

Tech Center: Database Security

 E-mail this page |  Print this page |  BOOKMARK 

Enterprises Still Plagued By SQL Injection Attacks

**Venerable database attack continues to be effective.
What can your organization do to protect itself?**

Jun 15, 2011 | 04:08 PM | [2 Comments](#)

By **Ericka Chickowski, Contributing Writer**

It has been the better part of a decade since SQL injection became a popular mode of attacking enterprises. But today's IT organizations are struggling more than ever with these broadsides against their data assets.

Just this week, an attack against the International Monetary Fund was whispered to be the result of SQL injection, though the claim is unconfirmed. More concrete evidence of splashy SQL injection attacks was registered this month in breaches at Sony and even the security firm Comodo.

What can your organization do to prevent potential damage from an SQL injection attack? Experts say it starts with doing a better job of securing the databases that these attacks target -- and the Web applications from which they originate.

"SQL injection attacks continue to be very low tech and very easy to carry out, and I think organizations still are struggling to figure out why they're so vulnerable," says Josh Shaul, CTO for database security vendor Application Security Inc.

Shaul, along with other database security experts, says the problem is a combination of factors, including poor coding practices, legacy code and legacy databases that haven't been hardened, and a false sense of security provided by Web application firewalls (WAFs).

"The Web application firewall is positioned as the solution to SQL injection, but the truth about the Web app firewall is it's only effective if you can program it with known vulnerabilities," Shaul explains. "If you can't tell it exactly what vulnerabilities you have, it really can't do anything for you. So a lot of organizations just buy a WAF and deploy it. They get this false sense of security that everything is cool when, in fact, their systems are still vulnerable."

WAFs have forced attackers to be a little more creative with how they construct their attack vectors, says Kyle Adams, architect and lead developer at next-generation WAF vendor Mykonos Software.

"And so began the race -- firewall vendors striving to create more effective signatures, and hackers relentlessly trying to find ways to evade the signatures," Adams says.

Adams believes the security industry has done an admirable job getting the word out about SQL injections, but the problem is so immense that

Advanced Threats

Authentication

Cloud Security

Compliance

Database Security

Insider Threat

NoSQL databases, and cloud-based data storage.

Mobile Security

Security Monitoring

Security Services

SMB Security

Vulnerability Management

enging, due to the proliferation of "big data,"



Stop SQL Injection: Don't Let Thieves in Through Your Web Apps

Think your corporate website isn't vulnerable to a SQL injection attack? Start rethinking. SQL injection is among the most prevalent -- and most dangerous -- techniques for exploiting Web applications and attacking back-end databases that house critical business information at companies of every size. And it persists despite relatively simple and effective countermeasures. Here, we explain how SQL injection works, and how to secure your Web apps and databases against it.



Database Breaches: Lessons Learned From Real-World Attacks

Recently, there's been a rash of major database breaches, including those at Gawker.com, McDonald's and Walgreens. All the companies had solid resources at their disposal, so what went wrong? In this Tech Center report, we profile five database breaches and extract the lessons to be learned from each. Plus: A rundown of six technologies to reduce your risk.

Other reports from the Database Security Tech Center:

- [The Long Arm Of Database Security](#)
- [DB2 Gets Safer: IBM Makes Security a Priority](#)
- [Database Security: Oracle Offers New Tools to Counter Threats](#)
- [You've Been Breached: Responding to a Database Compromise](#)
- [Beyond the Database: Protecting Unstructured Data](#)
- [Protecting Databases from Web Applications](#)
- [Database Activity Monitoring: Emerging Technology Keeps Tabs on Assets](#)
- [SQL Injection: A Major Threat to Data Security](#)
- [Protecting Your Databases From Careless End Users](#)
- [A Database Administrator's Guide to Security](#)
- [Why Your Databases Are Vulnerable To Attack - And What You Can Do About It](#)

Related Content

Sponsored
by:



Data security and privacy: A holistic approach

This paper examines the complex data security and privacy threat landscape; compliance and regulatory requirements; and, the IBM InfoSphere portfolio of integrated solutions designed to help you stay focused on meeting your organization's business goals, achieving compliance and reducing risk. IBM InfoSphere solutions for data security and privacy support a holistic approach ensuring the protection and integrity of your data.

holes still remain.

"As developers became more security conscious, better coding practices and input validation started to bolster protection into new and legacy applications," Adams says. "Efforts were also initiated in many companies to review and augment existing applications with input validation and more secure SQL statement construction.

"Unfortunately, it is extremely difficult to catch every possible hole," Adams continues. "So even with this increased effort, the insufficient security practices of the past bleed into more modern applications. This exposes obscure and difficult-to-identify SQL injection vulnerabilities -- which are just as powerful, but take a little longer to hunt down."

Even if organizations improve the secure coding and testing of new applications, there are still many more production applications that remain untested, notes Mandeep Khara, chief marketing officer for application security vendor Cenizc.

"We have seen a lot of progress in terms of people focusing on SQL injection testing," Khara says. "However, organizations are only testing a fraction of their apps -- and finding and fixing SQL injection vulnerabilities in a fraction of apps will give you fractional security.

"Partial testing is like partial heart surgery -- since your other arteries are blocked, you are still very vulnerable. What organizations need to do is to start facing the fact that they have to test all their applications -- and either fix the critical vulnerabilities, block those vulnerabilities, or take down the functionality until they are fixed. There are no shortcuts here."

Even more important, organizations need to stop seeing SQL injection attacks solely as a Web app problem, experts say. The reason why many of these attacks are so disastrous is that the database layer just behind the application is defenseless once the hacker gets a toehold.

"The main problem I see most of the time is that organizations run the database at the highest privilege level possible," says Daniel Clemens, owner of the security consultancy Packetninjas. "Then there's SQL injection and, boom, you can create your stored procedures, drop your own files on there, and then basically compromise the back-end database." Many organizations are also lax about locking down ingress and egress from the database, making it easier for attackers to move information off the database, he adds.

To help prevent damage from SQL injection vulnerabilities, organizations must harden their databases by reducing privileges, updating databases, and monitoring activity. Even when an attack slips through the WAF, it can often be detected through database activity monitoring, experts say. "DAM solutions that can monitor unsuccessful queries of low severity -- queries failing due to a missing or unknown object or syntax errors, which are symptomatic of a SQL injection attack -- can quite effectively detect an attack before the query succeeds to grab data illegally from the database," says Mel Shakir, CTO of database security vendor NitroSecurity.

Have a comment on this story? Please click "Comment" below. If you'd like to contact Dark Reading's editors directly, [send us a message](#).

Comments

[Quick View](#)

[Full View](#)

2 Comments

-- MOST RECENT COMMENT --

Response to All Wrong...

Comment by Packetninjas Jun 16, 2011, 14:55 PM EDT

In the first quote Josh in so many words stated organizations don't know

why they are vulnerable. This speaks to a general misunderstanding of

a few basic things Eg. Parameterized queries and prepared SQL statements

as well as basic input validation.

This is the basic premise for the article supporting the idea that

organizations don't know about the particular vulnerability class

Ten Database Activities Enterprises Need to Monitor

Enterprises are paying too little attention to security risks associated with their databases. Auditors, security/risk professionals and data owners need to watch for behaviors that may indicate database security problems. Learn the 10 critical database activities & behaviors enterprises should audit now.

The Forrester Wave: Database Auditing And Real-Time Protection

Database auditing has become critical as enterprises deal with regulatory compliance and security requirements. Learn why Forrester Research named IBM InfoSphere Guardium a Leader with #1 scores in all 3 top-level categories: Current Offering, Strategy and Market Presence.

Look Beyond Native Database Auditing to Improve Database Security

This Forrester Consulting study provides real-world findings from in-depth interviews with enterprises that have implemented database auditing and real-time protection solutions to ensure comprehensive auditing, real-time monitoring and protection of critical database and enterprise applications from internal and external attacks.

HOWTO Safeguard Against the Latest Cyber-Threats

2010 saw 27% rise in new vulnerabilities with the largest category being Web Application vulnerabilities. Tom Cross discusses these security events from the "IBM X-Force 10 Trend and Risk Report." Learn more about APTs, virtualization and cloud security threats.

Database Security Newsfeed

[New Secure Mobile App Developer Credential Planned By CompTIA And viaForensics](#)

[Imperva Rolls Out IPv6 Support](#)

[Qualys Launches New Version Of Web Application Scanner](#)

[NT OBJECTives Releases Free SQL Invader](#)

[RSA Shuts Down More Than 500,000 Cyber Attacks Across 185 Countries](#)

[Symantec Survey Finds Rapid Adoption Of Encryption By Enterprises Coupled With Growing Pains](#)

[MORE NEWSFEED >>>](#)

and or vulnerability classes which place them at risk in both custom code, or COTS applications.

Also , in defense of Khara his message could really be summed up to the following:

"Assumptions are the mother of all mess-ups".

Enterprises assume that if they only audit the highest priority applications for their business their enterprise are more secure.

While this is partially true only solving half of the problem doesn't solve the security problem.

In the end the article is talking about a few different things.

It speaks about the ongoing problem, assumptions, and some of the ways people have been employing solutions against these threats.

Some of the industry is asking questions, some of the responses are not always perfect or correct, but I don't think

this article was stating what the solutions exactly are

but more less stating what the problem was, what still exists,

what type of solutions exist etc.

In response to all of the things you stated.

I agree that many of the solutions you offer are good and work well.

In many environments its a bit hard to even get the basics implemented.

Those being parameterized queries, input validation,

db permissions, ingress/egress...

-Daniel Clemens

[Reply To Comment](#)

[Permalink](#)

[Share](#)

[Email](#)

[Report](#)

All wrong

Comment by [flast_name606](#) Jun 15, 2011, 18:47 PM EDT

[Response to All Wrong...](#)

Comment by [Packetninjas](#) Jun 16, 2011, 14:55 PM EDT

Care to Comment?

Subject (max length: 75):

Comment:

**Captcha:**

Type the characters you see in the picture above.

[Log On To Add Your Comment](#)
[XML](#) [Subscribe to RSS](#)

- » [Write To Editor](#)
- » [Reprint This Article](#)
- » [Download Top Reports](#)



Enabling People and Organizations to Harness the Transformative Power of Technology

CIOs & IT Professionals

Black Hat
 BYTE
 Cloud Connect
 Dark Reading
 Enterprise 2.0
 Enterprise Connect
 Enterprise Efficiency
 HDI
 InformationWeek
 InformationWeek 500
 InformationWeek 500 Conference
 InformationWeek Events
 InformationWeek Global CIO
 InformationWeek Healthcare
 InformationWeek India
 InformationWeek Reports
 InformationWeek SMB
 Interop
 Mobile Connect
 Network Computing
 No Jitter
 TechWeb.com
 The BrainYard

Software Developers

Dr. Dobb's
 Dr. Dobb's M-Dev
 Dr. Dobb's Journal
 Dr. Dobb's Update
 TechWeb.com

Web & Digital Professionals

Internet Evolution
 Online Marketing Summit
 TechWeb.com

Government Officials

GTEC Ottawa
 InformationWeek Government
 TechWeb.com

Vertical Markets

Advanced Trading
 Bank Systems & Technology
 CreateYourNextCustomer
 InformationWeek Government
 InformationWeek Healthcare
 Insurance & Technology
 Light Reading / Telecom
 The CMO Site
 Wall Street & Technology

Game Industry Professionals

Gamasutra.com
 Game Developers Conference (GDC)
 Independent Games Festival
 Game Developer Magazine
 GDC Europe
 GDC China
 Game Career Guide
 Game Advertising Online

Global Communications Service Providers

Heavy Reading
 Heavy Reading Insiders
 Pyramid Research
 Light Reading
 Light Reading India
 Light Reading Mobile
 Light Reading Cable
 Light Reading Europe
 Light Reading Asia
 Ethernet Expo
 TelcoTV
 Tower Summit
 Light Reading Live & Virtual Events
 Webinars

Most Popular

Cable Catchup
 Cloud Connect Blog
 Digital Life
 Evil Bytes
 InformationWeek Reports
 Interop Blog
 Monkey Bidness
 Over the Air
 Personal Tech
 The Philter
 Valley Wonk

UBM TechWeb Reader Services

[About UBM TechWeb](#) [Advertising Contacts](#) [Technology Marketing Solutions](#) [Contact Us](#) [Feedback](#)

[Reprints](#) [TechWeb Digital Library / White Papers](#) [TechWeb Events Calendar](#) [TechWeb.com](#)

[Dark Reading Home](#) [Attacks / breaches](#) [Vulnerabilities](#) [Application Security](#) [Client Security](#) [Perimeter Security](#) [Security Management](#) [Storage Security](#)
[Encryption](#) [NAC](#) [Antivirus](#) [Privacy](#) [Blogs](#) [Security discussions](#)

[Newsletters](#) [Video](#) [Webcasts](#) [Live events](#) [TechWeb Digital Library](#) [Registration/membership](#) [About us](#)
[Sales and marketing contacts](#) [Send us a tip or comments](#) [Site map](#) [Technology Marketing Solutions](#)