Epsilon Labs Въпросник за предварителна оценка на проект за инспекция на програмен код за проблеми със сигурността – v 2.0

Декември 2012

	Въпрос	Да	Не	Бележки
1 Основно описание на приложението				
1.1	Опишете накратко приложението (предназначението му) и избройте основните му функционални модули.			
2 Документация и изисквания за сигурност				
2.1	Документирана ли е архитектурата на приложението и до каква степен?			
2.2	Документирани ли са всички приложни интерфейси и до каква степен?			
2.3	Документирани ли са изискванията за сигурност към приложението и до каква степен?			
2.4	Документиран ли е модела на заплахите?			
2.5	Има ли дефинирани и документирани кодинг конвенции, към които програмистите би следвало да се придържат в процеса на разработка?			
2.6	На какъв език е написана документацията? (български, английски, немски и т.н.)			
3 Класификация на данните				
3.1	Данните, които приложението обработва, изпраща и съхранява обект ли са на класификация (според корпоративна политика или според регулаторно			

	изискваня)? Ако да моля да предоставите повече детайли.			
4 Архитектура на приложението и основни характеристики на кода				
4.1	Какъв е основния езика за разработка на приложението?			
4.2	Има ли части от приложението разработени с използването на програмни езици различни от основния? Ако да каки други програмни езици са използвани?			
4.3	Архитектурата на приложението многослойна ли е? Ако да колко и какви са слоевете?			
4.4	Изградено ли е приложението на базата на съществуваща платформа/и (комерсиалана или с отворен код) и ако да моля да предоставите детайли за патформата/ите (име, производител, версия)?			
4.5	Използван ли е приложен код разработен от трети лица (библиотеки, класове, методи etc.)? Ако да – колко на брой и какви?			
4.6	Комуникира ли приложението с база данни и ако да каква?			
4.7	Приложението сървис ориентирано ли е и ако да какви сървиси предоставя/консумира?			
4.8	Какви комуникационни протоколи използва?			
4.9	Имплементира ли приложението специално разработени конуникационни протоколи?			
5 Контрол на достъпа и управление на потребителите				

5.1	Използва ли приложениеот SSO и/или federated authentication?			
5.2	Какъв тип контрол на достъп изполва приложението - mandatory access control, discretionary access control, role based access control или друг?			
5.3	Дефинира ли приложението различни потребителски роли и ако да колко на брой и какви?			
5.4	Управлението на потребителите/ролите извършва ли се от самото приложение или се осъществава от външни оторизационни механизми (например активна директория)?			
6 Оразмеряване				
6.1	Какъв е броя на приложните файловете, които подлежат на инспекция?			
6.2	Какъв е броя на специално разработените библиотеки и класове?			
6.3	Какъв е броя на комуникационните интерфейси (интерфейсите гарантиращи връзката на приложението с външни обекти)?			
6.4	Какъв е броя на входните потоци (потребители, конфигурационни файлове, бази данни и т.н.)?			
6.5	Какъв е броя на специално разработените процедури и тригери?			