下面对于 cookie 的描述中错误的是？

正确答案: A 你的答案: 空 (错误)

Cookie 通过 HTTP Headers 从浏览器端发送到服务器端并存储在服务器端
Cookie 的大小限制在 4kb 左右，对于复杂的存储需求来说是不够用的
如果在一台计算机中安装多个浏览器，每个浏览器都会以独立的空间存放 cookie
由于在 HTTP 请求中的 Cookie 是明文传递的，所以安全性成问题

现有某函数，其方法声明为：int func(int x)
该函数对应的 ARM 汇编代码如下：

```
0000016A          PUSH    {LR}
0000016C          MOVS    R3, #1
0000016E          ADDS    R1, R3, #0
00000170 loc_170
00000170          CMP     R0, #0
00000172          BLE     loc_184
00000174          MOVS    R2, R0
00000176          MULS    R2, R3
00000178          ADDS    R3, R2, #1
0000017A          TST     R0, R1
0000017C          BEQ     loc_180
0000017E          ADDS    R3, R2, #0
00000180 loc_180
00000180          SUBS    R0, #1
00000182          B       loc_170
00000184 loc_184
00000184          MOVS    R0, R3
00000186          POP     {PC}
```

从上面的汇编代码可以得出 func(3)的值等于

正确答案: C 你的答案: 空 (错误)

5
6
7
8
9
10

安卓系统中所有 App 进程是下面的哪个进程 fork 产生的

正确答案: C 你的答案: 空 (错误)

init

system_server
zygote
kthreadd

以下关于内存文件 mmap 映射的说法不正确的是
正确答案: C 你的答案: 空 (错误)

当文件被映射到进程地址空间后，进程可以像访问普通内存一样对文件进行访问
子进程会继承父进程通过 mmap 映射的地址空间
使用 mmap 必须指定映射到内存的具体文件
同一个文件的不同段内容可以分别被映射到不同的内存空间

常见的网络嗅探器，以下哪个不是？
正确答案: B 你的答案: 空 (错误)

tcpdump
wvs
wireshark
sniffit

以下算法不能用于文本加密的是
正确答案: C 你的答案: 空 (错误)

RC4
RSA
MD5
DES

下列关于 Android 数字签名描述错误的是：
正确答案: D 你的答案: 空 (错误)

所有的应用程序都必须有数字证书，Android 系统不会安装一个没有数字证书的应用程序
Android 程序包使用的数字证书可以是自签名的，不需要一个权威的数字证书机构签名认证
数字证书都是有有效期的，Android 只是在应用程序安装的时候才会检查证书的有效期。如果程序已经安装在系统中，即使证书过期也不会影响程序的正常功能。
如果要正式发布一个 Android 程序，可以使用集成开发工具生成的调试证书来发布。

现有 Android 应用内某函数，其方法声明为：private int func()
该函数对应的 smali 反汇编代码如下：

```
.method private func()I
00000000   const-string        v2, "Didichuxing"
00000004   const/4             v0, 0
00000006   const/4             v1, 0
00000008   invoke-virtual       String->length()I, v2
```

```
0000000E  move-result          v3
00000010  if-ge                v1, v3, :2E
00000014  const/16             v3, 0x0069
00000018  invoke-virtual       String->charAt(I)C, v2, v1
0000001E  move-result          v4
00000020  if-ne                v3, v4, :28
00000024  add-int/lit8         v0, v0, 0x01
00000028  add-int/lit8         v1, v1, 0x01
0000002C  goto                 :8
0000002E  return               v0
.end method
```

从上面的 smali 反汇编代码可以得出该方法的返回值等于

正确答案: C　你的答案: 空 (错误)

1
2
3
4
5

凯撒（Caesar)密码是一种基于字符替换的对称式加密方法，它是通过对 26 个英文字母循环移位和替换来进行编码的。设待加密的消息为"Didi Family"，加密后的密文是"Nsns Pkwsvl"，则采用的密匙 k 是

正确答案: A　你的答案: 空 (错误)

10
11
13
15

当一个 HTTPS 站点的证书存在问题时，浏览器就会出现警告信息以提醒浏览者注意，下列描述中哪一条不是导致出现提示的必然原因？

正确答案: D　你的答案: 空 (错误)

证书过期
证书没有被浏览器信任
证书的 CN 与实际站点不符
浏览器找不到对应的证书颁发机构

攻击者采用某种手段,使用户访问某网站时获得一个其他网站的 IP 地址,从而将用户的访问引导到其他网站,这种攻击手段称为?

正确答案: B　你的答案: 空 (错误)

ARP 欺骗攻击

DNS 欺骗攻击
暴力攻击
重放攻击

下面关于 RSA 算法的描述,不正确的是?
正确答案: D 你的答案: 空 (错误)

RSA 是非对称加密算法
RSA 的运行速度相比 AES 算法要慢很多
RSA 的安全性依赖于大数分解
TLS/SSL 协议中 RSA 的公钥长度一般为 128 位或 256 位

攻击者截获并记录了从 A 到 B 的数据，然后又从早些时候所截获的数据中提取出信息重新发往 B 称为
正确答案: D 你的答案: 空 (错误)

中间人攻击
口令猜测器和字典攻击
强力攻击
重放攻击

以下哪一项不是针对操作体统的安全保护措施?
正确答案: B 你的答案: 空 (错误)

SELINUX
nProtect
DEP
ASLR

以下哪个算法不是对称加密算法
正确答案: C 你的答案: 空 (错误)

DES
RC5
ECDH
AES

文件 aaa 的访问权限为 rw-r--r--,现要增加所有用户的执行权限和同组用户的写权限，下列哪些命令是正确的?
正确答案: A D 你的答案: 空 (错误)

chmod a+x g+w aaa
chmod 764 aaa
chmod o+x g+w aaa
chmod 775 aaa

文件 aaa 的内容如下：

1001:1

1002:2

1003:1

1004:2

期望处理 aaa 文件得到以下输入结果：

1001

1003

以下命令能满足的有

正确答案: C D　你的答案: 空 (错误)

```
grep "1$" aaa | awk -d: '{print $1}'
grep "1$" aaa | cut -d: -f0
sed '/:2/d' aaa | sed 's/:1//g'
awk -F: '{if ($2==1){print $1}}' aaa
```

下列关于 SSL 的描述中，正确的有

正确答案: A B C　你的答案: 空 (错误)

SSL 即安全套接字层，是一种安全协议，它为网络的通信提供私密性，工作在应用层和传输层之间。
.SSL 能加密数据以防止数据中途被窃取,维护数据的完整性，确保数据在传输过程中不被改变。
SSL 实际上是共同工作的两个协议，SSL 记录协议和 SSL 握手协议。
SSL 握手协议为高层协议提供基本的安全服务。

以下说法中，哪些说法是正确的

正确答案: A C D　你的答案: 空 (错误)

缓冲区溢出指的是通过向程序的缓冲区写入超出其长度的内容，造成缓冲区的溢出，从而破坏程序的堆栈，使程序转而执行其他的指令，以达到攻击的目的。
在 C/C++语言中，缓冲区溢出的任何尝试通常都会被语言本身自动检测并阻止。
检查缓冲区长度、GS 编译选项、堆栈保护可以防御溢出攻击
溢出是程序设计者设计时的不足所带来的错误。

以下哪种加密方案是相对最安全的？

正确答案: C　你的答案: 空 (错误)

RSA 加密算法，密钥长度 512 位
AES 加密算法，选择 ECB 模式，密钥长度 128 位
AES 加密算法，选择 CBC 模式，密钥长度 128 位
DES 算法

Linux 系统下，关于权限描述正确的是：

正确答案: C D　你的答案: 空 (错误)

文件权限描述"-rwxrw-r-x"对应权限值为 754
文件权限描述"drw-rw-rw-"中的首字符'd'表示该文件为软链接文件
文件权限值为 723，表示其他用户可以执行该文件
文件权限值 744，表示除了文件所有者外其他用户不可执行

同一进程下的线程可以共享以下？

正确答案: B D　你的答案: 空 (错误)

```
stack
data section
register set
file fd
```

下列哪部分代码片段如果使用不当会导致安全漏洞？

正确答案: A C D　你的答案: 空 (错误)

```
<?php
...
$sql = "select * from admin where id=".$_GET['id'];
$result = mysql_query($sql);
...
<?php
$username = $_GET['name'];
echo  htmlspecialchars($username);
...
<?php
...
$file = $_GET['file'];
echo file_get_contents($file);
...
<?php
$string = $_GET['text'];
$pattern = '/(\w+) (\d+), (\d+)/ie';
$replacement = '${1}1,$3';
echo preg_replace($pattern, $replacement, $string);
?>
```

文件完整性校验所使用的加密算法有哪些

正确答案: A B　你的答案: 空 (错误)

```
md5
sha1
des
rsa
```

浏览器和服务器在基于 https 进行请求链接到数据传输过程中，用到了如下哪些技术：

正确答案: A B C D　你的答案: 空 (错误)

非对称加密技术
对称加密技术
散列（哈希）算法
数字证书

下列哪些函数可能导致缓冲区溢出?

正确答案: A B C　你的答案: 空 (错误)

wcscpy
vsprintf
scanf
strcat_s

iOS 平台上常见的 Hook 框架有:

正确答案: D　你的答案: 空 (错误)

Xposed
Intent Fuzz
Drozer
Substrate

黑客通过以下哪种攻击方式，可能大批量获取网站注册用户的身份信息

正确答案: A B C　你的答案: 空 (错误)

XSS
CSRF
越权
以上都不可以

使用以下哪些工具可以直接调试安卓 app 代码逻辑？

正确答案: C D　你的答案: 空 (错误)

baksmali
ddms
IDA
gdb

Android 应用中导致 HTTPS 中间人攻击的原因有？

正确答案: A B C　你的答案: 空 (错误)

没有对 SSL 证书校验
没有对主机名进行校验
SSL 证书被泄露

使用 WIFI 连接网络