应用安全

Web 安全 P10

定义 P10

Web（World Wide Web）即全球广域网，也称为万维网，它是一种基于超文本和 HTTP 的、全球性的、动态交互的、跨平台的分布式图形信息系统；为浏览者在 Internet 上查找和浏览信息提供了图形化的、易于访问的直观界面；Web 应用程序是运行在 Web 服务器上的应用软件，这些应用程序使用客户机/服务器（Client/Server）建模的结构进行编程。

XSS 攻击 P11~12

XSS 是攻击者通过往 Web 页面里插入恶意可执行网页脚本代码，当其他用户测览被攻击的 Web 页面时，注入其中的恶意代码就会被执行，从而达到攻击者盗取、侵犯其他用户隐私的目的。

防御方法 P13

一般有字符转义和 CSP 白名单

跨站请求伪造 CSRF P14

利用用户已登录的身份，在用户毫不知情的情况下，以用户的名义完成非法操作

CSRF 攻击的三个条件：用户已经登录了站点 A，并在本地记录了 cookie；在用户没有登出站点 A 的情况下（cookie 生效的情况下），访问了恶意攻击者提供的引诱危险站点 B (B 站点要求访问站点A)；站点 A 没有做任何 CSRF 防御。

防范方法 P15：对 Cookie 设置 SameSite 属性，避免第三方网站访问到用户 Cookie；阻止第三方网站请求接口；请求时附带验证信息，比如验证码或者 Token。

SQL 注入 P16~17

SQL注入是指web应用程序对用户输入数据的合法性没有判断或过滤不严，导致攻击者可以在web应用程序中事先定义好的查询语句的结尾上添加额外的SQL语句在管理员不知情的情况下实现非法操作，以此来实现欺骗数据库服务器执行非授权的任意查询，从而进一步得到相应的数据信息。

SQL 注入防御方法 P18

将数据与代码分离，具体四种办法。

点击劫持 P19

点击劫持是一种视觉欺骗的攻击手段，攻击者将需要攻击的网站通过 iframe 嵌套的方式嵌入自己的网页中，并将 iframe 设置为透明，在页面中透出一个按钮诱导用户点击。

用户在登陆 A 网站的系统后，被攻击者诱惑打开第三方网站，而第三方网站通过 iframe 引入了 A 网站的页面内容，用户在第三方网站中点击某个按钮（被装饰的按钮），实际上是点击了 A 网站的按钮。

URL 跳转漏洞 P21

借助未验证的URL跳转，将应用程序引导到不安全的第三方区域，从而导致的安全问题。黑客利用URL跳转漏洞来诱导安全意识低的用户点击，导致用户信息泄露或者资金的流失。原理：黑客构建恶意链接(链接需要进行伪装,尽可能迷惑)，发在QQ群或者是浏览量多的贴吧/论坛中，安全意识低的用户点击后，经过服务器或者浏览器解析后，跳到恶意的网站中。

OS 命令注入攻击 P22

OS命令注入攻击：通过Web应用，执行非法的操作系统命令达到攻击的目的。OS命令注入和SQL注入差不多，只不过SQL注入是针对数据库的，而OS命令注入是针对操作系统的。只要在能调用Shell函数的地方就有存在被攻击的风险。倘若调用Shell时存在疏漏，就可以执行插入的非法命令。命令注入攻击可以向Shell发送命令，让Windows或Linux操作系统的命令行启动程序，也就是说，通过命令注入攻击可执行操作系统上安装着的各种程序。

CDN 安全 P24

CDN 定义 P24

CDN（Content Delivery Network, 内容分发网络）：当前提高网站的性能、可靠性与安全性的最佳实践之一。CDN 是由分布在不同地理位置的服务器集群组成的分布式网络。目标：帮助其客户网站实现负载均衡、降低网络延迟、提升用户体验、过滤 SQL 注入等攻击，分散拒绝服务攻击的流量。

P25 工作流程

用户点击APP， APP会根据URL地址去DNS寻求IP地址解析。DNS服务器发现对应URL有CDN服务，将会返回CDN服务器对应的IP。用户向CDN服务器发起内容URL访问请求，如果CDN服务器有缓存内容，进行第4步，否则第5步。CDN服务器响应用户请求，将用户所需内容传送到用户终端。CDN缓存服务器上并没有用户想要的内容，CDN向网站的源服务器请求内容；源服务器返回内容给缓存服务器，缓存服务器发给用户。

P26 CDN 优势

加速了网站的访问，CDN 提供一定安全性。

P27 ~ 33 RangeAmp 攻击

通过一些漏洞，可以通过CDN进行DoS攻击，从而破坏原有系统的可用性。

RangeAmp攻击：一台电脑便可让世界上最流行的网站瘫痪，一种利用CDN和HTTP协议设计缺陷对任意部署Web服务的站点实施DDoS的攻击。

CDN和HTTP范围请求（range requests）机制都致力于提升网络性能，但是CDN对HTTP范围请求机制的实现存在安全缺陷，攻击者能够滥用CDN的漏洞对源网站服务器或其他CDN节点实施DDoS攻击。

1. P28~29 HTTP Range 请求
2. P30 CDN 处理 Range 请求
3. P31小字节范围攻击
4. P32 重叠字节范围攻击
5. P33 解决方案：服务器侧，CDN侧，协议侧

社交网络安全 P34

P35 数据挖掘

数字档案收集，运维数据收集。

P36 垃圾信息传递

增加网络负载；信任缺失；身份假冒。

P37 网络钓鱼

攻击者可以伪装成为合法用户的好友，通过各种诱惑手段使得用户访问恶意URL。社交网络用户为了达到结交朋友的目的，并不排斥与陌生人沟通并接受交友邀请，因此，钓鱼攻击很容易发生。

P38 女巫攻击 Sybil attack

伪装成为多种身份参与到正常网络中，一方面利用虚假身份盗取合法用户的各种数据；另一方面影响数据转发路径，从而可伪造出多条不同的路由，破坏网络的可用性。

P40 女巫攻击账号检测

特征提取，联通图构建， Sybils检测。

云计算安全 P42

P42 定义

云计算的定义：通过网络按需提供可动态伸缩的廉价计算服务；是与信息技术、软件、互联网相关的一种服务。

云计算的五大特点：大规模；虚拟化；高可用性和扩展性；按需服务；网络安全。

P43 服务类型

基础设施即服务IaaS (Infrastructure as a Service)：向云计算提供商的个人或组织提供虚拟化计算资源；如虚拟机、存储、网络和操作系统等。

平台即服务PaaS (Platform as a Service)：为开发人员提供通过互联网构建应用程序和服务的平台；开发、测试和管理软件应用程序提供按需开发环境。

软件即服务SaaS (Software as a Service)：通过互联网提供按需软件付费应用程序；云计算提供商托管和管理软件应用程序；允许其用户连接到应用程序并通过互联网访问应用程序。

P44 虚拟化与虚拟机

虚拟化是为一些组件（例如虚拟应用、服务器、存储和网络）创建基于软件的（或虚拟）表现形式的过程；虚拟计算机系统称为“虚拟机”(VM)，它是一种严密隔离且内含操作系统和应用的软件容器；表面来看，这些虚拟机都是独立的服务器，但实际上，它们共享物理服务器的CPU、内存、硬件、网卡等资源。

P45 Hypervisor 虚拟机监视器

Hypervisor，又称虚拟机监视器（virtual machine monitor，缩写为 VMM），是用来建立与执行虚拟机器的软件、固件或硬件。

P46 OpenStack 云管理平台

KVM这样的Hypervisor软件，实际上是提供了一种虚拟化能力，模拟CPU的运行，更为底层，但是它的用户交互并不良好，不方便使用。为了更好地管理虚拟机，就需要OpenStack这样的云管理平台。负责管理计算资源、存储资源、网络资源。本身不具备虚拟化能力，来自于各种虚拟化技术，VM、KVM、OpenStack等，都主要属于IaaS（基础设施即服务）

P47 Docker

容器（Container）：虚拟机是操作系统级别的资源隔离，而容器本质上是进程级的资源隔离

Docker是创建容器的工具，是应用容器引擎：启动时间很快，达到秒级，且对资源的利用率高（一台主机可以同时运行几千个Docker容器）；占用空间很小，虚拟机一般需几GB到几十GB，而容器仅需要MB级甚至KB级。

P48 K8S Kubernetes

K8S是Kubernetes的简称，中文意思是舵手或导航员。K8S是一个容器集群管理系统，主要职责是容器编排——启动容器，自动化部署、扩展和管理容器应用，还有回收容器。Docker和K8S，关注的不再是基础设施和物理资源，而是应用层，所以就属于PaaS。

P49 虚拟机逃逸

虚拟机逃逸指程序脱离正在运行并与主机操作系统交互的虚拟机的过程。虚拟化技术虽然可以在逻辑上提供软硬件的隔离，从而将各个用户分隔开，然而通过一些漏洞，虚拟机中的应用可以逃逸出逻辑的隔离，直接控制主操作系统，从而造成破坏。

P50 提权攻击

提权攻击是指用户通过系统漏洞，提升自己操作系统的使用权限的攻击。最简单的方法就是直接猜测管理员的弱口令等。比较可靠的提权方法就是攻击机器的内核，让机器以更高的权限执行代码，进而绕过设置的所有安全限制。

P51 侧信道攻击

侧信道攻击通过共享的信息通道，可以窃取到通道中的额外秘密。云计算中，虚拟机共享宿主硬件（CPU、内存、网络接口），因此可以通过CPU的计算时间，网络接口的占用时间，一定程度分析出其他用户的数据。已有攻击者利用侧信道攻击成功获取服务器中的私钥。

P52 镜像和快照攻击

镜像攻击：云计算平台往往通过特定的景镜像创建虚拟机或者服务实例。镜像的实例化是高度自动化的。攻击者入侵虚拟机管理系统并感染镜像。增大攻击效率和影响范围。

快照攻击：云平台可以随时挂起虚拟机并保存系统快照。攻击者非法恢复快照，造成一系列的安全隐患，且历史数据被清除，攻击行为被隐藏。

物联网安全 P53

定义 P53

物联网（Internet of Things）：通过各种信息传感器、射频识别技术、全球定位系统等，实时采集任何需要监控、连接、互动的物体或过程。通过各类可能的网络接入，实现物与物、物与人的泛在连接，实现对物品和过程的智能化感知、识别和管理。一个基于互联网、传统电信网等的信息承载体。让所有能够被独立寻址的普通物理对象形成互联互通的网络。

结构与挑战 P54 ~ 56

- 综合应用层：服务各种需求的物联网应用
- 管理服务层 : 将大规模数据存储、处理、 分析
- 网络构建层 : 使得感知设备接入互联网中
- 感知识别层 : 物理世界与信息世界的纽带， 获取现实世界的物理数据

移动应用安全 P57

P58 防御手段

- 源代码层面：应用代码调用的组合分析出潜在的恶意行为，从而进行识别
- 应用分发渠道层面：被篡改、盗版、二次打包、注入、反编译等破坏，需要对应用进行加固保护，构建正版指纹信息库
- 智能终端安全监测层面：通过样本特征、行为或者缺陷等分析技术，在终端处进行安全监控，检测异常行为，进行安全控制

应用安全攻击的共性特征及防御 P60

资源有限 DDoS P61

DDoS攻击（Distributed Denial of Service）：通过大量合法的请求占用大量网络资源，以达到使网络瘫痪的目的

分类：通过使网络过载来干扰甚至阻断正常的网络通讯；通过向服务器提交大量请求，使服务器超负荷；阻断某一用户访问服务器；阻断某服务与特定系统或个人的通讯。

占用网络资源类型：网络带宽、磁盘读写、CPU计算等。

Web、CDN、物联网、云计算都面临对应的安全风险

资源共享 非法访问 P62

攻击者可以合法、或者非法地获取应用数据，进而推理构造出目标数据

合法的越权访问：一些网络应用的数据是相互共享的，所有用户都可以合法的使用；这些数据往往由于隐私保护存在缺陷（差分隐私，互补隐私等）；这类攻击形式在Web应用和社交网络中最为常见。

非法的访问资源：逻辑上相互独立的用户数据存放在相同的一片物理区域；攻击者利用一些漏洞，非法访问其他用户的数据，造成一定程度的数据泄露；这种攻击形式主要存在于云计算中。

系统漏洞 P63

现有计算机体系结构复杂、应用丰富；不能确保多变、异构的应用硬件和软件的实现万无一失
完全没有任何漏洞是不可能的；漏洞的及时修复也存在问题。

防御原理 P64

1. P65 身份认证和访问控制：身份认证是保证信息安全的第一道门户；用户在被确认身份之后在信息系统中根据身份所有的权限享受相应的信息服务。
2. P66 隐私保护：隐私数据的泄露会引起严重的危险后果，通过身份认证和信任管理可以一定程度保护隐私，但是无法从数据本身保护；利用一些隐私保护算法或者技术来对隐私数据进行保护。
3. P67 监控防御，用第三方软件：一定网络应用系统的漏洞是无法避免的；在网络发生被攻击、破坏的情况下，可以通过监控检测，快速识别、恢复网络应用的服务，减少损失；在网络系统各个点上部署安全防御措施，避免出现安全的木桶效应。

典例

1. P69 微博被 XSS 攻击
2. P75 微信广告
3. P76 剑桥分析操纵大选