Definiendo requerimientos de seguridad sin morir en el intento

Arturo Sustaita

@arturo_io

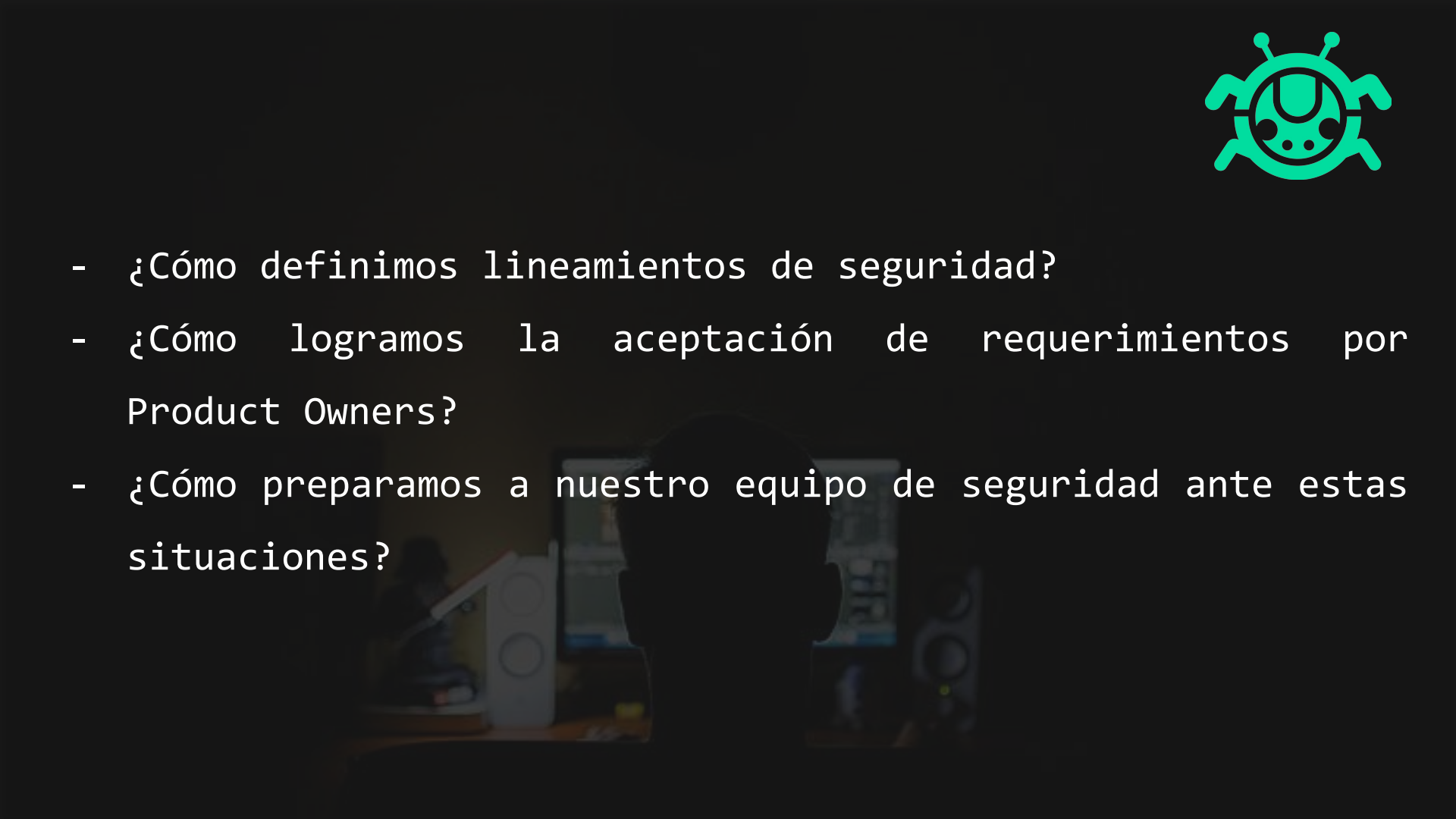
arturo-sustaita

$whoami

- ➔ Application Security Engineer
- ➔ CEH, CC.
- ➔ Ex-Auditor
- ➔ Developer (project side)
- ➔ Apasionado por la tecnología desde los 13

Disclaimer

El contenido de esta plática parte de experiencias profesionales, sin embargo no refleja en ningún momento escenarios reales. Cualquier parecido con la realidad es mera coincidencia.



- ¿Cómo definimos lineamientos de seguridad?
- ¿Cómo logramos la aceptación de requerimientos por Product Owners?
- ¿Cómo preparamos a nuestro equipo de seguridad ante estas situaciones?

Lineamientos, Frameworks y más

Back to Basics

Triada de la información

- Confidencialidad
- Integridad
- Disponibilidad
- No repudio

Principio de mínimo privilegio

El privilegio más bajo para realizar sus operaciones

Necesidad de conocer

No todos los usuarios necesitan conocer el 100% de la información

Sin inventar el hilo negro…

Políticas internas

Lineamientos creados por la propia organización en materia de seguridad de la información

Compliance

- PCI-DSS
- LFDPP
- CUB

Frameworks

- OWASP
- CIS Controls

File Upload Cheat Sheet

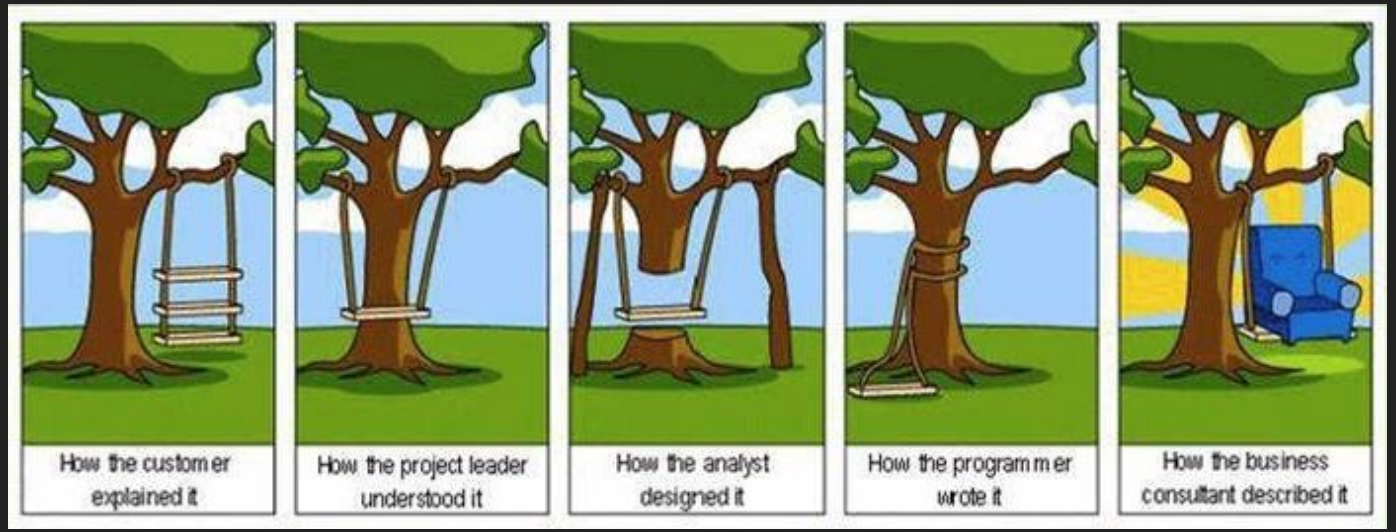
Introduction

File upload is becoming a more and more essential part of any application, where the user is able to upload their photo, their CV, or a video showcasing a project they are working on. The application should be able to fend off bogus and malicious files in a way to keep the application and the users safe.

In short, the following principles should be followed to reach a secure file upload implementation:

- **List allowed extensions. Only allow safe and critical extensions for business functionality**
  - **Ensure that input validation is applied before validating the extensions.**
- **Validate the file type, don't trust the Content-Type header as it can be spoofed**
- **Change the filename to something generated by the application**
- **Set a filename length limit. Restrict the allowed characters if possible**
- **Set a file size limit**
- **Only allow authorized users to upload files**
- **Store the files on a different server. If that's not possible, store them outside of the webroot**
  - **In the case of public access to the files, use a handler that gets mapped to filenames inside the application (someid -> file.ext)**
- **Run the file through an antivirus or a sandbox if available to validate that it doesn't contain malicious data**
- **Ensure that any libraries used are securely configured and kept up to date**
- **Protect the file upload from CSRF attacks**

Entendiendo a los usuarios



Retos principales…

Quiero vs Necesito

Las verdaderas necesidades de los usuarios pueden venir disfrazadas

Quiero, que mi sesión nunca caduque
Necesito, acceso rápido a mis aplicaciones.

Traducir el lenguaje técnico

Implementar doble factor de autenticación, autorización, cifrado.

Fácil vs Adecuado

Lo fácil para el usuario suele ser inseguro

Fácil: Descargar información.
Adecuado: Consulta a través de aplicaciones.

Enfrentando el reto

Confidencialidad

PCI-DSS

Se requiere analizar los pagos en una plataforma de ventas en línea. Se pretende partir de números de tarjeta como identificadores, además generación de reportes diarios que contendrán datos sensibles

¿Qué se necesita realmente?

¿Qué tipos de datos se requieren conocer?

Confidencialidad

Necesidad de conocer

La empresa está implementando una aplicación de recursos humanos (HR) que almacena información sensible de los empleados, como números de seguro social, historial salarial y evaluaciones de desempeño. Los requerimientos establecen que los gerentes de equipo deben tener acceso a la información de los miembros de su equipo para facilitar la gestión de recursos humanos.

¿Para que se necesita la información?

¿De qué manera se va a proteger la información?

Tipos de usuarios

Amables

Agresivos

Trucos

Escaladores

Concluyendo...

1. **Define cuanto antes.** Sesiones de requerimientos.
2. **Entiende el problema a fondo.** involucrate en el proceso.
3. **Pregunta todo lo necesario.** No lo sabemos todo.
4. **Prepárate para cambios inesperados.**. Cualquier cosa puede pasar.
5. **Evaluar el riesgo.** Seguridad vs Negocio

Consejos finales

Gracias

#BugCon2023

SAFETY IS JUST A MYTH!

Arturo Sustaita
@arturo_io
arturo-sustaita