

一、单项选择题

1、如果网站开发者为防止 SQL 注入，对用户输入的参数进行了过滤逗号的限制，则可以采用（ **B** ）函数进行绕过。

A. ally

B. join

C. union

D. alliance

2、MySQL 元数据是指数据库内部包含的数据，INFORMATION_SCHEMA 虚拟数据库中不包含（ **D** ）。

A. 数据库名称

B. 数据表名称

C. 访问权限

D. 字段内容

3、函数（ **C** ）能够把预定义的字符 "<"（小于）和 ">"（大于）转换为 HTML 实体。

A. trim

B. preg_replace

C. htmlspecialchars

D. stripslashes

4、攻击者拟获取远程主机的操作系统类型，则可以选用的工具是（ **A** ）。

A. nmap

B. whois

C. whisker

D. nslookup

5、基于 whois ~~数据库~~ 进行信息探测的目的是（ **C** ）。

A. 探测目标主机开放的端口及服务

B. 探测目标的网络拓扑结构

C. 探测目标主机的网络注册信息

D. 探测目标网络及主机的安全漏洞

6、在进行 Microsoft SQL Server 数据库口令猜测的时候，我们一般会猜测拥

有数据库最高权限登录用户的密码口令，这个用户的名称是（ B ）。

A. admin

B. sa

C. system

D. root

7、若 X、Y 是用于独立公网 IP 地址的计算机，X1，X2 是 X 中的 NAT 模式连接的 VMware Workstation 虚拟机，则访问规则是（ D ）。

A. X、X1、X2、Y 能互访。

B. X1、X2 不能访问 Y。

C. X1、X2、Y 能互访。

D. X1、X2 能访问 Y，但是 Y 不能访问 X1、X2。

8、LOAD_FILE 函数能够读取文件并将文件内容作为字符串返回，它的使用条件不包含（ A ）。

使用条件：文件存在，有完整路径和读取权限

A. MySQL 数据库版本大于 5.5

B. 有可访问路径

C. 有读取权限

D. 文件存在

9、关于中国菜刀的功能，下面说法错误的是（ B ）。

A. 支持文件上传、下载、编辑、改变时间戳等 ①文件管理

B. 命令行具有 root 权限

C. 内置了常见数据库的常用语句 ②数据库管理

D. 支持多种数据库

③虚拟终端

10、关于 PHP Cookie，下列说法错误的是（ C ）。

A. cookie 常用于识别用户

B. 每当同一台计算机通过浏览器请求页面时，计算机会发送 cookie

C. cookie_destroy() 函数用于删除 cookie

D. cookie 是一种服务器留在用户计算机上的小文件

session 消除

session-destroy

cookie 消除

将 setcookie 的时间设为 time() - 1

11、(A) 利用以太网的特点，将设备网卡设置为“混杂模式”，从而能够接受到整个以太网内的网络数据信息。

- A. 嗅探程序
- B. 木马程序
- C. 拒绝服务攻击
- D. 缓冲区溢出攻击

✓ 12、字典攻击被用于 (D)。

- A. 用户欺骗
- B. 远程登录
- C. 网络嗅探
- D. 破解密码

暴力破解

13、使用 FTP 协议进行文件下载时 (A)。

- A. 包括用户名和口令在内，所有传输的数据都不会被自动加密
- B. 包括用户名和口令在内，所有传输的数据都会被自动加密
- C. 用户名和口令是加密传输的，而其它数据则以明文方式传输
- D. 用户名和口令是不加密传输的，其它数据则以加密传输的

14、对攻击可能性的分析在很大程度上带有 (B)。

- A. 客观性
- B. 主观性
- C. 盲目性
- D. 上面 3 项都不是

15、从安全属性对各种网络攻击进行分类，截获攻击是针对 (A) 的攻击。

- A. 机密性
- B. 可用性
- C. 完整性
- D. 真实性

阻断攻击针对可用性

16、从攻击方式区分攻击类型，可分为被动攻击和主动攻击，被动攻击难以

(检测)，然而 (阻止) 这些攻击是可行的，主动攻击难以 (阻止)，然而 (检测) 这些攻击是可行的。

- A. 阻止，检测，阻止，检测
- B. 检测，阻止，检测，阻止

不导致
系统信息的
损失

会

C.检测，阻止，阻止，检测

D.上面 3 项都不是

17、信息安全管理中最核心的要素是 (C)

A.技术 B.制度 C.人 D.资金

18、使用快捷命令进入本地组策略编辑器的命令是? (B)

A. devmgmt.msc 设备管理器

B. gpedit.msc

C. fsmgmt.msc 共享文件夹管理器

D. lusrmgr.msc 本地用户和组 管理器

19、以下哪些不属于设置强口令的基本原则? (D)

A.扩大口令的字符空间 B.选用无规律的字串

C.设置长口令 D.共用同一口令

20、(C) 是一种自动检测远程或本地主机安全性弱点的程序。

A.杀毒软件 B.防火墙

C.扫描器程序 D.操作系统

二、判断题，请将“√”或“×”填到下面的表格中

1、SSH 等加密手段可有效防范 Wireshark 的嗅探。 (√)

2、地址支持组织 ASO 负责通用顶级域名的管理。 (×)

3、通过网络扫描可以判断目标主机的操作系统类型。 (√)

4、https://www.scu.edu.cn 与 http://www.scu.edu.cn 同源。 (×)

5、过滤用户输入可以防御 XSS，但不能防御 CSRF。 (√)

6、√ DOM (Document Object Model, 文档对象模型) 是一个平台中立和语言中立的接口。 (√)

7、为避免在插入 U 盘等移动存储设备时受到病毒感染，用户应在插入前先对其进行病毒检查，同时在系统中禁用 U 盘的自动播放功能。 (√)

8、域名信息探测工具 dig 显示的是非权威应答。 (×)

9、只要装了防火墙和防病毒软件，网络就是安全的。 (×)

10、盗版软件成为计算机病毒的重要来源和传播途径之一。（✓）

三、填空题

1、在 Wireshark 的过滤器中输入 bootp，表示只筛选 DHCP 数据包。

2、✓ 信息安全三原则中，机密性是指确保信息没有非授权的泄露，不被非授权的个人、组织和计算机程序使用。

3、Exp是一段对漏洞如何利用的详细说明或者一个演示的漏洞攻击代码，可以使得读者完全了解漏洞的机理以及利用的方法。

4、在使用 Google 搜索时，如果限定在我校域名下搜索“.docx”格式的文件，应输入命令 site:cuit.edu.cn filetype=docx 200 请求已成功接收
302 重定向
500 遇到了意外情况

5、✓ 如果无法找到指定位置的资源，将可能出现的 HTTP 状态码是 404。

6、✓ Web 应用程序在设置 Cookie 时，将其属性设置为 HttpOnly 可以避免该网页的 Cookie 被客户端 JavaScript 存取，保护用户的 Cookie 不被盗取。

7、✓ Cve 漏洞编号是安全业界标识漏洞的标准索引号。

8、tracert 是一个 Windows 下的路由跟踪实用程序，用于确定 IP 数据包访问目标所采取的路径。

9、✓ 所谓同源是指：域名、协议、端口相同。

10、ping 命令是用于测试网络连接量的程序，它使用的是 ICMP 协议。

11、✓ IANA 负责通用顶级域名（gTLD）分配包括.com、.net、.edu、.org 和.info 等。

12、✓ Tracert 命令使用 IP 生存时间 和 ICMP 错误消息 来确定从一个主机到网络上其他主机的路由。

13、✓ Oracle 数据库，默认的端口号为 1521；Mysql 数据库默认端口号 3306

—。

14、已知 `http://www.test.com/?id=1` 存在一个 SQL 注入漏洞，该网站的数据库名为 `sqldb`，使用 SQLMap 获取其表名，应输入命令 `sqlmap -u http://www.test.com/?id=1 -D sqldb -tables` (18)

15、为了安全起见，应保证程序的数据库访问在 最低权限 模型下运行。

16、Host 字段指定请求资源的 Internet 主机和端口号。站点 Referer 指定获取当前请求的来源
主机 Host 头字段 用户代理 User-Agent 头字段确定用户使用的 Web 浏览器

四、简答题。

1、现在非常多的 Web 程序没有正常的错误回显，这样就需要我们利用报错注入的方式进行 SQL 注入，通过构造 payload 让信息通过错误提示回显出来，请简述 3 个 SQL 报错注入用到的函数，并简单解释其功能。

2、请简要叙述 TCP ACK Ping 主机扫描的特点。

使用 TCP ACK 扫描不能确定端口的关闭或开放，但是可以利用它来扫描防火墙上配置，用它来发现防火墙上配置，确定它是有状态还是无状态的，哪些端口是被过滤的

3、请简要叙述基于 DOM 的 XSS 的漏洞利用过程。

五、分析题

1、请分析下面的代码，并回答问题：

a) `http://localhost/test.php?id=1' and 1=2 union select 1,2,database()-- xx`

b) `http://localhost/test.php?id=1' and 1=2 union select 1,2,TABLE_NAME from information_schema.TABLES where TABLE_SCHEMA=database() limit 1,1-- ss`

(1) 语句 a 的作用是？

使用联合注入查询当前数据库名

(2) 语句 b 的作用是？

使用联合注入查询当前数据库中的表名，选择第 1 个开始，只显示 1 个

(3) 如果已知表名为 `testable`，要获取字段 `flag` 的内容，应使用语句？

`http://localhost/test.php?id=1' and 1=2 union select group_concat(flag) from testable --ss`

2、某网站的部分核心代码如下所示：

```
.....
<form action="" method="get">
    <input type="text" name="myinput">
    <input type="submit">
</form>
<hr><hr>
<?php
    header("Content-Type: text/html; charset=gb2312");
    $input = "";
    @str_replace( '<script>', '', $_GET[ 'input' ] );
    echo '你输入的字符为<br>'.$input;
?>
.....
```

请分析代码，回答以下问题。

(1) 这段代码可能存在什么类型的漏洞？

(2) 请写出 3 条语句来验证该网站存在的漏洞。

3、某网站服务器采用的 PHP 版本为 5.6.0，存在 0x00 截断漏洞。代码中 address 变量是在 HTML 表单中获取的时间，值为 1400324078，将会以时间给文件重命名。上传时 BurpSuite 抓到的数据包如下图所示。

```
-----208498473118925698491232638877
Content-Disposition: form-data; name="file"; filename="1.jpg"
Content-Type: image/jpeg

<?php
phpinfo();
?>

-----208498473118925698491232638877
Content-Disposition: form-data; name="address"

1400324078
-----208498473118925698491232638877--
```

请回答以下问题：

(1)、请详细叙述利用 0x00 截断漏洞的上传攻击过程。

(2) 如果攻击成功，保存在服务器上的文件名是什么？

4、请分析如下代码，回答问题：

```
<?php
if( isset( $_POST[ 'btnSign' ] ) ){
    $message = trim( $_POST[ 'mtxMessage' ] );
    $name = trim( $_POST[ 'txtName' ] );

    $message = strip_tags( addslashes( $message ) );
    $message = ((isset($GLOBALS["__mysqli_ston"]) && is_object($GLOBALS["__mysqli_ston"])) ?
mysqli_real_escape_string($GLOBALS["__mysqli_ston"], $message ) : ((trigger_error("[MySQLConverterToo] Fix the mysql_escape_string() call! This code does not work.", E_USER_ERROR)) ? "" : ""));
    $message = htmlspecialchars( $message );

    $name = str_replace( '<script>', '', $name );
    $name = ((isset($GLOBALS["__mysqli_ston"]) && is_object($GLOBALS["__mysqli_ston"])) ?
mysqli_real_escape_string($GLOBALS["__mysqli_ston"], $name ) : ((trigger_error("[MySQLConverterToo] Fix the mysql_escape_string() call! This code does not work.", E_USER_ERROR)) ? "" : ""));
    $query = "INSERT INTO guestbook ( comment, name ) VALUES ( '$message', '$name' );";
    $result = mysqli_query($GLOBALS["__mysqli_ston"], $query ) or die( '<pre>' . ((is_object($GLOBALS["__mysqli_ston"])) ? mysqli_error($GLOBALS["__mysqli_ston"]) : (($___mysqli_res = mysqli_connect_error()) ? $___mysqli_res : false)) . '</pre>' );
}
?>
```

(1) 请分析这段代码存在什么漏洞？根据代码分析漏洞产生的原因是什么？

(2) 请解释 trim(), mysqli_real_escape_string(), htmlspecialchars() 函数的作用

(3) 请简单阐述这种攻击方式的防御措施。

5、页面 <http://www.cuit.cn/test.php?id=1> 的部分代码如下，请分析后回答问题：