

Evaluación continua 5.1

Hacking Ético. Caso Práctico.

1) Enumera y explica las fases de un pentesting:

Generalmente, siempre se podrán realizar la mayoría de las siguientes fases en las distintas auditorías de seguridad. Ahora, se enumeran las distintas fases del proceso:

Fase de recolección de información

- **Footprinting.** Esta primera fase propone recolectar información pública. También es conocida como parte del Information Gathering. Es una fase menos importante cuando el entorno es interno; por ejemplo, en una auditoría interna a una empresa. En el caso de una auditoría web y auditoría perimetral (ambas son caja negra) es una fase inicial importante ya que toda esa información pública que podamos recolectar, podremos usarla en fases siguientes.

- **Fingerprinting.** Esta fase permite al auditor analizar los servicios localizados en la fase de footprint. El objetivo es claro conseguir información detallada de los servicios que ofrece la organización. El análisis de puertos abiertos, el análisis de mecanismos de protección y la obtención de versiones de aplicaciones expuestas es algo muy útil en una auditoría y se obtiene en esta fase.

Fase de Búsqueda de vulnerabilidades

- **Análisis de vulnerabilidades.** En esta fase se analizan las vulnerabilidades conocidas sobre los servicios analizados en la fase de fingerprinting. Se suelen utilizar herramientas automáticas que tienen bases de datos de vulnerabilidades y se puede contrastar lo encontrado en el fingerprinting con la existencia de vulnerabilidades.

Fase de Explotación de vulnerabilidades

- **Explotación de vulnerabilidades.** En esta fase se lleva a cabo la explotación de vulnerabilidades identificadas en la fase anterior, para conseguir acceso a los sistemas de la organización. Lo usual en esta fase es ejecutar exploits contra las vulnerabilidades identificadas o simplemente utilizar credenciales obtenidas para ganar acceso a los sistemas.

Fase Post-explotación.

Post-explotación. (Si bien no aparece en el material del curso, la he visto en varias fuentes externas al mismo y quise incluirla).

Esta fase no se da siempre, cómo indica su nombre es lo que se realiza después de la explotación y de haber obtenido acceso. Sería posible hacer una recogida de información a nivel interno para intentar ganar privilegios o realizar otras acciones.

Fase de Informe

● **Generación de informes.** Luego de finalizar todas las etapas mencionadas previamente, es el momento de documentar todo lo realizado en un informe que especifique el proceso realizado en el test de intrusión, como herramientas utilizadas, técnicas utilizadas y vulnerabilidades descubiertas. En esta última fase, se presenta el trabajo llevado a cabo por el auditor, a la empresa que contrató el servicio. Hay dos tipos de informes: ejecutivo y técnico.

2) Define qué es un Cross-Site Scripting y cuántos tipos conoces, explicando cada uno.

XSS ó Cross-Site Scripting es un tipo de ataques es muy común y es conocido como de tipo Client-Side, ya que se produce en el navegador del usuario. Un atacante consigue introducir un código Javascript en un parámetro web, por ejemplo, y consigue a través de un enlace o la visita a un sitio web que dicho código sea ejecutado por el navegador de la víctima, aprovechando un fallo en la aplicación web.

Esto sucede cuando la aplicación no valida, ni la entrada ni la salida de los datos de la aplicación web. Se puede utilizar para robar sesiones o cookies, realizar un deface, ...Existen diferentes tipos de XSS, los cuales se describen a continuación:

● **No persistente o reflejado.** Los ataques llegan a la víctima a través de, por ejemplo, un enlace. En uno de los parámetros se inyecta el código Javascript y cuando la víctima accede al link su navegador ejecuta dicho código.

● **Persistente.** El código Javascript queda almacenado de forma persistente en una base de datos, por ejemplo, cuando un usuario introduce un comentario en un sistema y éste no valida la entrada, puede quedar almacenado en la base de datos el código malicioso. Entonces cuando otros usuarios accedan al comentario, los navegadores de estos podrán ejecutar el código malicioso. Es el XSS más potente.

● **DOM.** El código inyectado manipula el código Javascript de los objetos HTML.

3) Define qué es un SQLi y cuántos tipos conoces, explicando cada uno.

SQLi, Sql Injection ó Inyección SQL es una vulnerabilidad que permite al atacante enviar o “inyectar” instrucciones SQL de forma maliciosa y malintencionada. Permite que un atacante interfiera con las consultas que una aplicación realiza en su base de datos. En general, permite que un atacante vea ciertos datos que no debería de poder recuperar. Esto puede incluir datos pertenecientes a otros usuarios, accesos, estructura de tablas o cualquier otro dato al que la aplicación pueda acceder.

Inyección SQL en banda

La inyección SQL en banda es la forma más simple de inyección SQL. En este proceso, el atacante es capaz de utilizar el mismo canal para insertar el código SQL malicioso en la aplicación, así como para recoger los resultados. Discutiremos dos formas de ataques de inyección SQL en banda:

Ataque basado en errores

Un atacante utiliza una técnica de inyección SQL basada en errores durante las fases iniciales de su ataque. La idea detrás de una inyección SQL basada en errores es obtener más información sobre la estructura de la base de datos y los nombres de las tablas que sigue la aplicación web. Por ejemplo, un mensaje de error puede contener el nombre de la tabla incluido en la consulta y los nombres de las columnas de la tabla. Estos datos pueden ser utilizados para crear nuevos ataques.

Ataque basado en la Unión

En este método, un atacante que utiliza la unión SQL se une para mostrar los resultados de una tabla diferente. Por ejemplo, si un atacante está en una página de búsqueda, puede añadir los resultados de otra tabla.

Inyección SQL Inferencial (Blind SQL Injection)

Incluso si un atacante genera un error en la consulta SQL, la respuesta de la consulta puede no ser transmitida directamente a la página web. En tal caso, el atacante necesita investigar más.

En esta forma de inyección SQL, el atacante envía varias consultas a la base de datos para evaluar cómo la aplicación analiza estas respuestas. Una inyección SQL inferencial es a veces también conocida como **inyección SQL ciega**. A continuación veremos dos tipos de inyecciones SQL inferenciales: inyección SQL booleana e inyección SQL basada en tiempo.

Ataque Booleano

Si una consulta SQL da como resultado un error que no ha sido manejado internamente en la aplicación, la página web resultante puede arrojar un error, cargar una página en blanco o cargar parcialmente. En una inyección SQL booleana, un atacante evalúa qué partes de la entrada de un usuario son vulnerables a las inyecciones SQL probando dos versiones diferentes de una cláusula booleana a través de la entrada:

- «... and 1=1»
- «... and 1=2»

Si la aplicación funciona normalmente en el primer caso pero muestra una anomalía en el segundo, indica que la aplicación es vulnerable a un ataque de inyección SQL.

Ataque basado en el tiempo

Un ataque de inyección SQL basado en el tiempo también puede ayudar a un atacante a determinar si una vulnerabilidad está presente en una aplicación web. Un atacante utiliza una función predefinida basada en el tiempo del sistema de administración de la base de datos que es utilizada por la aplicación. Por ejemplo, en MySQL, la función sleep() le indica a la base de datos que espere un cierto número de segundos.

Inyección SQL fuera de banda

Si un atacante no puede obtener los resultados de una inyección SQL a través del mismo canal. Las técnicas de inyección SQL fuera de banda pueden utilizarse como alternativa a las técnicas de inyección SQL inferencial.

4) Dado el siguiente escenario:

Una aplicación web con una vulnerabilidad LFI en la dirección: <https://misecureapp.com/info?file=info/license.txt>

La aplicación se conecta a una base de datos, a través de la configuración almacenada en el fichero `config.php`, situado bajo la carpeta `config`, alojada en la raíz del sitio web

¿Cómo accederías a la configuración de la base de datos? Explica el proceso y escribe la URL.

Incluso sin la capacidad de cargar y ejecutar código, una vulnerabilidad de inclusión de archivos locales puede ser peligrosa. Un atacante aún puede realizar un ataque Directory Traversal / Path Traversal utilizando una vulnerabilidad LFI de la siguiente manera.

http: <https://misecureapp.com/../../../../config.php>

En el ejemplo anterior, un atacante puede obtener el contenido del archivo `/config.php` que contiene la configuración a través de la cual se conecta a una base de datos. Del mismo modo, un atacante puede aprovechar la vulnerabilidad Directory Traversal para acceder a archivos de registro (por ejemplo, acceso a `Apache.log` o `error.log`), código fuente y otra información confidencial. Esta información se puede utilizar para avanzar en un ataque.

5) Define qué es XXE y para qué podría utilizarse

La inyección de entidad externa XML (también conocida como XXE) es una vulnerabilidad de seguridad web que permite a un atacante interferir con el procesamiento de datos XML de una aplicación. A menudo permite a un atacante ver archivos en el sistema de archivos del servidor de aplicaciones e interactuar con cualquier sistema back-end o externo al que la propia aplicación pueda acceder. En algunas situaciones, un atacante puede escalar un ataque XXE para poner en peligro el servidor subyacente u otra infraestructura back-end, aprovechando la vulnerabilidad XXE para realizar ataques de falsificación de solicitudes del lado del servidor (SSRF).

Existen varios tipos de ataques XXE:

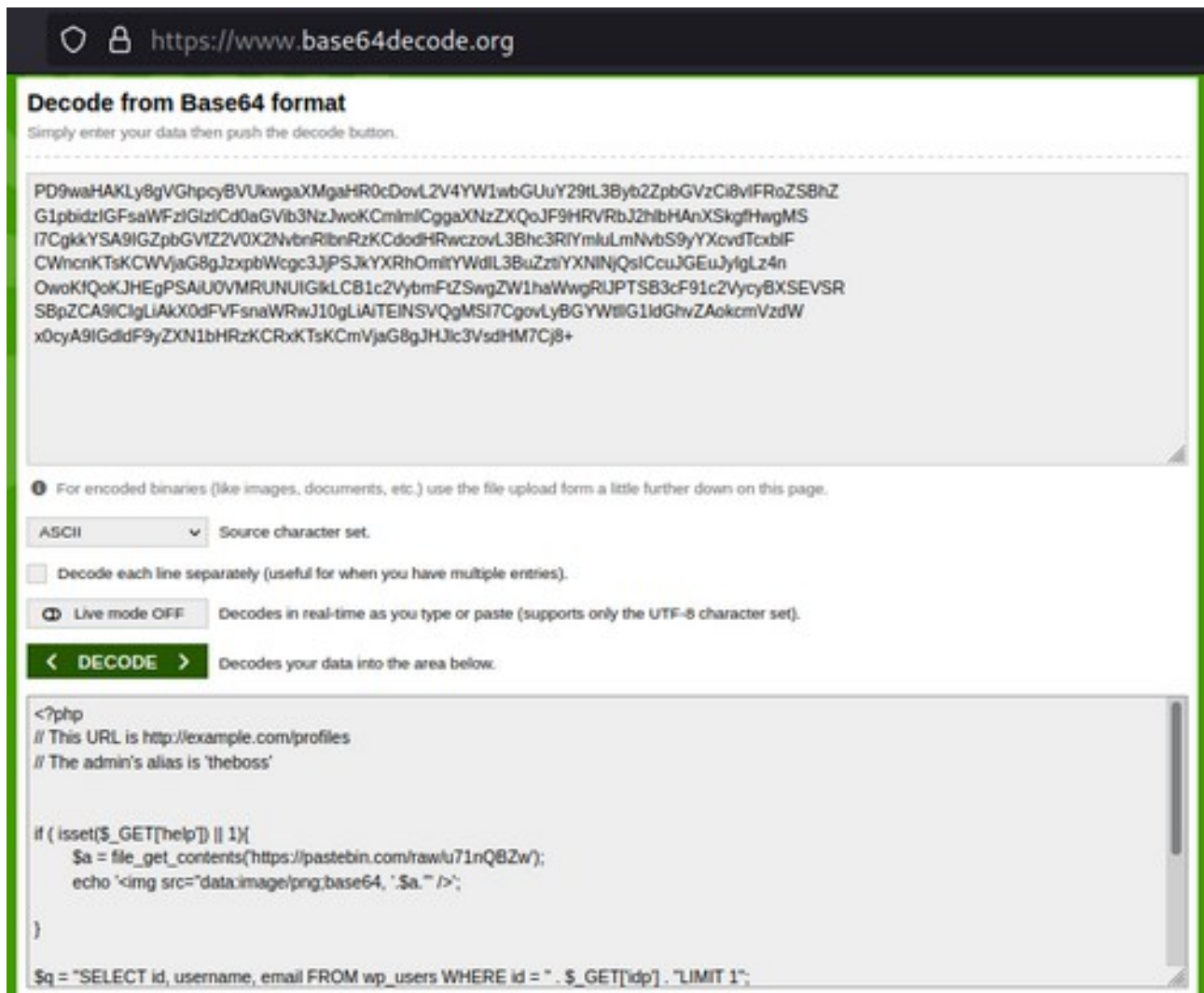
- Explotar XXE para recuperar archivos, donde se define una entidad externa que contiene el contenido de un archivo, y se devuelve en la respuesta de la aplicación.
- Explotar XXE para realizar ataques SSRF, donde se define una entidad externa en base a una URL a un sistema back-end.
- Explotar datos ciegos XXE exfiltrados fuera de banda, donde los datos confidenciales se transmiten desde el servidor de aplicaciones a un sistema que el atacante controla.
- Explotar XXE ciego para recuperar datos a través de mensajes de error, donde el atacante puede activar un mensaje de error de análisis que contiene datos confidenciales.

Con este necesito ayuda (no supe seguir).

6) Dada la siguiente información, indica qué petición harías (incluyendo payload encodeado, si es necesario) para obtener la contraseña hasheada y el “salt” del usuario administrador.

PD9waHAKLy8gVGhpcyBVUkwgaXMgaHR0cDovL2V4YW1wbGUuY29tL3Byb2ZpbGVzCi8vIFRoZSBhZ
G1pbidzIGFsaWFzIGlzlCd0aGVib3NzJwoKcmImICggaXNzZXQoJF9HRVRbJ2hlbHAnXSkgfHwgMS
I7CgkKYSa9IGZpbGVIZ2V0X2NvbniRlbnRzKCdodHRwczovL3Bhc3RIYmluLmNvbS9yYXcvdTcxblF
CWncnKTsKCWVjaG8gJzxpWgc3JjPSJkYXRhOmItYWdlL3BuZztiYXNINjQsICcuJGEuJyIgZ4n
OwoKfQoKJHEgPSAiU0VMRUNUIGklCB1c2VybmFtZSwgZW1haWwgRIJPTSB3cF91c2VycyBXSEVSR
SBpZCA9IClgLiAkX0dFVFfnaWRwJ10gLiAiTEINSVQgMSI7CgovLyBGYWtllG1dGhvZAokcmVzdW
x0cyA9IGdlidF9yZXN1bHRzKCRxKTsKCmVjaG8gJHJlc3VsdHM7Cj8+

<https://www.base64decode.org/>



The image shows a screenshot of the 'Decode from Base64 format' tool on the website <https://www.base64decode.org/>. The tool has a text input area containing a long Base64-encoded string. Below the input area, there are several options: 'Source character set' is set to 'ASCII'; 'Decode each line separately' is unchecked; 'Live mode' is set to 'OFF'; and a 'DECODE' button is visible. The output area shows the decoded content, which is a PHP script snippet. The script includes comments about a URL and an admin's alias, and contains a conditional statement that checks for a 'help' parameter and displays a Base64-encoded image if it is present. At the bottom, there is a SQL query snippet.

Decode from Base64 format

Simply enter your data then push the decode button.

PD9waHAKLy8gVGhpcyBVUkwgaXMgaHR0cDovL2V4YW1wbGUuY29tL3Byb2ZpbGVzCi8vIFRoZSBhZ
G1pbidzIGFsaWFzIGlzlCd0aGVib3NzJwoKcmImImICggaXNzZXQoJF9HRVRbJ2hlbHAnXSkgfHwgMS
I7CgkKYSa9IGZpbGVIZ2V0X2NvbniRlbnRzKCdodHRwczovL3Bhc3RIYmluLmNvbS9yYXcvdTcxblF
CWncnKTsKCWVjaG8gJzxpWgc3JjPSJkYXRhOmItYWdlL3BuZztiYXNINjQsICcuJGEuJyIgZ4n
OwoKfQoKJHEgPSAiU0VMRUNUIGklCB1c2VybmFtZSwgZW1haWwgRIJPTSB3cF91c2VycyBXSEVSR
SBpZCA9IClgLiAkX0dFVFfnaWRwJ10gLiAiTEINSVQgMSI7CgovLyBGYWtllG1dGhvZAokcmVzdW
x0cyA9IGdlidF9yZXN1bHRzKCRxKTsKCmVjaG8gJHJlc3VsdHM7Cj8+

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

Source character set: ASCII

☐ Decode each line separately (useful for when you have multiple entries).

☒ Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

< DECODE > Decodes your data into the area below.

```
<?php
// This URL is http://example.com/profiles
// The admin's alias is 'theboss'

if (isset($_GET['help']) || 1){
    $a = file_get_contents('https://pastebin.com/raw/u71nQ8Zw');
    echo '';
}

$a = "SELECT id, username, email FROM wp_users WHERE id = " . $_GET['idp'] . " LIMIT 1";
```

```

<?php
// This URL is http://example.com/profiles
// The admin's alias is 'theboss'

if ( isset($_GET['help']) || 1){
    $a = file_get_contents('https://pastebin.com/raw/u71nQBZw');
    echo '';
}

$q = "SELECT id, username, email FROM wp_users WHERE id = " . $_GET['idp'] . "LIMIT 1";

// Fake method
$results = get_results($q);

echo $results;
?>

```

7) Dado el siguiente código ASM (sintaxis y direcciones de memoria ficticias), indica el valor del registro edx en la dirección de memoria 0x0000401000 (marcada en rojo). Justifica tu respuesta siguiendo el flujo del programa.

Máquina de 2 direcciones

Línea 1 realiza un XOR (INSTRUCCIÓN LÓGICA), para el destino eax, y la fuente eax. El resultado queda almacenado en eax.

Línea 2 realiza un mov(INSTRUCCIÓN DE TRANSFERENCIA DE DATOS), asignando al registro ecx el valor 10

Línea 3 compara los valores de ambos registros(INSTRUCCIÓN ARITMÉTICA)

Línea 4 (INSTRUCCIÓN DE TRANSFERENCIA DE CONTROL), si el flag de ZERO de la operación anterior indica 1, salta a ejecutar la instrucción de la dirección de memoria indicada.

Sino continúa secuencialmente la ejecución.

Línea 5 (INSTRUCCIÓN ARITMÉTICA) incrementa en 1 el valor del registro eax.

La línea 6, se lee la instrucción dec, pero no se indica que registro debe ser decrementado.

0x0000400000	xor eax, eax
0x0000400010	mov ecx, 10
0x0000400020	cmp ecx, eax
0x0000400030	je 0x00004000B0
0x0000400040	inc eax
0x0000400050	dec
0x0000400060	cmp ecx, 7
0x0000400070	jne 0x0000400020
0x0000400080	mov ebx, 2
0x0000400090	imul ecx, ebx
0x00004000A0	add eax, ecx
0x00004000B0	xor ebx, ebx
0x00004000C0	add ebx, edx
0x00004000D0	xor edx, ebx
0x00004000E0	inc edx
0x00004000F0	mul edx, eax
0x0000401000	??????????

A partir de este punto, al no indicarse el registro a decrementar, ya no puede saberse a ciencia cierta cuál será el resultado del registro edx, ya que el programa daría error y no se sabe si la intención era decrementar este registro u otro.