2024年上海市高等学校信息技术水平考试试卷

四级 网络信息安全（A 场）

（本试卷考试时间 150 分钟）

一、单选题（ 本大题 15 道小题 ，每小题 1 分，共 15 分），从下面题目给出的A、B、C、D四个可供选择的答案中选择一个正确答案。

1.网络运营者违反网络安全法第二十四条第一款规定，未要求用户提供真实身份信息，或者对不提供真实身份信息的用户提供相关服务的，由有关主管部门责令改正；拒不改正或者情节严重的，处（）罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

A.一万元以上五万元以下

B.一万元以上十万元以下

C.一万元以上十五万元以下

D.五万元以上五十万元以下

2.A类私有IP地址10.172.16.211，子网掩码是255.255.192.0，使用无分类域间路由（CIDR）划分子网，请确定该IP地址所在子网有多少个主机IP地址？

A.4

B.8

C.512

D.1024

3.某网站攻击者在参数中输入了'id=1' and ExtractValue(1,concat(0x7e,database()))-- 后服务器返回错误信息：XPATH syntax error:'~database_name'.该网站受到了什么类型的攻击？

A.布尔型盲注攻击

B.时间型盲注攻击

C.堆栈查询注入攻击

D.报错注入攻击

4.区块链的去中心化特性主要通过（）实现。

A.所有数据存储在一个服务器上

B.数据由多个节点共同维护

C.数据存储在云服务器上

D.数据无法被加密

5.非对称加密算法中，用于加密的密钥是？

A.公钥

B.私钥

C.对称密钥

D.会话密钥

6.以下哪个工具软件不是用于密码破解的？
A.JohntheRipper
B.Hashcat
C.Wireshark
D.Hydra

7.SQLmap 主要用于以下哪个方面？
A.网络扫描
B.数据库渗透测试
C.无线网络渗透测试
D.代理拦截

8.以下哪个不是逻辑漏洞的防御策略？
A.输入验证
B.随机化鉴权 ID
C.权限控制
D.加密存储

9.逻辑漏洞的修复通常需要以下哪个步骤？
A.漏洞报告
B.代码重构
C.系统升级
D.安全培训

10.为方便距离较远的两个机构通过互联网安全地传输数据，需要在互联网上为两个机构的私有网络提供安全通信通道，通过加密通道保证连接的安全，IPSec 协议是实现这一需求的成熟协议。IPSec 协议中的隧道模式具体使用以下哪种技术实现相关功能？
A.包封装
B.单点登录 SSO
C.负载均衡
D.流量识别

11.在信息化办公中通常涉及众多信息系统，每个信息系统都有身份管理体系，包括用户账户、认证、权限等，用于系统用户的安全接入。为方便用户日常办公的便捷性，通常需要进行身份管理的统一化，由此提出了“4A”的概念，以下哪种是“4A”技术之一？
A.集中修改
B.集中删除
C.集中账号
D.集中保存

12.下列哪个不属于 XSS 攻击类型？（XSS 又为跨站脚本攻击，攻击者将恶意脚本注入到其他用户会浏览的页面，脚本会导致用户的身份信息如 cookie 被攻击者窃取，攻击者可以伪装成用户的身份进行登录）
A.反射型 XSS（黑客输入恶意脚本数据被立即反射回浏览器）

B. 存储型 XSS（黑客输入的数据被存储在目标服务器上）
C. DOM 型 XSS（黑客通过修改 DOM 元素来注入恶意脚本）
D. 延时型 XSS

13. Linux 操作系统中，哪个命令可以用于修改文件或目录的权限？
A. chmod
B. chown
C. useradd
D. passwd

14. 下一代防火墙（NGFW）不包含的功能特性是？
A. 集成入侵防御系统
B. 恶意软件检测
C. 资产测绘
D. 应用程序控制

15. 文件上传漏洞成因不包括以下哪个？
A. 服务器配置不当
B. 开放了文件上传功能，并进行严格限制
C. 系统特性、验证或者过滤不严格
D. web 用户对目标目录有可写权限甚至执行权限

二、多选题（本大题 10 道小题，每小题 2 分，共 20 分），从下面题目给出的 A、B、C、D 四个可供选择的答案中选择所有正确答案。

1. FE70:0000:0000:BBBB:0000:0000:0000:0001 是一个合法的 IPv6 地址，可以缩写成以下哪种？
A. FE70::BBBB:0:0:0:1
B. FE70::BBBB::0001
C. FE70:0:0:BBBB::1
D. FE70::BBBB::1

2. 防御 SqL 注入可以采用以下哪些方法？
A. 使用预编译语句
B. 使用安全的存储过程
C. 参数校验过滤
D. 使用安全函数

3. 在云存储安全中，以下哪些是常见的安全威胁？
A. 数据泄露
B. 数据篡改
C. 数据丢失
D. 非法访问

4. 以下哪些算法可以用于密钥交换？

A. Diffie-Hellman
B. RSA
C. ECC
D. SHA-1

5. 中钓鱼邮件后可能有哪些危害？
A. 信息泄露
B. 木马控制
C. 数据勒索
D. 成为跳板机

6. 为了应对超大数据规模带来的开发使用及安全保障等方面的挑战，国家提出健全完善数据分类分级保护制度的要求。以下哪几种属于 GB/T 43697-2024《数据安全技术 数据分类分级规则》中划分的数据级别？
A. 一般数据
B. 关键数据
C. 核心数据
D. 重要数据

7. 请指出下列哪些原因可能导致计算机蓝屏故障？
A. 软件不正确更新
B. 软件运行错误
C. cpu、内存故障
D. 永恒之蓝病毒攻击

8. 目前常见的针对网站的攻击包括哪些？
A. 跨站攻击（攻击者将恶意脚本注入到其他用户会浏览的页面中）
B. SQL 注入（攻击者通过构造特定的 SQL 语句来达到非授权的操作，如非法查询数据）
C. 客户端木马（攻击者控制服务器所需要的代码文件）
D. 网络抓包窃取（攻击者监听网络信息，通过抓包获取用户的敏感信息，如账号密码等）

9. 下列哪些属于弱密码？
A. admin
B. 88888888
C. 123xyz
D. QY19#rh8!09

10. 在文件上传漏洞的利用过程中，攻击者可能采取哪些步骤？
A. 伪造文件扩展名以绕过文件类型检查
B. 上传包含恶意代码的脚本文件
C. 利用 Web 服务器的错误配置执行上传的恶意文件
D. 在上传文件之前，对文件进行加密处理

三、是非题（ 本大题 15 道小题 ，每小题 1 分，共 15 分）。

1.《中华人民共和国网络安全法》明确规定要维护我国的网络空间主权。网络空间主权是国家主权在网络空间中的自然延伸和表现。

2.TCP/IP 协议栈中的应用层功能相当于于 OSI 模型中应用层、表示层和会话层的功能。而 TCP/IP 协议栈中的传输层功能对应 OSI 模型中的数据链路层和物理层的功能。

3.http 头部注入是指注入字段在 http 请求头中的字段中，这些字段通常有 User-Agent 和 Referer 等。

4.get 方式提交就是直接在网址后面加上需要注入的语句。post 则是通过表单方式，get 和 post 的不同之处就在于前者可以通过 IE 地址栏处看到提交的参数，而后者却不能。

5.信息系统等级保护测评工作需要向公安局备案并取得备案号后，有资质的第三方等保测评机构才能开始测评。

6.访问控制是防止未经授权访问数据的有效措施之一。

7.全网行为管理应用控制技术只能基于端口和协议来识别和控制应用，无法基于具体的应用程序特征进行管理。

8.凯撒密码是一种简单的替换加密方法。

9.SQLmap 可以自动检测和利用 SQL 注入漏洞。

10.逻辑漏洞的防御策略包括定期更新软件和使用强密码。

11.为使用户在任意位置通过互联网便捷地访问企业内网的信息系统，将信息系统的服务端口以端口映射的方式直接发布在互联网上。这样做极有可能导致信息系统遭到外部恶意扫描、入侵攻击，进而给企业带来无法估量的损失。

12.使用白名单进行文件类型过滤可以有效防止出现文件上传漏洞。

13.在 Windows 操作系统中，默认情况下，IIS 服务器是预先安装和启用的。

14.下一代防火墙不仅提供传统防火墙功能，还能对应用程序进行深度检查和控制。

15.为了防止文件上传漏洞，简单的文件扩展名检查足以确保文件的安全性。

四、操作题

（一）基础实践题

随着 Web 技术的发展与成熟，Web 在成为互联网主流服务的同时，也暴露了越来越多

的攻击面，为黑客带来更多的可乘之机。常见的 Web 安全攻击手段主要包括 **SQL 注入漏洞攻击**、**CSRF（跨站请求伪造）漏洞攻击**、**XSS（跨站脚本）漏洞攻击**、**XXE（XML 外部实体）漏洞攻击**、**命令执行漏洞攻击**、**文件上传漏洞攻击**等。请对下列题目中的 Web 漏洞进行进一步分析：

1. SQL 注入漏洞分析

场景： SQL 注入漏洞是一种安全漏洞，允许攻击者通过输入恶意 SQL 代码来操纵数据库查询。你是一名安全分析师，负责审查一个 Web 应用程序。该应用程序允许用户通过输入查询条件来搜索数据库中的数据。你需要测试该应用程序是否存在 SQL 注入漏洞。

任务： 设计并执行测试，以验证系统是否存在 SQL 注入漏洞，并回答以下问题：

（1）SQL 注入漏洞产生的原因是什么？（3 分）

答：*请在此作答*

（2）写出一种常用的检测登录框 SQL 注入漏洞的 payload。（3 分）

答：*请在此作答*

（3）在单引号被过滤时，可以使用什么方式绕过？（4 分）

答：*请在此作答*

2. CSRF（跨站请求伪造）漏洞分析

场景： CSRF（跨站请求伪造）漏洞是一种安全漏洞，允许攻击者诱导受害者在不知情的情况下执行恶意操作。你是一名安全分析师，负责审查一个 Web 应用程序。该应用程序允许用户进行敏感操作，如修改密码或转账。你需要测试该应用程序是否存在 CSRF（跨站请求伪造）漏洞。

任务： 设计并执行测试，以验证系统是否存在 CSRF 漏洞，并回答以下问题：

（1）CSRF 漏洞产生的原因是什么？（3 分）

答：*请在此作答*

（2）下列是一种常用的检测 CSRF 漏洞的 payload，其功能是什么？（3 分）

```html
<form action=""http://example.com/change_password"" method=""POST"">
<input type=""hidden"" name=""new_password"" value=""hacked"">
<input type=""submit"" value=""Click Me"">
</form>
```

答：*请在此作答*

（3）在 CSRF 令牌被过滤时，可以使用什么方式绕过？（4 分）

答：*请在此作答*

（二）场景设计与应用题

答题说明：场景设计与应用题的代码在"C:\素材\网信安代码.rar"文件中！

1. 网络安全方向

在数字化时代，网络空间不仅是信息交流和经济活动的重要平台，也是国家战略竞争的新高地。随着互联网技术的广泛应用，网络空间的安全问题也变得愈发严峻。全球范围内，网络攻击、数据泄露、信息窃取、个人信息被滥用等安全事件频发，对个人隐私、企业运营乃至国家安全构成了严重威胁。

国际社会已经认识到网络安全的重要性，并采取了一系列措施来应对这一挑战。超过 50 个国家已经发布了各自的网络安全战略，强调保护关键基础设施和政府信息系统的安全。这些战略不仅涉及技术层面的防护，还包括法律法规的制定、国际合作的加强以及公众网络安全意识的提升。我国也高度重视网络安全，近年来密集出台了一系列政策文件，加强信息安全等级保护建设，提高全社会的信息安全防护能力。

XSS（跨站脚本）攻击是一种常见的网络安全威胁，允许攻击者将恶意脚本注入到受信任的网站上。当其他用户浏览这些页面时，嵌入的脚本会在他们的浏览器中执行，可能导致信息泄露、会话劫持甚至完全控制用户的浏览器。XSS 攻击的危害包括但不限于：盗取用户 cookie、模拟用户行为、操纵网站内容以及在不知情的情况下重定向用户到恶意网站。

弱口令问题则是指用户设置的密码过于简单，容易被猜测或通过自动化工具破解。使用弱口令的危害极大，一旦账户被破解，攻击者可以访问敏感数据、进行非法交易、散布恶意软件，甚至利用该账户作为进一步攻击的跳板，对整个系统的安全性构成威胁。

WebShell，也就是网站的"木马后门"，通常是黑客利用网站的配置问题或安全漏洞植入的可执行脚本文件。一句话木马，作为 WebShell 的一种，通过使用如 PHP 的 eval()或 ASP 的 execute()等函数，执行用户通过 POST 或 GET 提交的变量，这些变量名成为连接后门的"密码"。一旦 WebShell 被植入，攻击者便可以远程控制服务器，执行任意命令，窃取或破坏数据，甚至利用受感染的网站作为发起进一步攻击的基地。

现在某企业管理员接到反馈，该公司的 web 网站出现异常，被黑客入侵了。管理员提供了网站的全部源代码，并对代码结构进行了说明：

a	2024/7/16 11:52	文件夹	
data	2024/7/16 11:54	文件夹	
dede 管理员目录	2024/7/16 11:52	文件夹	
error	2024/7/16 11:51	文件夹	
images 静态图片资源	2024/7/16 11:51	文件夹	
include	2024/7/16 11:51	文件夹	
install	2024/7/16 11:59	文件夹	
m	2024/7/16 11:51	文件夹	
member	2024/7/16 11:51	文件夹	
plus	2024/7/16 11:52	文件夹	
special	2024/7/16 11:52	文件夹	
templets 模板	2024/7/16 11:51	文件夹	
uploads 上传目录	2024/7/16 15:42	文件夹	
.htaccess	2024/7/16 11:51	HTACCESS 文件	0 KB
favicon.ico	2019/6/4 8:56	ICO 文件	2 KB
index.php	2019/6/4 8:56	PHP 文件	2 KB
nginx.htaccess	2024/7/16 11:51	HTACCESS 文件	0 KB
robots.txt	2019/6/4 8:56	文本文档	1 KB
tags.php	2019/6/4 8:56	PHP 文件	1 KB

请帮助管理员解决以下问题:

（1）该网站管理员给出了网站的后台管理页面与网站代码，如下图，你能根据管理员给出的信息找到黑客登录系统所使用的账号和密码吗？请按照如下格式给出答案：账号/密码（如zhangsan/123456）。同时找到此页面对应的源代码文件，并将此文件名当作答案进行提交。（2 分）

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title>织梦内容管理系统 V57_UTF8_SP2</title>
<link href="css/base.css" rel="stylesheet" type="text/css" />
<link href="css/login.css" rel="stylesheet" type="text/css" />
<script src="../include/js/jquery/jquery.js" language="javascript" type="text/javascript"></script>
<script type="text/javascript">
$ = jQuery;
function changeAuthCode() {
    var num =   new Date().getTime();
    var rand = Math.round(Math.random() * 10000);
    num = num + rand;
    $('#ver_code').css('visibility','visible');
    if ($("#vdimgck")[0]) {
        $("#vdimgck")[0].src = "../include/vdimgck.php?tag=" + num;
    }
    return false;
}
</script>
</head>
<body>
<div id="login-box">
   <div class="login-top"><a href="../index.php" target="_blank" title="返回网站主页">返回网站主页</a></div>
   <div class='safe-tips'>您的管理目录的名称中包含默认名称dede，建议在FTP里把它修改为其它名称，那样会更安全！</div>   <div class="login-main">
    <form name="form1" method="post" action="login.php">
      <input type="hidden" name="gotopage" value="/acm12345/dede/index.php" />
      <input type="hidden" name="dopost" value="login" />
      <input name='adminstyle' type='hidden' value='newdedecms' />
      <dl>
       <dt>用户名：</dt>
       <dd><input type="text" name="userid"/></dd>
       <dt>密  码：</dt>
       <dd><input type="password" class="alltxt" name="pwd"/></dd>
           <dt>验证码：</dt>
       <dd><input id="vdcode" type="text" name="validate" style="text-transform:uppercase;"/><img id="vdimgck" align="absmiddle" onClick="this.src=th
           <a href="#" onClick="changeAuthCode();">看不清？ </a></dd>
                <dt> </dt>
        <dd><button type="submit" name="sml" class="login-btn" onclick="this.form.submit();">登录</button></dd>
      </dl>
    </form>
   </div>
   <div class="login-power">Powered by<a href="http://www.dedecms.com" title="DedeCMS官网"><strong>DedeCMSV57_UTF8_SP2</strong></a>&copy; 2004-2011 <
</div>
<div class="dede-iframe"><iframe name="loginad" src="login.php?dopost=showad" frameborder="0" id="loginad" scrolling="no" marginwidth="0" marginheigh
</body>
</html>
<!——默认用户名密码为admin/admin——>>
```

答：_____ *请在此作答* _____

（2）采用验证码技术是防止密码暴力破解的重要手段，该网站管理员给出了下图页面，请你根据该页面，描述红框处可能存在的安全风险。（2 分）

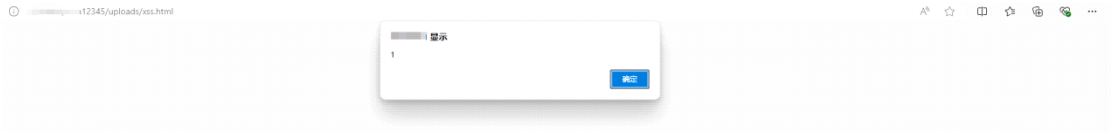
答：_____ *请在此作答* _____

（3）攻击者在网站中上传了一句话木马文件，你能找出木马文件的文件名吗？你能找到黑

客连接木马的密码吗？将文件名和密码作为答案提交，如 xxxx.php-123。（2 分）

答：_____请在此作答_____

（4）管理员在问这个页面时发生弹窗，这个是什么漏洞？（2 分）



答：_____请在此作答_____

（5）管理员点击了别人发给他的链接，发现域名是自己的服务器，点进去查看发现发生了弹窗。管理员给出了发生弹窗页面的 url 地址，你能找出发生此弹窗的文件吗？管理员给出的 url 地址为：：http://xxxxxx/acm12345/uploads/xss.html。将页面中的答案提交即可。(2 分)

答：_____请在此作答_____

2. 数据安全方向

用户首次登录网站系统需要注册账号，网站提供了查询功能，用于精确查询，输入身份证号码可以提供年龄、身高、体重、爱好、健康程度、最近一次购物记录、最近一次的地理位置信息等详细信息。在登录系统过程中，运维人员抓包发现用户登录密码在网络中明文传输。系统中的数据存储在数据库中。数据库管理员定期备份数据。有一天企业断电导致数据丢失，使用备份数据进行恢复却无法成功。由于数据重要，数据库管理员在百度贴吧发布求助信息，将数据库文件存入网盘，提供了数据加密的算法，并将代码上传到 Github。

（1）在网站注册环节，网站系统收集了用户个人信息：姓名、身份证号、手机号、短信验证码。身份证号在该网站系统中没有使用场景。那么网站系统在个人信息收集阶段存在什么问题？（2 分）

答：_____请在此作答_____

（2）在数据传输和数据查询过程中，有哪些内容可以改进？（2 分）

答：_____请在此作答_____

（3）在发现数据库备份数据无法恢复问题后，数据库管理员的哪些行为你认为需要改进？（2 分）

答：_____请在此作答_____

（4）企业管理员为了防止数据彻底丢失的情况，后续应该如何改进？（2 分）

答：_____请在此作答_____

（5）为了防止数据泄露，还可以采取哪些措施。（简述两条即可）（2 分）

答：_____请在此作答_____

3. 密码学方向

2021 年 6 月 25 日，我国 SM4 分组密码算法作为国际标准 ISO/IEC 18033-3：2010/AMD1：

2021《信息技术 安全技术 加密算法 第 3 部分：分组密码 补篇 1：SM4》，由国际标准化组织 ISO/IEC 正式发布。SM4 分组密码算法是继 SM2/SM9 数字签名算法、SM3 密码杂凑算法、祖冲之密码算法和 SM9 标识加密算法之后，我国又一个被纳入 ISO/IEC 国际标准且正式发布的商用密码算法，标志着我国商用密码算法国际标准体系进一步完善，展现了我国先进的密码科技水平和国际标准化能力，对提升我国商用密码产业发展、推动商用密码更好服务“一带一路”建设具有重要意义。

网站管理员逐步对网站进行防护，开始考虑逐步采用国产商用密码算法，然而仍然存在一些问题，针对网站管理员遇到的问题和正在使用的防护手段，请给他提一些建议。

（1）该网站管理员在登陆界面抓登录请求包时，发现请求包中非常熟悉的片段为“……userid= YWRtaW4=;password= YWRtaW4=;……”,请问该网站登录的用户名和密码是什么？（解码 Base64 编码工具 CertUtil 的用法：CertUtil [选项] -decode InFile OutFile
【举例说明】:
a.先将需要解码的内容 cGFzc3dvcmQ= 复制到 notepad 文本编辑器，并保存为 D 盘根目录下 pass.txt 文件。
b.然后在 CMD 命令行下运行：certutil -decode d:\pass.txt d:\pass2.txt
打开 D 盘根目录下 pass2.txt 文件就可发现已将原编码 cGFzc3dvcmQ=解码成原文 password)（2 分）
答：_____请在此作答_____

（2）网站管理员通过搭建 ssl，尝试避免基于网络监听的攻击行为，网站管理员委托你看一下防护的效果，你通过抓取和分析通信数据包，使用的密码套件为 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384，由此你能够分析出来，用户采用什么算法数字信封功能进行密钥协商(最好写出安全的算法)，采用 AES 算法的什么模式来保护数据的机密性和完整性保护？（2 分）
答：_____请在此作答_____

（3）在公钥体制中，每一用户 U 都有自己的公开钥 PK_U 和秘密钥 SK_U 。如果任意两个用户 A、B 按以下方式通信，用户 A 发给用户 B 消息 (Enc(PK_B,Msg),A)，用户 B 收到后,自动向用户 A 返回消息(Enc(PK_A,Msg),B)，以使用户 A 知道用户 B 确实收到报文 Msg，那么攻击者 C 怎样通过攻击手段获得消息报文 Msg？该攻击称为什么攻击？（2 分）
答：_____请在此作答_____

（4）IBC（基于标识的密码）是基于用户的唯一标识产生公钥的密码算法，其优势在于无需证书管理，减少了公钥基础设施的复杂性。网站管理员想通过 SM9 作为系统认证的安全防护措施之一，直接使用用户的身份信息生成用户公钥，提高效率并降低部署成本。经过你的建议没有采用姓名、性别等作为标识，请说明原因并写出你推荐的标识。（2 分）
答：_____请在此作答_____

（5）攻击者对密码系统的攻击类型可按攻击者能获取的信息量划分为唯密文攻击、已知明文攻击、选择明文攻击、选择密文攻击，请问唯密文攻击和选择密文攻击中攻击者所掌握内容的区别是什么？两者之间哪种对于攻击者而言相对更困难？（2 分）
答：_____请在此作答_____