Secure programming

Alfred Sawaya

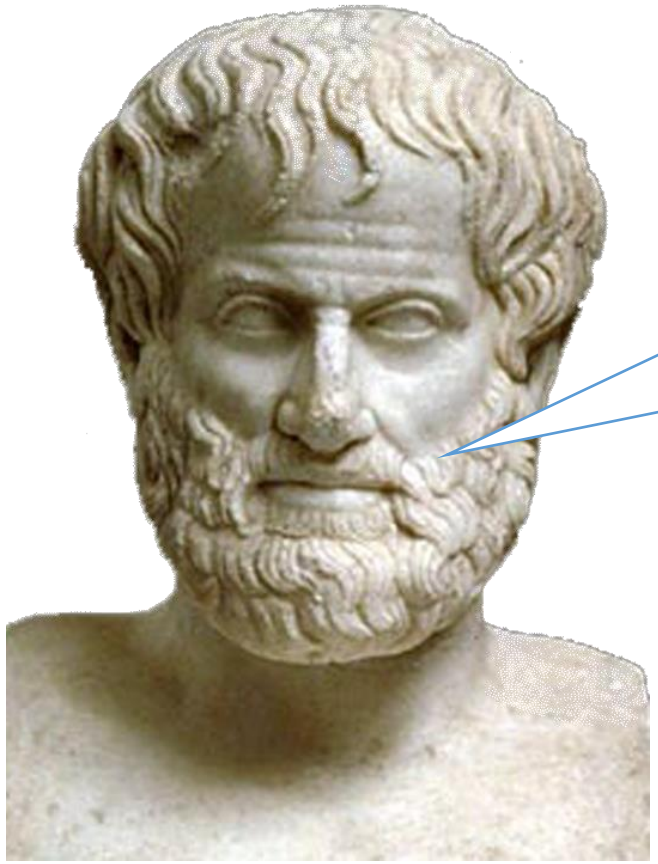
Planning

	Matin	Aprem
Lundi	Cours théorique	Programmation des challenges
Mardi	CTF	
Mercredi	Développement d'une messagerie instantanée sécurisée	
Jeudi		
Vendredi	Interrogation écrite (1h)	

Qu'est-ce qu'un programme ?

Qu'est-ce qu'un programme ?

Qu'est-ce qu'un bon développeur ?

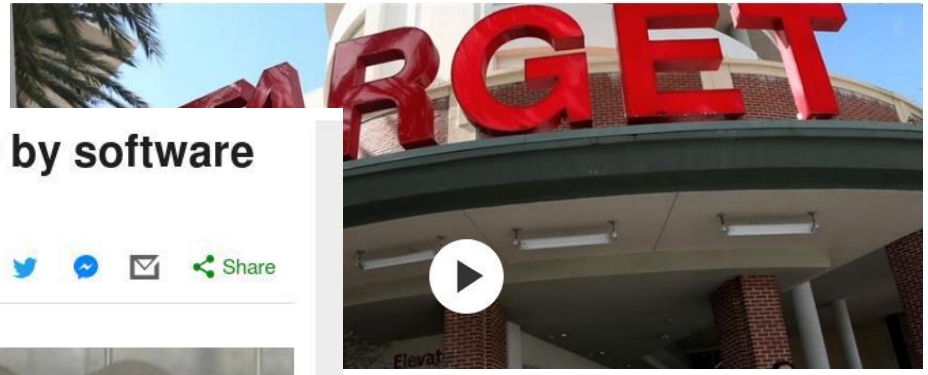


L'excellence est un art que l'on n'atteint que par l'exercice constant. Nous sommes ce que nous faisons de manière répétée.
L'excellence n'est donc pas une action mais une habitude.

Qu'est-ce qu'un bon développeur ?

Qu'est-ce que la sécurité dans le développement logiciel ?

Target Earnings Slide 46% After Data Breach



US prisoners released early by software bug

23 December 2015 Share

Qu'est-ce que la sécurité dans le développement logiciel ?

Boeing 737 MAX : la facture monte à plus de 18 milliards de dollars pour le constructeur américain

Chiffre d'affaires du trimestre en baisse de 37% par rapport à l'année précédente

Qu'est-ce que la sécurité dans le développement logiciel ?

NordVPN admet avoir été victime d'une brèche chez un fournisseur

Sécurité Par **Remi Lou** le 22 octobre 2019 à 10h29 3 commentaires

Cyberattaque géante chez Bouygues Construction, 3200 employés au chômage technique

Lignes téléphoniques coupées, plus de mails... Une attaque massive touche le siège social et tous ses services informatiques, à Guyancourt (Yvelines). Le géant mondial du BTP assure qu'il n'y a pas de paralysie de l'activité.

Qu'est-ce que la sécurité dans le développement logiciel ?

Une faille massive révèle plus d'un million d'empreintes digitales

Un système biométrique utilisé aussi bien par les banques, que par la police ou la défense britannique, a subi une grave violation qui a révélé plus d'un million d'empreintes digitales.

Les empreintes digitales d'un million de personnes exposées

Les systèmes biométriques, tels que la reconnaissance faciale, rétinienne ou bien encore d'empreintes digitales sont réputés plus fiables que les mots de passe, les codes ou bien encore les cartes d'accès. Cependant, lorsque les données biométriques sont exposées, des **hackers peuvent facilement contourner ces protections**. En Grande Bretagne, une faille massive d'un système de

Qu'est-ce que la sécurité dans le développement logiciel ?

TOUTE L'ACTUALITÉ / **SÉCURITÉ**

Fuite de données pour 2,4 millions clients de Wyze

Dominique Filippone , publié le 30 Décembre 2019

0 Réaction

Un défaut de configuration d'une base de données Elasticsearch du fabricant de caméras IP Wyze a exposé des informations personnelles de 2,4 millions de clients. Au moins 40 millions d'enregistrements comprenant notamment des noms d'utilisateurs, e-mails et numéros WiFi SSID auraient fuité.

SUIVRE TOUTE L'ACTUALITÉ

Newsletter

Recevez notre newsletter comme plus de 50 000 professionnels de l'IT!

JE M'ABONNE

Qu'est-ce que la sécurité dans le développement logiciel ?

Pourquoi M6 redoute les vendredis soirs...

HASSAN MEDDAH | FRANCE , LOISIRS , CYBERSÉCURITÉ | PUBLIÉ LE 22/01/2020 À 18H15

Le 11 octobre dernier, un vendredi soir, M6 était victime d'une cyberattaque. Pour la première fois, un dirigeant du groupe de médias raconte la crise de l'intérieur, l'électrochoc pour les salariés, les efforts pour assurer la diffusion coûte que coûte des programmes.

Développeurs, bientôt responsable de leurs codes ?

VW engineer sentenced to 40-month prison term in diesel case

David Shepardson and Joseph White

WASHINGTON/DETROIT (Reuters) - A federal judge in Detroit sentenced former engineer James Liang to 40 months in prison on Friday for his role in Volkswagen AG's (VOWG_p.DE) multiyear scheme to sell diesel cars that generated more pollution than U.S. clean air rules allowed.

Qu'est-ce que la sécurité dans le développement logiciel ?

Confidentialité

Intégrité

Disponibilité

Non-répudiation

Auditabilité

Threat	Property	Definition	Example
Spoofing	Authentication	Impersonating something or someone else.	Pretending to be any of Billg , microsoft.com or ntdll.dll
Tampering	Integrity	Modifying data or code	Modifying a DLL on disk or DVD, or a packet as it traverses the LAN.
Repudiation	Non-repudiation	Claiming to have not performed an action.	"I didn't send that email," "I didn't modify that file," "I *certainly* didn't visit that web site, dear!"
Information Disclosure	Confidentiality	Exposing information to someone not authorized to see it	Allowing someone to read the Windows source code; publishing a list of customers to a web site.
Denial of Service	Availability	Deny or degrade service to users	Crashing Windows or a web site, sending a packet and absorbing seconds of CPU time, or routing packets into a black hole.
Elevation of Privilege	Authorization	Gain capabilities without proper authorization	Allowing a remote internet user to run commands is the classic example, but going from a limited user to admin is also EoP

Les acteurs


Common Criteria


IEEE


ISO


AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI


CERT


COMPUTER SECURITY INCIDENT
CSIRT
EUROPE
RESPONSE TEAM


MITRE


OWASP
Open Web Application
Security Project


IETF


NIST

Critères Communs

Common Criteria Evaluation Assurance Level (EAL)	Process rigor required for development of an IT product
EAL 1	Functionally tested
EAL 2	Structurally tested
EAL 3	Methodically tested and checked
EAL 4	Methodically designed, tested and reviewed
EAL 5	Semi-formally designed and tested
EAL 6	Semi-formally verified, designed and tested
EAL 7	Formally designed and tested

Évaluation des risques

		Niveau de gravité des dommages			
		Catastrophique	Grave	Signifiant	Insignifiant
Niveau de probabilité d'occurren-ce de l'accident potentiel	Fréquent				
	Probable				
	Occasionnel				
	Rare				
	Improbable				
	Hautement improbable				

Risque intolérable

Risque non souhaitable

Risque tolérable

Risque négligeable

Top 10 des failles Web

Programmation par coïncidence

Buffer Overflow

```c
#include <stdio.h>
#include <string.h>

int verifie_mot_de_passe() {
        int res = 0;
        char tampon[10];
        scanf("%s", &tampon);
        if (strcmp (tampon, "secret") == 0)
                res = 1;
        return res;
}

int main() {
        if (verifie_mot_de_passe ()) {
                // code privilégié
        }
        return 0;
}
```

SQL Injection

```
SELECT * FROM users
  WHERE login = '$login'
  AND password = '$pwd';
```

Race condition / TOCTOU

```
#include <stdio.h>
#include <unistd.h>
int main(int argc, char *argv[]) {
        FILE *fd;
        if (access(filename, W_OK) == 0) {
                printf("access␣granted.\n");
                fd = fopen(filename, "wb+");
                if (fd != NULL) {
                        /* écriture dans le fichier */
                        fclose(fd);
                }
        }
        ...
        return 0;
}
```

Tools

- Analyseur statique (cppcheck, findbugs...)
- Debugger (gdb, valgrind...)
- Fuzzer (libfuzzer...)
- Compiler options (checksec.sh)
- Security unit tests
- Vulnerability scanner (OpenVas...)
- Dependancy scanner
- Code review
- DAST / RASP / WAF

=> **DevSecOps**