1. readme.txt 中哪一部分是扩展名
   A、readme
   B、readme.
   C、.txt
   D、me.txt
   参考答案：C
2. 关于 html 语言，描述错误的有
   A、html 语言不区分大小写
   B、浏览器可以直接解释执行 html 代码
   C、浏览器无法执行 html 页面中的 js 脚本
   D、HTML 是用于创建网页的一种标记语言
   参考答案：C
3. 如果页面提示，不能上传 php 文件，那么使用扩展名绕过方式上传文件的话，下列那种方式不能上传成功（）
   A、123.php
   B、123.PHP
   C、123.PhP
   D、123.Php
   参考答案：A
4. 关于文件上传漏洞以下说法正确的是（）
   A、content-Type 检测文件类型绕过原理是服务器对上传文件的 content-Type 类型进行检测，如果是白名单允许的则可以正常上传，否则上传失败
   B、绕过 content-Type 文件类型检测的方法可以用 BurpSuite 截取并修改数据包中文件的 content-Type 类型使其符合白名单的规则
   C、文件系统 00 截断绕过将文件名 evil.php 改成 evil.php.abc，服务器只要验证该扩展名符合服务器端黑白名单规则即可上传。
   D、文件系统 00 截断绕过是当文件系统读到 00 时，会认为文件已经结束。
   参考答案：ABD
5. 下列关于 linux 文件夹权限中“rw-”描述正确的是？（）
   A、有执行、读权限，无写权限
   B、有读、写权限，无执行权限
   C、有读权限，无写、执行权限
   D、有写权限，无读、执行权限
   参考答案：B
6. 下列关于 http 请求描述正确的是（）
   A、当请求包含机密信息的话，使用 get 方式比 post 方式更安全
   B、http 请求头中的 Host 字段用于指定被请求资源的主机和端口号
   C、http 响应头中的 content-type 字段显示客户端实际返回内容的类型
   D、http 状态码 403 含义是服务器收到请求，但是拒绝提供服务
   参考答案：BCD
7. 在 Linux 系统中,哪一个是管道符()
   A、>
   B、<
   C、|

D、:

参考答案：C

8. 以下哪个不属于关系型数据库？（）

A、MySQL

B、SQLserver

C、oracle

D、MongoDB

参考答案：D

9. 下列关于 MySQL 数据库操作命令描述正确的有？（）

A、DROP DATABASE 用于删除数据库

B、truncate table 用于清空某数据表中的数据

C、desc 用于显示数据库下的所有数据表

D、create table 用于创建数据库

参考答案：AB

10. 数据库服务器、数据库和表的关系，正确的说法是？（）

A、一个数据库服务器只能管理一个数据库，一个数据库只能包含一个表

B、一个数据库服务器可以管理多个数据库，一个数据库可以包含多个表

C、一个数据库服务器只能管理一个数据库，一个数据库可以包含多个表

D、一个数据库服务器可以管理多个数据库，一个数据库只能包含一个表

参考答案：B

11. 以下关于 CTF 赛事描述正确的有（）

A、CTF 赛事主要是程序设计领域的一种竞赛模式的统称

B、解题模式常见于 CTF 比赛线上选拔

C、攻防模式常见于 CTF 比赛线下决赛

D、CTF 赛事起源于 DEFCON 全球黑客大会

参考答案：BCD

12. 下列关于 ASCII 码描述正确的有（）

A、大写字母与小写字母都是连续编码

B、小写字母的码值比任意的大写字母码值都大

C、ASCII 码能够对汉字进行编码

D、ASCII 码有可打印字符和不可打印字符之分

参考答案：ABD

13. “Y3Rme2l0J3MgfQ==”可能是以下哪一种编码？（）

A、BASE64

B、BASE32

C、BASE16

D、摩斯码

参考答案：A

14. 以下内容解码输出的结果为（）

98W1F>VET)W,@9G5N+&-H:6=O?0``

A、ctf{it's fun}

B、ctf{it's fun,chigo}

C、ctf{it's not fun}

D、ctf{it's not fun,chigo}

参考答案：B

15. 佛曰：罰耶俱竟婆勝夷漫鉢老奢明老是跋曳想梵夜即室梵羯死不穆俱爍都罰波吶蘇呼皤得俱訶吶特呼苦哆若怯迦。请参悟佛的真意（）
A、i love ctf
B、ctf{it's fun}
C、ctf{it's not fun}
D、我无法参透佛的真意
参考答案：D

16. 请将以下内容解码（结果：ctf{***}）（）
MN2GM63CMFZWKMZSPU======
A、ctf{base32}
B、ctf{base64}
C、ctf{base16}
D、以上都不对
参考答案：A

17. 下列关于 ctf 密码学描述不正确的有（）
A、ctf 密码学可以分为古典密码学和现代密码学两大类
B、古典密码学中的单表替换加密方式可以用词频分析法破解
C、现代密码学相比古典密码学加密效果更好，因此任何情况下都无法被破解
D、DES、AES、RSA 属于现代密码学中的算法
参考答案：C

18. 下列关于维吉尼亚密码描述正确的有（）
A、属于单表替换
B、明文需要通过秘钥加密
C、明文和密文有一一对应关系
D、维吉尼亚密码无法破解
参考答案：B

19. 以下内容的解码结果是 （）
666c61677b6374666973736f656173797d
A、flag{ctfissoeasy}
B、flag{ctfiseasy}
C、flag{ctfeasy}
D、flag{ctfsoeasy}
参考答案：A

20. 以下关于 RSA 算法描述错误的有（）
A、RSA 算法属于对称加密算法
B、RSA 加密秘钥和解密秘钥是不同的
C、RSA 算法的设计主要是基于大整数因式分解非常困难
D、RSA 算法在某些特殊情况下依然可以被人工破解
参考答案：A

21. 听说你对键盘很熟悉，能解出来这一串字符的结果吗（）
xdfvr56ydrgawdgyjqwse45tsef
A、ctfsohard

B、ctfsocool
C、ctfsofun
D、ctfsonice
参考答案：A

22. 10 进制数 113714760761412731246959279065154592 59 可以分解为两个质数的乘积，你能手工算出来吗？（）
A、134145274764149706 7*8476985936429195377
B、134145274764149706 3*8476985936429195373
C、134145274764149704 7*8476985936429195367
D、134145274764149706 1*8476985936429195379
参考答案：A

23. 以下属于 RSA 算法攻击方式的有（）
A、小公钥指数攻击
B、共模攻击
C、低解密指数攻击
D、N 分解攻击
参考答案：ABCD

24. 以下属于 SQL 注入类型的有？（）
A、基于联合查询的注入
B、基于报错的注入
C、基于时间的盲注
D、基于布尔的盲注
参考答案：ABCD

25. SQL 注入中 orderby 子句的功能是（）
A、查字段数
B、查表名
C、查数据库名
D、查表数
参考答案：A

26. 通过 information_schema 表得到 sec 数据库中所有数据表名字的查询语句为（）
A、select table_name from information_schema.tables where table_schema='sec'
B、select table_name from information_schema.tables where database='sec'
C、select culumn_name from information_schema.tables where table_schema='sec'
D、select column_name from information_schema.tables where database='sec'
参考答案：A

27. 以下关于 burpsuite 描述正确的有（）
A、burpsuite 是用于攻击 web 应用程序的集成平台
B、burpsuite 中的 Proxy 模块可以拦截、查看、修改 http 请求和响应包，且无需设置代理
C、burpsuite 中的 Scanne 模块能自动地发现 web 应用程序的安全漏洞

D、burpsuite 中的 Repeater 模块允许用户手动操作补发 HTTP 请求并分析应用程序响应

参考答案：ACD

28. 以下可以实现弹窗的 js 代码有（）

A、<script>alert(1)</script>

B、<body onload=alert(1)>

C、<img src onerror=alert(1)>

D、<input onmousemove=alert(1)>

参考答案：ABCD

29. 以下 python 代码执行的结果为：（）

```
for i in range(0,10):
    print (i)
```

A、打印出 0-9 这 10 个数字

B、打印出 0-10 这 11 个数字

C、打印出 0 和 10 这 2 个数字

D、打印出 0 这 1 个数字

参考答案：A

30. 以下能绕过 js 验证的是（）

A、禁用 JS 功能

B、中间人攻击

C、重启电脑

D、重新加载页面

参考答案：AB

31. 以下不属于文件上传漏洞利用方式的是（）

A、绕过前端 JS 验证上传

B、数据包 type 绕过上传

C、文件扩展名绕过上传

D、修改文件内容

参考答案：D

32. 关于 linux 中 vim 编辑器说法正确的是（）

A、vim 与 vi 完全相同

B、vim 有 4 种模式

C、vim 有 3 种模式

D、vim 有 2 种模式

参考答案：C

33. 以下关于 linux 命令说法正确的是？（）

A、cat 命令可查看文件内容

B、touch 可以创建文件夹

C、cp 可以删除文件

D、rm 可以创建文件

参考答案：A

34. CTF 中文一般译作_____在网络安全领域中指的是网络安全技术人员之间进行技术竞技的一种比赛形式。（）

A、抢手赛

B、争夺赛
C、锦标赛
D、夺旗赛
参考答案：D

35. TCP／IP 参考模型中，应用层协议常用的有（）
A、TELNET，FTP，SMTP 和 HTTP
B、IP，FTP，SMTP 和 HTTP
C、TELNET，FTP，SMTP 和 TCP
D、IP，FTP，DNS 和 HTTP
参考答案：A

36. URL 只允许用_____字符集中可打印的字符(0×20—0x7x)，其中某些字符在 HTTP 协议里有特殊的意义，所以有些也不能使用。（）
A、UTF-8
B、ASCII
C、Unicode
D、Little endian
参考答案：B

37. 命令 create table student(id int primary key,name char(50) not null,sex char(2) ,mail char(50))中，哪一个字段是主键？（）
A、id
B、name
C、sex
D、mail
参考答案：A

38. 整形报错注入如何判断显示位？（）
A、group by
B、limit 0,1
C、无显示位
D、select 1,2,3
参考答案：D

39. 以下对于 SQL 注入的说法错误的是？（）
A、SQL 注入攻击指的是通过构建特殊的输入作为参数传入 Web 应用程序
B、SQL 注入攻击方法复杂，危害又极小，所有在 owasp 中不占主要地位
C、SQL 注入可以在未经授权状况下操作数据库中的数据
D、程序员水平和经验欠缺，对 SQL 注入不重视往往是 SQL 注入攻击的来源之一
参考答案：B

40. phpinfo 是什么文件（）
A、存放着一些 PHP 函数。
B、存放着一些网站数据库文件。
C、存放着 PHP 一些具体配置信息。
D、存放着一些 PHP 代码
参考答案：C

41. 下列软件工具中不属于逆向破解软件工具的是？（）

A、OllyDbg
B、IDA
C、SublimeText3
D、WinDbg
参考答案：C

42. 关于编程语言的描述，错误的是（ ）
A、java、python、php、C 语言都属于高级语言
B、高级语言需要经过编译、链接后才能被计算机执行
C、计算机可以直接识别并执行高级语言
D、计算机所能识别的语言只有机器语言，即由 0 和 1 构成的代码
参考答案：C

43. 以下 PHP 代码的输出结果是（）
```
<?php
    $t=date("H");
    if ($t<"20")
    {
        echo "hello";
    }
?>
```
A、若当前时间小于 20，程序将会输出 hello
B、若当前时间超过 20，程序将会输出 hello
C、程序会输出 hello，无论当前时间多少
D、程序不会输出 hello，无论当前时间多少
参考答案：A

44. 关于 php 语言的描述，错误的是（ ）
A、PHP 是一种通用开源脚本语言
B、PHP 文件可包含文本、HTML、JavaScript 代码和 PHP 代码
C、PHP 文件的默认文件扩展名是 ".php"
D、PHP 代码可以通过浏览器直接解释执行
参考答案：D

45. 关于 php 函数，错误的是（ ）
A、mysqli_connect()功能是打开一个到 MySQL 服务器的连接
B、mysqli_error()功能是返回最近调用函数的最后一个错误描述
C、mysqli_query()功能是执行某个针对数据库的查询
D、mysqli_select_db()功能是返回当前系统状态
参考答案：D

46. 关于 http 和 https 协议，描述错误的是（）
A、双方都用于浏览器和服务器之间的通信
B、HTTP 协议以明文方式发送内容，不提供任何方式的数据加密
C、HTTPS 在 HTTP 的基础上加入了 SSL 协议，依靠证书来验证服务器的身份，并为浏览器和服务器之间的通信加密
D、https 协议更加安全，可以对黑客攻击免疫
参考答案：D

47. 请将以下内容解码（格式：flag{***}）（）

%61%6c%66%7b%67%79%72%63%74%70%72%67%6f%70%61%69%5f%79%5f%73%73%61%65%7d%79

A、flag{cryptograpy_is_easy}

B、flag{cryptograpyiseasy}

C、flag{cryptograpy_so_easy}

D、flag{cryptograpysoeasy}

参考答案：A

48. 以下关于隐写术，描述不正确的是（B）

A、文本、图片、音频、视频都可以作为隐写的载体

B、追加插入指的是在文件的起始部分增加新的内容

C、替换隐藏通过修改字节或调整字节位置实现数据隐藏

D、jpeg 文件的批注区可以进行数据隐藏

参考答案：B

49. 以下不属于图片隐写解题常用工具的是（）

A、Binwalk

B、Stegsolve

C、zsteg

D、IDA

参考答案：D

50. 栅栏被捣乱了！第一根和第二根都被换了位置，只有第三根还能站在那，却也短了一截了。变成了这样：

nZWRfbXlfZnVuemZmxhZ3tJX0NoYW5N1X2x1Y2t5IX0=谁能帮我修好呢？（）

A、flag{I_Changed_my_funzcu_funny!}

B、flag{I_Changed_my_funzcu_lucky!}

C、flag{I_Changed_my_funzcu_great!}

D、flag{I_Changed_my_funzcu_easy!}

参考答案：B