GREENSQL
Database Security

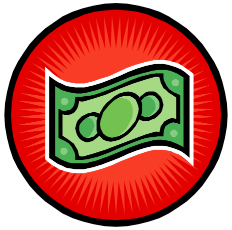
Yuli Stremovsky

Agenda

- Database Security
- What is GreenSQL ?
- Management Console
- Demo
- GreenSQL Roadmap

The need

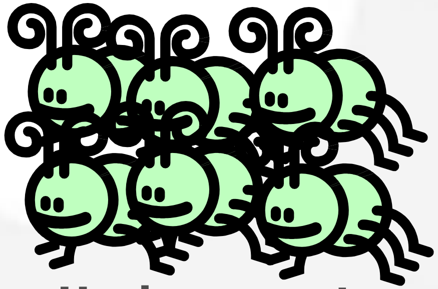
Hackers have become professional



There are business models that finance them

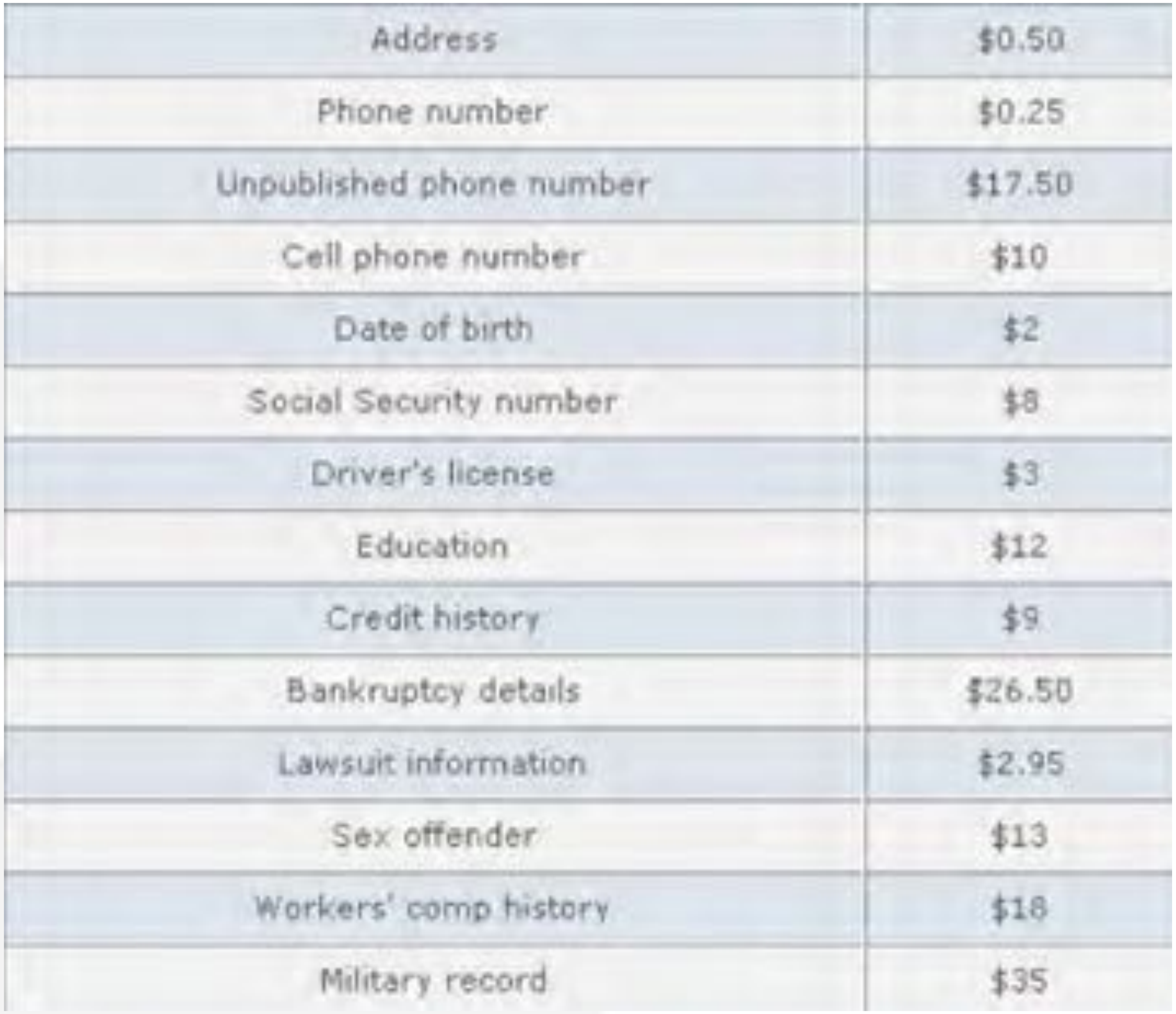
SQL Injection attacks are becoming increasingly sophisticated and difficult to combat.

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



Hackers create much more SQL Injection attacks

Pricelist

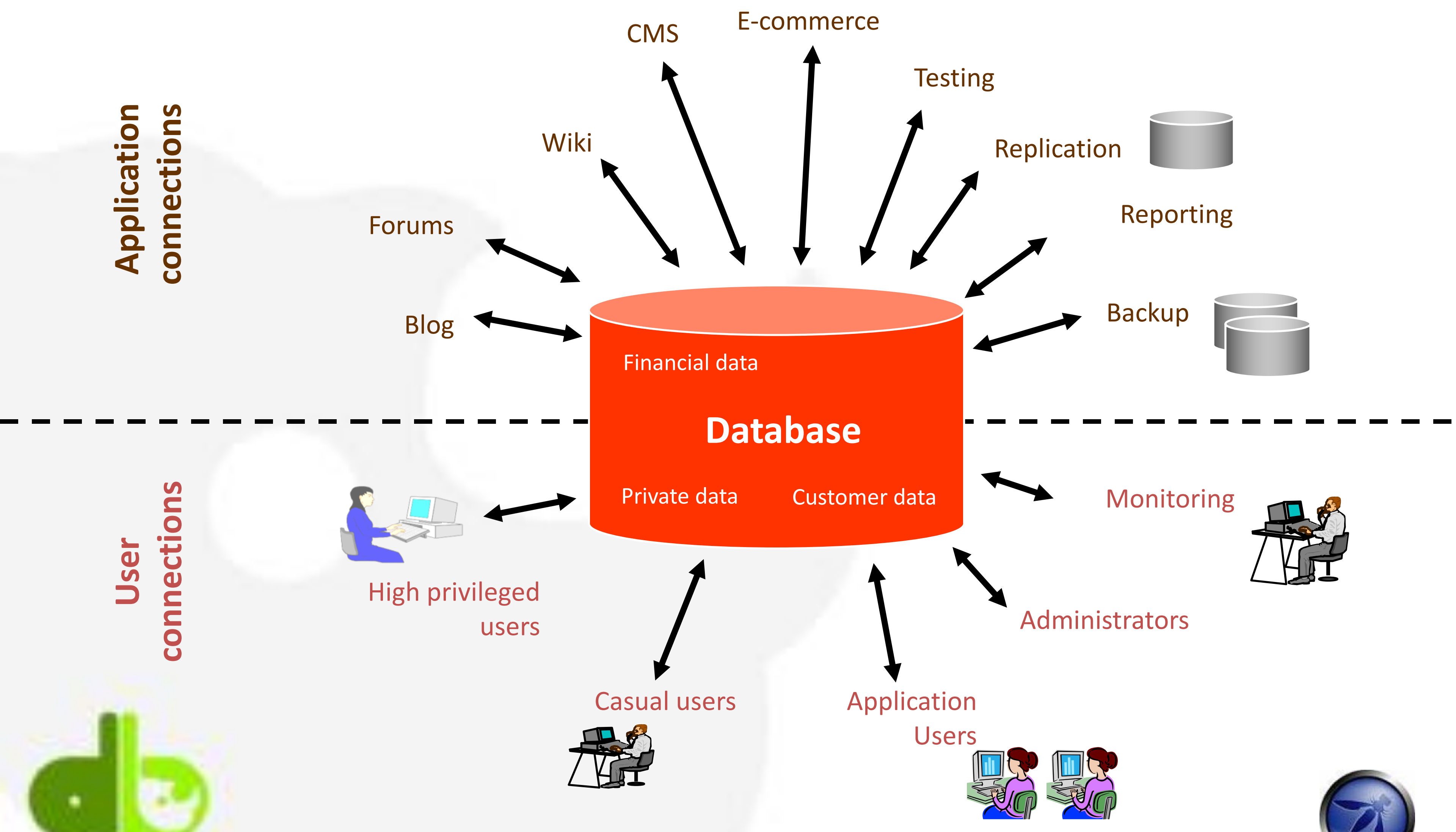


Address	$0.50
Phone number	$0.25
Unpublished phone number	$17.50
Cell phone number	$10
Date of birth	$2
Social Security number	$8
Driver's license	$3
Education	$12
Credit history	$9
Bankruptcy details	$26.50
Lawsuit information	$2.95
Sex offender	$13
Workers' comp history	$18
Military record	$35

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.
- Mar 2009 & Nov 2009 - SQL injection attack exposes sensitive customer data on **Symantec** web server.
- 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 ?



Application connections

Forums

Blog

Wiki

CMS

E-commerce

Testing

Replication

Reporting

Backup

Financial data

Database

Private data

Customer data

User connections

High privileged users

Casual users

Application Users

Administrators

Monitoring

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.

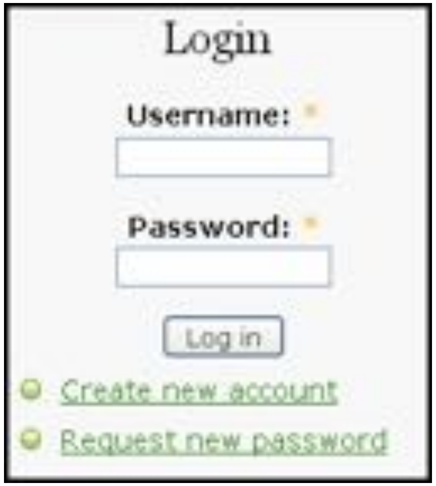
What is SQL Injection?

- **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’

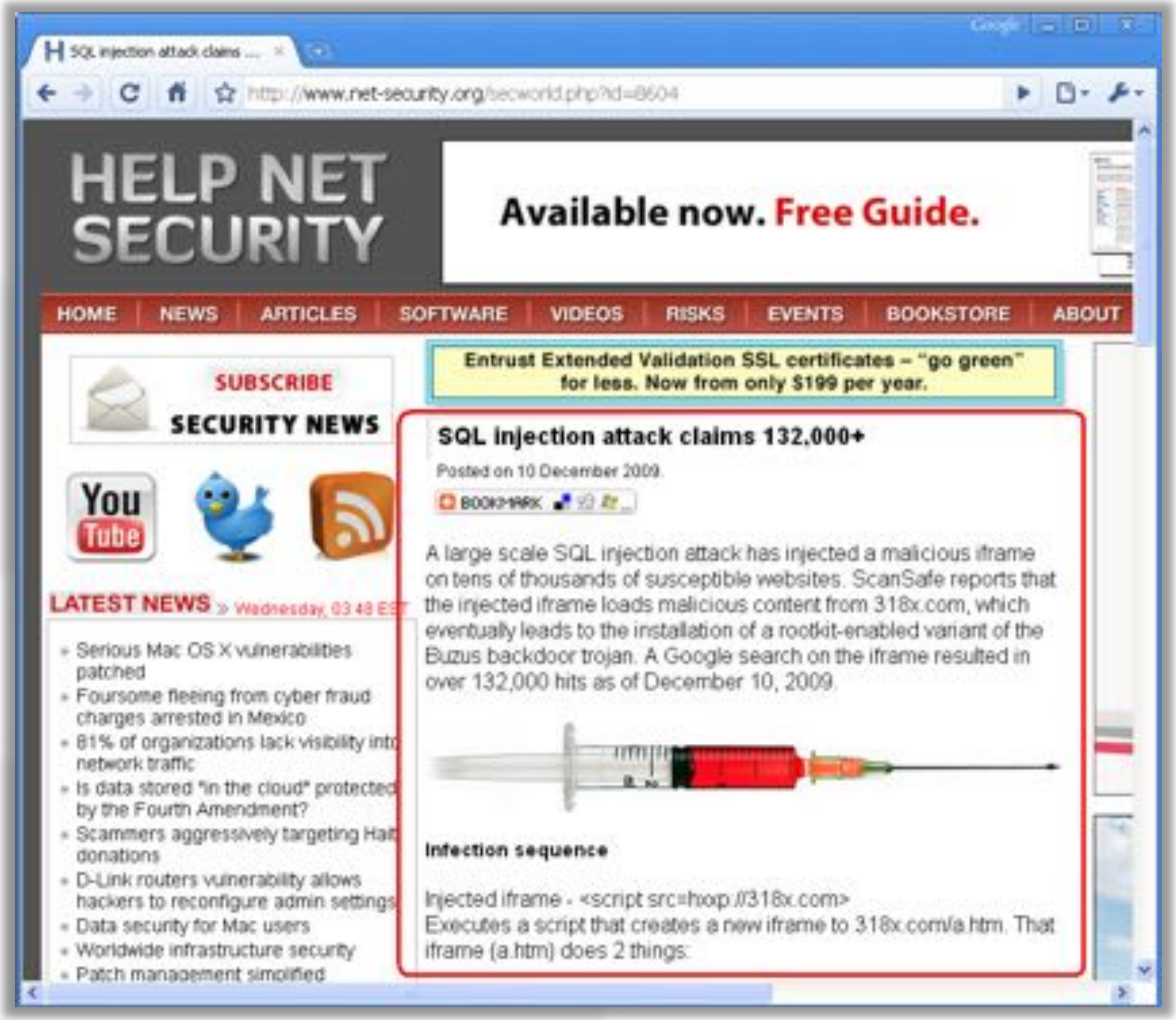
SQL Injection after effect

- 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



LATEST NEWS » Wednesday, 03:48 EST

- Serious Mac OS X vulnerabilities patched
- Foursome fleeing from cyber fraud charges arrested in Mexico
- 81% of organizations lack visibility int network traffic
- Is data stored "in the cloud" protected by the Fourth Amendment?
- Scammers aggressively targeting Hait donations
- D-Link routers vulnerability allows hackers to reconfigure admin settings
- Data security for Mac users
- Worldwide infrastructure security
- Patch management simplified

SQL injection attack claims 132,000+

Posted on 10 December 2009.

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

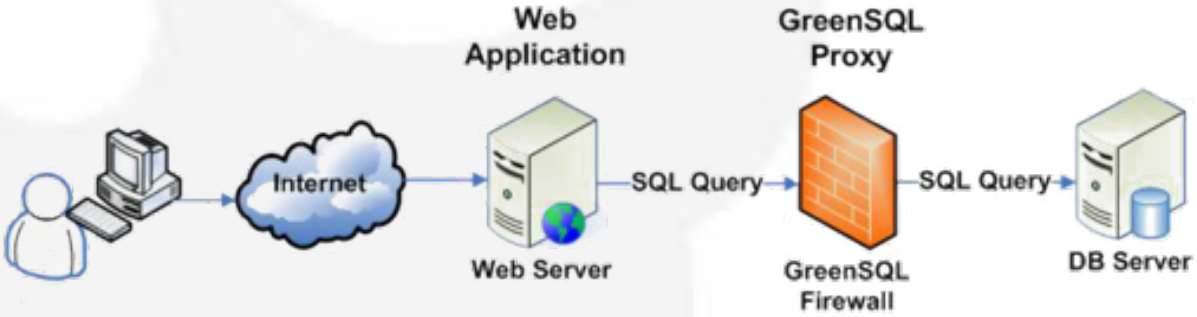
Injected iframe - <script src=hxxp://318x.com>
Executes a script that creates a new iframe to 318x.com/a.htm. That iframe (a.htm) does 2 things:

GreenSQL History

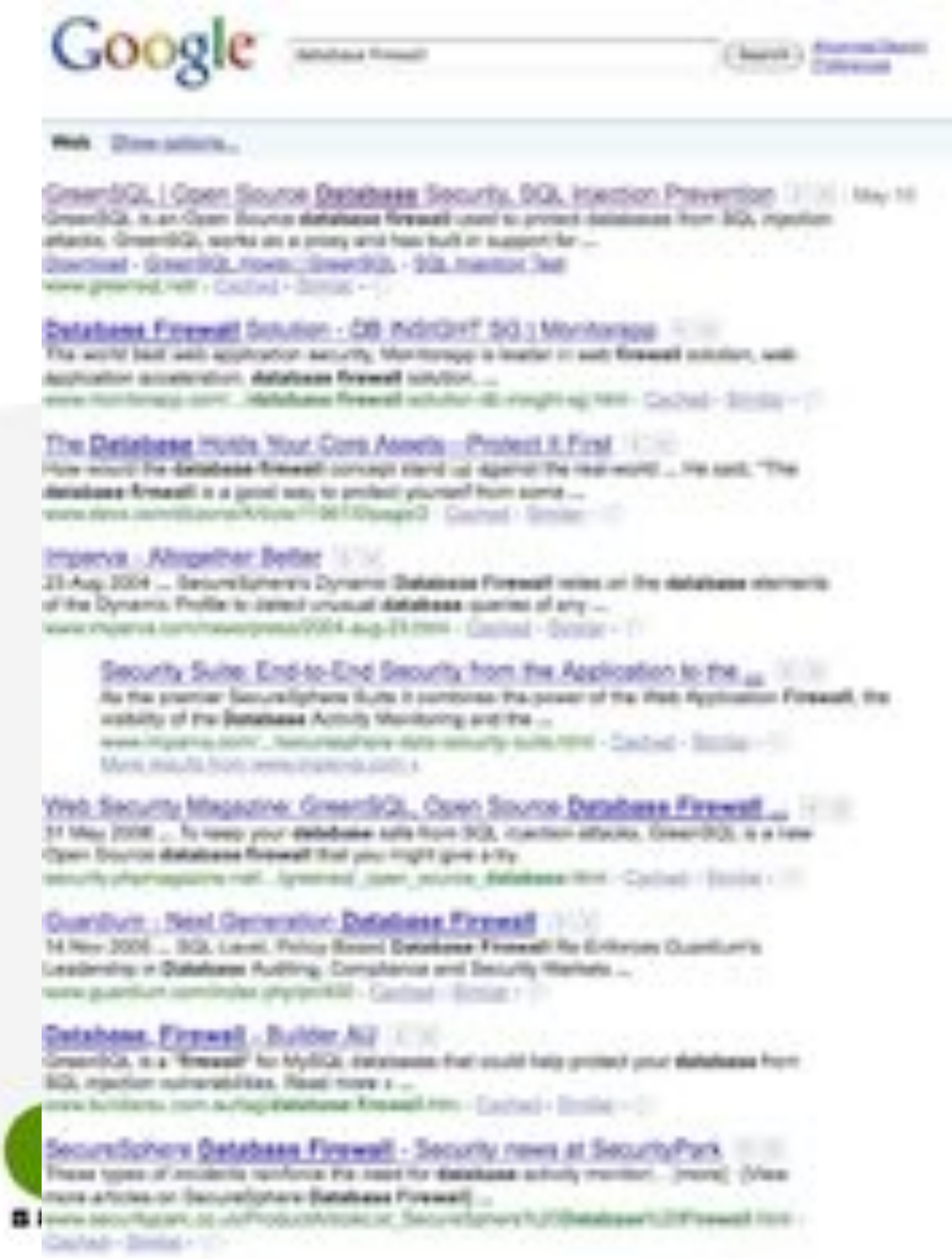
- Open Source project
- Started at 2007
- Hosted at sourceforce
- More than 30,000 downloads
- Version 1.2 - 3k downloads in it’s first month

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



Database Firewall



GreenSQL | Open Source **Database** Security, SQL Injection Prevention - May 10
GreenSQL is an Open Source **database firewall** used to protect databases from SQL injection attacks. GreenSQL works as a proxy and has built in support for ...
Download - GreenSQL Howto / GreenSQL - SQL Injection Test
www.greensql.net/ - Cached - Similar

Database Firewall Solution - DB INSIGHT SQ | Monitorapp
The world best web application security, Monitorapp is leader in web **firewall** solution, web application acceleration, **database firewall** solution, ...
www.monitorapp.com/.../**database**-**firewall**-solution-db-insight-sq.html - Cached - Similar

The **Database** Holds Your Core Assets - Protect It First
How would the **database firewall** concept stand up against the real-world ... He said, "The **database firewall** is a good way to protect yourself from some ...
[illegible] - Cached - Similar

Imperva - Altogether Better
23 Aug 2004 ... SecureSphere's Dynamic **Database Firewall** relies on the **database** elements of the Dynamic Profile to detect unusual **database** queries of any ...
www.imperva.com/news/press/2004-aug-23.html - Cached - Similar

Security Suite: End-to-End Security from the Application to the ...
As the premier SecureSphere Suite it combines the power of the Web Application **Firewall**, the visibility of the **Database** Activity Monitoring and the ...
www.imperva.com/.../securesphere-data-security-suite.html - Cached - Similar
More results from www.imperva.com »

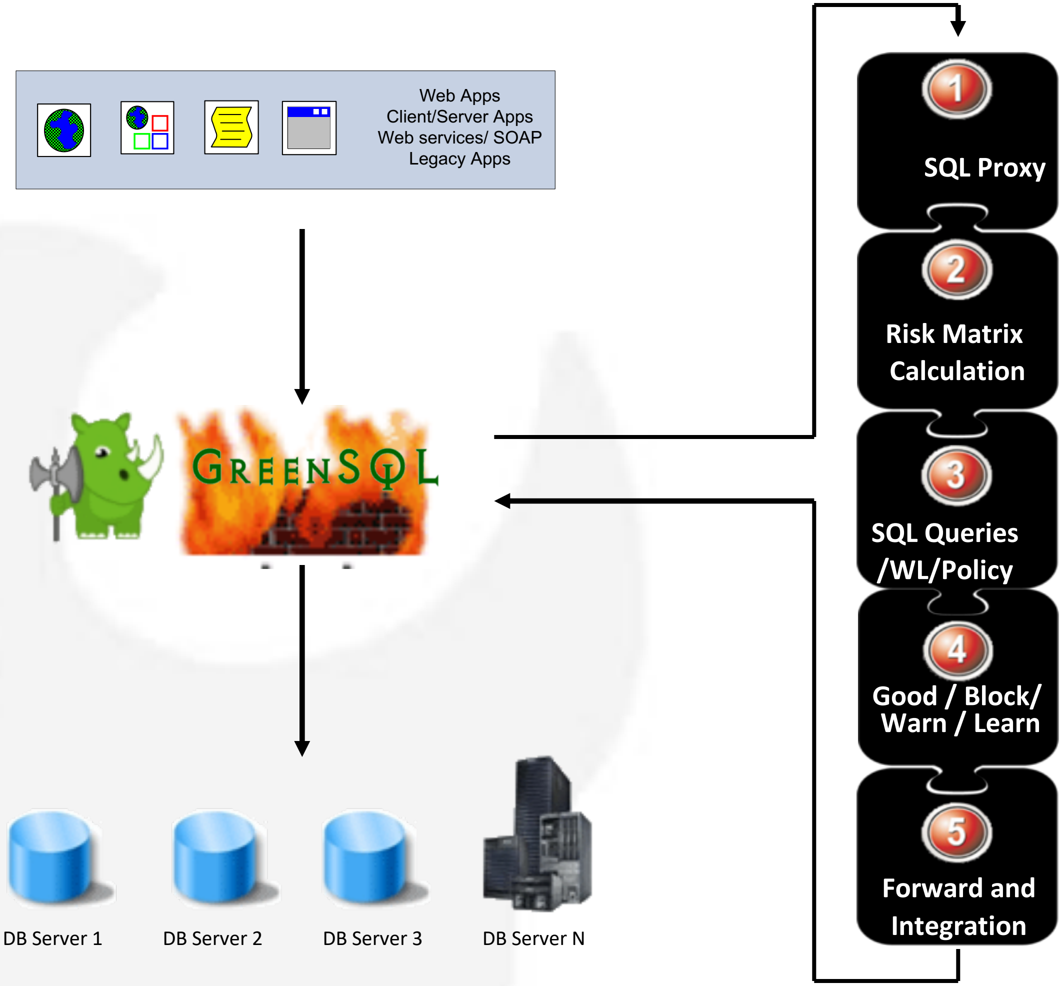
Web Security Magazine: GreenSQL, Open Source **Database Firewall** ...
31 May 2008 ... To keep your **database** safe from SQL injection attacks, GreenSQL is a new Open Source **database firewall** that you might give a try.
[illegible]_greensql_open_source_**database**.html - Cached - Similar

Guardium : Next Generation **Database Firewall**
14 Nov 2006 ... SQL Level, Policy Based **Database Firewall** Re-Enforces Guardium's Leadership in **Database** Auditing, Compliance and Security Markets ...
www.guardium.com/index.php/[illegible] - Cached - Similar

Database Firewall - Builder AU
GreenSQL is a "**firewall**" for MySQL databases that could help protect your **database** from SQL injection vulnerabilities. Read more » ...
www.builderau.com.au/tag/**database**-**firewall**.htm - Cached - Similar

SecureSphere **Database Firewall** - Security news at SecurityPark
These types of incidents reinforce the need for **database** activity monitors ... [more] [View more articles on SecureSphere **Database Firewall**] ...
www.securitypark.co.uk/[illegible]_SecureSphere%20**Database**%20**Firewall**.html -
Cached - Similar

GreenSQL – High Level Architecture

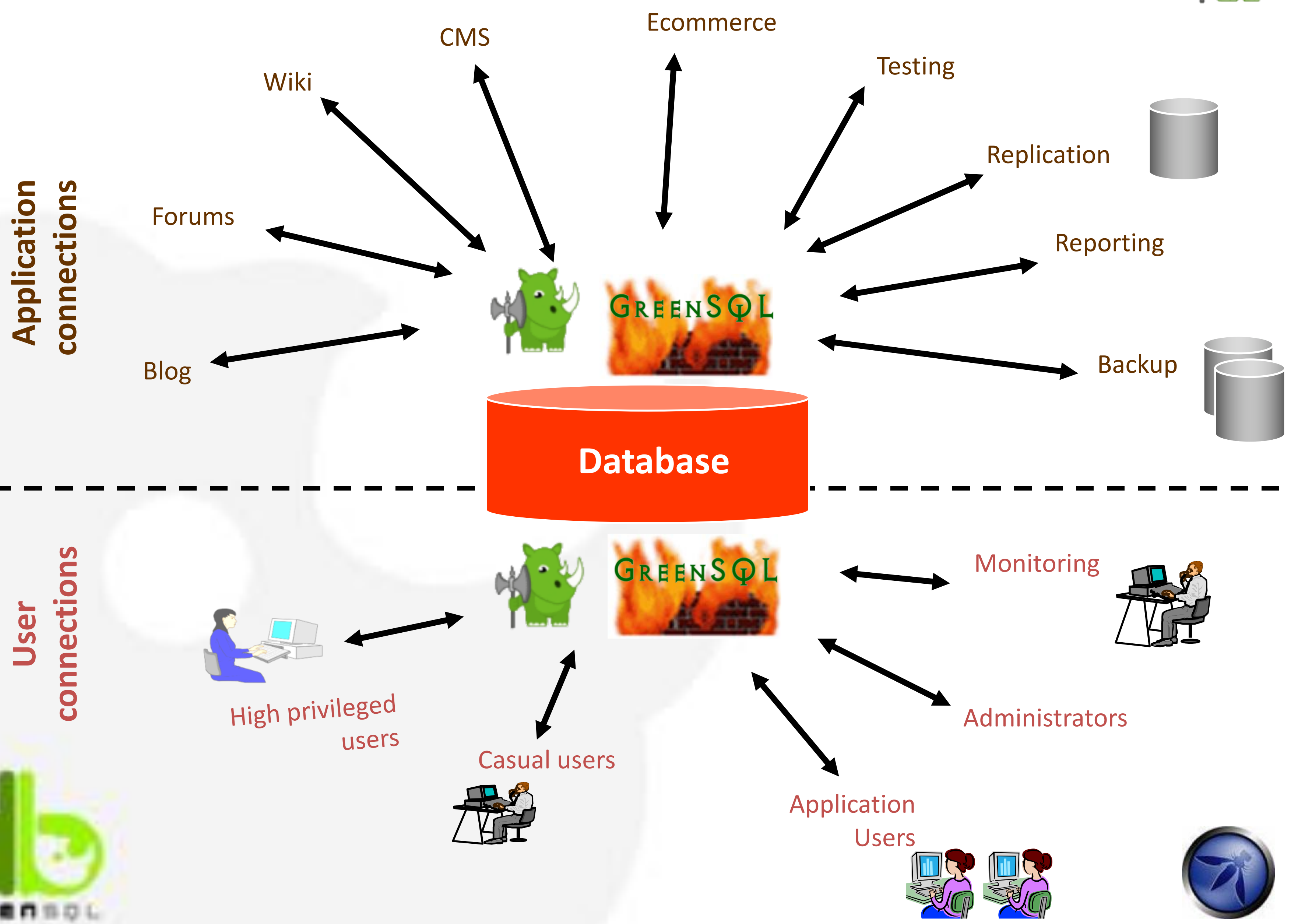


Web Apps
Client/Server Apps
Web services/ SOAP
Legacy Apps

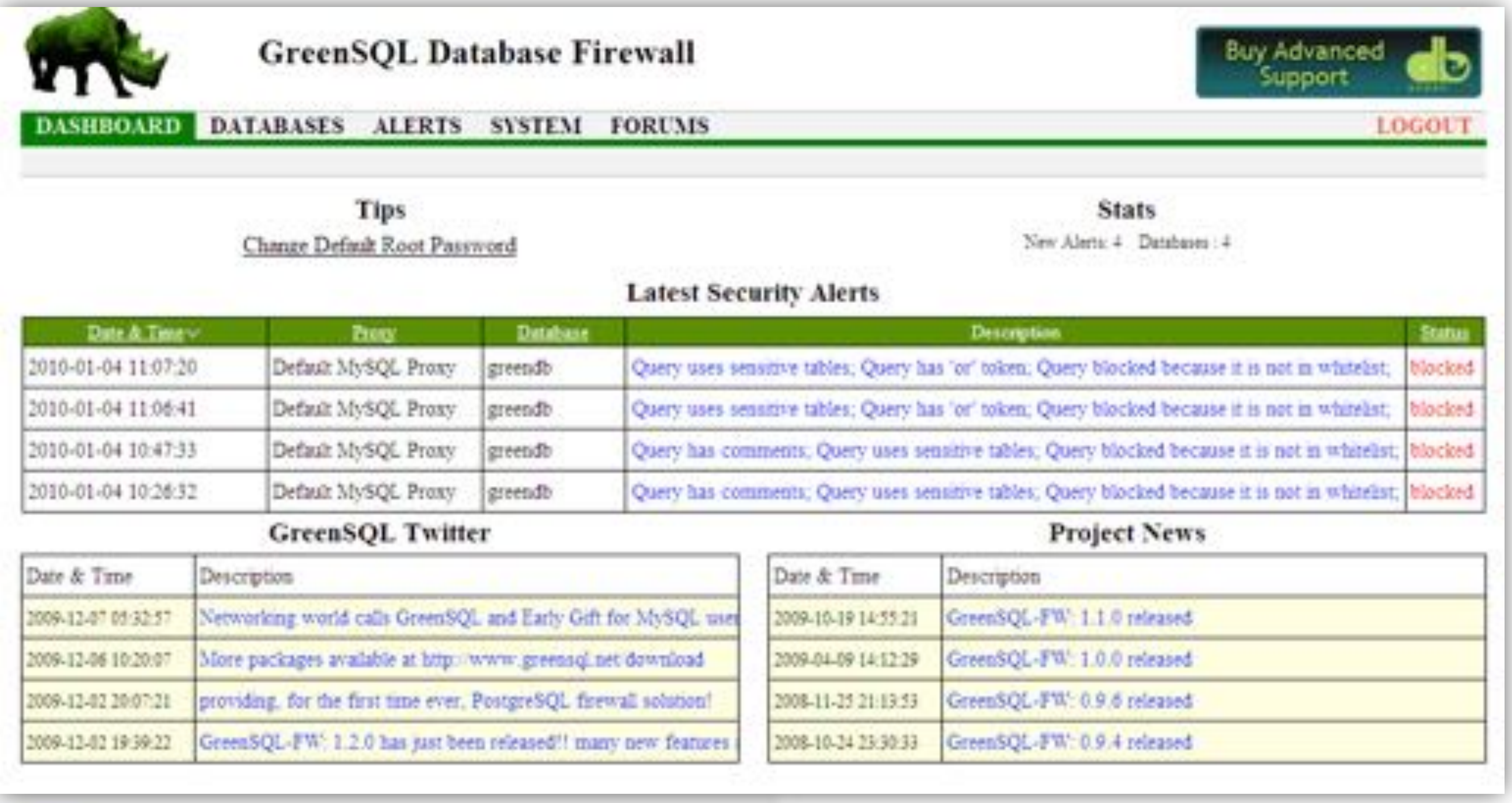
How it works?

- 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



GreenSQL management console



GreenSQL Database Firewall

Tips

Change Default Root Password

Stats

New Alerts: 4 Databases : 4

Latest Security Alerts

Date & Time	Proxy	Database	Description	Status
2010-01-04 11:07:20	Default MySQL Proxy	greendb	Query uses sensitive tables; Query has 'or' token; Query blocked because it is not in whitelist;	blocked
2010-01-04 11:06:41	Default MySQL Proxy	greendb	Query uses sensitive tables; Query has 'or' token; Query blocked because it is not in whitelist;	blocked
2010-01-04 10:47:33	Default MySQL Proxy	greendb	Query has comments; Query uses sensitive tables; Query blocked because it is not in whitelist;	blocked
2010-01-04 10:26:32	Default MySQL Proxy	greendb	Query has comments; Query uses sensitive tables; Query blocked because it is not in whitelist;	blocked

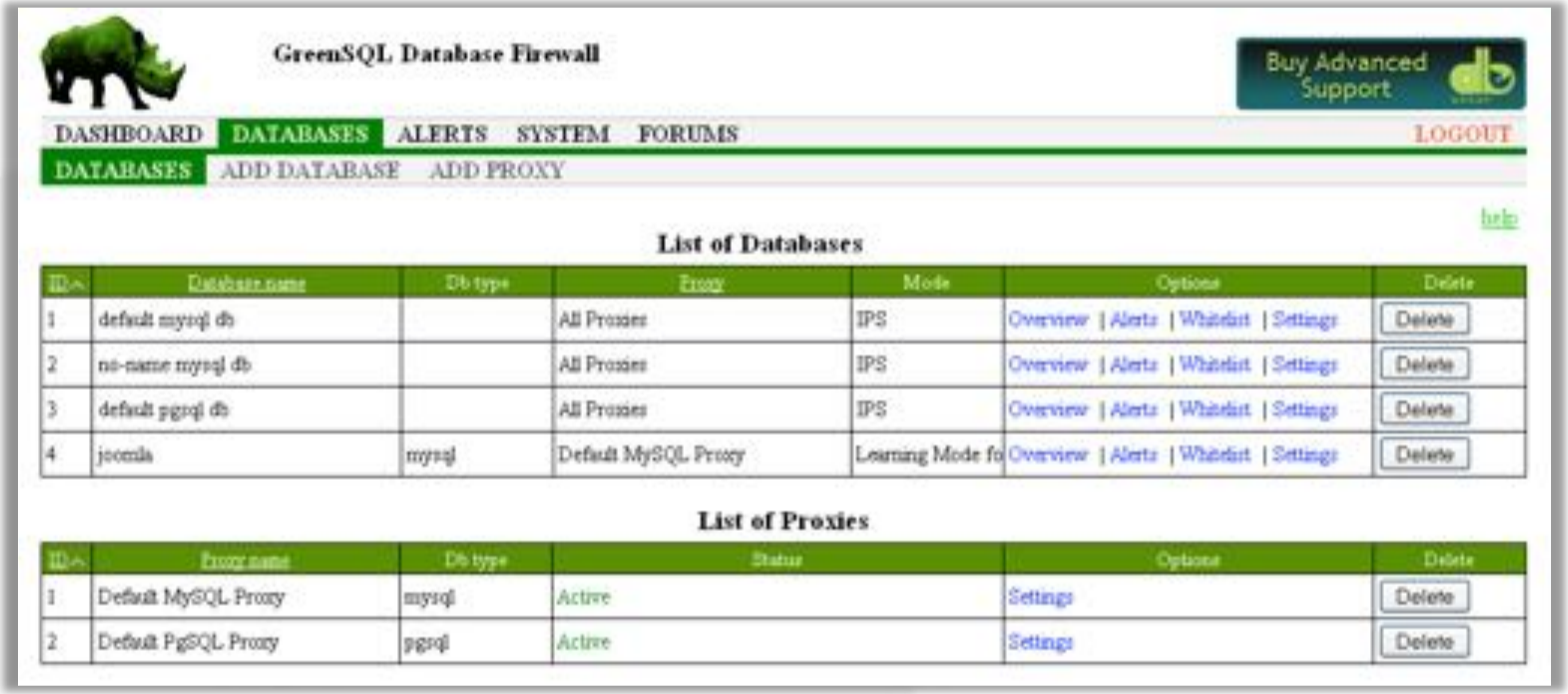
GreenSQL Twitter

Date & Time	Description
2009-12-07 05:32:57	Networking world calls GreenSQL and Early Gift for MySQL user
2009-12-06 10:20:07	More packages available at http://www.greensql.net/download
2009-12-02 20:07:21	providing, for the first time ever, PostgreSQL firewall solution!
2009-12-02 19:39:22	GreenSQL-FW: 1.2.0 has just been released!! many new features

Project News

Date & Time	Description
2009-10-19 14:55:21	GreenSQL-FW: 1.1.0 released
2009-04-09 14:12:29	GreenSQL-FW: 1.0.0 released
2008-11-25 21:13:53	GreenSQL-FW: 0.9.6 released
2008-10-24 23:30:33	GreenSQL-FW: 0.9.4 released

Multiple Databases / Proxies



GreenSQL Database Firewall

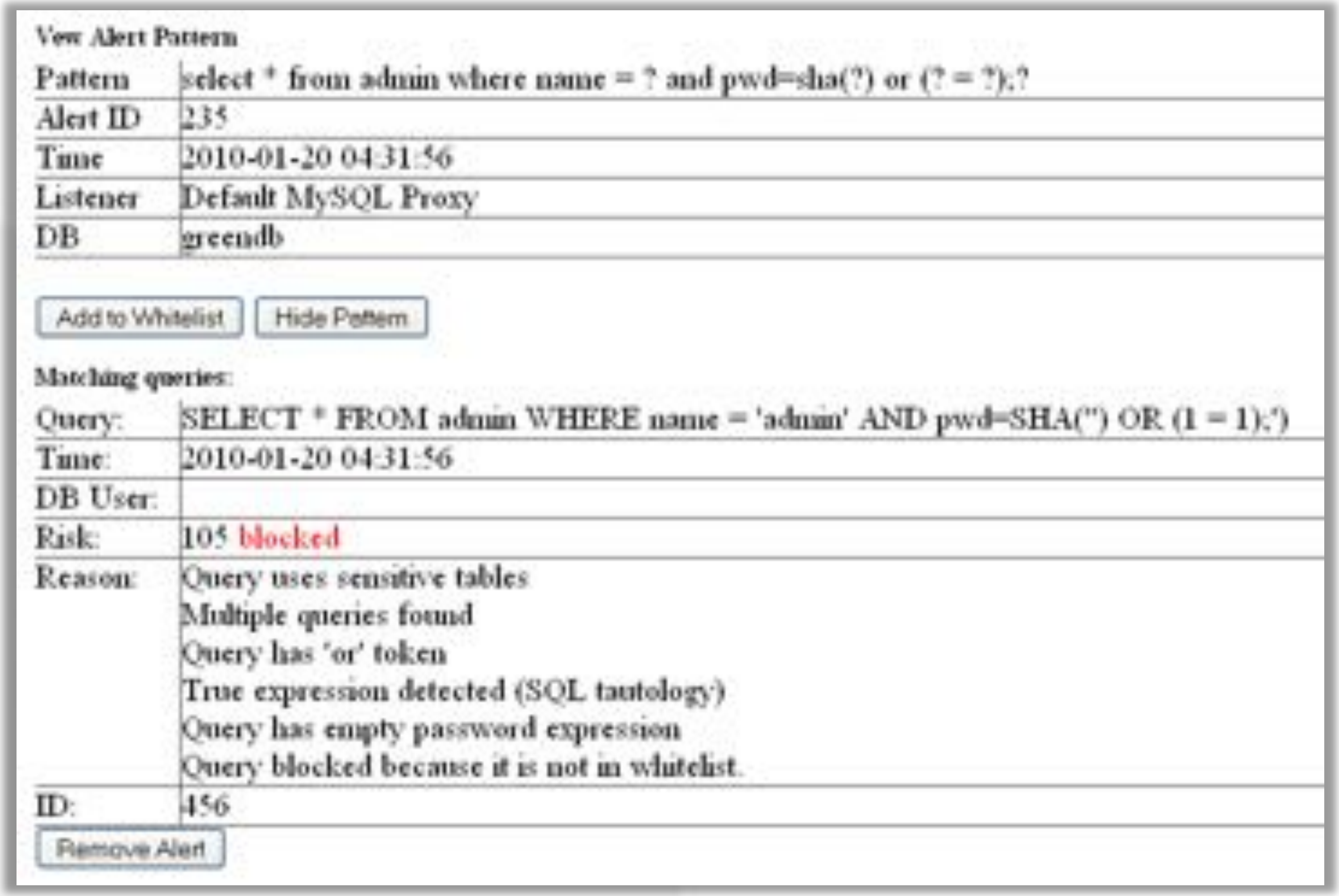
List of Databases

ID	Database name	Db type	Proxy	Mode	Options	Delete
1	default mysql db		All Proxies	IPS	Overview | Alerts | Whitelist | Settings	Delete
2	no-name mysql db		All Proxies	IPS	Overview | Alerts | Whitelist | Settings	Delete
3	default pgsql db		All Proxies	IPS	Overview | Alerts | Whitelist | Settings	Delete
4	joomla	mysql	Default MySQL Proxy	Learning Mode fo	Overview | Alerts | Whitelist | Settings	Delete

List of Proxies

ID	Proxy name	Db type	Status	Options	Delete
1	Default MySQL Proxy	mysql	Active	Settings	Delete
2	Default PgSQL Proxy	pgsql	Active	Settings	Delete

Alert Example



View Alert Pattern

Pattern	select * from admin where name = ? and pwd=sha(?) or (? = ?);?
Alert ID	235
Time	2010-01-20 04:31:56
Listener	Default MySQL Proxy
DB	greendb

Matching queries:

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

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 / Wordpres 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

- Consulting
- Service portal
- Software Updates

Questions

Thank You

- Yuli Stremovsky
- yuli@greensql.com

http://blog.greensql.com

http://twitter.com/greensql