

Epsilon Labs Въпросник за предварителна оценка на проект за инспекция на програмнен код за проблеми със сигурността – v 1.0
Юли 2012

	Въпрос	Да	Не	Бележки
	Документация и изисквания за сигурност			
1	Архитектурата на приложението документирана ли е и до каква степен?			
2	Документирани ли са всички приложни интерфейси и до каква степен?			
3	Документирани ли са изискванията за сигурност към приложението и до каква степен?			
4	Документиран ли е модела на заплахите?			
5	Има ли дефинирани и документиран коднинг конвенции, към които програмистите би следвало да се придържат в процеса на разработка?			
6	На какъв език е написана документацията? (български, английски, немски и т.н.)			
	Класификация на данните			
7	Данните, които приложението обработва, изпраща и съхранява обект ли са на класификация (според корпоративна политика или според регулаторно изискване)? Ако да моля да предоставите повече детайли.			
	Архитектура на приложението			
8	Какъв е основния езика за разработка?			

Epsilon Labs Въпросник за предварителна оценка на проект за инспекция на програмнен код за проблеми със сигурността – v 1.0
Юли 2012

9	Има ли части от приложението разработени с използването на програмни езици различни от основния? Ако да какви други програмни езици са използвани?			
10	Архитектурата на приложението многослойна ли е? Ако да колко и какви са слоевете?			
11	Изградено ли е приложението на базата на съществуваща платформа (комерсиалана или с отворен код) и ако да моля да предоставите детайли за платформата (име, производител, версия)?			
12	Изполван ли е приложен код разработен от трети лица (библиотеки, класове, методи etc.)? Ако да – колко на брой и какви?			
13	Комуникира ли приложението с база данни и ако да каква?			
14	Приложението сървис ориентирано ли е и ако да какви сървиси предоставя/консумира?			
	Контрол на достъпа и управление на потребителите			
15	Дефинира ли приложението различни потребителски роли и ако да колко на брой и какви?			
16	Управлението на потребителите/ролите извършва ли се от самото приложение или се осъществява от външни оторизационни механизми (например активна директория)?			
17	Имплементира ли приложението SSO?			

Epsilon Labs Въпросник за предварителна оценка на проект за инспекция на програмен код за проблеми със сигурността – v 1.0
Юли 2012

	Оразмеряване			
18	Какъв е броя на приложниет файловете, които подлежат на инспекция?			
19	Какъв е броя на специално разработените библиотеки и класове?			
20	Какъв е броя на комуникационните интерфейси (интерфейсите гарантиращи връзката на приложението с външни обекти)?			
21	Какъв е броя на входните потоци (потребители, конфигурационни файлове, бази данни и т.н.)?			
22	Какъв е броя на специално разработените процедури и тригери?			