Database Security

Yuli Stremovskiy
Agenda

• Database Security
• What is GreenSQL?
• Management Console
• Demo
• GreenSQL Roadmap
Hackers have become professional.

There are business models that finance them.

SQL Injection attacks are becoming increasingly sophisticated and difficult to combat.

It uses stealth techniques to go unnoticed for as long as possible.

Hackers create much more SQL Injection attacks.
# Pricelist

<table>
<thead>
<tr>
<th>Information</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>$0.50</td>
</tr>
<tr>
<td>Phone number</td>
<td>$0.25</td>
</tr>
<tr>
<td>Unpublished phone number</td>
<td>$17.50</td>
</tr>
<tr>
<td>Cell phone number</td>
<td>$10</td>
</tr>
<tr>
<td>Date of birth</td>
<td>$2</td>
</tr>
<tr>
<td>Social Security number</td>
<td>$8</td>
</tr>
<tr>
<td>Driver’s license</td>
<td>$3</td>
</tr>
<tr>
<td>Education</td>
<td>$12</td>
</tr>
<tr>
<td>Credit history</td>
<td>$9</td>
</tr>
<tr>
<td>Bankruptcy details</td>
<td>$26.50</td>
</tr>
<tr>
<td>Lawsuit information</td>
<td>$2.95</td>
</tr>
<tr>
<td>Sex offender</td>
<td>$13</td>
</tr>
<tr>
<td>Workers’ comp history</td>
<td>$18</td>
</tr>
<tr>
<td>Military record</td>
<td>$35</td>
</tr>
</tbody>
</table>
Latest Victims

- Oct 2009 - One of NASA's was vulnerable to a SQL injection attacks. All of this despite the fact that the agency’s IT budget in fiscal year 2009 was $1.6 billion, of which $15 million was dedicated to IT security.


- Nov 2009 - Russian cyber gang uses SQL injection attack crack deep inside the network of a giant U.S. debit and credit-card processor.

- Nov 2009 - An SQL injection flaw has been detected on the Yahoo! Website. The vulnerability was on the Yahoo job section.

- Dec 2009 - Wall Street Journal website, Intel, Apple
Who uses the Database?

Database

- Financial data
- Private data
- Customer data

Connections:
- Application
- User

Applications:
- CMS
- E-commerce
- Testing
- Replication
- Reporting
- Backup
- Monitoring

Users:
- High privileged users
- Administrators
- Application Users
- Casual users
- Forums
- Blog
- Wiki

Data Types:
- Financial data
- Private data
- Customer data
Using Shared Hosting Services?
You are under attack!!!

- Hundreds of websites are on the same database server - **hundreds of attack vectors**

- If your neighbor's web site database is vulnerable, then so are you, no matter how carefully you've vetted your own code.
What is SQL Injection?

• **Legitimate Query:**
  SELECT * from users
  WHERE username = 'admin' and password = '123'

• **Injected SQL code:**
  SELECT * from users where username = 'admin'
  and password = 'XXX' or '1'='1
SQL Injection after effect

- Bypass login page
- DOS - Deny of service
- Install web shell
- Iframe injection
- Access system files
- Install db backdoor
- Theft of sensitive information / credit cards
- Additional step of the attack:
  - Attack computers on the LAN
How iframe injection works

- Automated SQL Injection
- Injecting `<iframe src=http://xxxxx.com>`
- User visits infected site/page
- Trojan horse drive by installation
- Your PC is controlled by black hat hackers
  - Send SPAM
  - Records all login information
  - Records all transactions with bank websites
  - Online money transfer
Buzus Trojan

A large scale SQL injection attack has injected a malicious iframe on tens of thousands of susceptible websites. ScanSafe reports that the injected iframe loads malicious content from 318x.com, which eventually leads to the installation of a rootkit-enabled variant of the Buzus backdoor trojan. A Google search on the iframe resulted in over 132,000 hits as of December 10, 2009.

Infection sequence:
Injected iframe - `<script src="hop://318x.com">` Exeutes a script that creates a new iframe to 318x.com/a.htm. That iframe (a.htm) does 2 things:
GreenSQL History

- Open Source project
- Started at 2007
- Hosted at sourceforce
- More than 30,000 downloads
- Version 1.2 - 3k downloads in it’s first month
What is GreenSQL

- GreenSQL is a database firewall solution
- Protects against SQL injections and other known and unknown Database attacks
- Cool web based management interface
- MySQL / PostgreSQL built in support
GreenSQL – High Level Architecture

1. SQL Proxy
2. Risk Matrix Calculation
3. SQL Queries /WL/Policy
4. Good / Block/ Warn / Learn
5. Forward and Integration

Web Apps
Client/Server Apps
Web services/ SOAP
Legacy Apps

DB Server 1  DB Server 2  DB Server 3  DB Server N
How it works?

- Reverse Proxy
- Number of databases
- Number of backend DB servers
- Deployment options:
  - Can be installed together with the DB server
  - Can be installed on dedicated server / VPS
Using the Database Securely

- Application connections
  - Wiki
  - Forums
  - Blog

- User connections
  - High privileged users
  - Casual users
  - Application Users
  - Administrators

- Database
  - CMS
  - Ecommerce
  - Testing
  - Replication
  - Reporting
  - Backup
  - Monitoring
GreenSQL management console
Multiple Databases / Proxies

### List of Databases

<table>
<thead>
<tr>
<th>ID</th>
<th>Database name</th>
<th>Db type</th>
<th>Proxy</th>
<th>Mode</th>
<th>Options</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>default mysql db</td>
<td>mysql</td>
<td>All Proxies</td>
<td>IPS</td>
<td>Overview</td>
<td>Alerts</td>
</tr>
<tr>
<td>2</td>
<td>no-name mysql db</td>
<td>mysql</td>
<td>All Proxies</td>
<td>IPS</td>
<td>Overview</td>
<td>Alerts</td>
</tr>
<tr>
<td>3</td>
<td>default pgsql db</td>
<td>pgsql</td>
<td>All Proxies</td>
<td>IPS</td>
<td>Overview</td>
<td>Alerts</td>
</tr>
<tr>
<td>4</td>
<td>joomla</td>
<td>mysql</td>
<td>Default MySQL Proxy</td>
<td>Learning Mode</td>
<td>Overview</td>
<td>Alerts</td>
</tr>
</tbody>
</table>

### List of Proxies

<table>
<thead>
<tr>
<th>ID</th>
<th>Proxy name</th>
<th>Db type</th>
<th>Status</th>
<th>Options</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Default MySQL Proxy</td>
<td>mysql</td>
<td>Active</td>
<td>Settings</td>
<td>Delete</td>
</tr>
<tr>
<td>2</td>
<td>Default PgSQL Proxy</td>
<td>pgsql</td>
<td>Active</td>
<td>Settings</td>
<td>Delete</td>
</tr>
</tbody>
</table>
Alert Example

<table>
<thead>
<tr>
<th>Pattern</th>
<th><code>select * from admin where name = ? and pwd=sha(?) or (?) = ?);</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert ID</td>
<td>235</td>
</tr>
<tr>
<td>Time</td>
<td>2010-01-20 04:31:56</td>
</tr>
<tr>
<td>Listener</td>
<td>Default MySQL Proxy</td>
</tr>
<tr>
<td>DB</td>
<td>greendb</td>
</tr>
</tbody>
</table>

Matching queries:

<table>
<thead>
<tr>
<th>Query</th>
<th><code>SELECT * FROM admin WHERE name = 'admin' AND pwd=SHA('') OR (1 = 1);</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>2010-01-20 04:31:56</td>
</tr>
<tr>
<td>DB User</td>
<td></td>
</tr>
<tr>
<td>Risk</td>
<td><strong>105</strong> blocked</td>
</tr>
<tr>
<td>Reason</td>
<td>Query uses sensitive tables</td>
</tr>
<tr>
<td></td>
<td>Multiple queries found</td>
</tr>
<tr>
<td></td>
<td>Query has 'or' token</td>
</tr>
<tr>
<td></td>
<td>True expression detected (SQL tautology)</td>
</tr>
<tr>
<td></td>
<td>Query has empty password expression</td>
</tr>
<tr>
<td></td>
<td>Query blocked because it is not in whitelist.</td>
</tr>
<tr>
<td>ID</td>
<td>456</td>
</tr>
</tbody>
</table>
GreenSQL Advantages

- Multiple modes
  - IDS/IPS / learning / Firewall
- Easy to use
- Pattern Recognition (signatures)
- Heuristics (risk calculation)
- Open Source
GreenSQL Advantages – Cont’

• Cross Platform (any Linux and Unix system)
• Rapid Deployment (pre built packages)
• Well established (30,000 downloads and counting)
• Web application independent
• The only free security solution for MySQL
• The only security solution for PostgreSQL
• User Friendly WEB GUI/Management tool
GreenSQL IPS / IDS

- Sensitive tables
- Multiple queries ( ; / UNION )
- SQL comments
- Empty password
- SQL tautology - true statements (1=1)
- Administrative commands
- Information disclosure commands
But, I’m a kick ass developer
So why should I use GreenSQL

- Legacy code
- Not only Web application and web services use your database
- Protects the database console access
- 0 day database attacks prevention
- No direct access to the database machine
GreenSQL: Demonstration

http://demo.greensql.net/

http://www.greensql.net/sql-injection-test
Open Source Roadmap

- Native Joomla / Drupal / Wordpress plugins
- Integrated GreenSQL Console as CMS plugin (you will use Joomla Admin to manage GreenSQL)
- Web user name / IP address reporting in GreenSQL alerts
- Auditing
GreenSQL Support Program

- Installation Support
- GreenSQL Optimization
- E-mail Submission
- Service portal
- Consulting
- Software Updates

No More Injections
Questions
Thank You

• Yuli Stremovskiy
• yuli@greensql.com

http://blog.greensql.com
http://twitter.com/greensql