

Application Security Compliance Index(ASCI)

Presented By : Birlasoft

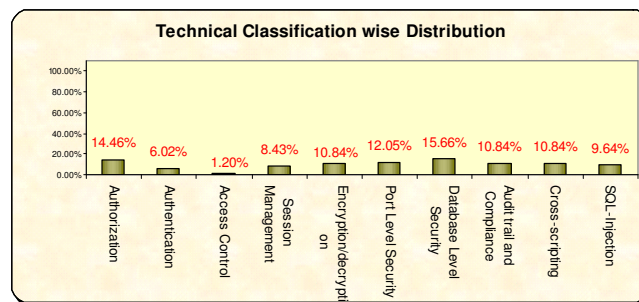
7th April 2009

© 2007 Birlasoft® Inc. All rights reserved.
Birlasoft® is a registered trademark of Birlasoft® Inc.



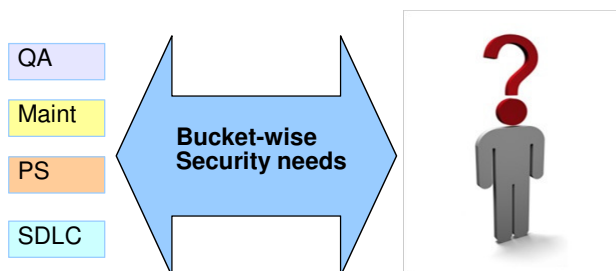
Challenges

- ◆ Increasing defect database due to the loop holes in identifying the security threats. At organization level we found through defect database that customer has started reporting application security vulnerabilities due to which the cost of rework increased.
- ◆ During the categorization of defects, this was identified that the major chunk of defects falls in the Application Security category-Database level Security, Authorization and Session management.



Major Needs

- Identifying the criticality of the application with respect to Application Security
- Identifying the potential security threats against which an application should be assessed
- To identify the improvement areas to implement in a project in terms of application security in different categories of projects. (Maintenance, QA, SDLC and Production Support)



Solution - Application Security Compliance Index

- Application Security Compliance Index was designed to assess the security of the applications to prioritize the focus of Application security testing.
- The standards set were; each application is required to be assessed on the following Application level Security parameters:
 - 0 – implying no threat
 - 3 – implying High Level threat
 - 9 – implying Low-level threat.

$$\text{ASCI} = \text{Score} * \text{Weightage}$$

- The weightage was kept standard as 0.1 for each application.



Application Security Compliance Index

Technical Compliance Index									
SI No.	Application level Security	Score	Weightage	TCI	Guidelines	Development	Deployment	Run time	
1	Authorization				No-0, High Level (private - Application specific) -3, Low-level (Work flow / Server based) -9	Y		Y	
2	Authentication				No-0, UserID and Password -3, Any model-mechanism-9	Y		Y	
3	Access Control				No-0, General-3, Any Application-specific -9	Y		Y	
4	Session Management				No-0, Plain (Web application Sessions should be handled) -3, (Web server as well as Application specific sessions should be handled) -9	Y		Y	
5	Encryption/decryption				No-0, Algorithm-SHA,DES-3, RSA-9	Y		Y	
6	Port Level Security				Everything on Port 80-0, Logical change in port-3, Port change and URL is hidden-9	Y		Y	
7	Database Level Security				No-0, Plain (Control on DDL and DML activities) -3, (DBA level control) Any model-mechanism-9	Y		Y	
8	Audit trail and Compliance				No-0, Yes-9	Y		Y	
9	Cross-scripting				No-0, General (Input validations & Filters) -3, Advanced (Disable scripting / Cookie security handling) -9	Y		Y	
10	SOL Injection				No(Plain SQL with defined condition) -0, SQL with dynamic conditions -3, Parametrized SQL query -9	Y		Y	
Network level Security									
11	Protocol Firewall				No-0, Yes-9		Y	Y	
12	Domain Firewall				No-0, Yes-9		Y	Y	
13	Application Firewall				No-0, Yes-9		Y	Y	
14	Antivirus				No-0, Yes-9		Y	Y	
15	Secure Socket layer E/D - SHA 1-16,32,64, - RSA -Length of PK - DES				No-0, Yes-9		Y	Y	

Application Security Compliance Index Score Card

S.No	Application Name	Authorization	Authentication	Access Control	Session Management	Encryption/decryption	Port Level Security	Database Level Security	Audit trail and Compliance	Cross-scripting	SOL-Injection	Overall Score	Target Score
1	ABC	0.9	0.9	0.9	0.9	0.9	NA	NA	0.9	0.9	0.9	7.2	8.1
2	XYZ	0.9	0.3	0.9	0.3	0.1	NA	NA	0.9	0.9	0.9	5.2	8.1
3	-	0.9	0.9	0.9	0.3	0	NA	NA	0.9	0.9	0.3	5.1	8.1
4	-	0.3	0.3	0.9	0.3	0	0.1	NA	0.9	0.9	0.3	4	8.1
5	-	0.9	0.9	0.9	0.3	0	NA	NA	0	0.9	0.3	4.2	8.1
6	-	0.3	0.9	0.9	0.3	0	0.3	NA	0.9	0.9	0.9	5.4	8.1
7	-	0.9	0.3	0.9	0.3	0	NA	NA	0.9	0.9	0.3	4.5	8.1
8	-	0.3	0.9	0.9	0.3	0	NA	NA	0	0.9	0.1	3.4	8.1
9	-	0.3	0.3	0.3	0.3	NA	NA	NA	0	0.9	0.9	3	8.1
10	-	0.9	0.9	0.3	0	NA	NA	NA	0	0.9	0.3	3.3	8.1
11	-	0.3	0.9	0.1	0	NA	NA	NA	0	0.9	0.3	2.5	8.1
12	-	0.3	0.3	0.3	0	NA	0.1	NA	0	0.1	0.3	1.4	8.1

Results

- Able to prioritize the applications for performing security assessments
- Able to identify application wise potential threats
- Able to reduce the security defects and leverage the security of the applications
- Able to showcase improvements with respect to security and gain WOW from customers.



THAN
KS
 Birlasoft®