

SONATA SOFTWARE

Best Practices in Performance & Security Testing

Mr. Sanjeev Padasalgi,
Senior Project Manager, Sonata Software

www.sonata-software.com



SONATA SOFTWARE

Agenda

- Why performance testing
- How to fix
- Case study
- Security testing challenges
- Case study
- About Sonata

1

SONATA
SONATA SOFTWARE

Functional vs. Load Testing

Functional test

Objective	Example
Functionality	Do business processes function properly after implementation?

Load test

Objective	Example
Stability	Will 2,000 concurrent hits crash the server?
Performance	Is response time acceptable according to specifications?
Functionality under load	Do business processes function properly under heavy load?
Endurance	Will this business process sustain 24*7


2

SONATA
SONATA SOFTWARE

Why Performance Testing

- **Change of needs**
 - Applications are built for today's need
 - Business processes change
- **Business growth**
 - Exponential growth leads to more internal, customers and partners
 - Disruption is a huge business loss
- **Process changes**
- **People changes**
- **Technology changes**

3




SONATA SOFTWARE

What should be done

- **Build performance expectation into contracts**
 - Response time, no of users, expected business growth, cost of provisioning
- **Should this be a capex or opex?**
- **How often should I do this?**
- **Identify the critical business processes**
- **Test for endurance, twice the expected business load**

4

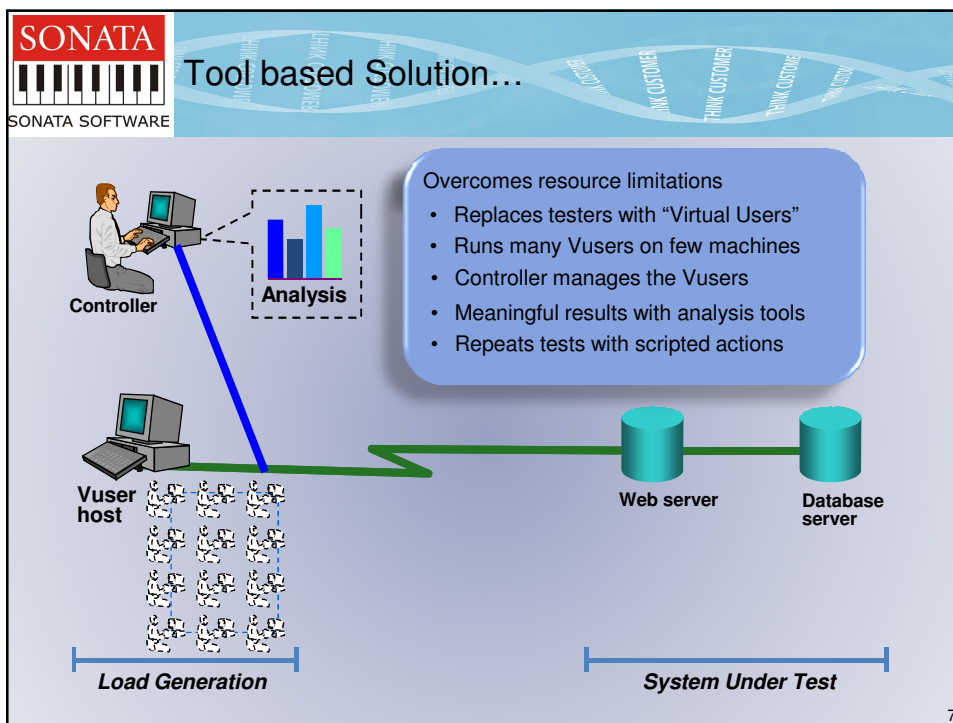
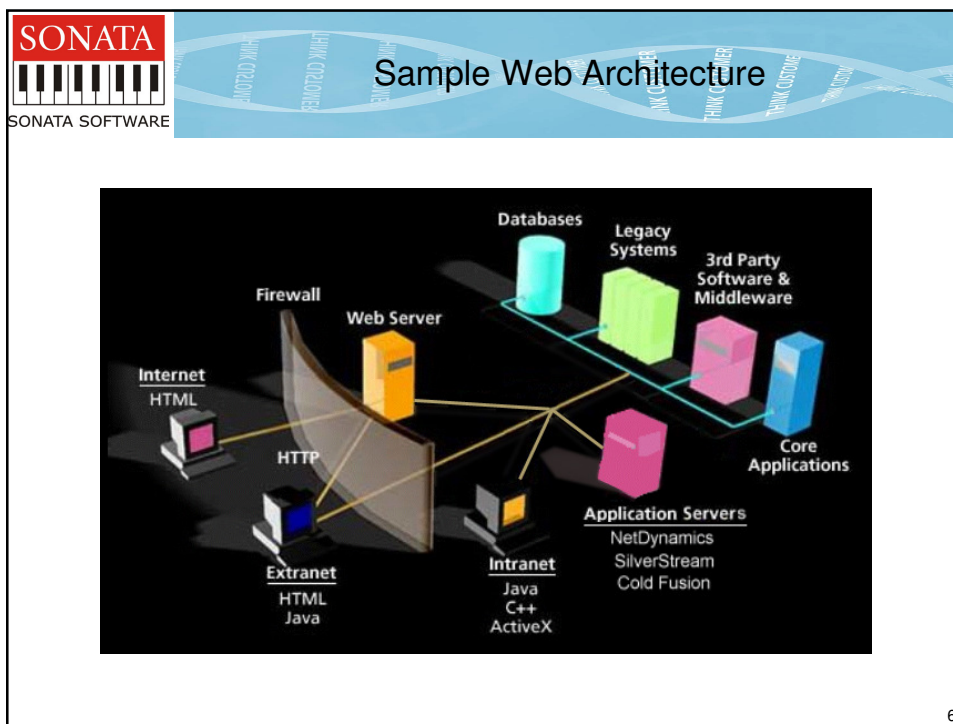


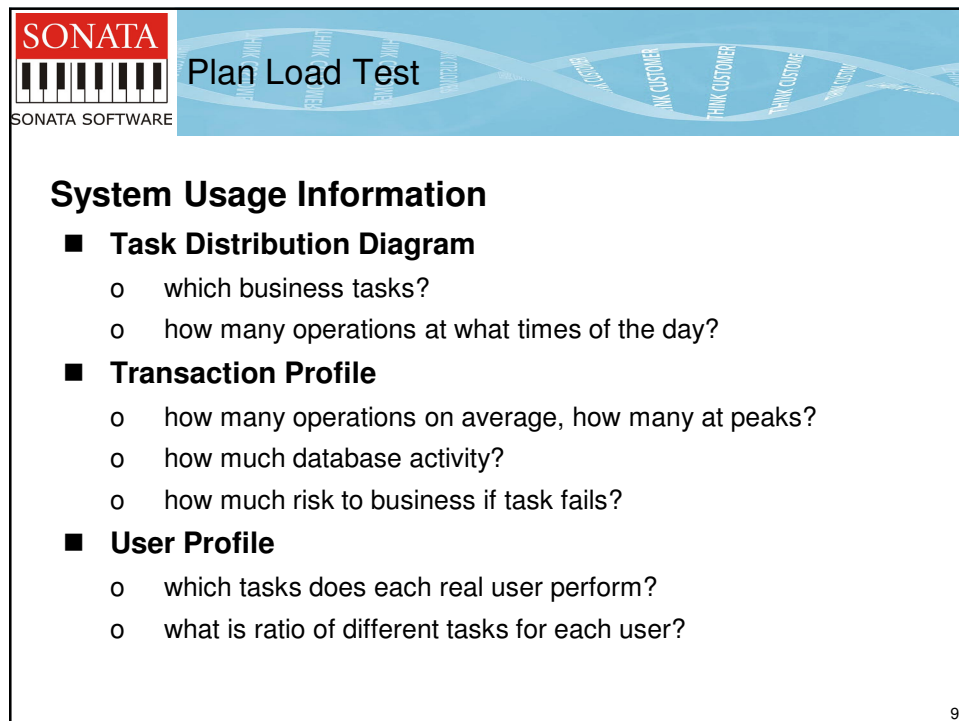
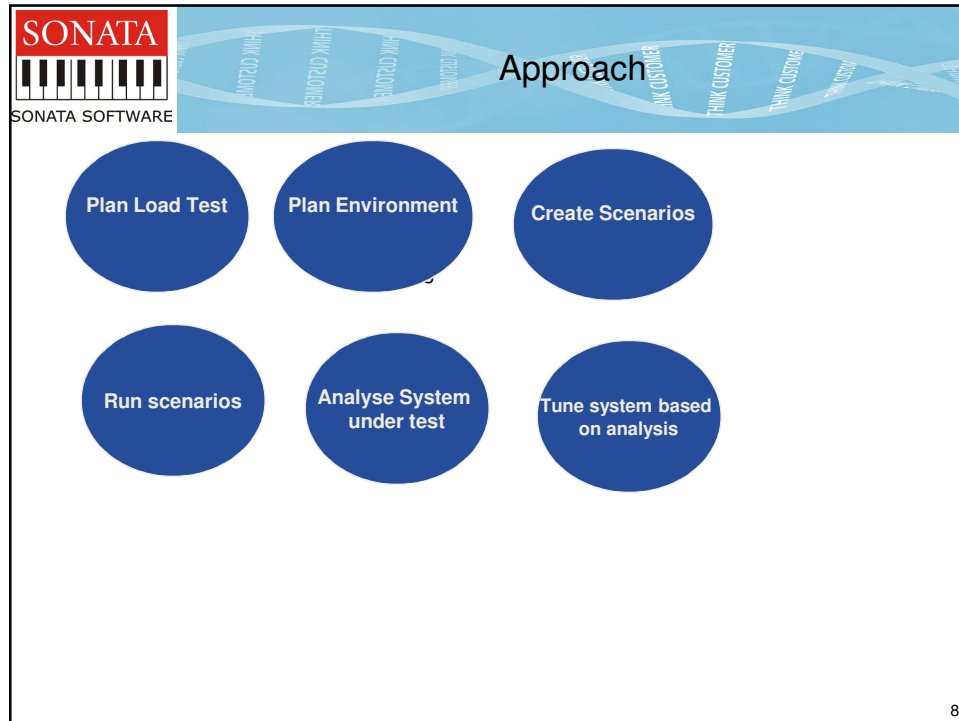
SONATA SOFTWARE


How?

- **Identify the critical business processes**
- **Identify the applications associated**
- **Plan what stage of business are you in**
 - Legacy systems getting exposed to Web?
 - Pure play ecommerce solutions
 - Complex architectures
 - Hub and spoke applications
 - Packaged ERP
- **Choose the tool that fits the protocol**

5








Plan Environment

- Identify the deployment environment or mimic
- Identify the servers
- Baseline applications
- Capacity assessment
- Load in incremental steps for non-replication of env
- Curve fitting to predict
- Measure vital stats memory growth, cpu utilization, disk reads
- Special tools for analysis

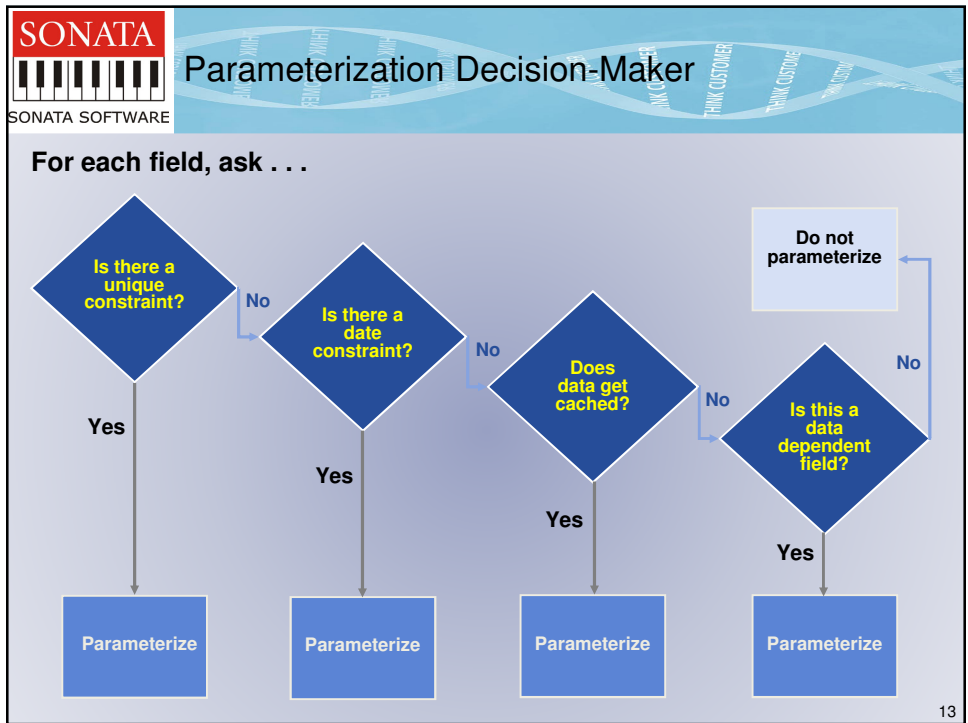
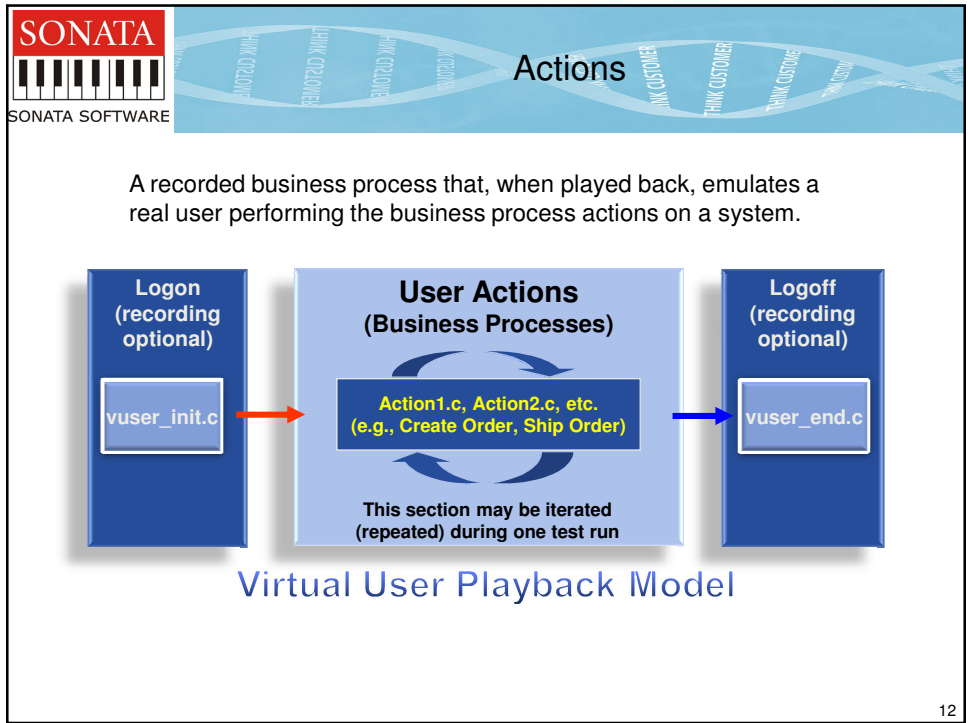
10



Create Vuser Script

- Record Vuser Actions
- Add Load Runner Transactions
- Parameterize data
- Verify correct Execution

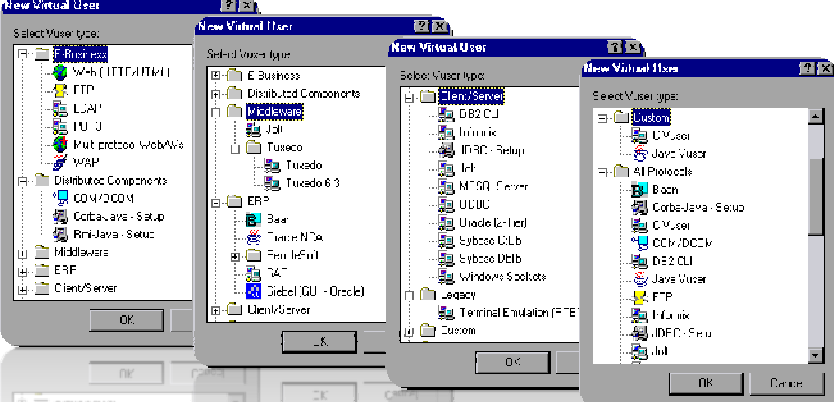
11



SONATA
SONATA SOFTWARE

The Load Runner Solution...

Provides support for many protocols and APIs




14

SONATA
SONATA SOFTWARE


CASE STUDY

15



SONATA SOFTWARE

Security- Testing



Website Attacks and Security Myths

SONATA SOFTWARE

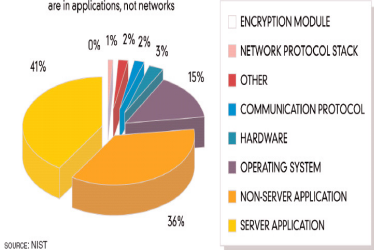
25 Jan, 2009 Monster.com Database Hacked

- ❖ Hackers gained access to confidential details provided by 4.5 million people to Monster.co.uk, the online recruitment site.
- ❖ Private information like names, email ids, and birth dates were stolen

CheckFree Warns 5 Million Customers After Hack

- ❖ CheckFree and some of the banks that use its e-bill payment service are notifying more than 5 million customers after criminals hacked their website.
- ❖ Criminals took control of the company's Internet domains and redirected customer traffic to a malicious Web site hosted in the Ukraine.
- ❖ This same technique was used by hackers one year ago, to take control of Comcast's Web site.
- ❖ Security experts believe that CheckFree may have fallen prey to a phishing attack.

92% of reported vulnerabilities are in applications, not networks



Category	Percentage
SERVER APPLICATION	36%
NON-SERVER APPLICATION	15%
OPERATING SYSTEM	15%
OTHER	3%
COMMUNICATION PROTOCOL	2%
NETWORK PROTOCOL STACK	2%
ENCRYPTION MODULE	1%
HARDWARE	0%


SOURCE: NIST

Some myths regarding web security

- We use SSL
- Firewalls protect the web site
- My network scanner found no issues
- We have annual security assessments

All these measures are network related not application related


17



Impact Of Security Non-Compliance


- Business Interruption leading to**
 - o Loss of customers
 - o Loss of revenue
 - o Loss of vendors/partners
 - o Privacy compliance violation
- Access to Sensitive Information**
 - o Loss/unauthorized access to private information
- Statutory Non-compliance**
 - o PCI
 - o SOX
- Reputation**
 - o Loss of credibility in the market
- Social Responsibility**
 - o The website should not be used as a tool for fraud

18




Business Benefits of Security Compliance

- ❖ Enhanced credibility with customers
 - ❖ **Independent validation of web application security**
- ❖ Adherence to statutory compliance standards like PCI DSS
- ❖ Reduction in overall test effort leading to faster time to market and cost reduction.
 - ❖ **Reduction in test efforts in OWASP compliance testing due to deployment of accelerators, best practices and methods.**
- ❖ Reduced business interruptions due to secure web applications
 - ❖ **Increased credibility with customers and market**



SONATA SOFTWARE

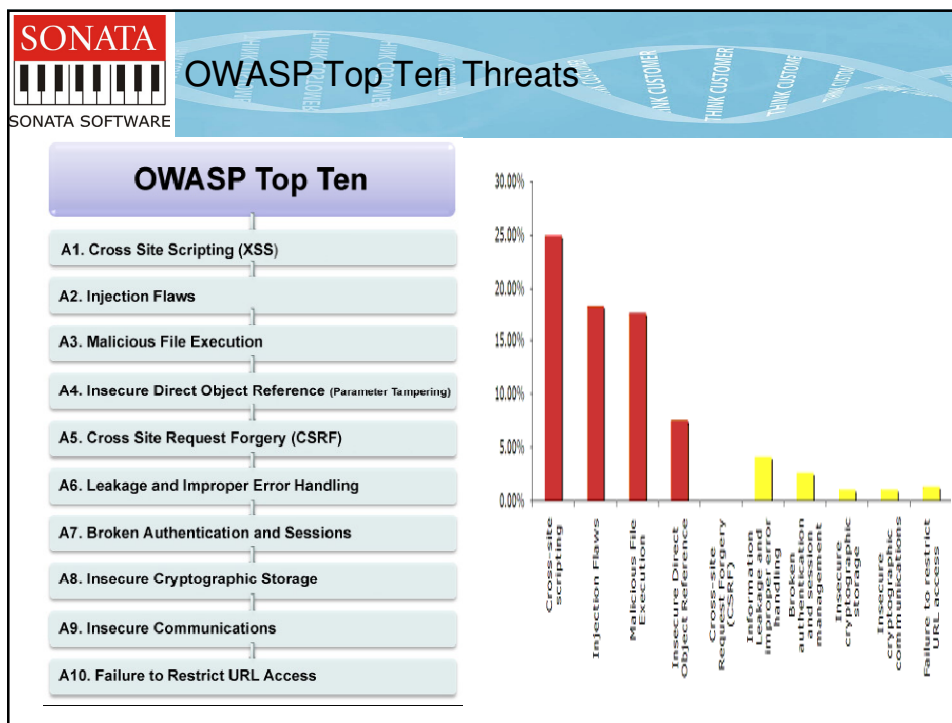
OWASP: An Overview



What is OWASP?

- Short for Open Web Application Security Project, OWASP is an open source community project set up to develop software tools and knowledge-based documentation for Web application security.
- The intent is to assist individuals, businesses and agencies in finding and using trustworthy software.
 - Some of the project's work includes:
 - A guide to define security requirements to build secure Web applications.
 - Developing an industry standard testing framework for Web application security.
 - Web Scarab - An open source enterprise-level Web application scanner.
 - Developing a component-based approach to filtering malicious input and output to a Web application.
 - WebGoat & Webmaven- An intentionally insecure web application, users can download and learn from.

20



SONATA
SONATA SOFTWARE

What is a Cardholder Data Compromise?

Hacker taking advantage of a flaw in a system that:

Stores, processes or transmits cardholder data

Gains Access to:


- **Card Numbers**
- **Expiration Dates**
- **CVV2/CVC2/CID**
- **Track Data**

SONATA
SONATA SOFTWARE

Six Goals: Twelve Requirements –PCI

The Payment Card Industry Data Security Standard

Build and Maintain a Secure Network	<ol style="list-style-type: none"> 1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	<ol style="list-style-type: none"> 3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	<ol style="list-style-type: none"> 5. Use and regularly update anti-virus software 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	<ol style="list-style-type: none"> 7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	<ol style="list-style-type: none"> 10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain Information Security Policy	<ol style="list-style-type: none"> 12. Maintain a policy that addresses information security




SONATA SOFTWARE

PCI Non Compliance - The Aftermath

In the event of compromise, a merchant must:

- **Have a forensic investigation performed** (\$10,000 average)
- **Rebuild all systems** (following ALL PCI DSS guidelines)
- **Upgrade to the latest version or switch software vendors**
- **Pay card re-issuance fees** (40,000 cards on average)
\$25 per card (average) is \$1,000,000.00 (average)
- **Pay non-compliance fees** (\$50,000 average)
- **Be classified as a Level 1 merchant for a year**
- **Have a card data removal audit performed** (\$10,000 average)
- **Have a Level 1 merchant PCI DSS audit performed**
(\$25,000 average)



SONATA SOFTWARE

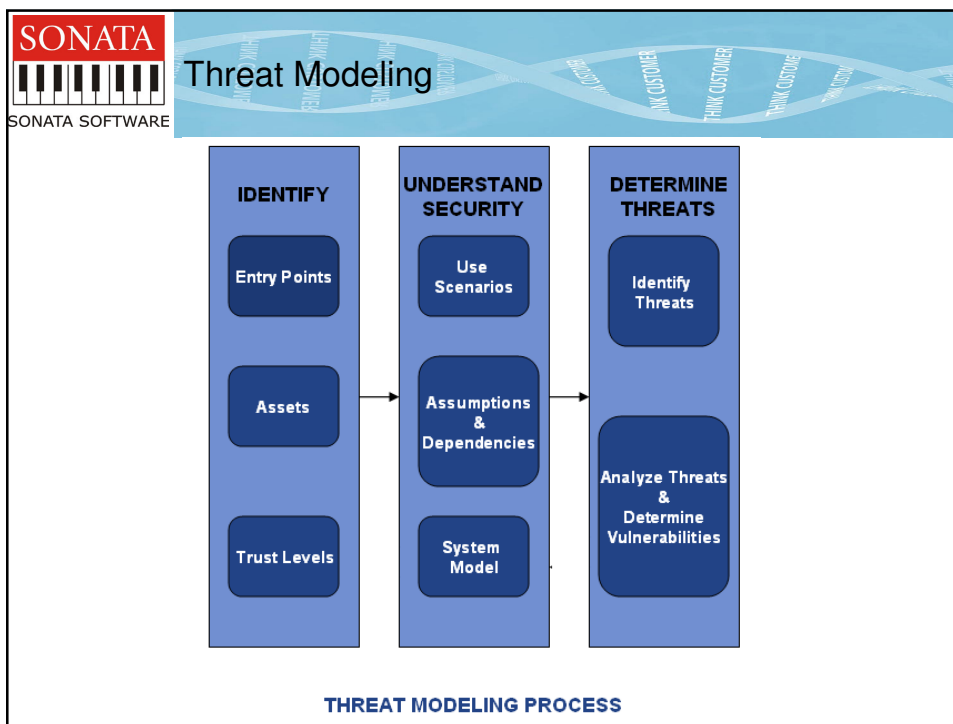
Enhanced Security : Why Security is top priority?

- **Web Applications are the #1 focus of hackers**
 - o 75% of attacks are at the application layer (Gartner)
 - o XSS and SQL Injection are the #1 and #2 reported vulnerabilities (Mitre)
- **Most sites are vulnerable**
 - o 90% of sites are vulnerable to application attacks (Watchfire)
 - o 78% of the easily exploitable vulnerabilities affected web applications (Symantec)
 - o 80% of organizations will experience and application security incident by 2010
- **Web apps are high value targets for hackers**
 - o Customer data, credit cards, ID Theft, Fraud, site defacement etc
- **Compliance requirements**
 - o Payment card industry (PCI) standards
 - o Federal Information Security Management Act (FISMA)
 - o Sarbanes-Oxley Act (SOX)

Security	Spending
% of Attacks	% of Dollars
<div style="display: flex; justify-content: center; align-items: center;"> <div style="background-color: #0056b3; color: white; padding: 20px; border: 1px solid #ccc; margin-right: 10px;">75%</div> <div style="background-color: #800040; color: white; padding: 20px; border: 1px solid #ccc;">25%</div> </div>	<div style="display: flex; justify-content: center; align-items: center;"> <div style="background-color: #0056b3; color: white; padding: 20px; border: 1px solid #ccc; margin-right: 10px;">10%</div> <div style="background-color: #800040; color: white; padding: 20px; border: 1px solid #ccc;">90%</div> </div>

2/3 of All Web Applications Are Vulnerable
Gartner

25



SONATA
SONATA SOFTWARE



STRIDE & DREAD RATING

Category	Description
Spoofing	Allows an attacker to pose as another user, component or other system that has an identity in the system being modeled
Tampering	The modification of data within the system to achieve a malicious goal
Repudiation	The ability of an attacker to deny performing some malicious activity because the system does not have sufficient privilege to prove it
Information Disclosure	The exposure of protected data to user that is not otherwise allowed access to that data
Denial Of Service	The exposure of protected data to user that is not otherwise allowed access to that data. Occurs when an attacker prevent legitimate users from using the normal functionality of the system.

Category	Description	Rating
Damage Potential	Ranks the extent of damage that occurs if vulnerability is exploited	1-Low 3-Medium 5-High
Reproducibility	Ranks how often an attempt at exploiting vulnerability works.	1-Low 3-Medium 5-High
Exploitability	Assigns a number to effort required to exploit a vulnerability	1-Low 3-Medium 5-High
Affected Users	A numeric value characterizing the ratio of installed instances of the system that would be affected if an exploit became widely available	1-Low 3-Medium 5-High
Discoverability	Measures the likelihood that vulnerability will be found by external researchers, hackers.	1-Low 3-Medium 5-High

STRIDE CLASSIFICATION: A method of classifying the top ten threats.



DREAD RATING: A rating given to the potential vulnerabilities in the application



Case Study

www.sonata-software.com

28



About Us

- 12+ years in software testing
- 500+ Member Testing Team
- SLA based service offer
- SonnetTest- Test accelerator
- Reusable assets
- SAP/Oracle APPs Accelerators
- e-Signature for Quality Center
- Monitor Bridge for VMware (LR, PC, BAC, Site Scope)
- VMware Lab Manager Add-in for Quality Center

Domains

- Travel
- Telco OSS
- Manufacturing
- Financial services
- Life sciences
- Software products

Sonata - Mercury Relationship
Gold Partner since 2004
Best Solution Partner- 2006

29

