

○ EJERCICIO NUMERO 1

○ Link

○ <http://www.phpauction.net/workshop/ejercicio1/>

○ Objetivo

○ Comprobar si es vulnerable a HTML Injection

○ El alumno debe:

○ Exponer algún ejemplo de HTML Injection

○ Estimado: 10 minutos

○ EJERCICIO NUMERO 2

○ Link

○ <http://www.phpauction.net/workshop/ejercicio2abc/>

○ Objetivo

○ Comprobar si es vulnerable a HTML Injection

○ El alumno debe:

○ En alguna de las páginas del aplicativo, cambiar el logo superior por un externo

○ Que aparezcan alerts

○ Insertar un enlace a un javascript externo

○ Estimado: 15 minutos

○ EJERCICIO NUMERO 3

○ Link

○ <http://www.phpauction.net/workshop/ejercicio3yxz/>

○ Objetivo

○ Comprobar si es vulnerable a SQL Injection

○ El alumno debe:

○ Recuperar algún password de la estructura de la base de datos dada.

○ Estimado: 15 minutos

○ EJERCICIO NUMERO 4

○ Link

○ <http://www.phpauction.net/workshop/ejercicio4n/>

○ Objetivo

○ Comprobar si es vulnerable a Remote File Intrusion

○ El alumno debe:

○ Recuperar algún dato esencial o privado

○ Estimado: 15 minutos

Ejercicios

EJERCICIO CONCURSO

Link

<http://www.phpauction.net/workshop/concursoV/>

Objetivo

Comprobar que existe alguna vulnerabilidad web en un programa no modificado por nosotros

El alumno debe:

Encontrar una vulnerabilidad en la aplicación (ejecución de código remoto PHP) y explicar cómo la ha encontrado.

GANA: el que primero nos comunique su “fechoría”.

