Pentest web

Desarrollo

1. Regístrese en el portal *Web Security Academy* de la compañía *Port Swigger*, para poder acceder a los laboratorios de prácticos, en este enlace https://portswigger.net/web-security.

2. Elija una categoría, lea la explicación del tipo de ataque, y después resuelva alguno de los laboratorios prácticos que se encuentran en https://portswigger.net/web-security/all-labs, las categorías son:

   - SQL injection
   - Cross-site scripting
   - Cross-site request forgery (CSRF)
   - Clickjacking
   - DOM-based vulnerabilities
   - Cross-origin resource sharing (CORS)
   - XML external entity (XXE) injection
   - Server-side request forgery (SSRF)
   - HTTP request smuggling
   - OS command injection
   - Server-side template injection
   - Directory traversal
   - Access control vulnerabilities
   - Authentication
   - WebSockets
   - Web cache poisoning
   - Insecure deserialization
   - Information disclosure
   - Business logic vulnerabilities
   - HTTP Host header attacks
   - OAuth authentication
   - File upload vulnerabilities

3. Elabore el Informe de pentest siguiendo el formato del archivo Plantilla informe de pentest.docx. Las partes que lo componen son:

   - Resumen ejecutivo. Es un resumen de los hallazgos encontrados. Debe ser claro y conciso. No está dirigido a un público con conocimientos técnicos, por lo que se debe tener cuidado en su redacción. Tendrá un resumen del estado de seguridad actual de los activos, indicando la severidad (Crítico, Alto, Medio, Bajo o Sin impacto) de los hallazgos encontrados. Además de que, a partir de lo escrito en esta parte del documento, se podrán tomar acciones. Se recomienda escribir hasta que todo el resto del informe esté terminado.

   - Objetivos. Se indicarán los resultados esperados del pentest sobre los activos indicados. Éstos se definen desde el acuerdo celebrado previo al inicio del pentest.

   - Alcance. Se escribirán de forma explícita los activos a los cuáles se les aplicó el pentest. Éstos se definen desde el acuerdo celebrado previo al inicio del pentest. Así también se debe indicar las fechas y horarios en los que se llevaron a cabo las actividades.

- Seguridad actual de los activos. Se presentará un concentrado de los hallazgos del pentest por activo. Se recomienda asignarles tanto un identificador de activo como un identificador de hallazgo o vulnerabilidad, para poder hacer referencia a ellos con facilidad. Se debe indicar un nivel de severidad de acuerdo con la CVSS v3.1. Es altamente recomendable también colocar un identificador de recomendación por hallazgo o vulnerabilidad, una recomendación sobre cómo gestionar el hallazgo enriquece el reporte.

- Recomendaciones de seguridad generales. A partir de los hallazgos encontrados, dar recomendaciones de seguridad que pueden aplicarse a diferentes ambientes para fortalecer la seguridad de la organización.

- Anexo A. Recomendaciones específicas. Por cada hallazgo o vulnerabilidad, dar una recomendación para mejorar el estado de seguridad actual, la intención es proveer información técnica específica que pueda servir de referencia para el personal técnico de la organización. Además, deberá de incluirse el puntaje de la CVSS, junto con su vector.

- Anexo B. Hallazgos por activo de información. En este anexo se deberá de dar detalles técnicos específicos con la forma de explotar los hallazgos o vulnerabilidades, adjuntando la evidencia suficiente para que el personal técnico de la organización lo pueda reproducir.

- Elaboración del informe. Indicar las personas que participaron en la elaboración del informe.

Elementos a calificar

1. Se deberá subir el Informe de Pentest en PDF a Moodle.
2. Se puede entregar en equipo de dos personas, sin embargo, cada integrante deberá de explotar y reportar una vulnerabilidad.

Referencias

- NIST. *Common Vulnerability Scoring System Calculator*. https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator
- NIST. *NVD Vulnerability Severity Ratings*. https://nvd.nist.gov/vuln-metrics/cvss
- FIRST. *Common Vulnerability Scoring System v3.1: User Guide*. https://www.first.org/cvss/v3.1/user-guide

CIENCIAS

Universidad Nacional Autónoma de México

Paulo Contreras Flores
paulo.contreras.flores@ciencias.unam.mx