Global Information Assurance Certification Paper

Web Application and Databases Security
Darrell E. Landrum
April 2, 2001

Introduction

Internet web sites are increasingly using web applications to access database systems for information retrieval, transactions and publication. These Internet web applications are commonly being used for e-commerce, e-banking, and e-government to purchase goods, make reservations, pay taxes, enroll in classes, retrieve academic transcripts, acquire account balances and pay bills, to name a few. In order to provide these Internet services many are connecting their security sensitive information stored in databases directly to the Internet. And, in many cases, the securities of these applications have been designed with the same securities as for trusted internal applications. By doing this organizations are creating security risks of possibly exposing sensitive information, critical business applications being disabled or compromised. This paper looks at the problems associated with using web applications that access databases for Internet services. It also discusses some options of securing web services that utilize databases, as well as the overall security layers needed.

Increasingly the Internet is becoming the source for security attacks. The Computer Security Institute, 2001 survey, reported that 70% of the respondents cited their Internet connection as a frequent point of security attacks. Ninety percent of those attacked reported vandalism. Seventy-eight percent reported denial of service. Thirteen percent reported theft of transaction information and Eight percent reported financial fraud (http://www.gocsi.com/prelea_000321.htm).

National Infrastructure Protection Center (NIPC) on December 1, 2000 has also observed an increase in attacks on e-commerce and other internet-hosted sites. (http://www.nipc.gov/warnings/advisories/2000/00-060.htm)

Security Threats

There are numerous vulnerabilities that threaten web and database services. No matter how secure the Web and database server are there will always be a possibility that someone will discover a new vulnerability that threatens its security.

Types of security threats:

- **Denial of service attack** - slows down or disables a web and/or database server, denies access to users (easy to perpetrate and very hard to guard against).
- **Sniff attack** – captures network traffic to obtain database passwords or private information to ether alter, corrupt or steal information.
- **Spoofing Attack** – falsify a site to steal data or disrupt services

Attack Motivations

There are several different motivation factors for someone to break into a site. These can range from a difference in politics to just shear enjoyment. A few of the more common are:

- Hatred or revenge
- Fun of it, challenge or curiosity
- Money or hired gun
- Ignorance or stupidity
- Politics or government/business espionage or warfare

Overlooked Security

Security can be easily overlooked. This usually happens when the focus is on getting web services up and running and security becomes an after thought once everything is running or security incident happens. Some of the following are common security errors that can be easily fixed:

- Passwords and names are coded in readable text scripts
- No passwords are used or the default (accounts with known name & password)
- Internet web uses the same permissions as internal applications
- Running Internet programs with maximum permissions
- Development or default web service tools are put on a production server that could allow an Internet user to upload and run programs on your server
- Programs are written by novice programmers without security knowledge
- System patches or service packs are not up to date

Most applications that access databases have multiple pieces of programs and services that work to deliver the application. Some of these can be complex and invisible making security risks difficult to recognize. If any one piece has security problems it may expose the entire system.

Security Options and Layers

There are several different security options available and associated layers for securing a web system and databases for electronic services. In order to know which one will work the best depends on factors that will differ by the organizations. Some of the following factors should be analyzed before implementing a system**:**

- **Risks** – Business interruption, property damaged and associated costs
- **Regulator requirements** – State, Federal, Company or e-merchant regulations
- **Resources** – Staff expertise and costs to implement and maintain
- **Type of data and use** – Is the content public, sensitive or private information

Security Layers

As stated earlier there are multiple layers involved with delivering a Web application that accesses a database securely. These layers can include:

Networks
Operating systems
Web servers
Firewalls
Application/programming
Databases

Closer Look at the Layers and Options

Location of the database on the network

One obvious way to promote security of sensitive information stored in a database is to isolate the systems used for Internet web services from the internal systems. This reduces the risks of sensitive information being accessed and allows security to be tightened around the perimeter of the internal production databases.

Figure 1, Web Database in DMZ, and Figure 2, Web Database Not in DMZ, show system model options for isolating security critical databases. If attacked by a denial of service or sniff attacks the security critical internal database (DB) servers should be able to continue performing most business functions to support internal operations. It is, however, critical that intrusion detection systems (IDS) be in place to quickly identify a compromise to the web system before an internal DB or File system is broken into. Included in this model are documents and images that could also be distributed from a web and used internally as a part of a business function.

By isolating the security critical databases and creating a web only database as shown in Figure 1 and 2, you will have some notable benefits. One, is the ability to define database access policies with "finer granularity" or more detailed control. Second, break-ins can be identified and contained before it gets into valued internal business systems.

Many in-house applications are designed for a trusted environment and when security is tightened the application may not work properly. As an example, there are vendor applications that only rely on the application security and require access to the database with system-admin privileges and blank passwords in order to work.

By creating a web only database you have created the ability to have a more secure environment for your database but you have also created more work and complexity in having to replicate the needed information back and forth from the Web DB server to the internal DB servers. Most all enterprise database systems have this functionality but staff time or expertise to implement this may be more difficult. There are also no benefits if critical information stored or left on the web server so a program will need to be created to transport this information out of harms way and into the business databases.

Figure 1 is considered to be the most secure in protecting an internal network of the two options and also the more complex and costly. Complexity is added by moving data securely from the private internal network through the firewall and to the public web network especially if data needs to move frequently between the databases.

Figure 1, Web Database in DMZ

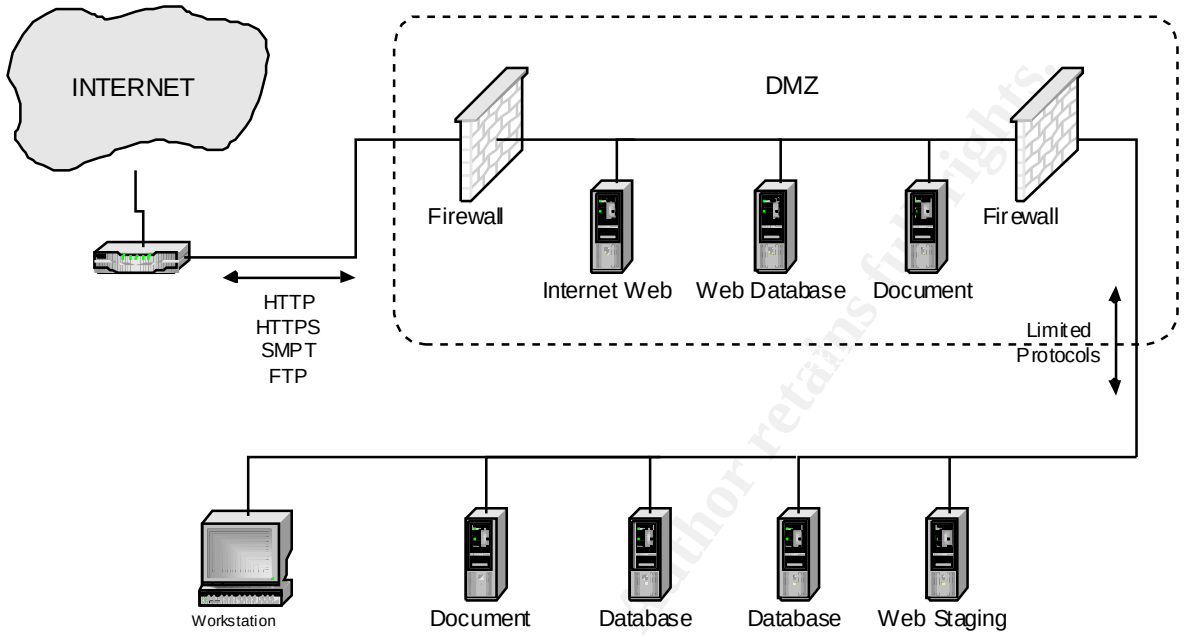
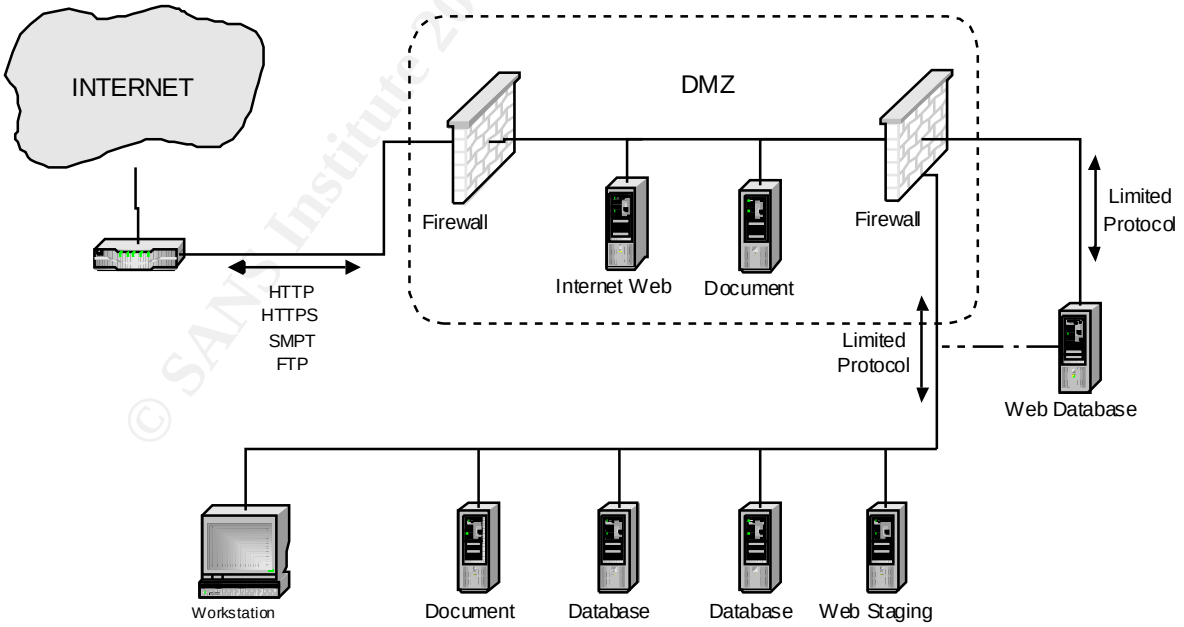


Figure 2, Web Database Not in DMZ



Encryption

There are two main areas where secure network communications are needed. One is with the web user that is transmitting private information to the web server. The other is the connection from the web application to web database server. Encryption is a good method to secure these types of traffic and prevent a hacker from intercepting sensitive information. The encrypted information is disguised in a non-readable format that only the intended user can decipher by having the known code. Some database products offer Encryption options. There are also third party products like PGP by Network Associates that can be purchased. The downfall, however, is that it will take more computer processing to encrypt and decrypt the transmitted information.

Firewalls

Firewalls are the first layer of defense and an important layer in keeping outsiders from getting to your internal or private network. They limit access by electronically screening or blocking transmissions, which are called rules. There are several different types of firewalls and each has its strengths and weakness depending on needs and uses.

If you must open an internal hole in the firewall to connect to a Web database server, reference figure 2, a rule will need to be established for a secure connection that does not identify the server or port. Limit connectivity between the web server and database server to a specific protocol that only supports the level of functionality that is needed. Using encrypted traffic limited to the needed protocol like TCP/IP or a virtual private network (VPN) is also a good solution. The use of connection objects in a compiled VB or C++ program like a DLL using COM+ or CORBA running on an application server like MTS, or Tuxedo should also be used for database connections.

Some common problems with firewall security is not keeping the system current with latest patches, improper configuration and not monitoring and auditing logs. As with most operating systems Firewalls never come out-of-the-box configured to secure any given site and is only as good as the staff administrating it.

Operating System and Internet Web Server

Securing the Operating System (OS) and Web service is very important. Once it has been compromised, attacks into your internal systems are possible. There are numerous documents available to secure an OS and Internet server. Some obvious but often overlooked areas include:

- Use of strong passwords
- Only installing services that are needed
- Document what is installed and monitor for any changes
- Run logging and monitor log files
- Limit open ports to required needs
- Block the ability to know OS and web server information
- Limit access to the system
- Keep the system up to date with latest fixes and patches.
- Image, ghost, or back up the system at appropriate stages
- Stage and test application and system on a staging server

If vulnerability is found most vendors provide fixes fairly quickly. There are also programs like PatchWorks distributed by Computer Security Institute (CSI) that will check your Windows NT system to make sure it is up to date with the latest patches or contains known file corruption. Experience has proven that sometimes the installation of patches can break an application so care and proper testing must be taken.

Application programming

Most web sites are driven to get their services and products out quickly. In doing this applications are sometimes not designed with security in mind. As well, most programmers are use to developing trusted internal applications that do not need to be "highly-secure." Applications can create security holes that can be hard to detect. Therefore, applications need to be designed with security in mind and not as an after thought.

Some best practices in application programming:

- Use compiled programs like C++, VB, and Java for connection and stored procedure calls and run these on an application server such as Microsoft's MTS or BEA Tuxedo and create server objects in scripts such as VBS, JavaScript or HTML to use the connections.
- Use J2EE, CORBA or COM+ object protocols
- Use database stored procedures
- Use native database connections instead of ODBC
- Do not hard code user names and passwords in scripts
- Use simple clean HTLM - no active content such as ActiveX
- Use OS authentication to access DB servers
- Do not use persistent connection
- Develop programming security templates

There are automated analysis tools available called application scanners that scan for known holes in web applications. These can be very helpful in automating or double-checking the human process. Some products that do this are AppScan from Sanctum, Retina from eEye and Web Inspect from SPI Dynamics. It should be noted that attackers have used these products to break in, as was the case with Double Click that was reported on Security Focus News (http://www.securityfocus.com/news/181).

These products look for possible vulnerabilities that can be exploited by some of the following attacks:

Hidden Manipulation
Cookie Poisoning
Backdoors/Debug options
Buffer Overflow
Stealth Commanding
Tampering Cross Site Scripting/Server Side Includes
Forceful Browsing

Database servers

Web applications bypass normal client server OS and application security making the databases the lowest common denominator for implementing security. Database systems utilize critical pieces of the OS to function so once compromised these services are now available to the attacker. Some best practices for securing a database are:

- Transaction logging and auditing
- No generic or default passwords or user names
- Application specific passwords or user names
- Encryption of Stored procedures, triggers, views and network protocols
- Only install needed service - know what's is on you system
- Keep up to date with service releases or patches
- Do not use Extended stored procedure
- Limit admin accounts to DBA use only
- Back system at appropriate levels for recovery

Network

Web network traffic should be separated from the internal network. This isolates the less secure systems from the secure. Making it difficult for an attacker to pick up or sniff internal traffic for valuable information. Using a firewall as previously discussed can do this. Another option is to put all database and file servers providing web support service on a protected subnet. It is also important to disable any source routing that will allow the originator to influence routing decisions. The next piece is to monitor the network for abnormalities.

Intrusion Detection Systems

Intrusion detection is the process of monitoring a network to identify, and prevent network-based attacks. Software applications or hardware devices known as Intrusion Detection System (IDS) can automate this process. An IDS provides a wide range of monitoring techniques including packet sniffing, file integrity monitoring, and even algorithms that detect deviations in network traffic.

Host based firewalls like Black Ice and Zone Alarm are low-cost simple solutions that have proven to be very useful. These provide reports of possible attacks or probes, block known attacks, identification of ports and server information. These can be installed on the web and database server as well as a file integrity monitoring software like TripWire.

Summary

There are many layers to protecting critical databases. There are also several ways to secure these systems, all of which are dependent upon the risks involved in having secure information accessed by unauthorized users. The difficult aspect of this environment is that it is continually changing. Businesses and governments have opened their information vaults to the world in order to do business and in doing so they have increased the security risks to their internal databases of valuable information. Careful thought and policy development must be done as well as a thorough understanding as to what it takes to secure these systems.

Appendix
The following is a list of known vulnerabilities to e-commerce sites:

- Unauthorized Access to IIS Servers through Open Database Connectivity (ODBC) Data Access with Remote Data Service (RDS):
  http://www.microsoft.com/technet/security/bulletin/ms99-025.asp

- SQL Query Abuse Vulnerability
  Affected Software Versions: Microsoft SQL Server Version 7.0 and Microsoft Data Engine (MSDE) 1.0
  http://www.microsoft.com/technet/security/bulletin/ms00-014.asp

- Web Server File Request Parsing
  While they have not been shown to be a vector for the current attacks, Microsoft has advised us http://www.microsoft.com/technet/security/bulletin/ms00-014.asp

- Oracle8 JSP/SQLJSP Servlet Execution
  A vulnerability exists in the way input is handled by the JSP agent which could let a remote malicious user execute arbitrary .jsp files
  http://otn.oracle.com/

References

Microsoft TechNet Web site - database security
http://www.microsoft.com/technet/security/database.asp

Microsoft SQL Server Extended Stored Procedure Vulnerability
http://www.atstake.com/research/advisories/2000/a120100-1.txt

Computer Security Institute
http://www.gocsi.com/prelea_000321.htm

National Infrastructure Protection Center (NIPC)
http://www.nipc.gov/warnings/advisories/2001/01-003.htm

Improving Computer Security through Network Design
Danny Smith, *Technical Director*, *AUSCERT*
http://www.auscert.org.au/Information/Auscert_info/Papers/Security_Domains.html

National Infrastructure Protection Center (NIPC)
ADVISORY 00-060, "E-Commerce Vulnerabilities" December 1, 2000
http://www.nipc.gov/warnings/advisories/2000/00-060.htm

Update to NIPC Advisory 00-060 "E-Commerce Vulnerabilities" Issued 03/08/2001
http://www.nipc.gov/warnings/advisories/2001/01-003.htm

North Carolina State University
http://ecommerce.ncsu.edu/topics/security/security.html

Internet Firewalls: Frequently Asked Questions
Matt Curtin and Marcus J. Ranum
http://pubweb.nfr.net/~mjr/pubs/fwfaq/#SECTION00041000000000000000

Certifying E-Commerce Software for Security
Anup K. Ghosh
http://www.cigital.com/papers/download/wecwis99.pdf

Web apps pose security threat By Scot Petersen and Dennis Fisher, eWEEK
http://www.zdnet.com/eweek/stories/general/0,11011,2679177,00.html

BEA home page for Tuxedo application server
http://www.bea.com/index.shtml

Last Updated: July 25th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event