sedian

Seguridad Digital
de Andalucía

Ficha técnica

Detección y explotación de vulnerabilidades SQL y XSS en aplicaciones web

Modalidad: Charla virtual
Fecha de celebración: 29 de enero de 2021

Junta de Andalucía

© 2020 Junta de Andalucía. Este documento y, en su caso, cualquier documento anexo al mismo, contiene información de carácter confidencial exclusivamente dirigida a su destinatario o destinatarios. Queda prohibida su divulgación, copia o distribución a terceros sin la previa autorización escrita de "Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.". Si no es Ud. el destinatario del documento le ruego lo destruya sin hacer copia digital o física, comunicando a "Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A." vía e-mail o fax la recepción del presente documento. Toda declaración de voluntad contenida deberá ser tenida por no producida.

ÍNDICE

1 DATOS BÁSICOS DE LA ACCIÓN FORMATIVA

Nombre de la acción formativa: Detección y explotación de vulnerabilidades SQL y XSS en aplicaciones web

Modalidad: Charla Virtual.

Fecha de celebración: 29 de Enero de 2021.

Horario: 09:00 a 10:30 A.M.

Dirigido a: Profesionales TIC de la Junta de Andalucía y entidades vinculadas.

Número máximo de personas participantes: 100.

2 DESCRIPCIÓN

En la sesión, se tratará de aproximar y transmitir conceptos básicos de las *vulnerabilidades de inyección SQL y XSS* así como sus diferencias, detección, explotación y posibles soluciones a nivel de código que se pueden aplicar a este tipo de problemas. Se trata de una sesión práctica en la que se explicará por medio de ejemplos, el impacto y características de estas vulnerabilidades.

3 OBJETIVOS

Generales

Describir y enseñar de forma práctica cómo detectar y explotar vulnerabilidades de inyección, concretamente aquellas basadas en *SQL* y *XSS*.

Específicos

Enseñar los **conceptos básicos de las vulnerabilidades de inyección** en aplicaciones web.

Explicar el ***OWASP Top 10*** y las posiciones en las que se encuentran las vulnerabilidades de inyección basadas en *SQL y XSS.*

Enseñar **Dojo Web Security** para la explotación de vulnerabilidades en aplicaciones web desde un entorno controlado, haciendo énfasis en las vulnerabilidades *SQLi y XSS*.

4 CONTENIDOS

- Introducción a las **vulnerabilidades de inyección** y el ***OWASP Top 10***.
- Introducción a ***Dojo Web Security*** así como el uso y ubicación de aplicaciones.
- Explotación de vulnerabilidades de ***SQL injection*** en ***DVWA***.
- Explotación de vulnerabilidades de ***XSS*** en ***DVWA***.
- Explotación de vulnerabilidades de ***SQL injection*** en ***OWASP WEB GOAT***.
- Explotación de vulnerabilidades de **XSS en OWASP WEB GOAT**.

5 TEMPORALIZACIÓN

Fecha: 29/01/2021. **Horario:** 09:00 a 10:30.

Modalidad: Charla Virtual

5 minutos.	Bienvenida e Introducción.
75 minutos.	Exposición de los contenidos
10 minutos.	Dudas y pregunta

6 METODOLOGÍA

La sesión formativa se desarrollará en **modalidad Charla Virtual**, es decir, un seminario impartido en línea donde la interactividad con el alumno es en tiempo real de forma virtualizada con herramientas informáticas diseñadas para tal fin. La herramienta usada para esta sesión se denomina **GoToWebinar**.

7 DOCENTE

IMPARTIDO POR: Daniel Echeverri (Aka. Adastra).

Pentester y formador autónomo. | SPSE - SecurityTube Python Scripting Expert | SLAE - SecurityTube Linux Assembly Expert |buguroo - Deep Learning Fraud Prevention

Fundador y formador en The Hacker Way Academy, iniciativa de formación que pretende apoyar el proceso de aprendizaje libre que tienen muchos de los entusiastas y profesionales de la seguridad informática de habla hispana.

Acceso a su perfil Linkedin.

8 EVALUACIÓN

Para la evaluación de la Charla Virtual se tendrán en cuenta las siguientes variables: la asistencia y el tiempo de conexión a la Charla Virtual, que deberá ser igual o superior al 50%.

- Asistencia a la jornada con un tiempo de conexión superior al 50%.

- Superar el cuestionario de conocimientos con un porcentaje de acierto del 60% o superior (en un plazo de 72 horas tras el evento).

Los valores de estas variables serán extraídos de diferentes informes generados por la herramienta **GoToWebinar** usada para celebrar la sesión.

Criterios de evaluación

Evidencias para la evaluación	Peso
Asistencia	**50%**
Evaluación de Conocimientos	**50%**

Sistema de evaluación.

Valoración de Asistencia.

Cálculo realizado a partir de los informes extraídos de la plataforma **GoToWebinar** denominados:

✓ Informe de Rendimiento.

✓ Informe de Asistentes.

Valoración de Conocimientos.

Indicador obtenido a partir de un cuestionario de 10 ítems sobre aspectos tratados durante la sesión.