

防范黑客攻击的措施:防范黑客攻击Oracle系统的 8大常用思路方法

疯狂代码 <http://CrazyCoder.cn/> j:<http://CrazyCoder.cn/DataBase/Article62774.html>

Oracle销售在向客户兜售其数据库系统直把它吹捧为牢不可破耍嘴皮子轻易兑现起来可就不那么轻易了不管什么计算机系统人们总能够找到攻击它思路方法Oracle也不例外本文将和大家从黑客角度讨论是用哪些思路方法把黑手伸向了你们原以为他们不能触及数据希望作为Oracle数据库治理员能够清楚阐明自己基础架构哪些区域比较轻易受到攻击同时我们也会讨论保护系统防范攻击思路方法

1. SQL注入攻击

如今大部分Oracle数据库都具有为某种类型网络应用服务后端数据存储区网页应用使数据库更轻易成为我们攻击目标体现在 3个方面其这些应用界面非常复杂具有多个组成成分使数据库治理员难以对它们进行彻底检查其 2阻止员侵入屏障很低即便不是C语言编程专家也能够对些页面进行攻击下面我们会简单地解释为什么这对我们这么重要第 3个原因是优先级问题网页应用直处于发展模式所以他们在不断变化推陈出新这样安全问题就不是个必须优先考虑问题

SQL注入攻击是种很简单攻击在页面表单里输入信息静静地加入些非凡代码诱使应用在数据库里执行这些代码并返回些员没有料到结果例如有份用户登录表格要求输入用户名和密码才能登录在用户名这栏输入以下代码: `cyw'); select username, passWord from all_users;--` 假如数据库员没有聪明到能够检查出类似信息并“清洗”掉我们输入该代码将在远程数据库系统执行然后这些有关所有用户名和密码敏感数据就会返回到我们浏览器 你可能会认为这是在危言耸听不过还有更绝David Litchfield在他著作Oracle黑客手册(Oracle Hacker's Handbook)中把某种非凡pl/sql注入攻击美其名曰:圣杯(holy grail)它曾通杀Oracle 8到Oracle10g所有Oracle数据库版本很想知道其作用原理吧你可以利用个被称为DBMS_EXPORT_EXTENSION包使用注入攻击获取执行个异常处理代码该会赋予用户或所有相关用户数据库治理员特权 这就是Oracle发布闻名安全升级补丁Security Alert 68所针对漏洞不过据Litchfield称这些漏洞是永远无法完全修补完毕

防范此类攻击思路方法

总而言之虽说没有万能防弹衣但鉴于这个问题涉及到所有面向网络应用软件Software还是要尽力防范目前市面上有各式各样可加以利用SQL注入检测技术可以参照<http://www.securityfocus.com/infocus/1704> 系列文章具体介绍 还可以用区别入侵检测工具在区别水平上检测SQL注入攻击访问专门从事Oracle安全性研究Pete Finnigan安全网站WebSite<http://www.petefinnigan.com/orasec.htm>在该网页搜索“sql injection”可以获得更多相关信息Pete Finnigan曾在其博客上报告称Steven Feurstein目前正在编写个称为SQL Guard pl/sql包专门用来防止SQL注入攻击详情请查看以下网页<http://www.petefinnigan.com/weblog/archives/00001115.htm> 对于软件Software开发人员来说很多软件Software包都能够帮助你“清洗”输入信息假如你对从页面表单接受每个值都清洗例行进行处理这样可以更加严密保护你系统不过最好使用SQL注入工具对软件Software进行测试和验证以确保万无失

1. 默认密码 Oracle数据库是个庞大系统提供了能够创建切模式绝大部分系统自带用户登录都配备了预设默认密码想知道数据库治理员工作是不是够勤奋?这里有个思路方法可以找到答案看看下面这些最常用预设用户名和密码是不是能够登录到数据库吧:

	Username	Password	applsys	apps			
ctxsys	change_on_	dbsnmp	dbsnmp	outln	outln	owa	owa
	perfstat	perfstat	scott	tiger	system	change_on_	system
manager	sys	change_on_	sys	manager			

就算数据库治理员已经很勤奋把这些默认配对都改了有时候想猜出登录密码也不是件困难事情逐个试试“oracle”、“oracle4”、“oracle8i”、“oracle11g”看看碰巧是不是有个能登录上去 Pete Finnigan提供了份有关缺省用户和对应密码名单该名非常全面而且是最新并包括已经加密密码假如你用all_users来进行查询可以尝试并比较下这份名单具体名单请参阅http://www.petefinnigan.com/default/default_password_list.htm 防范此类攻击思路方法 作为数据库治理员应该定期审核所有数据库密码假如某些商业方面阻力使你不能轻易更改轻易被人猜出密码你可以尽量心平气和地和和有关人员解释用些直观例子来阐明假如不修改密码话会有什么不好事情发生会有什么样风险存在 Oracle也提供了密码安全profile你可以激活该profile在某种水平上加强数据库密码复杂性还可以执行定期密码失效要注重要把这个功能设置为只对通过网络服务器或中间层应用服务器登录事件起作用

2. 蛮力攻击(Brute Force) 蛮力攻击就像其名字所暗示就是不停撬直到“锁”打开为止思路方法对于Oracle数据库来说就是用某种自动执行进程通过尝试所有字母数字组合来破解用户名和密码 Unix治理员就可以利用款名为John the Ripper密码破解软件Software来执行这类攻击现在假如你下载某个补丁你也可以利用这款软件Software来对Oracle进行蛮力攻击敲开其密码不过根据密码复杂程度区别这可能是个很费时过程假如你想加快这个进程可以事先预备张包含所有密码加密表这样表叫做Rainbow table你可以为每个用户名预备张区别rainbow table这种密码加密算法把用户名作为助燃剂在这里就不再深入介绍更多细节问题了大家可以查阅<http://www.antsight.com/zsl/rainbowcrack/>获得更多信息 Oracle服务器默认设置是对某个特定帐户输错密码达十次就会自动锁定该帐户不过通常“sys as sysdba”权限没有这个限制这可能是假如你锁定了治理员那所有人都将被锁定这样设置为我们黑客破解软件Software(OraBrute)如开辟了条生路它们会昼夜不停地敲打你数据库前门直到它乖乖打开为止 防范此类攻击思路方法 想要抵御此类攻击可以使用的前提及对付预设密码攻击思路方法不过好奇心过重数据库治理员也可能下载上面提到工具侵入自己系统这介绍说明了你真正风险来自何方

4. 从后门偷窃数据 在安全领域这个概念被称为数据向外渗漏(exfiltration)这个词来自军事术语其反面是向敌人内部渗透(infiltration)意思就是在不被发现情况下偷偷潜出对于从目标数据库获取数据过程可能就像从些磁带备份中挑拣数据和还原数据库或者像从个被毁坏磁盘重复制份拷贝样简单不过也有可能涉及到窥探网络传输以获得相关数据包 Oracle有个名为UTL_TCP包能够使外部连接指向其他服务器对它稍微改编下就可以利用它从数据库发送套低带宽数据流到远程主机Oracle也附带了些有用包来隐藏数据流里信息假如你在发动潜入行动时候担心入侵检测系统会监测到你不法活动那么可以充分利用这些功能秘密嵌入包括DBMS_OBFUSCATION_TOOLKIT和DBMS_CRYPTO 防范此类攻击思路方法 防范此类攻击最佳办法是安装入侵检测系统这些系统能够检测网络中流入和流出数据包有些检测系统还提供深入数据包检测可以确实检查某些SQL并可以通过设定规则在某种情况下触发报警器这些工具还能够查找泄密迹象例如添加UNION、各种类型- circuiting命令、利用“--”注释进行截断等等

5. 监听器 计算机世界最让人觉得了不起事情就是不管有多么困难事总有办法驯服它尤其是在安全领域些漏洞如此简单而这些漏洞出现仅仅是用户(也包括我们现在扮演角色——黑客)并没有像软件Software设计者(员或软件Software开发员)本来预想那样研究和行动 Oracle监听器设置是为了能够实现远程治理那么假如攻击者把监听器logfile设置为Unix .rhosts文件呢?这样

攻击者就可以轻松对.rhosts文件进行写操作Unix上这个文件设置了什么人可以不用密码而使用rsh、rlogin和rcp命令登录你可以想想将会发生什么事情

这其实只是围绕Oracle监听器安全问题冰山角而已其他还有缓冲区溢出等大堆问题需要注重事实上LitchfieldOracle黑客手册里花了整章内容来讨论这个主题 防范此类攻击思路方法 从预防角度而言Oracle已经做出了定措施来更好保障系统安全前提是你能够把它实施到位首先为监听器设置个治理密码对于担负着治理不断增加密码重担治理员而言这看起来像是多余不过在你需求其他途径来保障监听器安全的前好好地想想上面提到和没提到威胁Oracle也添加了ADMIN_RESTRICTIONS能够阻止特定远程控制事件

6. 权限提升 简单说“权限提升”包括使用现有低权限帐户利用巧取、偷窃或非法方式获取更高权限甚至是数据库治理员权限 下面举个使用CREATE ANY权限例子假设我能通过个拥有CREATE ANY TRIGGER权限用户CYW访问数据库这样我就能在任意模式里创建触发器假如你能追踪到个任何用户都能执行写入操作表你在SYSTEM里创建了个能够在低权限你对该可写表进行插入或更新操作时执行触发器你编写触发器会个存储过程(也是你自己编写)该存储过程会使用AUTHID CURRENT_USER为者授权这就意味着当该触发器运行“你”存储过程时拥有SYSTEM权限现在你非法存储过程内部包含了“EXECUTE IMMEDIATE 'GRANT DBA TO CYW'”这样我就可以在触发器运行时候插入到我公共表里该触发器由SYSTEM所有而SYSTEM会我change_privileges存储过程这个存储过程使用AUTHID CURRENT_USER为我授权这样“我”就可以在不改变我自身权限情况下获得并执行SYSTEM权限 防范此类攻击思路方法 数据库治理员该如何应对这个问题呢?首先你应该审核数据库CREATE ANY权限删除其中不需要那些部分其次看看类似于

www.securityfocus.com这类论坛看看有关权限提升最新漏洞最后激活对某些特定类型数据库活动审计功能并没有什么坏处这样数据库就能让你实现自我保护当数据库自行审核类似于GRANT DBA这样事件时你可以通过查看审计日志知道有没有出现恶意或突发活动 7. 操作系统指令和安全 黑客并不总是通过shell命令行提示符登录到你系统 不过通过诱使Oracle数据库运行操作系统水平指令我们确给黑客提供了条运行指令有效途径这些指令能够删除和破坏文件、改写日志(以便隐藏他们行踪)、创建帐户以及其他些能通过命令行输入指令达成操作他们是如何做到呢?尽管思路方法有很多最轻易种就是通过Java和PL/SQL这些语言通常可以利用创建外部存储过程能力使的执行个具备系统功能存储这个系统指令能够以首次安装时使用oracle帐户权限执行 防范此类攻击思路方法 虽然Oracle在保护用户免受此类攻击上已经取得了定进展不过你最好还是把希望寄托在你预防监测工作上严密留意你系统内部有没有出现这类活动当有攻击者试图对你使用此类恶意攻击时你最好能够事先把握主动权 8. 文件系统安全 对文件系统(filesystem)访问是个让你头大棘手问题“oracle”操作系统用户拥有所有Oracle软件Software和数据库数据文件访问权限所以假如数据库内部某些用户利用

UTL_FILE包访问filesystem上文件时他们就可以访问的前由于权限和角色限制而无权访问很多数据库内部文件 防范此类攻击思路方法 Oracle引入Directory对象在防止此类攻击上也有定作用在10g系统中必须通过DIRECTORY对象来定义某些类型读写操作这意味着用户必须拥有CREATE DIRECTORY权限而在前面介绍权限提升问题中我们已经看到可以通过很多思路方法获取这种权限即使这些也被解决了还是有很多思路方法可以通过PL/SQL或Java语言来获取对filesystem访问权限和对文件读写权限 总论: 就像上面讨论样Oracle数

数据库产品有很多漏洞有时候看起来就像由些聪明透顶工程师建造所豪宅工程师固然聪明但比那些觊觎此宅黑客们忠厚老实多了因此他们没有预料到有人会利用这种种思路方法来偷砖窃瓦削弱豪宅根基黑客可以通过很多区别思路方法进行攻击侵入到目标数据库 不过只要数据库治理员能够花点时间和精力来解决其中很多问题都是可以避免Oracle已经针对很多漏洞在数据库内部打上了补丁而且入侵监测系统能体构额外安全保障所以数据库治理员应该对每种漏洞都铭记在心警惕性才是防范要害尽量执行好自己制定安全计划

2009-2-14 22:11:03

疯狂代码 <http://CrazyCoder.cn/>