云维互联安全服务方案v2.0

云维互联
技术部：田秋荣

目录

CONTENTS

Part ONE

1 Part

公司介绍

北京云维互联信息技术有限公司成立于2016年，是一家专注信息安全服务及定制化整体安全解决方案的高新技术企业。

我们公司具备ISO9000质量认证、CCRC信息安全风评资质、国家高新企业、北京市新技术新产品企业等资质。内部骨干人员来自知名外企，安全厂家和大型互联网公司。团队技术人员具有CISAW、PMP、CISP、CCIE、CISA、OSCP、SCSA、CSSLP、ITIL、COBIT、Security+证书 。

1 Part

公司介绍

企业文化

云维目标

提高各行业信息安全意识，
建立各企业纵深防御体系

云维使命

持续聚焦客户挑战及痛点，
提供有价值的服务与方案。

云维愿景

积极响应国家网络安全法，
为企业信息安全保驾护航。

Part TWO

2 Part

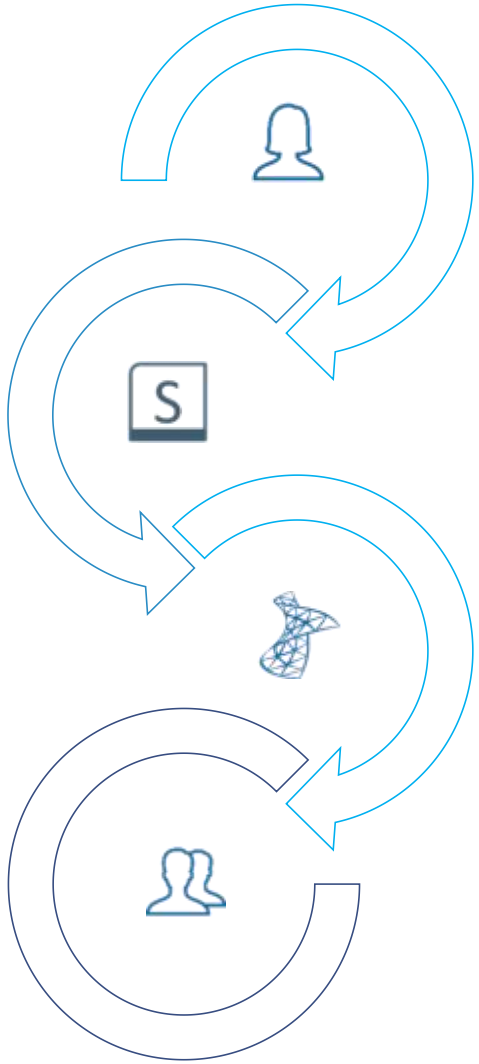
政策背景–网络安全法

第一次审议（2015年6月26日）明确了网络空间主权原则；对关键基础设施安全实行重点保护；加强网络安全监测预警和应急制度建设。

第二次审议（2016年6月28日）明确了重要数据境内存储，建立数据跨境安全评估制度并鼓励关键信息基础设施以外的网络运营者自愿参加关键信息基础设施保护体系。

第三次审议（2016年10月31日）进一步界定关键信息基础设施范围；增加了惩治攻击破坏我国关键信息基础设施的境外组织和个人的规定以及惩治网络诈骗等新型网络违法犯罪活动的规定；同时加强网络安全人才培养、保护未成年人上网安全的相关问题。

《网络安全法》正式发布（2016年11月7日），2017年6月1日实施。



客户的行业特定安全服务场景

等保建设对安全服务的硬性要求

客户针对安全体系建设的困难和弊端

客户业务对长久安全运营的刚性需要

客户对安全合规的迫切需求

2 Part 政策背景-等保

等级保护发展路线

1.计算机系统安全保护等级划分思想提出:
1994年国务院颁布的《计算机信息系统安全保护条例》；
1999年国家强制标准GB 17859——1999《计算机信息系统安全保护等级划分准则》发布；

2.等级保护工作试点:
2002年7月18日，公安部在GB17859的基础上，又发布实施了5个公安行业等级保护标准，分别是：GA/T 389——200《计算机信息系统安全等级保护网络技术要求》、GA 388——2002<计算机信息系统安全等级保护操作系统技术要求》、GA/T 390——2002<计算机信息系统安全等级保护数据库管理系统技术要求》、GA/T 390——2002<计算机信息系统安全等级保护通用技术要求》、GA/T 391——2002<计算机信息系统安全等级保护管理要求》；

3.等级保护相关政策文件颁布:
2004年，公安部、保密局、密码委、信息办联合发文《关于信息安全等级保护工作的实施意见的通知》；2007年，公安部、保密局、密码委、信息办联合发文《信息安全等级保护管理办法》；

4.等级保护相关标准发布:
GB/T 22239——2008《信息安全技术 信息系统安全等级保护基本要求》和GB/T 22240——2008《信息安全技术 信息系统安全等级保护定级指南》；

5.《网络安全法》明确我国实行网络安全等级保护制度:
2016年11月发布的《网络安全法》第二十一条明确指出“国家实行网络安全等级保护制度”。正式宣告在网络空间安全领域，我国将等级保护制度作为基本国策。同时也正式将针对信息系统的等级保护标准变更为针对网络安全的等级保护标准；
2017年8月，公安部评测中心根据网信办的安标委的意见将等级保护在编的5个基本要求分册标准进行了合并形成《网络安全等级保护基本要求》一个标准。

服务方式

1.调查问卷: 根据客户的业务情况和信息系统现状，制定详细的调查表，并由客户相关人员进行填写，以获得业务系统信息安全及管理情况，具体内容包括安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理机构、安全管理制度、安全管理人员、安全建设管理和安全运维管理等；
2.人员访谈: 针对组织内的安全管理人员、安全员、安全主管、工作人员、关键活动批准人、管理人员、机房值守人员、人事负责人、人事工作人员、审计员、网络管理员、文档管理员、物理安全负责人、系统管理员、系统建设负责人、系统运维负责人、资产管理员等不同类型岗位的人员访谈；
3.文档检查: 查看安全管理机构、安全管理制度、人员安全管理、系统建设管理、系统运维管理等方面的文档；
4.人工培植检查: 查看安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心等方面的技术配置信息；
5.漏洞扫描: 对网络设备、服务器、终端、操作系统（win/去问问/Solaris/AIX/）数据库（Oracle/SQL）、中间件、安全设备进行漏洞扫描；
6.渗透测试: 采用黑盒和白盒的技术手段对信息系统进行测试；
7.会议: 召集客户信息系统相关的技术人员、管理人员、使用人员以及应用系统的开发厂商、运维服务商等对系统基本情况进行识别和分析，并就安全风险测试项目进行讨论。

THREE

Part

3 Part 客户痛点

企业视角

国际信息安全立法在不断发展和完善，更多的组织在建立业务链的过程中所保留的用户信息、企业信息被国际相关法规明确规定了隐私保护、信息保护以及知识产权保护等权利和义务，使得组织一方面要考虑业务数据的可用性和完整性，另一方面还要关注它的保密性问题。

解决方案

根据具体客户项目，制定最优的方案。满足客户需求，提供最佳路径。针对客户的痛点业务连续性管理、资产保护、合规性进行合规方案的设计与制定。

客户痛点

信息部门人员少：没有研发团队，信息化建设基本靠外包开发实现；
没有专门安全团队：只有基础的运维人员，运维人员既要管理公司网络情况，还要关注公司的安全情况；
技术能力不强：运维人员只有简单的网络基础知识，对安全方面的技术掌握不多。

服务内容

服务范围	服务内容
基线核查	自动化检查基线，防止安全配置错误不自知，提供基线加固服务。
漏洞扫描	自动化漏扫，检查系统存在的脆弱性。
代码审计	自动化与人工的配合，检查代码规范性与代码安全性，找到网站脆弱性，给出相关安全措施。
渗透测试	以黑客的视角来看待问题，找到一些不易发现的漏洞。协助客户完善自己的系统。

5 Part 客户案例-某电商

电商介绍

有非常专业的开发团队，没有相应的安全部门。客户那边频频被恶意刷单，客户希望自己的产品安全得到保障。团队对安全只知其一不知其二，没有真正懂安全的人。

客户痛点

没有专门安全团队：只有基础的运维人员，运维人员既要管理公司网络情况，还要关注公司的安全情况；

解决方案

根据电商的特点和痛点，我们帮助电商解决了他们很棘手问题。前期做了一次基线，漏扫，后期提供对接式的渗透服务，即满足客户的开发需求，又体现了我们服务的价值。

服务内容

服务范围	服务内容
基线核查	自动化检查基线，防止安全配置错误不自知，提供基线加固服务。
漏洞扫描	自动化漏扫，检查系统存在的脆弱性。
渗透测试	以黑客的视角来看待问题，找到一些不易发现的漏洞。协助客户完善自己的系统。

典型案例

仁和 药房网 yaofang.com

索菲亚 柜类定制专家

5 Part 客户案例–某线上平台

线上介绍

某线上平台，经营自己的线上业务，同时拥有强大的安全开发团队，却没有安全渗透方面的人员。想要确保自己的代码是符合安全规范的，却没有代码审计。

客户痛点

安全团队人员稀缺：有安全团队，人员方面比较少，懂的广度不够。安全人员也只是开发安全软件的技术人员。

解决方案

线上平台有自己的开发团队，没有专业的安全人员。懂得开发安全产品，却没有安全服务的能力。针对这样的客户我们提供的解决方案是代码审计服务。代码审计服务针对的是代码质量规范和代码安全这两大方面的问题的解决方案。防止开发上线维护成本的剧增。

服务内容

服务范围	服务内容
代码审计	自动化与人工的配合，检查代码规范性与代码安全性，找到网站脆弱性，给出相关安全措施。

典型案例

仁和 药房网 yaofang.com

索菲亚 柜类定制专家

FOUR

Part

4 Part 产品业务流程-基线（加固）

基线核查服务介绍（是什么）

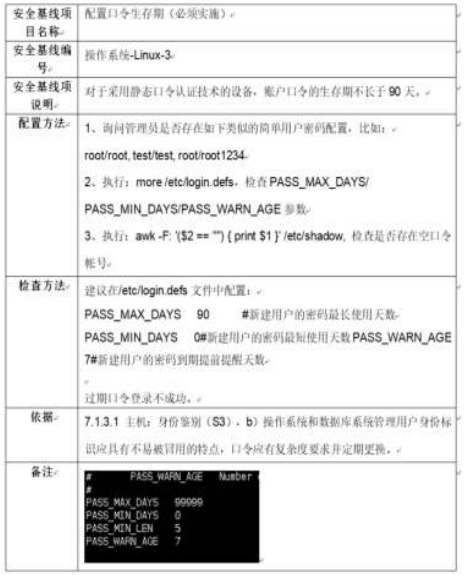
针对客户Windows、Linux操作系统的身份鉴别、访问、控制、安全审计、入侵防御、资源控制几大内容进行核查，找到操作系统的脆弱项内容，提出加固方案，最终抵御安全风险的发生。

应用场景	合规场景	配置安全持续巡检	入侵风险防范
解决问题	准备阶段	配置加固变更红线	弱口令高危治理
技术路径	等保标准Benchmarks	安全实践	高危配置风险

基线核查服务流程

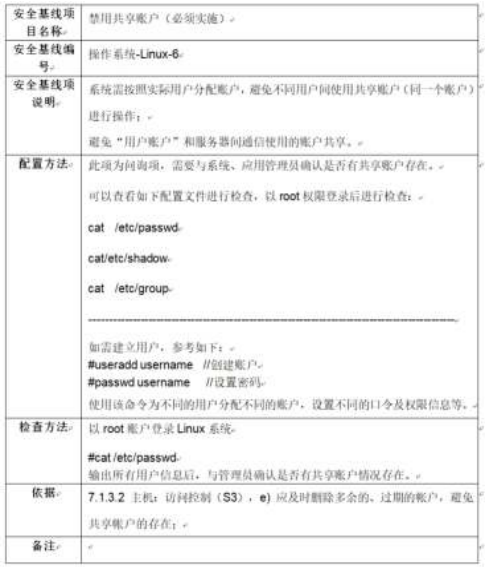
准备阶段 → 核查阶段 → 核查报告 → 加固阶段

阶段	工作内容
准备阶段	确认底层硬件资产、操作系统、网络环境
核查阶段	核查工具：身份、访问、审计、入侵、资源
核查报告	信息采集记录、核查记录、加固意见
加固阶段	报告讲解、加固协作跟踪、核查复验（亮点）



安全基线项目名称	配置口令生存期（必须实施）
安全基线编号	操作系统-Linux-3
安全基线项说明	对于采用静态口令认证技术的设备，账户口令的生存期不长于 90 天。
配置方法	1、询问管理员是否存在如下类似的简单用户密码配置，比如： root/root, test/test, root/root1234。 2、执行：more /etc/login.defs，检查 PASS_MAX_DAYS/ PASS_MIN_DAYS/PASS_WARN_AGE 参数。 3、执行：awk -F: '($2 == "") { print $1 }' /etc/shadow，检查是否存在空口令帐号。
检查方法	建议在/etc/login.defs 文件中配置： PASS_MAX_DAYS 90 #新建用户的密码最长使用天数 PASS_MIN_DAYS 0#新建用户的密码最短使用天数 PASS_WARN_AGE 7#新建用户的密码到期提前提醒天数 过期口令登录不成功。
依据	7.1.3.1 主机：身份鉴别（S3），b）操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换。
备注	# PASS_WARN_AGE Number # PASS_MAX_DAYS 99999 PASS_MIN_DAYS 0 PASS_MIN_LEN 5 PASS_WARN_AGE 7

安全基线项目名称	配置使用 SSH 方式远程访问（必须实施）
安全基线编号	操作系统-Linux-4
安全基线项说明	远程访问服务器时，建议使用 SSH（安全）方式。
配置方法	登录服务器，使用 root 权限执行下列命令。 查看 SSH 服务状态： # service ssh status 若返回的结果为 查看 telnet 服务状态： # service telnet status
检查方法	SSH 服务状态查看结果为：running telnet 服务状态查看结果为：not running/unrecognized
依据	7.1.3.1 主机：身份鉴别（A3），e）主机系统应对与之相连的服务器或终端设备进行身份标识和鉴别，当通过互联网对服务器进行远程管理时，应采取加密措施，防止鉴别信息在网络传输过程中被窃听；
备注	[check@pbbcapl4 ~]$ service telnet status telnet: unrecognized service [check@pbbcapl4 ~]$ service sshd status /etc/init.d/sshd: line 33: /etc/sysconfig/sshd: Permission denied



安全基线项目名称	禁用共享账户（必须实施）
安全基线编号	操作系统-Linux-6
安全基线项说明	系统需按照实际用户分配账户，避免不同用户间使用共享账户（同一个账户）进行操作； 避免“用户账户”和服务器间通信使用的账户共享。
配置方法	此项为问询项，需要与系统、应用管理员确认是否有共享账户存在。 可以查看如下配置文件进行检查，以 root 权限登录后进行检查： cat /etc/passwd cat/etc/shadow cat /etc/group --- 如需建立用户，参考如下： #useradd username //创建账户 #passwd username //设置密码 使用该命令为不同的用户分配不同的账户，设置不同的口令及权限信息等。
检查方法	以 root 账户登录 Linux 系统 #cat /etc/passwd 输出所有用户信息后，与管理员确认是否有共享账户情况存在。
依据	7.1.3.2 主机：访问控制（S3），e）应及时删除多余的、过期的账户，避免共享账户的存在；
备注	

图例：某金融行业客户基线核查报告说明及修复建议

典型案例

民生电商 MINSHENG E-COMMERCE　SHELL　新东方 XDF.CN

4 Part 产品业务流程-漏洞扫描服务

漏洞扫描服务介绍（是什么）

漏洞扫描是指基于漏洞数据库，通过扫描等手段对指定的计算机系统的安全脆弱性进行检测，发现可利用漏洞的一种安全检测行为。包括：网络漏扫、主机漏扫、数据库漏扫等。

漏洞扫描服务流程

准备阶段 → 扫描阶段 → 漏扫报告 → 加固阶段

阶段	工作内容
准备阶段	计算机系统资产情况、网络环境等内容
扫描阶段	扫描工具（Nessus）：系统、软件、Web、应用、应急漏洞
漏扫报告	信息采集记录、扫描记录、加固意见
加固阶段	**报告讲解、加固协作跟踪、扫描复验（亮点）**

典型案例

民生电商 MINSHENG E-COMMERCE　SHELL　新东方 XDF.CN

基线核查和漏洞扫描的区别

基线：最低的安全配置要求。（服务和应用程序设置、操作组建配置、权限、管理规则等）

漏洞：系统实现或系统安全策略上存在的缺陷。（软件逻辑上缺陷，被利用的可能）

总结：漏洞更多指系统设计和开发缺陷。（基线配置也是一种系统漏洞，场景不同）

漏洞扫描和渗透测试的区别

渗透：通过人工“黑盒测试”，模拟黑客行为，达到可以控制目标主机的过程；（侵略性）

漏洞：通过工具“漏洞扫描”，仔细定义和量化所有系统漏洞的过程；（非侵略性）

总结：渗透测试难度大，（人工与工具的区别）、专业性极强。二者搭配可起到好的效果

漏洞描述	Apache Tomcat 的 servlet / JSP 容器中安装有示例 JSP 和 Servlet 文件。应该删除这些文件，因为它们可以帮助攻击者发现 Tomcat 或者远程主机的安装信息。而且他们本身可能也存在安全弱点，比如：跨站点脚本问题。
风险级别	中危
风险来源	172.16.0.1，172.16.0.104，172.16.0.14，172.16.0.15，172.16.0.21，
安全建议	确认以下目录的文件与业务系统是否无关。 /examples/ /docs/ 若不需要些文件，建议移除。

漏洞描述	Redis 是美国 Redis Labs 公司赞助的一套开源的使用 ANSI C 编写、支持网络、可基于内存亦可持久化的日志型、键值（Key-Value）存储数据库，并提供多种语言的 API。Lua subsystem 是其中的一个支持 Lua 脚本语言的子系统。 Redis 3.2.12 之前版本、4.0.10 之前的 4.x 版本和 5.0RC2 之前的 5.x 版本中的 Lua 子系统的 cmsgpack 库存在基于栈的缓冲区溢出漏洞，该漏洞源于程序没有执行正确的内存操作。远程攻击者可通过发送请求利用该漏洞造成拒绝服务或执行任意代码。
风险级别	高危
风险来源	172.16.0.104
安全建议	目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://github.com/antirez/redis/issues/5017

图例：某电商行业客户漏洞扫描报告说明及修复建议

4 Part 产品业务流程–渗透测试服务

渗透测试服务介绍（是什么）

安服（渗透）人员在不同的边界区域（内网、外网）在黑客视角，利用各种手段对特定网络进行测试，发现和挖掘系统中存在的漏洞，出渗透的测试报告，确认隐患和整改办法的过程。

渗透测试服务流程

准备阶段 → **渗透阶段** → **渗透报告** → **加固阶段**

阶段	工作内容
准备阶段	确认测试范围、方案、授权书、**合同条款**
渗透测试	信息采集、渗透（系统、网络、应用）
渗透报告	信息采集记录、渗透测试记录
加固阶段	**报告讲解、加固协作跟踪、渗透复验（亮点）**

典型案例

民生电商 MINSHENG E-COMMERCE　SHELL　新东方 XDF.CN

测试工具（常用）：

信息收集工具： Nmap、Nessus、X-Scan等（主机扫描、系统&应用判别等）

应用层工具： Acunetix Web Vulnerability Scanner（Web网站监测）

系统层工具： Shadow Security Scanner（系统漏洞、弱口令）

网络层工具： SolarWindEngineer’s Edintion（网络性能监控）

其他工具： Whois（Internet目录识别）、Nslookup、端口扫描等

测试内容： 端口扫描、权限提升、VLAN渗透、溢出测试、SQL注入、页面隐藏字段、跨站攻击、WEB应用测试、第三方软件错误配置、Cookies、后门程序。**关键名词：“薅羊毛”（电商网站刷单）、“越权”、“HTTP请求走私”**

3.1.1 短信轰炸

3.1.1.1 脆弱性评价

威胁级别	严重		中度		轻度	

3.1.1.2 漏洞危害

每隔 60 秒可下发一条短信，无限下发，短信轰炸。在测试过程中，可通过编写 Python 脚本来计算短信下发时间间隔，实现短信轰炸。

3.1.1.3 详细信息

直接输入可以接收短信的手机号码，填上对应的验证码，抓包得到一个请求包，然后每隔大概 60 秒即可重新发送一次手机验证码。

当前小程序未对手机号码进行账号验证，任意可以接收短信的手机号码均可进行短信发送。

3.1.1.4 修复建议

建议对获取验证码的手机账号进行验证，防止发送垃圾短信，并对验证码发送量进行限制，防止短信轰炸的出现。虽然做了时间上的控制，但是并没有有效阻止验证码的大量发送，页面上的验证码并没有对手机验证码的发送起到阻止作用，显然不刷新页面完全可以复用，因此弃用也可。

图例：某教育行业客户渗透测试报告说明及修复建议

4 Part 产品业务流程-代码审计服务

渗透测试服务介绍（是什么）

代码审计是一种通过人工或自动化工具对应用程序或服务的源代码进行安全性检测以发现安全漏洞和风险，从而提升应用程序或服务整体安全能力的一种产品服务。

代码审计服务流程

准备阶段 → 审计阶段 → 复查阶段 → 汇报阶段

阶段	工作内容
准备阶段	前期沟通：确定审计对象、审计方式和时间
审计阶段	报告沟通、审计整理、人工审计、自动扫描
复查阶段	回归检查、复测报告、报告内容沟通
汇报阶段	**整理审计成果、客户反馈。（亮点）**

典型案例

民生电商 MINSHENG E-COMMERCE

好大夫在线 网上问诊 双手点赞好大夫

云维互联代码审计服务

服务范围	Web应用代码审计：SQL注入、XSS、越权、逻辑漏洞、验证码安全等；
	WIN/MAC/LINUX客户端：栈溢出、堆溢出、拒绝服务、提权、劫持等；
	APP应用代码审计：Andiroid、IOS源代码、Webview安全、URL安全等；
服务原则	标准性原则：GAT711-2007、GBT28448-2012、ISO/IEC27034、OWASP
	整体性原则：服务中，云维互联可以提供多个角度的测试过程，避免遗漏；
	保密性原则：服务中，项目组成员必须和客户签署相关保密协议。

和漏洞扫描的区别：代码审计工具虽然可以发现程序中潜在的安全漏洞，但是不能算作漏洞挖掘工具，代码审计产品/服务定位为安全编码的辅助工具进行使用。


目录

一 摘要 4
二 项目概述 4
2.1 审计目的 5
2.2 审计对象 5
2.3 审计方法 5
三 前端代码审计 6
3.1 跨站脚本攻击（XSS）漏洞 7
四 Java 代码审计 8
4.1 文件路径遍历漏洞 8
4.2 服务端敏感信息泄露漏洞 10
五 附录 1：Web 安全编码要求 11
5.1 输入验证 11
5.2 输出编码 12
5.3 身份验证和密码管理 12
5.4 会话管理 14
5.5 访问控制 15
5.6 加密规范 16
5.7 错误处理和日志 17
5.8 数据保护 18
5.9 通讯安全 18
5.10 系统配置 19
5.11 数据库安全 20
5.12 文件管理 20
5.13 内存管理 21
六 附录 2 22
6.1 漏洞定级标准 22


编号 SCA-01
级别 中危
描述 跨站脚本攻击漏洞（XSS）是一种经常出 Javascript 代码插入到其他 Web 用户页面里执行以达到攻击目的的漏洞。Web 应用软件将用户提交的交互信息没有作有效验证和过滤就输出给了其他用户，攻击者插入的可执行脚本就可能形成跨站脚本攻击。跨站脚本攻击又分为反射型 XSS、存储型 XSS 以及基于 DOM 的 XSS 漏洞。跨站脚本漏洞（XSS）一般产生在如下场景：
1. 数据通过一个不可信赖的资源进入 Web 应用软件，通常是一个网页请求或者数据库；
2. 在未检验包含数据的动态内容是否存在恶意代码的情况下，便将其传送给了 Web 用户。
潜在威胁 跨站脚本攻击漏洞（XSS）可用于触发其他攻击如 cookie 盗窃、帐户劫持、拒绝服务攻击等。
<script>
var html = "test2";
document.write(html);
//或 yyy.innerHTML = html;
</script>
出现的文件 XXX/xx.js 第 28-32 行
合规解决方案 正确保如下字符有正确转义/编码：
"<" 转成 "<"，">" 转成 ">"。
"'" 转成 "'"，"" 转成 """。

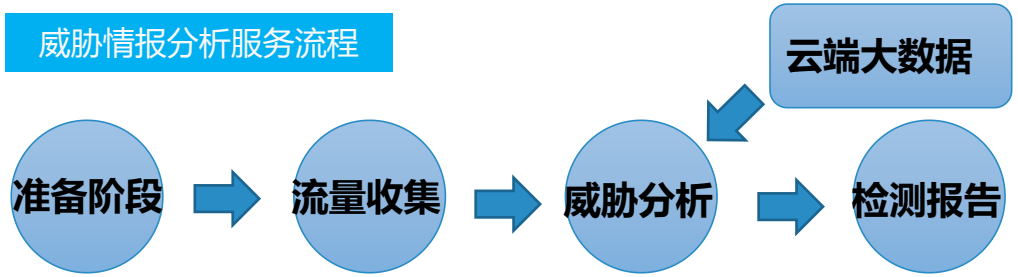

编号 SCA-02
级别
描述 在 Web 应用软件出错时，会将同一些程序异常信息，从而暴露很多对攻击者有用的信息。攻击者可以利用这些错误信息，制定下一步攻击方案。
潜在威胁 当系统异常时直接抛出了错误信息，没有经过任何处理，很容易产生信息泄露。
源码重现
try {
PreparedStatement pst = conn.prepareStatement(sql);
ResultSet rs = pst.executeQuery();
while(rs.next()){
User u = new User();
u.setId(rs.getLong("id"));
u.setName(rs.getString("name"));
u.setPass(rs.getString("pass"));
u.setType(rs.getInt("type"));
userlist.add(u);
}
System.out.println();
if(rs != null) rs.close();
if(pst != null) pst.close();
if(conn != null) conn.close();
} catch (SQLException e) {
// TODO Auto-generated catch block
e.printStackTrace();
}
出现的文件 XXX/xx.jsp 第 67-87 行
合规解决方案 应用软件应通过配置来指定一个默认的错误页面，以保证应用软件永远不会向攻击者泄露错误消息。

4 Part 产品业务流程-威胁情报分析服务

威胁情报分析服务介绍（是什么）

威胁情报分析服务是使用相关信息收集设备对网络中的流量进行实时收集，结合云端威胁大数据的匹配能力，对威胁进行展现、分析的过程。

威胁情报分析服务流程



阶段	工作内容
准备阶段	确认威胁检测工具和整体方案
流量收集	通过工具、方案对网络中的额流量进行采集
威胁分析	集合云端大数据的联动进行分析，形成展现
检测报告	针对精准事件和新的线索，出具分析报告

高级可持续威胁背景（APT）

驱动力
- 地下黑客产业
- 政治利益
- 黑客行动主义
- 国家政治背景

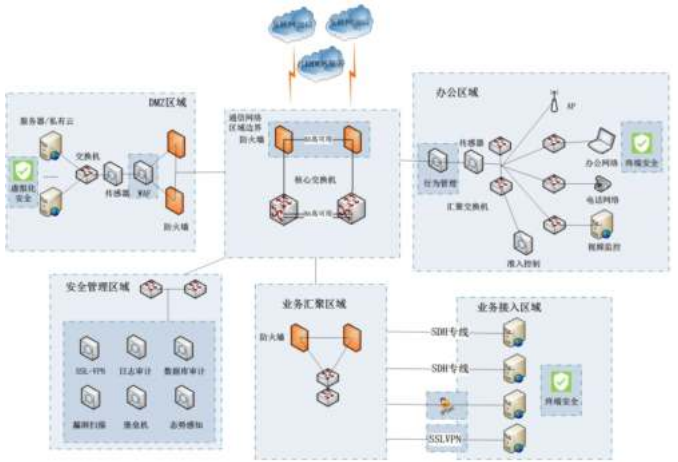
攻击手段
- 零日攻击
- 水坑攻击
- 鱼叉攻击
- 多种逃逸技术

攻击对象
- 中小企业
- 大型企业
- 基础设施行业
- 国家机关

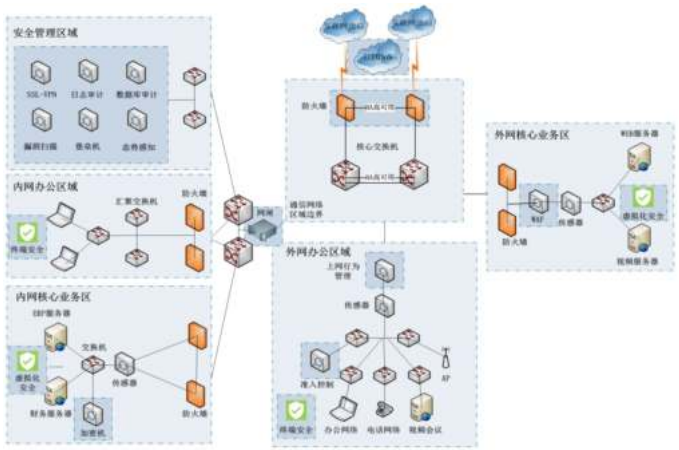
造成影响
- 商业机密泄露
- 中断业务
- 破话声誉
- 盗窃国家机密

国家相关政策驱动（部分摘录）

等保 V2.0	8.1.3.3	应采取技术措施对网络行为进行分析，尤其是对网络攻击行为的分析；
	8.1.3.3.1	应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为；
	8.1.3.3.3	抗APT攻击系统、网络回溯系统和威胁情报检测系统或相关组件；



图例：某医院客户威胁感知部署方案



图例：某金融行业感知部署方案

典型案例

久康云 JKOM Cloud　建银咨询 CCB Consulting　国新国际投资有限公司 CNIC CORPORATION LIMITED

4 Part 产品业务流程-应急响应服务

应急响应服务介绍（是什么）

应急响应机制是针对各种突发公共事件而设立的各种应急方案，通过该方案将损失减少到最小。

应急响应服务流程

收集信息 → **判断问题** → **溯源分析** → **处置恢复** → **安全运营**

阶段	工作内容
收集信息	收集客户信息和中毒主机信息，包括样本；
判断问题	判断是否是安全事件，安全事件的类型；
溯源分析	日志分析、进程分析、启动项分析、样本分析；
处置恢复	杀掉进程、删除文件、打补丁、抑制或修复；
安全运营	**基线、漏扫、代码、渗透等服务的运营（亮点）**

典型案例

仁和 药房网 yaofang.com

索菲亚 柜类定制专家

云维互联应急响应服务

服务范围	钓鱼邮件、黑客入侵、APT攻击、漏洞利用、网络攻击、数据外泄、事件通报、攻击溯源、网络异常、网站被黑、非法访问、网站挂马、网站暗链、网站篡改
服务特点	丰富的应急响应经验：核心团队人员持证上岗，诸多项目实施案例；
	本地威胁与云端结合：安全厂商的云端威胁授权，知识库匹配权限；
	深入研判分析及溯源：挖掘潜在安全威胁隐患，以点延伸至线；
	安全运营服务：结合云维其他服务内容，协助客户后期的安全运营过程。

图例：应急响应工程师资质证明文件

FIVE

Part

4 Part

客户案例

成功案例

success case

4 Part

客户案例

成功案例

success case

云维互联
WWW.CLOUDWE.COM.CN

感谢观看

电话：010-64528994
网址：www.cloudwe.com.cn
邮箱：service@cloudwe.com.cn
地址：北京市朝阳区洛克时代大厦C座901室

云维互联官方公众号