**西安邮电大学**

**网络空间安全学院**

**平时考核报告**

**（2022/ 2023学年第1学期）**

课程名称： 网络空间安全导论

学生姓名： 王璐

专 业： 网安2101班

学 号： 26213035

指导教师： 冯景瑜

**网络空间安全导论课程平时考核成绩表**

|  |  |  |  |
| --- | --- | --- | --- |
| **学生姓名** | **王璐** | **班级/学号** | **网安2101/26213035** |
| **指导教师** | **冯景瑜** | **职务或职称** | **副教授** |
| **案例分析**  **（60分）** | **案例分析一**  **（20分）** |  | |
| **案例分析二**  **（20分）** |  | |
| **案例分析三**  **（20分）** |  | |
| **大作业**  **（40分）** |  | | |
| **总分**  **（100分）** |  | | |

**案例分析一**

**“拒绝服务”这个词来源于英文Denial of Service（简称DoS），它是一种简单的破坏性攻击，通常攻击者利用TCP/IP协议中的某个弱点，或者系统存在的某些漏洞，对目标系统发起大规模的进攻，致使攻击目标无法对合法的用户提供正常的服务**。

**材料**：2016年10月21黑客通过互联网控制了美国大量的网络摄像头和相关的 DVR 录像机，然后操纵这些「肉鸡」攻击了美国的多个知名网站，包括 Twitter、Paypal、Spotify 在内多个人们每天都用的网站被迫中断服务。据了解，黑客们使用了一种被称作「物联网破坏者」的 Mirai 病毒来进行肉鸡搜索。更为致命的是，Mirai 病毒的源代码在 9月的时候被开发者公布，致使大量黑客对这个病毒进行了升级，传染性、危害性比前代更高。Mirai 病毒是一种通过互联网搜索物联网设备的一种病毒，当它扫描到一个物联网设备（比如网络摄像头、智能开关等）后就尝试使用默认密码进行登陆（一般为 admin/admin，Mirai 病毒自带 60 个通用密码），一旦登陆成功，这台物联网设备就进入「肉鸡」名单，开始被黑客操控攻击其他网络设备。根据国外网站 KerbsonSecurity 的调查，导致大规模断网事件的原因绝非我们想象的那么简单，其背后暴露出物联网设备的重大安全隐患。据报道，一共有超过百万台物联网设备参与了此次 DDoS 攻击。

**问题：**分析电脑主机被DDOS攻击时的会出现哪些现象？如何防范DDOS攻击？

**一、ddos定义**

  DDOS（Distribution Denial of Service，中文名为分布式拒绝服务攻击）是指处于不同位置的多个攻击者同时向一个或数个目标发动攻击，或者一个攻击者控制了位于不同位置的多台机器并利用这些机器对受害者同时实施攻击。DDOS是一种分布的、协同的大规模攻击方式，攻击时可以对源IP地址进行伪造，非常难以防范。

二、如何预防ddos攻击  
  1、定期扫描：要定期扫描现有的网络主节点，清查可能存在的安全漏洞，对新出现的漏洞及时进行清理。骨干节点的计算机因为具有较高的带宽，是黑客利用的最佳位置，因此对这些[主机](https://www.xinnet.com/tag/11139" \t "/Users/wanglu/Documents\\x/blank)本身加强[主机安全](https://www.xinnet.com/tag/25350" \t "/Users/wanglu/Documents\\x/blank)是非常重要的。而且连接到网络主节点的都是[服务器](https://www.xinnet.com/tag/12523" \t "/Users/wanglu/Documents\\x/blank)级别的计算机，所以定期扫描漏洞就变得更加重要了。  
  2、在骨干节点配置防火墙：防火墙本身能抵御DdoS攻击和其他一些攻击。在发现受到攻击的时候，可以将攻击导向一些牺牲主机，这样可以保护真正的主机不被攻击。当然导向的这些牺牲主机可以选择不重要的，或者是linux以及unix等漏洞少和天生防范攻击优秀的系统。  
  3、用足够的机器承受黑客攻击：这是一种较为理想的应对策略。如果用户拥有足够的容量和足够的资源给黑客攻击，在它不断访问用户、夺取用户资源之时，自己的能量也在逐渐耗失，或许未等用户被攻死，黑客已无力支招儿了。不过此方法需要投入的资金比较多，平时大多数设备处于空闲状态，和目前中小企业网络实际运行情况不相符。  
  4、充分利用网络设备保护网络资源：所谓网络设备是指路由器、防火墙等[负载均衡](https://www.xinnet.com/tag/11199" \t "/Users/wanglu/Documents\\x/blank)设备，它们可将网络有效地保护起来。当网络被攻击时最先死掉的是路由器，但其他机器没有死。死掉的路由器经重启后会恢复正常，而且启动起来还很快，没有什么损失。若其他服务器死掉，其中的数据会丢失，而且重启服务器又是一个漫长的过程。特别是一个公司使用了负载均衡设备，这样当一台路由器被攻击死机时，另一台将马上工作。从而最大程度的削减了DdoS的攻击。  
  5、过滤不必要的服务和端口：过滤不必要的服务和端口，即在路由器上过滤假IP……只开放服务端口成为目前很多服务器的流行做法，例如WWW服务器那么只开放80而将其他所有端口关闭或在防火墙上做阻止策略。   
  6、检查访问者的来源：使用Unicast Reverse Path Forwarding等通过反向路由器查询的方法检查访问者的IP地址是否是真，如果是假的，它将予以屏蔽。许多黑客攻击常采用假IP地址方式迷惑用户，很难查出它来自何处。因此，利用Unicast Reverse Path Forwarding可减少假IP地址的出现，有助于提高[网络安全](https://www.xinnet.com/tag/25292" \t "/Users/wanglu/Documents\\x/blank)性。

  7、过滤所有RFC1918IP地址：RFC1918 IP地址是内部网的IP地址，像10.0.0.0、192.168.0.0 和172.16.0.0，它们不是某个网段的固定的IP地址，而是Internet内部保留的区域性IP地址，应该把它们过滤掉。此方法并不是过滤内部员工的访问，而是将攻击时伪造的大量虚假内部IP过滤，这样也可以减轻DdoS的攻击。

三、ddos攻击时会出现什么现象  
  1、被攻击主机上有大量等待的TCP连接；  
  2、网络中充斥着大量的无用的数据包，源地址为假；  
  3、制造高流量无用数据，造成网络拥塞，使受害主机无法正常和外界通讯；  
  4、利用受害主机提供的服务或传输协议上的缺陷，反复高速的发出特定的服务请求，使受害主机无法及时处理所有正常请求。

**案例分析二**

**网络钓鱼是通过大量发送声称来自于银行或其他知名机构的欺骗性垃圾邮件，意图引诱收信人给出敏感信息(如用户名、[口令](https://baike.so.com/doc/6537624-6751363.html" \t "_blank)、帐号 ID 、 ATM PIN 码或信用卡详细信息)的一种攻击方式。**

**材料：**网络钓鱼是上世纪90年代中期以来兴起的一种网络诈欺行为。自从1996年前后在美国首先发生之后，迅速扩散到其他发达的欧洲资本主义国家。近几年，中国也屡次发生网络钓鱼攻击的案件，而且形势是愈演愈烈。最典型的网络钓鱼攻击是将收信人引诱到一个通过精心设计与目标组织的网站非常相似的钓鱼网站上，并获取收信人在此网站上输入的个人敏感信息，通常这个攻击过程不会让受害者警觉。在网络钓鱼活动中至少涉及两个角色，分别是钓鱼者（phisher）和受害者（victim），钓鱼者诱骗受害者，在未授权情况下获取对方的姓名、年龄、邮箱账号、甚至是银行卡密码等私人信息。网络钓鱼活动往往和运用社会工程学（social engineering）知识相结合进行诱导，社会工程学可以看作是黑客的“内功”，能否灵活运用可以体现一个犯罪分子的攻击手段高低。2018年，电子邮件安全提供商VadeSecure发布了一份新的网络钓鱼报告，该报告记录了北美地区25个被威胁分子伪装从而进行网络钓鱼攻击的企业公司。在这些企业公司中，网络钓鱼攻击最喜欢伪装成微软、Paypal和Netflix这些顶级企业公司。在他们的2018年第三季度报告中，共调查了86个企业公司，占到了该公司检测到的所有攻击的95％

**问题：**分析网络钓鱼的攻击步骤有哪些？如何在生活中防范网络钓鱼？

网络钓鱼手法一，发送电子邮件，以虚假信息引诱用户中圈套。

不法分子大量发送欺诈性电子邮件，邮件多以中奖、顾问、对账等内容引诱用户在邮件中填入金融账号和密码，或是以各种紧迫的理由要求收件人登录某网页提交用户名、密码、身份证号、信用卡号等信息，继而盗窃用户资金。

网络钓鱼手法二，建立假冒网站骗取用户账号密码实施盗窃。

不法分子建立起域名和网页内容都与真正的网上银行系统、网上证券交易平台极为相似的网站，引诱受骗者输入账号密码等信息，进而窃取用户资金。

网络钓鱼手法三，利用虚假的电子商务进行诈骗。

不法分子在知名电子商务网站发布虚假信息，以所谓“超低价”、“免税”、“走私货”、“慈善义卖”等名义出售商品，要求受骗者先行支付货款达到诈骗目的。

网络钓鱼手法四，利用“木马”和“黑客”技术窃取用户信息。

不法分子在发送的电子邮件中或在网站中隐藏“木马”程序，在感染“木马”计算机上进行网上交易时，“木马”程序即以键盘记录方式获取用户账号和密码。

网络钓鱼手法五，网址诈骗。

不法分子设计的诈骗网站网址与正规网站网址极其相似，往往只有一个字母的差异，不仔细辨别很难发现。当用户登录虚假网站进行资金操作时，其财务信息将泄露。

网络钓鱼手法六，破解用户“弱口令”窃取资金。

不法分子利用部分用户贪图方便、在网上银行设置“弱口令”的漏洞，从网上搜寻到银行储蓄卡卡号，进而登录该银行网上银行网站，破解“弱口令”。

网络钓鱼手法七，手机短信诈骗。

由储存手机号码的电脑控制的手机短信“群发器”大量发出虚假信息，以“中奖”、“退税”、“投资咨询”等名义诱骗受骗者实施汇款、转账等操作。

**钓鱼网站的防范方法**

第一种方法：域名对比法

其实辨别钓鱼网站的最佳方法就是对比它的域名是不是官方域名，请一定要仔细查看您所打开页面后的具体网址，而不是只看打开网页前的网址。如果不是官方域名，哪怕页面再相似，那么我们都可以断定其为钓鱼网站。

第二种方法：聊天工具的反钓鱼功能

充分利用聊天软件的反钓鱼功能,一般来说骗子都是通过QQ或淘宝旺旺联系,而在这些聊天工具的窗口中就加入了反钓鱼网站的功能,它会在每个链接的前面显示一个信任图标,绿色打勾的图标才是受信任的,而有问号的图标大家就最好不要去点击!

第三种方法：不要泄露身份资料

养成良好的习惯,尽量不要在网上留下自己身份的任何资料,包括手机号码、身份证号、银行卡号码、电子商务网站账户等,这些资料都很可能被一些不发分子利用。

第四种方法：利用杀毒软件

很多杀毒软件都具有反钓鱼功能,可以给网站进行把关了,一旦误入了一些钓鱼网站,软件就会自动弹出警告和提示。

钓鱼网站攻击的过程

攻击原理:

钓鱼网站攻击是指在上网时引导用户访问精心伪造的虚假网站，骗取用户的个人信息。

典型攻击——QQ页面伪造钓鱼

1.攻击方式:

搭建类似QQ首页的网站，诱导用户点击，登录并获取用户信息。

2.攻击流程：

(1)根据www.qq.com的页面元素，精心构造样式一样的网站；

(2) 利用SEO，将伪造的网址置于搜索引擎结果页的首页位置；

(3) 用户访问钓鱼网站，输入正确的QQ号和密码。此时已经获取到了基本的QQ号码信息；

(4) 前三次无论输入任何号码和密码都反馈用户输入错误，之后引导用户利用密保问题寻回密码，进而获得用户的密码保护问题信息；

(5)此时用户的QQ账户密码以及个人密保信息均已泄露。

防护手段:

1.安装最新的杀毒客户端，对上网行为进行防护。

2.使用专业的安全网关，智能识别钓鱼网站，避免财产损失。

**案例分析三**

**验证码（CAPTCHA）是“Completely Automated Public Turing test to tell Computers and Humans Apart”（全自动区分计算机和人类的图灵测试）的缩写，是一种区分用户是计算机还是人的公共全自动程序。**

**材料：**验证码恶意破解密码、刷票、论坛灌水，有效防止某个黑客对某一个特定注册用户用特定程序暴力破解方式进行不断的登陆尝试，实际上用验证码是现在很多网站通行的方式，我们利用比较简易的方式实现了这个功能。这个问题可以由计算机生成并评判，但是必须只有人类才能解答。由于计算机无法解答CAPTCHA的问题，所以回答出问题的用户就可以被认为是人类。然而，尽管验证码对表单提交流程的安全起到了很重要的作用，但其自身的安全性却为很多站点所忽略，以致成为新的安全隐患。比如，文本验证码内容会原原本本地写在用户浏览到的网页中，编写程序对HTML文件进行一定分析后，同样可以获知验证码内容。短信验证码可能造成对手机的DoS攻击：将指定手机号用于接收验证码，编写程序不断向服务器提交请求，就会使该手机不断收到验证码短信，对用户造成骚扰，甚至导致手机死机等后果。

**问题：**分析当前较为常见的验证码类型？验证码攻击的防范方法有哪些？

1、数字验证码

数字验证码：比较常见的是短信验证码和语音验证码，一般是由系统将验证码短信发送到用户填写的手机号码或者系统记录好的手机号码上，或者拨打该手机号码给客户语音播报验证码，此类验证码一般由4-6个数字组成。

2、字母验证码

字母验证码：常见于短信验证和web网站应用，其中web网站应用更为常见。展现形式为，在页面的验证码输入框附近以图片的形式展示字母，用户通过识别字数获取验证码，此类验证码一般由4个字母组成，也有字母与数字的混合组合，一般不区分大小写。

**3、文字验证码**

文字验证码：常见于web网站应用。展现形式与字母验证码相似，在验证码输入框附近以图片形式展示文字，用户通过识别图片中的文字获取验证码。此类验证码一般由4个文字（汉字）组成。

**4、图片验证码**

图片验证码：常见于web网站应用。展现形式为根据页面提示选择正确的图片，比如12306网站，会在图片区域展示8张图片，系统提示某个名词，如：仙人掌，用户则需要按照系统要求展示的图片中所有含有仙人掌的图片，不能错选，也不能漏选。

除了以上四种验证码之外，还有一种比较少见的验证码类型，就是通过数学等式获取验证码，比如，系统的验证条件为“4-1=”或“4减1=”，我们可以明显的得出答案是3，那么这个验证码就是3，只要在指定位置输入数字3就能完成验证。

除了上面的分类以外，我们还可以根据接收方式将验证码分为手机验证码和电脑验证码。不论是何种形式的验证码，企业的最终目的都是为了保护用户的账户信息与财产安全。因此，用户在接收验证码后，一定要保护好自己的验证码，避免因验证码丢失而造成损失。

防范措施：

１、静态密码设置一定要复杂

静态密码首先要足够复杂，并妥善保管防止泄露。其次，攻击者经常利用各种手段对短信进行伪装，并千方百计地对攻击对象进行误导、甚至恐吓。所以一定要对"运营商"、"银行"等身份的手机短信和来电进行认真甄别，冷静应对。

２、遭遇“干扰信息”仔细甄别莫慌张

攻击者经常利用各种手段对短信进行伪装，并千方百计地对攻击对象进行误导、甚至恐吓。所以一定要对“运营商”、“银行”等身份的手机短信和来电进行认真甄别，冷静应对。

３、手机离奇“瘫痪” 紧急“挂失”当先

如果手机通讯出现瘫痪，一定要马上查清故障原因。如非手机本身或信号故障，要立刻挂失手机卡，并及时冻结第三方支付和银行账户，避免攻击者趁用户处于"信息孤岛"时，冒名顶替机主身份窃取账户。

４、短信验证码不要告诉任何人！

最最重要的是：短信验证码不要告诉任何人！电信运营商和提供相关服务的企业只会将短信验证码下发给用户，绝对不会要求用户通过短信或电话进行所谓“回复验证码”的操作。

**大作业**

**结合课程所学，列出网络空间安全领域有哪些网络攻防方向？选择某一个网络攻防方向展开，详细说明具体的学习路线、能力的提升途径、未来的职业规划等。（1000字以上）**

**第一类 网络安全方向**

网络安全领域是安全行业最基本的领域，研究的技术范畴主要围绕防火墙/NGFW/UTM、网闸技术、入侵检测/防御、VPN网关（IPsec/SSL）、抗DDOS、上网行为管理、负载均衡/应用交付、流量分析、漏洞扫描等。

**第二类 主机安全方向**

主机安全主要研究Windows、Linux、micros系统的安全问题，如何保障电脑和服务器的安全，就是这个方向需要解决的。

主机网络安全体系涉及到的技术主要包括：入侵检测、访问控制、加密传输、身份认证。

为了应对外在环境的不断演进，主机安全防护软件也在不断更新迭代，衍生出了一系列细分领域的主机安全产品。从主机安全产品发展级别来看，大体上可以概括为“基础性的主机安全产品”、“以应用为核心的主机安全产品”、“以检测响应为核心的主机安全产品”、“以主动防御为核心的主机安全产品”、“新形态下的主机安全产品”五个阶段。

**第三类**  **Web安全方向**

web安全主要分为保护服务器及其数据的安全、对WEB客户机的安全威胁、对通信信道的安全威胁这三个方面。

**第四类 移动安全方向**

为了实现5G万物互联的宏伟愿景，5G必须实现智能化，以同时支持异构的网络（3G，4G和WiFi等接入方式）和设备（移动手持设备、物联网设备）对资源的正常使用。而智能化需要实现移动通信技术与云计算、大数据、虚拟现实等信息技术的高度融合以及系统架构的创新。这些变革意味着5G将迎来全面的演进，包括核心和管理系统的演进以及无线端协议到应用层协议的演进。在这些演进中，安全的影响无处不在，5G将面临更复杂的安全挑战。

5G的安全面临的挑战主要是：接入安全（用户/设备认证抗拒绝服务攻击）、网络安全、用户安全、 应用安全、可信安全、安全管理、密码算法等。

**第五类 大数据安全方向**

大数据方向的安全研究主要包括：网络安全态势感知、高级持续威胁检测、伪基站发现与追踪、反钓鱼攻击、平台安全、 服务安全、数据确权问题、数据版权保护、数据跨境安全、供应链安全、敏感数据共享等。

**第六类 云计算安全方向**

云安全(Cloud Security）是一个从“云计算”演变而来的新名词。云安全就是基于云计算商业模式的安全软件、硬件、用户、机构安全云平台的总称。它通过对网络软件的行为进行监测，获取互联网中木马、恶意程序的最新信息，并发送到服务端进行自动分析和处理，再把病毒和木马的解决方案分发到每一个客户端。

“云安全”相关的技术可以分两类：

一类为使用云计算服务提供防护，即使用云服务时的安全（security for using the cloud），也称云计算安全（Cloud Computing Security）,一般都是新的产品品类；

一类源于传统的安全托管（hosting）服务，即以云服务方式提供安全（security provided from the cloud），也称安全即服务（Security-as-a-Service, SECaaS），通常都有对应的传统安全软件或设备产品。

**第七类 物联网安全方向**

随着 5G 等关键技术突破，物联网的发展突飞猛进，同时受疫情影响，远程办公需求增加，随之而来的是海量的设备接入互联网。“万物互联”带来便利的同时，也为攻击者带来了更多的攻击选择。物联网已经渗透进我们衣食住行的各个领域，频发的智能设备 攻击威胁着个人的隐私安全，关键基础设施在实现数字化联网转型时也面临巨大风险。物联网安全不应局限在技术方面提高智能设备的安全性能，在处理随之产生的海量数据时，也需要合理的法规和完善的管理方案，确保风险的及时发现、准确定位和高效恢复。

物联网安全问题主要涉及的有：数据安全、隐私、复制、RFID系统的威胁。

**第八类 工业互联网安全**

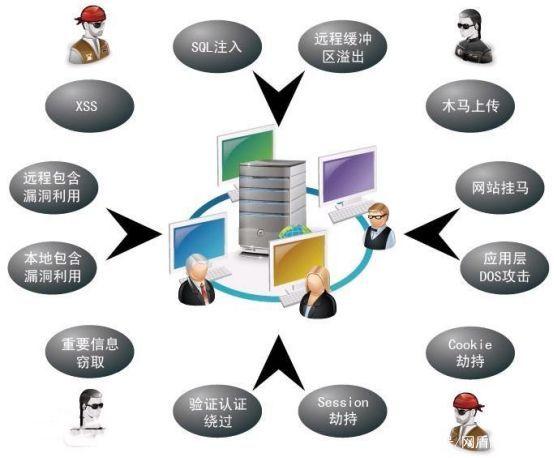
工业互联网有三个特征，一个数字化、网络化和智能化，这3个特征支撑着工业资源的优化配置。在数字化方面，目前工业互联网主要的体现在数字化的采集，数字化的设计，数字化的生产制造，数字化的管理，数字化建模等技术的应用。在网络化的特征，包括像5g等新一代信息基础设施，那么工业是以以太网、工业以太网边缘计算，业务协同在智能化的特征，包括大数据、人工智能等智能技术的运用，全生命周期的智能化的优化，生产制造系统本身的智能化，工控系统到工业互联网制造资源的接入方式范围，以工业生产的数据的去向，以资源优化配置的主体都发生了变化。

整个工业互联网安全涉及到六大安全的问题：设备的安全，控制的安全，网络的安全、标识解析的安全，平台的安全、数据的安全，其中标识解析的安全，平台的安全，数据的安全，是新生的安全问题，标识的安全是工业互联网安全的新问题。

**Web安全方向**

Web安全是计算机术语。随着Web2.0、社交网络等一系列新型的互联网产品诞生问世，基于Web环境的互联网应用越来越广泛，企业信息化的过程中各种应用都架设在Web平台上，Web业务的迅速发展也引起黑客们的窥探，接踵而至的就是Web安全威胁的凸显。

黑客利用网站操作系统的漏洞和Web服务程序的SQL注入漏洞等得到Web服务器的控制权限，轻则篡改网页内容，重则窃取重要内部数据，更为严重的则是在网页中植入恶意代码，使得网站访问者受到侵害。



目前，很多业务都依赖于互联网，无论是网上银行、网上购物、还是网络游戏等，恶意攻击者们出于各种不良目的，对Web 服务器进行攻击，想方设法通过各种手段获取他人的个人账户信息谋取利益。正是如此，Web业务平台最容易遭受攻击。

而针对Web服务器的攻击也是五花八门，常见的有挂马、SQL注入、缓冲区溢出、嗅探、利用IIS等针对Webserver漏洞进行攻击。

一方面，由于TCP/IP的设计是没有考虑安全问题的，网络上传输的数据是没有任何安全防护。攻击者们可利用系统漏洞造成系统进程缓冲区溢出，攻击者可能获得或者提升自己在有漏洞的系统上的用户权限来运行任意程序，甚至安装和运行恶意代码，窃取机密数据。

而应用层面的软件在开发过程中也没有过多考虑到安全的问题，这使得程序本身存在很多漏洞，诸如缓冲区溢出、SQL注入等等流行的应用层攻击，这些都属于在软件研发过程中疏忽了对安全的考虑所致。

另一方面，个人用户由于好奇心，被攻击者利用木马或病毒程序进行攻击，攻击者将木马或病毒程序捆绑在一些诱人的图片、音视频或免费软件等文件中，然后将这些文件置于某些网站当中，再引诱用户去单击或下载运行，或通过电子邮件附件和QQ、MSN等即时聊天软件，将这些捆绑了木马或病毒的文件发送给用户，让用户打开或运行这些文件。

**Web安全的三个细分**

Web安全主要分为:1、保护服务器及其数据的安全。2、保护服务器和用户之间传递的信息的安全。3、保护Web应用客户端及其环境安全这三个方面。

**Web应用防火墙**



Web应用安全问题本质上源于软件质量问题。但Web应用相较传统的软件，具有其独特性。Web应用往往是某个机构所独有的应用，对其存在的漏洞，已知的通用漏洞签名缺乏有效性；

需要频繁地变更以满足业务目标，从而使得很难维持有序的开发周期；需要全面考虑客户端与服务端的复杂交互场景，而往往很多开发者没有很好地理解业务流程；人们通常认为Web开发比较简单，缺乏经验的开发者也可以胜任。

Web应用安全，理想情况下应该在软件开发生命周期遵循安全编码原则，并在各阶段采取相应的安全措施。

**然而，多数网站的实际情况是：大量早期开发的Web应用，由于历史原因，都存在不同程度的安全问题。对于这些已上线、正提供生产的Web应用，由于其定制化特点决定了没有通用补丁可用，而整改代码因代价过大变得较难施行或者需要较长的整改周期。**

这种现状，专业的Web安全防护工具是一种合理的选择。WEB应用防火墙（以下简称WAF）正是这类专业工具，提供了一种安全运维控制手段：基于对HTTP/HTTPS流量的双向分析，为Web应用提供实时的防护。

**Web应用漏洞的防御实现**

对于常见的Web应用漏洞，应该从3个方面入手进行防御：

1、对 Web应用开发者而言

大部分Web应用常见漏洞都是在Web应用开发中，由于开发者没有对用户输入的参数进行检测或者检测不严格造成的。所以，Web应用开发者应该树立很强的安全意识，开发中编写安全代码；

对用户提交的URL、查询关键字、HTTP头、POST数据等进行严格的检测和限制，只接受一定长度范围内、采用适当格式及编码的字符，阻塞、过滤或者忽略其它的任何字符。通过编写安全的Web应用代码，可以消除绝大部分的Web应用安全问题。

2、对Web网站管理员而言

作为负责网站日常维护管理工作Web管理员，应该及时跟踪并安装最新的、支撑Web网站运行的各种软件的安全补丁，确保攻击者无法通过软件漏洞对网站进行攻击。

除了软件本身的漏洞外，Web服务器、数据库等不正确的配置也可能导致Web应用安全问题。Web网站管理员应该对网站各种软件配置进行仔细检测，降低安全问题的出现可能。

此外，Web管理员还应该定期审计Web服务器日志，检测是否存在异常访问，及早发现潜在的安全问题。

3、使用网络防攻击设备

前两种都是预防方式，相对来说很理想化。在现实中，Web应用系统的漏洞仍旧不可避免：部分Web网站已经存在大量的安全漏洞，而Web开发者和网站管理员并没有意识到或发现这些安全漏洞。

由于Web应用是采用HTTP协议，普通的防火墙设备无法对Web类攻击进行防御，因此需要使用入侵防御设备来实现安全防护。