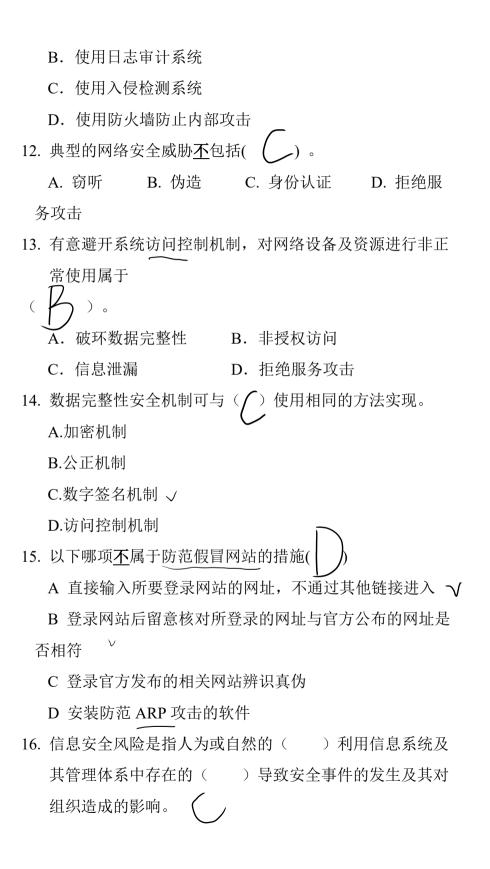
一、单项选择题

ľ	1 70.04170
1.	在短时间内向网络中的某台服务器发送大量无效连接请求,
	导致合法用户暂时无法访问服务器的攻击行为是破坏了
	A. 机密性 B. 完整性 C. 可用性 D. 可控性
2.	负责通用顶级域名(gTLD)分配包括.com、.net、.edu、.org
	和.info 等的组织是(\bigwedge)。
	A. GNSO B. CNNSO
	C. CNNIC D. CDNC
3.	在使用 Google 搜索时,如果限定在 bilibili 中 完全匹配 搜索
	"XSS 攻击"相关的网页,应输入哪个命令? ()
	A. "XSS 攻击" cache:bilibili.com
	B. XSS 攻击 cache:bilibili.com
	C. XSS 攻击 site:bilibili.com
	D. "XSS 攻击" site:bilibili.com
4.	以下哪种扫描方式采用了完整的"三次握手"机制?(
	A. ACK 扫描 B. SYN 扫描
	C. connect 扫描 D. CDNC
5.	基于 whois 数据库进行信息探测的目的是(()。
	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.	上传漏洞攻击必要条件不包括以下哪个?(人)

A. 木马上传成功, 未被杀 B. PHP 文件在对方过滤白名单里 C. 知道木马的路径在哪 D. 上传的木马能正常运行 7. 以下哪个方式不能防范 CSRF? (A. 使用 POST 提交用户数据,来代替 GET ✓ B. 校验 HTTP Referer 🗸 C. 对上传进行过滤 D. 使用请求令牌 Token 🗸 8. 黑客利用 IP 地址进行攻击的方法有? (A. 窃取口令 B. 解密 C. IP 欺骗 D. 发送病毒 9. UDP 主机扫描需要选择一个(✓)的目标端口才能完成 探测。 A. 关闭 B. 打开 C. 待定 D. 过滤 10. 当 Cookie 设置了 HttpOnly 属性后,可以(()。 A. 与 WEB 服务器之间就通过 HTTPS 传递数据 B. 与 WEB 服务器之间就通过其他安全协议传递数据 C. 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 D. Cookie 内容被加密 11. 根据统计显示, 80%的网络攻击源于内部网络, 因此, 必 须加强对内部网络的安全控制和防范。下面的措施中,**无** <u>助于</u>提高局域网内安全性的措施是(

A. 使用防病毒软件



- A、脆弱性、威胁 B、威胁、弱点
- C、威胁、脆弱性
- D、弱点、威胁
- 17. 乱扫二维码,支付宝的钱被盗,主要是中了?(
 - A、僵尸网络 B、病毒 C、蠕虫

- 18. 为防止办公用计算机上的数据丢失或遭破坏,用户应主要 做好(┃)措施。
 - A、对计算机上的数据进行加密保护
 - B、合理设置计算机登录密码并定期更改
 - C、购置防病毒、防入侵等软件,提升计算机安全防护能力
 - D、对计算机上的重要数据进行备份 レ
- 19. 哪项不是网络钓鱼的常用手段(

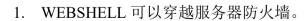


- A、利用计算机木马
- B、利用虚假的电子商务网站
- C、利用垃圾邮件
- D、利用假冒网上银行、网上证券网站
- 20. 若要在公共场合使用 WiFi, 应尽量选择以下哪个无线信号



- A, hacker
- B ChinaNet-link
- C, AirPort123 D, starbucks

二、 判断题。

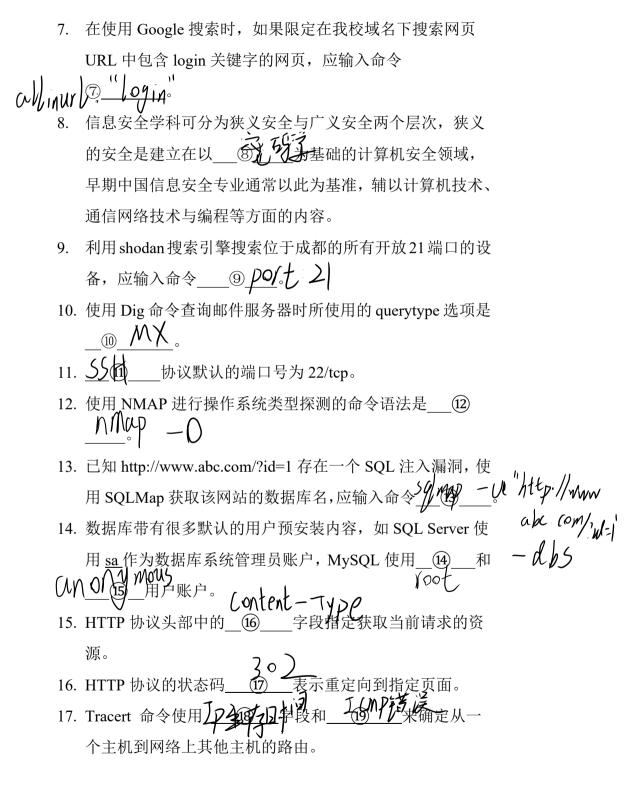




- 在整个 CSRF 的攻击过程中, 交易是以受害者的身份发起 的。
- 3. XSS 是由于 Web 应用程序对用户的输入过滤不足而产生的



4.	进行上传漏洞攻击不需要知道木马上传的路径。
5.	如果一个网站存在 XSS,不可能也存在 CSRF。 X
6.	htmlspecialchars() 函数把预定义的字符转换为 HTML 实体。 \/
7.	VPN、SSL、SSH 等加密手段可有效防范 Wireshark 的嗅探。
8.	运行命令 ipconfig /release,可以重新获取到 DHCP 分配的
	IP 地址。
9.	whois 的查询是逐级查询。 V
10.	在 google 高级搜索功能中,搜索指定文件类型的网页所使
	用的搜索关键字是 intitle。 🗶
三、	<i>/</i> ` 填空题,请将答案填入下列对应方框中。
1.	在安全漏洞生命周期中,从安全漏洞被发现到厂商发布补
	丁程序用于修补该漏洞之前的这段时间,被安全社区普遍
	地称为 <u>①</u> ② day
2.	信息安全三原则俗称 CIA 是指的机密性、完整性 J
	2 THE DOME DOME
3.	XSS 攻击可分为反射型、存储型和③ UNITED TO THE TOTAL TO THE TOTAL TOTA
4.	Cookie,有时也用其复数形式 Cookies,指某些网站为了辨
	别用户身份、进行 session 跟踪而 的数据 通常
,	经过加密)。它是用户和服务器之间的桥梁。
5.	<u> </u>
	构。
6.	HTTPS 协议的默认端口号是



18. 暴力破解因场景、______、认证方式的不同,所采用的 破解方法也是不同的。

四、 简答题。

五、分析题

1. 请分析下面的代码,并回答问题。

某网站保存留言页面 saveleaveword.php 的部分内容如下:

if(mysqli_query(\$conn,"insert into tb_leaveword(userid,createtime,title,content)values('\$userid','\$creat etime','".\$_POST['title']."',"".\$_POST['content']."')")){
 echo "<script>alert('留言发表成功! ');history.back();</script>";
}else{

echo "<script>alert(' 留 言 发 表 失 败 !
');history.back();</script>";

...

}

lisi 构造了一个 cookie.php 页面,代码如下:

<?php

```
$cookie = $ GET['cookie'];
  $log = fopen("cookie.txt", "a+");
  fwrite($log,$cookie . "next\n\r");
  fclose($log);
?>
```

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?

存在XSS编洞、攻击荒州各是宣化的强力发表的多样存在数据的

(2) lisi 构造的 cookie.php 页面主要实现什么功能。

用低下放接收收入的cookie,并将其这种保存在cookie txt中

请分析下面的代码,并回答问题

```
<?php
if( isset( $ GET[ 'Submit' ] ) ) {
         // Get input
         $id = $ GET[ 'id' ];
         // Check database
         $getid = "SELECT first name, last name FROM users WHERE user id = '$id';";
         $result = mysqli query($GLOBALS[" mysqli ston"], $getid ); -
         // Get results
         $num = @mysqli num rows( $result );
         if( $num > 0 ) {
                  // Feedback for end user
                  $html .= 'User ID exists in the database.';
         else {
                  // User wasn't found, so the page wasn't!
                  header( $ SERVER[ 'SERVER PROTOCOL' ] . ' 404 Not Found' );
                  // Feedback for end user
                  $html .= 'User ID is MISSING from the database.';
         ((is null($ mysqli res = mysqli close($GLOBALS[" mysqli ston"]))) ? false : $ mysqli res);
}
```

接收到01月日中,可能 页的链接是 http://www.cuit.cn/login.php?id=1

?id=| sclect 1,2,3 -- ** * 页片分 select, 1,2, databasec) --

攻击语句,并简单阐述攻击思路?

```
3. 请分析下面的代码,并回答问题:
  function blacklist($id)
  {
    $id= preg replace('/or/i',"", $id);
    $id= preg replace('/and/i',"", $id);
    return $id;
 }
(1) Web 应用考虑了对用户输入的 id 进行过滤限制。 该语句
                  01
对什么进行了过滤?
击者构造了一个js文件,内容如下所示:
    document.body.innerHTML=(
    '<div
 style="position:absolute;top:-2px;left:-2px;width:100%;height:100%;"
 >'+
    '<iframe src=http://localhost/xss/login/phishing.html width=100%
 height=100% frameborder="no" marginwidth="0" marginheight="0"
 scrolling="no">'+
    '</iframe></div>');
```

用工产的LESTES 了手它面,在力量外面是有多种的作用是什么。

- accept JPEG or PNG images.';
 }
 - (1) 这段代码存在什么漏洞? 具体产生漏洞的原因是什么?
- (2) 请简单阐述如果成功实施攻击获得 webshell。
- (1) 文件上件温湿。 没有对上程的文件的名字是儿子类型性 发发制, 导致攻击和确立上投那文件摩其正服务器上执行。
- (2) 将导好的一句话本写文件进行上後,土楼的时间即即以下城包,将 Content Type 中的基型楼垫为 imagel ipeg 然后做包。用对多连线上传的文件就得wohshell。