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() 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())。 | |
| 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() 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 | 茂类型,则可以选用的工具是(/)。 |
| | |
| A. nmap | B. whois |
| A. nmap C. whisker | |
| - | B. whois D. nslookup |
| C. whisker | B. whois D. nslookup 可目的是()。 |
| C. whisker 5、基于 whois <mark>数据库</mark> 进行信息探测的 | B. whois D. nslookup 可目的是()。 |
| C. whisker 5、基于 whois <mark>数据库</mark> 进行信息探测的 A. 探测目标主机开放的端口及 | B. whois D. nslookup 可目的是()。 服务 |
| C. whisker 5、基于 whois 数据库进行信息探测的 A. 探测目标主机开放的端口及 B. 探测目标的网络拓扑结构 | B. whois D. nslookup 可目的是()。 服务 |

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



A. admin

B. sa

C. system

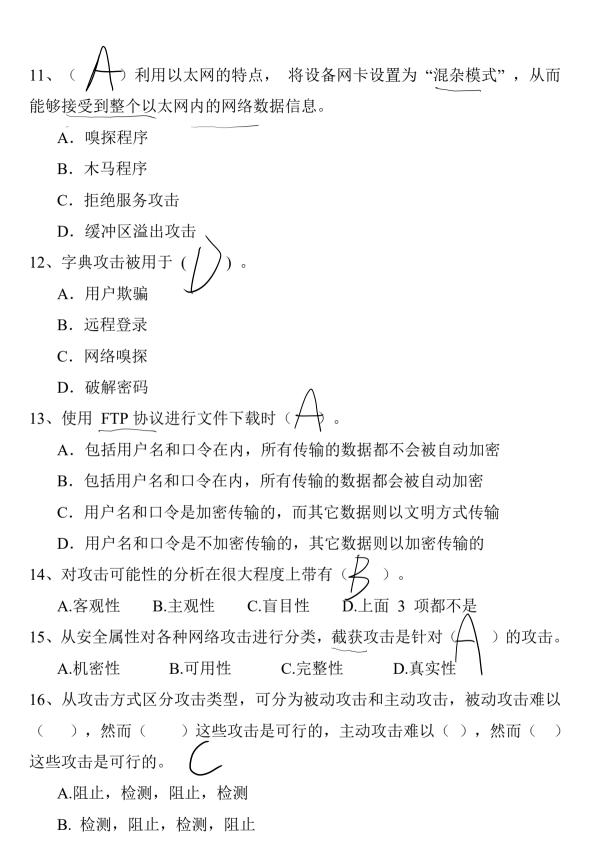
D. root

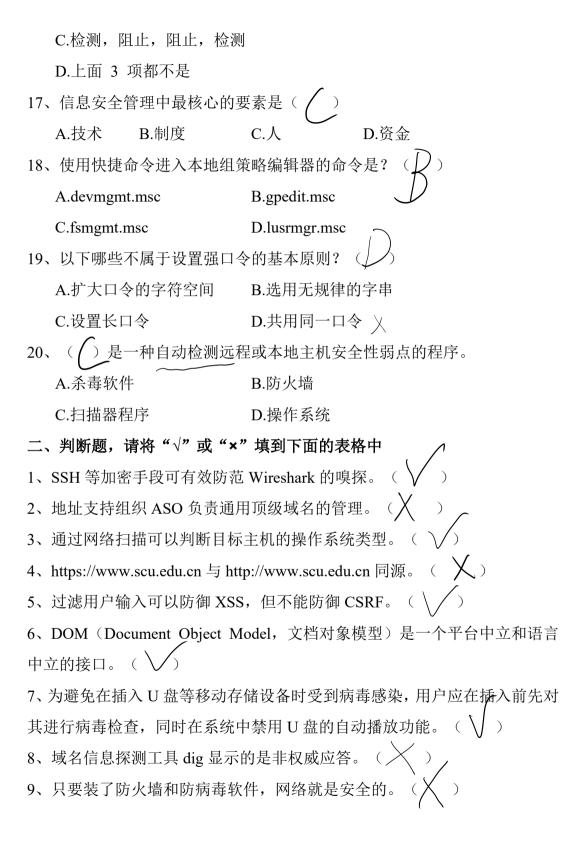
7、若 X、Y 是用于独立公网 IP 地址的计算机,X1, X2 是 X 中的 NAT 模式连接的 VMware Workstation 虚拟机,则访问规则是())。

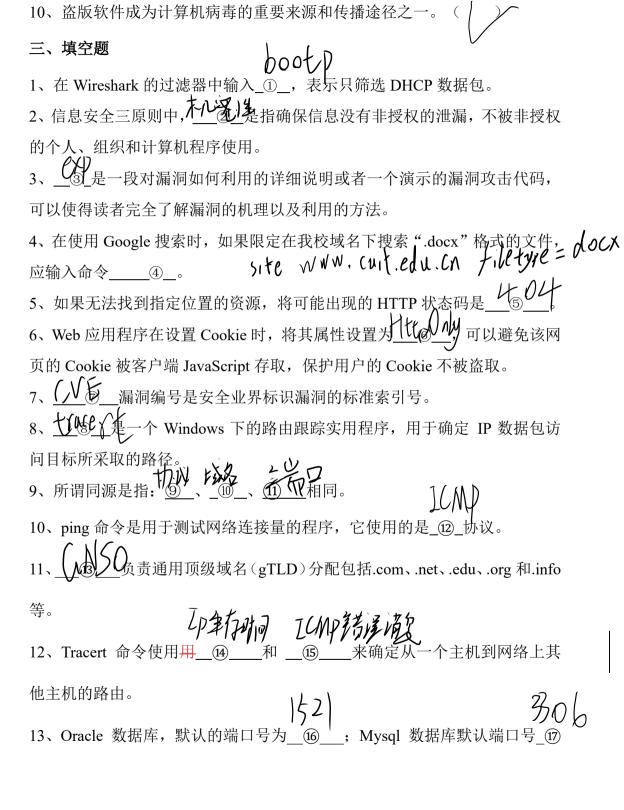
- A. X、X1、X2、Y 能互访。
- B. X1、X2 不能访问 Y。
- C. X1、X2、Y能互访。
- D. X1、X2 能访问 Y, 但是 Y 不能访问 X1、X2。
- 8、LOAD_FILE 函数能够读取文件并将文件内容作为字符串返回,它的使用条件 $\underline{\Lambda}$ 包含($\underline{\Lambda}$)。
 - A. MySQL 数据库版本大于 5.5
 - B. 有可访问路径
 - C. 有读取权限
 - D. 文件存在
- - A. 支持文件上传、下载、编辑、改变时间戳等
 - B. 命令行具有 root 权限
 - C. 内置了常见数据库的常用语句
 - D. 支持多种数据库
- 10、关于 PHP Cookie,下列说法<u>错误</u>的是(



- 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







| | 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 |
|-------|--|
| | 5 り wap - ル かttp し 5 りり 名为 sqldb,使用 SQLMap 获取其表名,应输入命令®。 |
| | 15、为了安全起见,应保证程序的数据库访问是一个技术是型下运行。tables |
| | 16、字段指定请求资源的 Internet 主机和端口号。 |
| | 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 |
| | 注入的方式来进行 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。 EXPC)适回 e选件到的这数量的线 flood) myslan flood |
| | Up tateral() 对XML文档的行行。 2、请简要叙述 TCP ACK Ping 主机扫描的特点。 发送一个只有ACK特色的7CP数据已经因指生机,大學外段一个TCPRST数据的,从表 |
|)UVa. | 3、请简要叙述基于DOM的XSS的漏洞利用过程。例子和744。尹子为29年一点无知,对MN SG元素指 |
| | 五、分析题们可,这个约例以及如此,在dannent get lement Byld lifext") |
| | 1、请分析下面的代码,并回答问题:我们说为《imp Schillent By Lot l'fext') 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? 利用50让人多数好点 |
| | (2) 语句 b 的作用是? 支 多的 数据库有 邓兰夫 |

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

from testable -- ss

(3) 如果已知衣白为 restation, and 1=2 union Secret 1.2. group concat (Hag)

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
'.\$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? 人力 (2) 请写出3条语句来验证该网站存在的漏洞。 くSC <SCript>//pt> alert(1x/ss) くSC <SCript>//pt> alert(1x/ss) く/SCRipT > alert(1x/ss) 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

-----208498473118925698491232638877--

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

1488324078

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。 在 本写外件 1·JP9上传的时行用如 抓包,在 140824078 在 力上·Php 和 主格,他们整 到 版义为 2 发放处型 20 基格为 00 世纪松斯,但是我们是一个大人的一个人们是这种,们 到 版义为 2 发放 成功,保存在服务器上的 文件名是什么是于上传成 的,从们上传文件,们 1400324078 . Php

4、请分析如下代码,回答问题:

(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? 5QLixx偏同

没有对 mane 多量的值类行转义, 左接放在了SQL冷却。

(2) 请解释 trim(), mysqli real escape string(), htmlspecialchars() 函数的作

用 主样等解状尾至的 把意义字符段的机构写体

(3) 请简单阐述这种攻击方式的防御措施。

strip-togs (add slashes (\$nome)) & fz | sname = htmlspecialchars (\$nome)

グナ **JNMC 片灯 移**ソ 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: