Puesta en Producción Segura

Unidad 3.

Detección y corrección de vulnerabilidades en aplicaciones web

JUNTA DE EXTREMADURA

Plan de Recuperación, Transformación y Resiliencia

Financiado por la Unión Europea NextGenerationEU

MINISTERIO DE EDUCACIÓN, FORMACIÓN PROFESIONAL Y DEPORTES

"En cada búsqueda apasionada cuenta más la persecución que el objeto perseguido"

—El Tao del Jeet Kune Do" (1975), Bruce Lee

JUNTA DE EXTREMADURA
Plan de Recuperación, Transformación y Resiliencia
Financiado por la Unión Europea NextGenerationEU
MINISTERIO DE EDUCACIÓN, FORMACIÓN PROFESIONAL Y DEPORTES

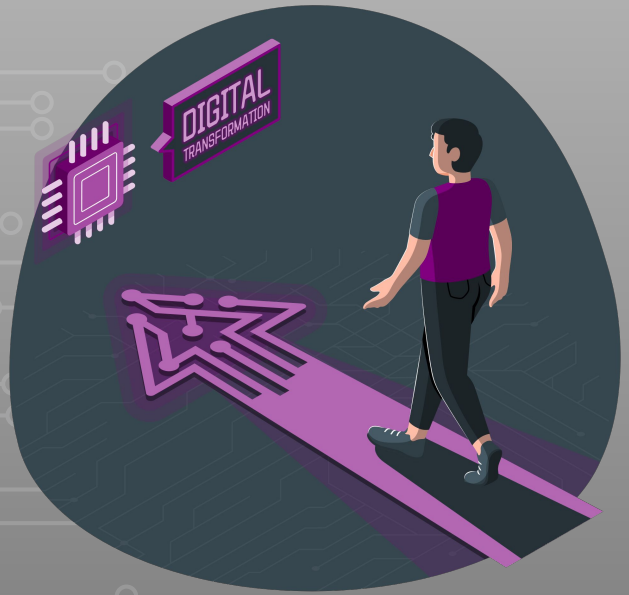
Objetivos

- Conocer las principales vulnerabilidades web que vamos a estudiar en la presente unidad.

Contenidos

01 Vulnerabilidades web y mecanismos de protección

02 Vulnerabilidades de datos de entrada.



01

Vulnerabilidades y mecanismos de protección.

JUNTA DE EXTREMADURA

Plan de Recuperación, Transformación y Resiliencia

Financiado por la Unión Europea NextGenerationEU

MINISTERIO DE EDUCACIÓN, FORMACIÓN PROFESIONAL Y DEPORTES

Vulnerabilidades en aplicaciones.

A la hora de producir software se pueden introducir ciertas debilidades o malas prácticas de programación que pueden
dar lugar a vulnerabilidades.

- Es necesario saber prevenirlas, y llegado el caso, identificarlas,clasificarlas y subsanarlas.
- También es importantes conocer los marcos de referencia creados por las organizaciones que trabajan en ciberseguridad para poder encontrar información y formación en la detección y mitigación de estas vulnerabilidades: CVE, CWE, CAPEC, etc.

Vulnerabilidades que estudiaremos

Durante esta unidad veremos vulnerabilidades que tienen que ver con los riesgos principales. Las podemos agrupar en:

1. Vulnerabilidades en el tratamiento de datos de entrada.
2. Vulnerabilidades en la autenticación.
3. Vulnerabilidades en la gestión de la sesión.
4. Exposición de información sensible.
5. Vulnerabilidades en el control de acceso.
6. Configuración incorrecta.
7. Monitorización y log insuficiente.
8. Vulnerabilidades en las librerías de terceros.

02

Vulnerabilidades de datos de entrada

JUNTA DE EXTREMADURA

Plan de Recuperación, Transformación y Resiliencia

Financiado por la Unión Europea NextGenerationEU

MINISTERIO DE EDUCACIÓN, FORMACIÓN PROFESIONAL Y DEPORTES

Lenguajes de intercambio de datos

- Cuando una aplicación interactúa con otra, tienen que utilizar algún tipo de lenguaje, formato o protocolo de intercambio de datos.
- En los mensajes escritos en dicho lenguaje suelen ser dinámicos y para eso se incluyen datos que proceden del usuario.
  - P.ej.: datos introducidos a través de un campo de texto de un formulario.
- Por lo tanto tendremos diferentes vulnerabilidades dependiendo del lenguaje en el que se intercambian esos datos: SQL, OS, etc.

Tipos de ataques más comunes

Algunos de los tipos de **ataques** más comunes relacionados con los datos de entrada son:

- **Inyección de código**: SQL Injection, NoSQL Injection.
- **Ejecución de código**: Remote Code Execution (RCE).
- **Manipulación de entrada**: Cross-Site Scripting (XSS), Cross-Site Request, Forgery (CSRF), Server-Side Request Forgery (SSRF).
- **Acceso indebido**: Local File Inclusion (LFI), Remote File Inclusion (RFI).
- **Explotación de datos**: XML External Entities (XXE), Unsafe Deserialization.

Vulnerabilidades de datos de entrada

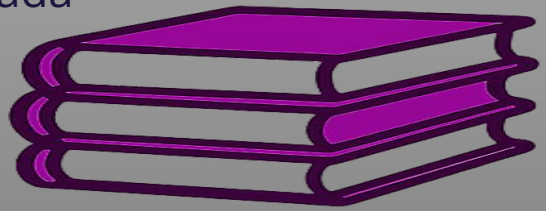
Para ver las diferentes vulnerabilidades en el tratamiento de datos de entradas vamos a dividirlas en:

1. Inyección de código
2. Entidades externas en documentos XML (XEE)
3. Deserialización y carga dinámica inseguras
4. Desbordamiento de pila y buffer
5. Validación de datos

Cada una de ellas la veremos en una presentación diferente.

Bibliografía y Webgrafía

- **Presentaciones de Puesta en Producción Segura.** *Rafael López García*.
- **Seguridad de aplicaciones.** José Losada Pérez.
- **Presentaciones de Puesta en Producción Segura.** *Rafael Fuentes Ferrer*.



Gracias!

¿Alguna pregunta?

informatica.iesvalledeljerteplasencia.es

coordinacion.cenfp@iesvjp.es

C/ Pedro y Francisco González, s/n
10600, Plasencia (Cáceres)

927 01 77 74