相同的访问控制检查。如果请求没有被验证，攻击者能够伪造请求以在未经适当授权时访问功能。

F、好的安全需要对应用程序、框架、应用程序服务器、Web服务器、数据库服务器和平台定义和执行安全配置。

G、攻击者通过在应用程序预先定义好的查询语句结尾加上额外的查询语句元素，欺骗数据库服务器执行非授权的任意查询。

H、攻击者通过在这种链接中插入恶意代码，当用户不小心单击这样带有恶意代码的链接时，其用户信息就有可能被攻击者盗取。

I、用户使用公共计算机浏览网站，登录验证身份之后，离开时没有退出账户而是选择直接关闭浏览器，使得下一个用户使用相同计算机浏览相同浏览器，可以看到上一个用户的对话。

J、作为授权的系统用户，攻击者只需要修改指向一个系统对象的直接引用参数值，让其指向另一个无权的对象。

【问题2】（2分）

SQL注入攻击有4个基本的特点：A、局限性，B、隐蔽性，C、攻击时间短，D、危害大。其中哪个错误的？（1分）应该是什么？（1分）

【问题3】（3分）

SQL注入攻击的危害性很大，应该从哪些方面来避免这种漏洞攻击？

【问题4】（5分）

如何防范跨站脚本（XSS）？（3分）如何防范跨站请求伪造（CSRF）？（2分）

**参考答案**

【问题1】

1.g

2.i

3.h

4.j

5.f

6.b

7.e

8.d

9.a

10.c

【问题2】

a错误，应该是广泛性

【问题3】

1.对任何输入信息进行详细的验证

2.严格控制数据库访问权限

【问题4】

1. 服务器设置，包括硬盘权限设置、组件安全、iis用户、服务器安全和性能、本地安全策略和系统服务的设置。

2、禁用guests组调用cmd.exe