Application Security

Anderson Dadario

Agenda

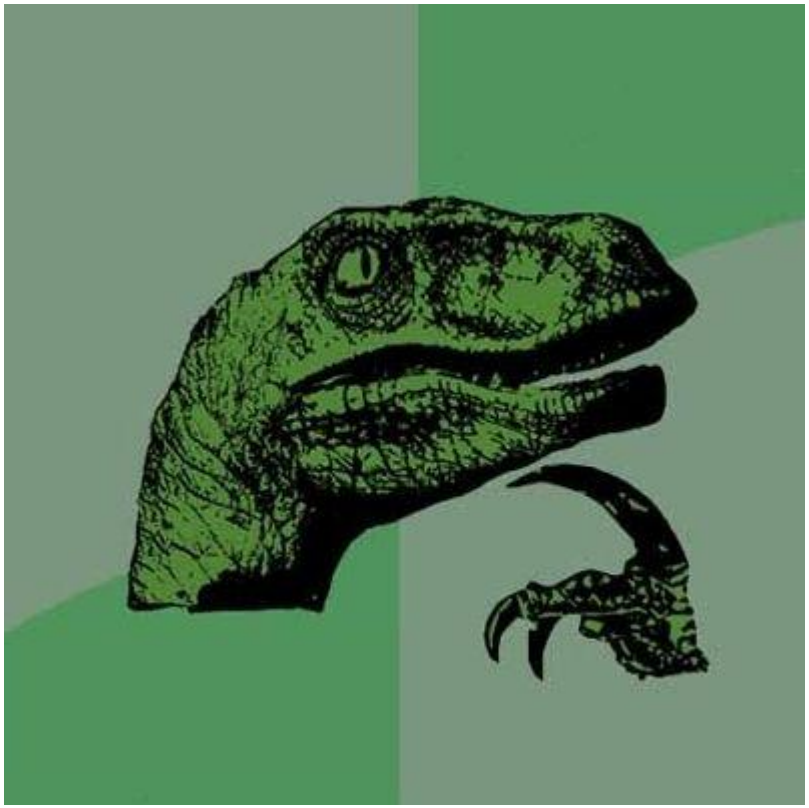
* Quem sou eu?
* Introdução à Segurança da Informação
* Segurança, para quê?
* Segurança no SDLC
* Owasp Top 10
* Estudo de caso: LinkedIn
* Leituras recomendadas
* Contato

Quem sou eu?

Anderson Dadario

Consultor em Segurança de Software

Introdução à Segurança da Informação



Significado

A **segurança da informação** está relacionada com proteção de um conjunto de dados, no sentido de preservar o valor que possuem para um indivíduo ou uma organização.

Segurança, para quê?

Last.fm alerta para vazamento de senhas e aconselha troca

Site de música é o terceiro a investigar publicação d
Empresa não divulgou detalhes, nem o número de u

Roubo de senhas do LinkedIn coloca reputação do site em xeque

Site da prefeitura de SP invadido

por Gustavo Lima em 25/06/12 às 6:46 pm

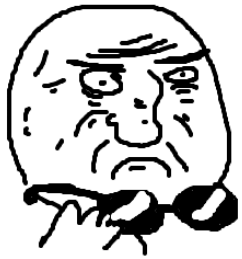
Ter amigos é muito bom, mas ter um amigo figura
bem, este figura descobriu uma vulnerabilidade n
simplesmente colocou um WebShell por lá. Vejam

Site do IBGE é invadido por hackers

'Governo vivenciará maior número de ataques na história', diz mensagem.
Hackers se identificam como um grupo nacionalista.

Possível falha no site do Fies expõe dados de estudantes de todo o Brasil

Número de documentos e dados bancários de alunos podem ser acessados.
Aluno de Sananduva, RS, teme que dados sejam usadas por criminosos.



Segurança, para quê? (cont.)

* Encontre as falhas e bugs mais cedo
* Economize dinheiro
* Compliance (Ex: PCI-DSS)
* Ganhe credibilidade:

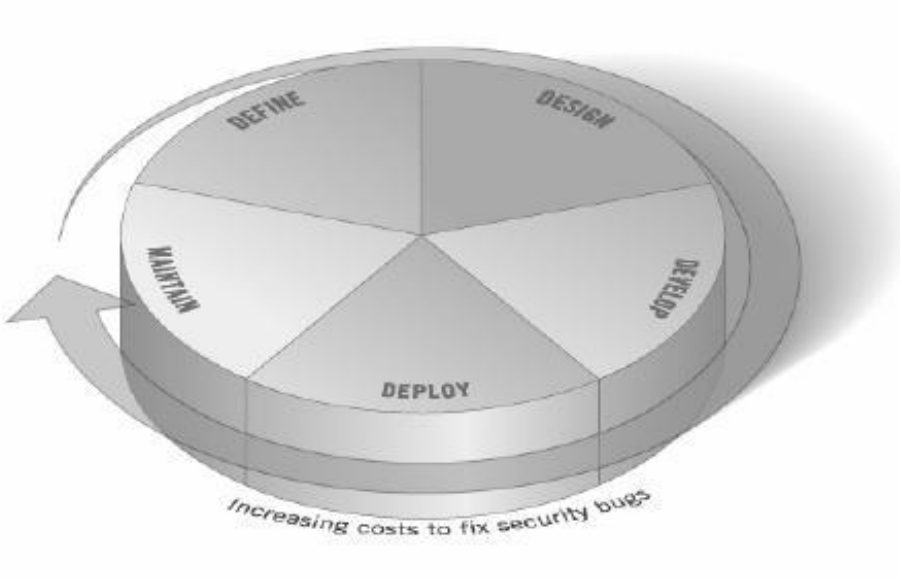
Mikko Hypponen @mikko 28 jun

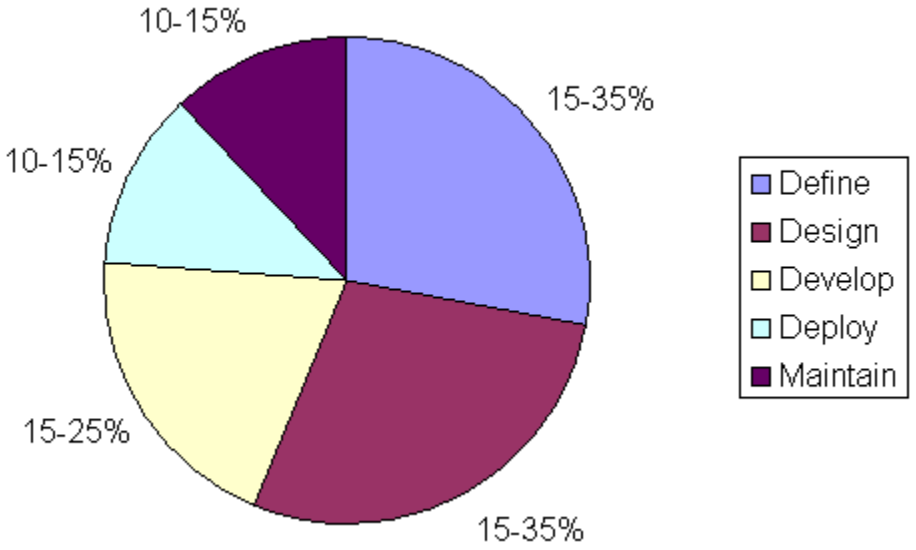
iPhone is 5 years old today. After 5 years, not a single serious malware case. It's not just luck; we need to congratulate Apple on this.

Retweetado por Anderson Dadário

Expandir

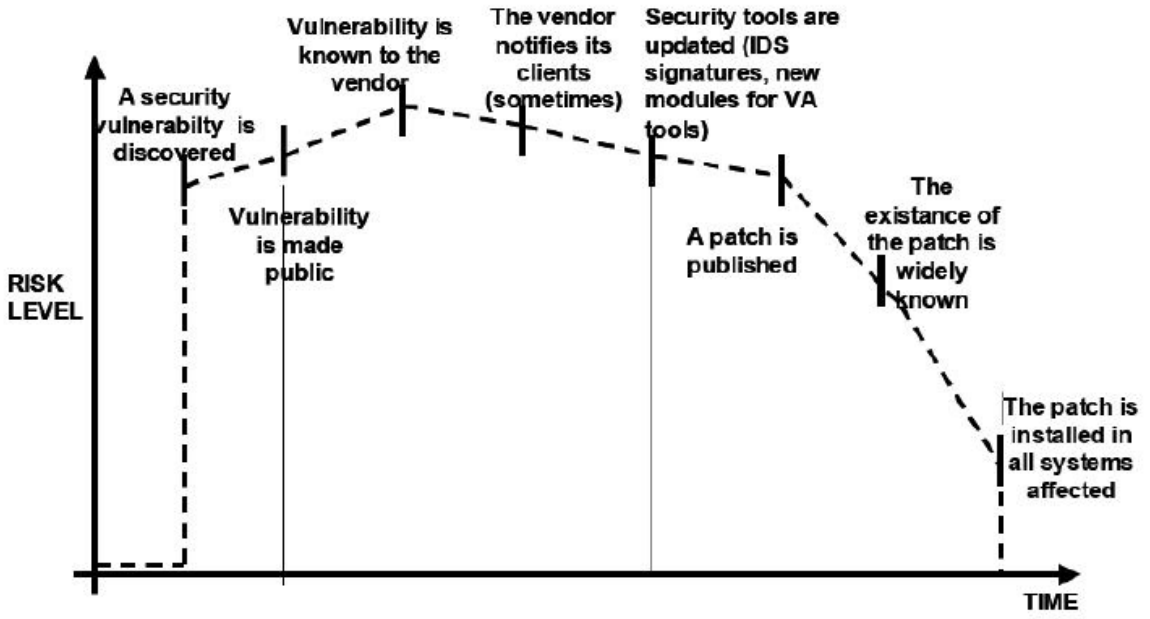
Segurança no SDLC





Segurança no SDLC

* There is no Silver Bullet
* Think Strategically,
  Not Tactically
* Test Early and Test Often
* Understand the Scope of Security
* Develop the Right Mindset
* The Devil is in the Details
* Develop Metrics
* Document the Tests Results



OWASP – Top 10 Project (1-4)

The Open Web Application Security Project

* **A1 –Injection**
* **A2 –Cross-Site Scripting (XSS)**
* **A3 –Broken Authentication and Session Management**
* **A4 –Insecure Direct Object References**
* **A5 –Cross-Site Request Forgery (CSRF)**
* **A6 –Security Misconfiguration**
* **A7 –Insecure Cryptographic Storage**
* **A8 –Failure to Restrict URL Access**
* **A9 –Insufficient Transport Layer Protection**
* **A10 –UnvalidatedRedirects and Forwards**

OWASP – Top 10 Project (2-4)

The Open Web Application Security Project

A1 – Injection	•Injection flaws, such as SQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing unauthorized data.
A2 – Cross-Site Scripting (XSS)	•XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation and escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
A3 – Broken Authentication and Session Management	•Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, session tokens, or exploit other implementation flaws to assume other users' identities.
A4 – Insecure Direct Object References	•A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.

OWASP – Top 10 Project (3-4)

The Open Web Application Security Project

A5 – Cross-Site Request Forgery (CSRF)	•A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim.
A6 – Security Misconfiguration	•Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. All these settings should be defined, implemented, and maintained as many are not shipped with secure defaults. This includes keeping all software up to date, including all code libraries used by the application.
A7 – Insecure Cryptographic Storage	•Many web applications do not properly protect sensitive data, such as credit cards, SSNs, and authentication credentials, with appropriate encryption or hashing. Attackers may steal or modify such weakly protected data to conduct identity theft, credit card fraud, or other crimes.
A8 - Failure to Restrict URL Access	•Many web applications check URL access rights before rendering protected links and buttons. However, applications need to perform similar access control checks each time these pages are accessed, or attackers will be able to forge URLs to access these hidden pages anyway.

OWASP – Top 10 Project (4-4)

The Open Web Application Security Project

A9 - Insufficient Transport Layer Protection	• Applications frequently fail to authenticate, encrypt, and protect the confidentiality and integrity of sensitive network traffic. When they do, they sometimes support weak algorithms, use expired or invalid certificates, or do not use them correctly.
A10 – Unvalidated Redirects and Forwards	• Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.

Estudo de caso

LinkedIn

LinkedIn confirma vazamento de senhas de usuários da rede

06 de junho de 2012 • 15h29 • atualizado às 18h13

Roubo de senhas do LinkedIn coloca reputação do site em xeque

Troque a sua: 6,5 milhões de senhas foram roubadas do LinkedIn

Hackers teriam roubado senhas e agora buscam ajuda para quebrar a criptografia dos dados.

LinkedIn Password Break - Unsalted SHA1 Hash available to hackers

It appears that the developers at LinkedIn may not have had "encryption training" on their own resumes. On a separate note, if you are unfamiliar with the importance of salting your hashes, or you're using an broken algorithm like MD5, visit http://thecodemechanic.wordpress.com

Vote up Vote down 8 0 1695 939

Leituras recomendadas

* Owasp Testing Guide v3
  https://www.owasp.org/images/5/56/OWASP_Testing_Guide_v3.pdf
* OpenSAMM
  http://www.opensamm.org/
* Microsoft SDL
  http://www.microsoft.com/security/sdl/default.aspx
* CLASP
  https://www.owasp.org/index.php/Category:OWASP_CLASP_Project
* Webinar Clavis
  http://www.blog.clavis.com.br/webinar-video-workshop-online-seguranca-da-informacao

Contato

Anderson Dadario

anderson@dadario.com.br
https://dadario.com.br