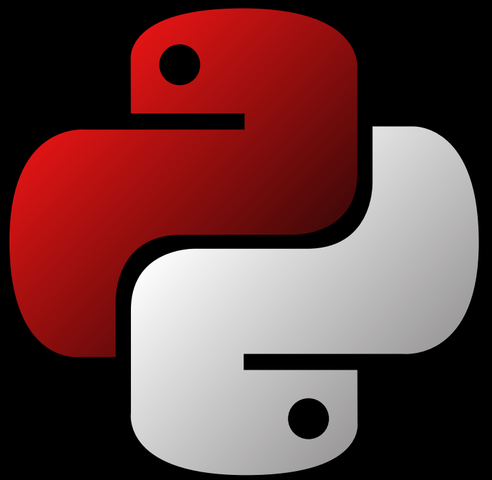
DEEPSEC ACADEMY

DeepSec Pentesting Web Python Course



DEEPSEC ACADEMY

Cookie Hijacking

¿Que es una cookie?

Las cookies permiten que los sitios web lo identifiquen mientras pasa tiempo en linea y son mas beneficiosas para los sitios web que tienen usuarios recurrente.

DEEPSEC ACADEMY

Cookie Hijacking

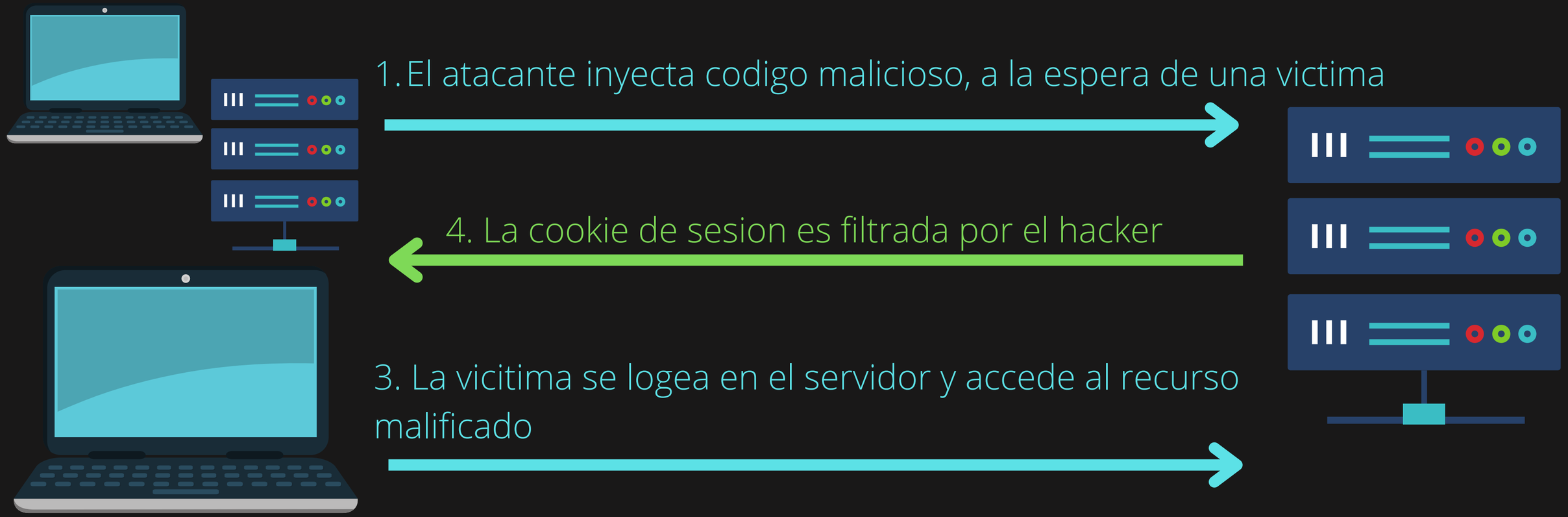
¿Que es el Cookie Hijacking?

Es el secuestro de estos datos (cookies), como consecuencia se puede dar la suplantacion de identidad y posterior hacer un robo a tu cuenta bancaria, comprar articulos con tu cuenta, etc

DEEPSEC ACADEMY

Cookie Hijacking

¿Como funciona el Cookie Hijacking?



DEEPSEC ACADEMY

SQL INJECTION

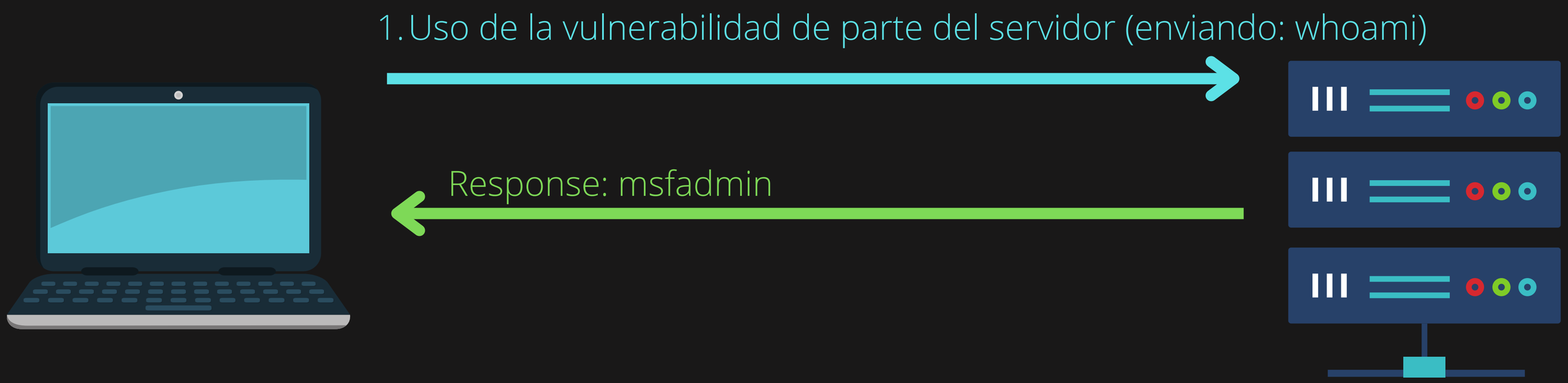
¿Que es el SQL Injection?

Es una tecnica de inyeccion de codigo que se la puede aprovechar para que se nos de informacion de interes como ser: cuentas bancarias de los clientes, usuarios administradores del servidor, etc.

DEEPSEC ACADEMY

RCE (Remote Code Execution)

¿Como funciona RCE?

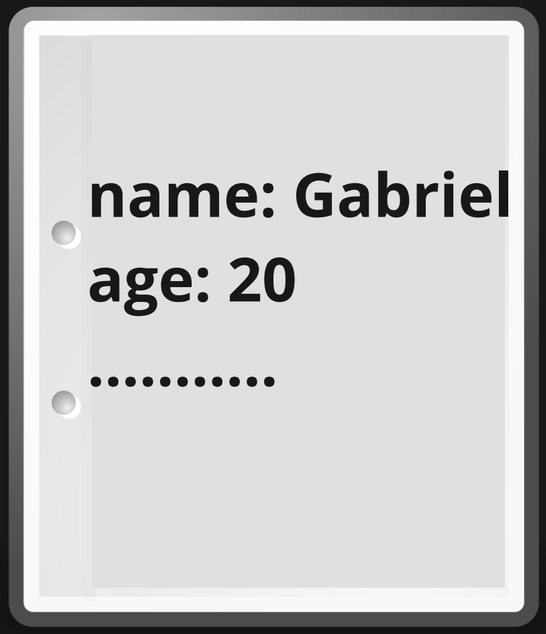


DEEPSEC ACADEMY

DESEARILIZATION ATTACK

¿Que es la serializacion?

La serializacion es el proceso de convertir un objeto en un formato "mas plano", el cual se pueda enviar y recibir como un flujo secuencial de bytes. La serializacion de datos hace que sea mucho mas sencillo



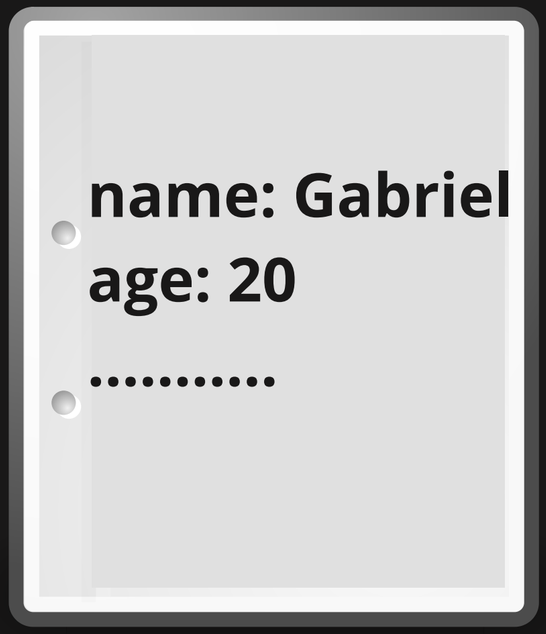
10101010111110101010101010100101.....

DEEPSEC ACADEMY

DESEARILIZATION ATTACK

¿Que es la Deserializacion?

La Deserializacion es el proceso de restaurar este flujo de bytes a una replica completamente funcional del objeto original, es decir transforma este flujo de bits al estado al que se lo serializo dicho objeto

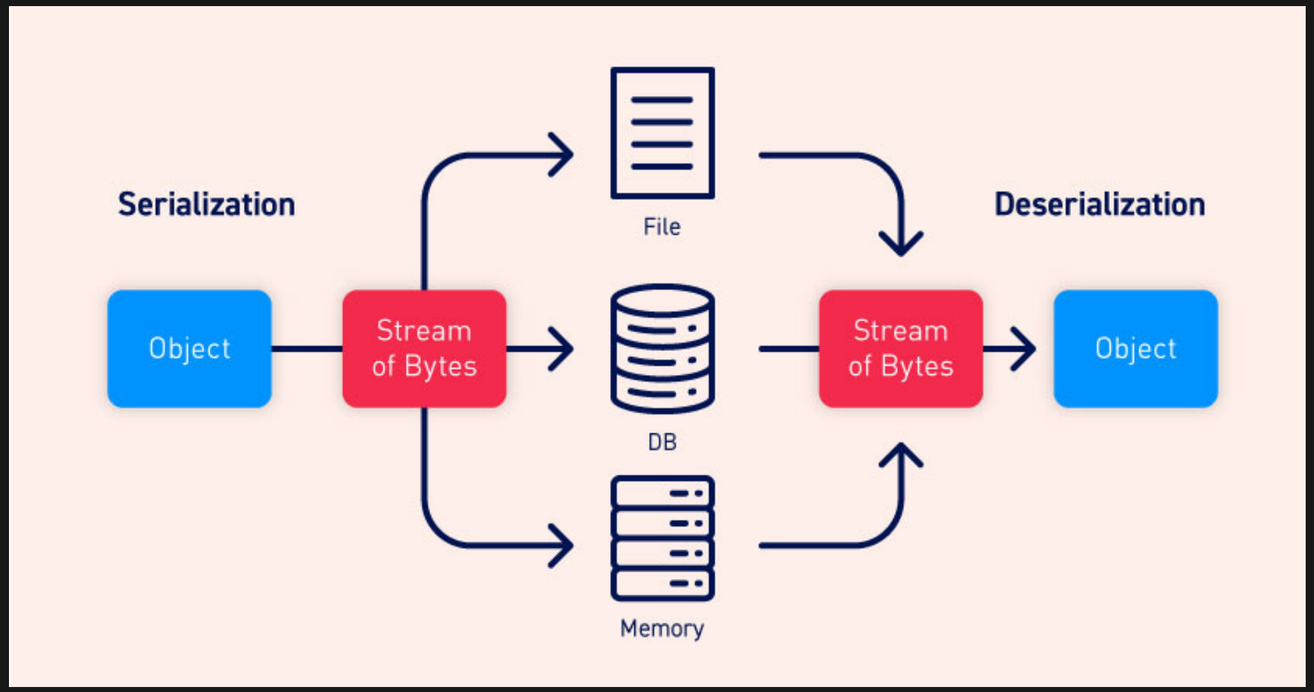


10101010111110101010101010100101.....

DEEPSEC ACADEMY

DESEARILIZATION ATTACK

Serializacion vs Deserializacion

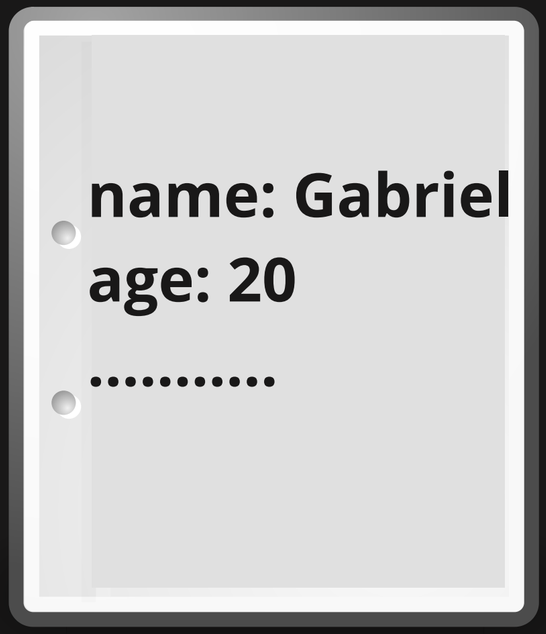


DEEPSEC ACADEMY

DESEARILIZATION ATTACK

¿Que es la Deserializacion insegura?

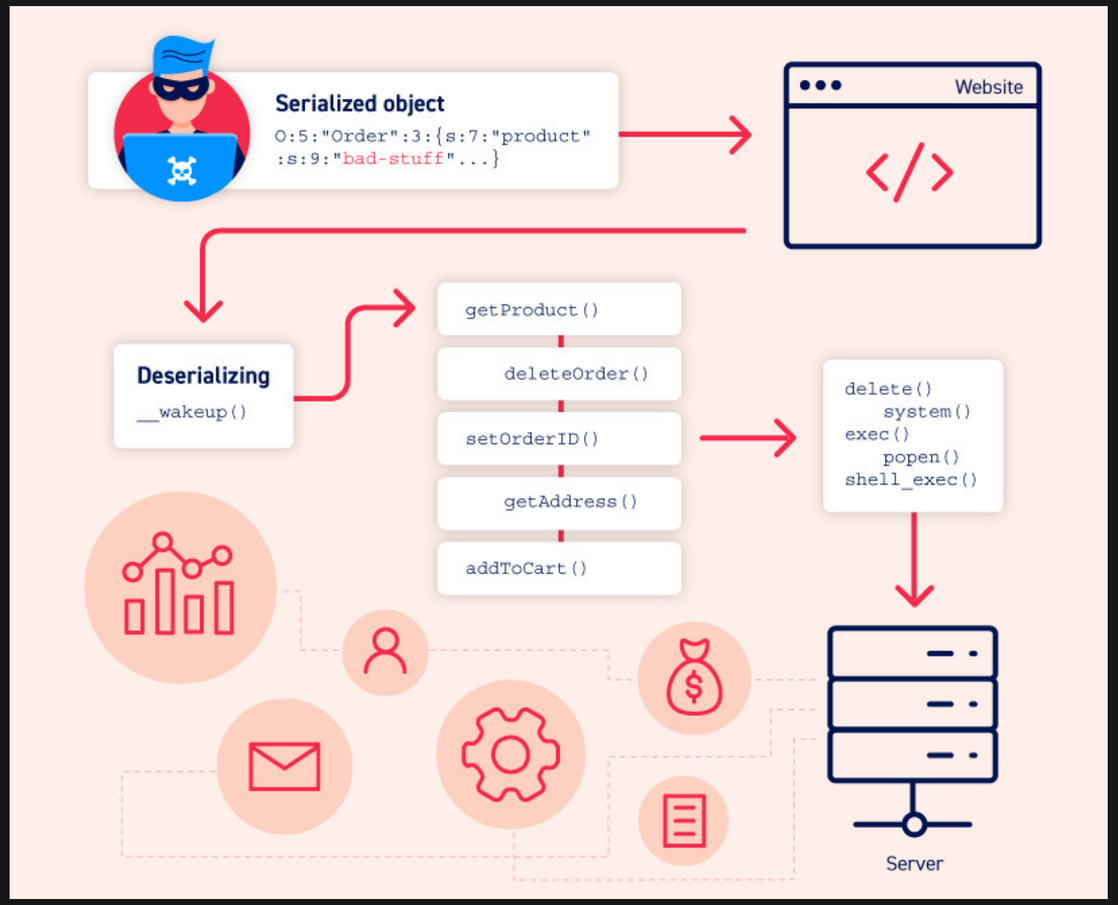
Es cuando un sitio web deserializa los datos controlables por el usuario. Esto potencialmente permite que un atacante manipule objetos serializados para pasar datos dañinos al codigo de la aplicacion. Podemos sustituir el objeto por uno malicioso y obtener un RCE.



10101010111110101010101001010.....

DEEPSEC ACADEMY

DESEARILIZATION ATTACK



¡Muchas gracias!