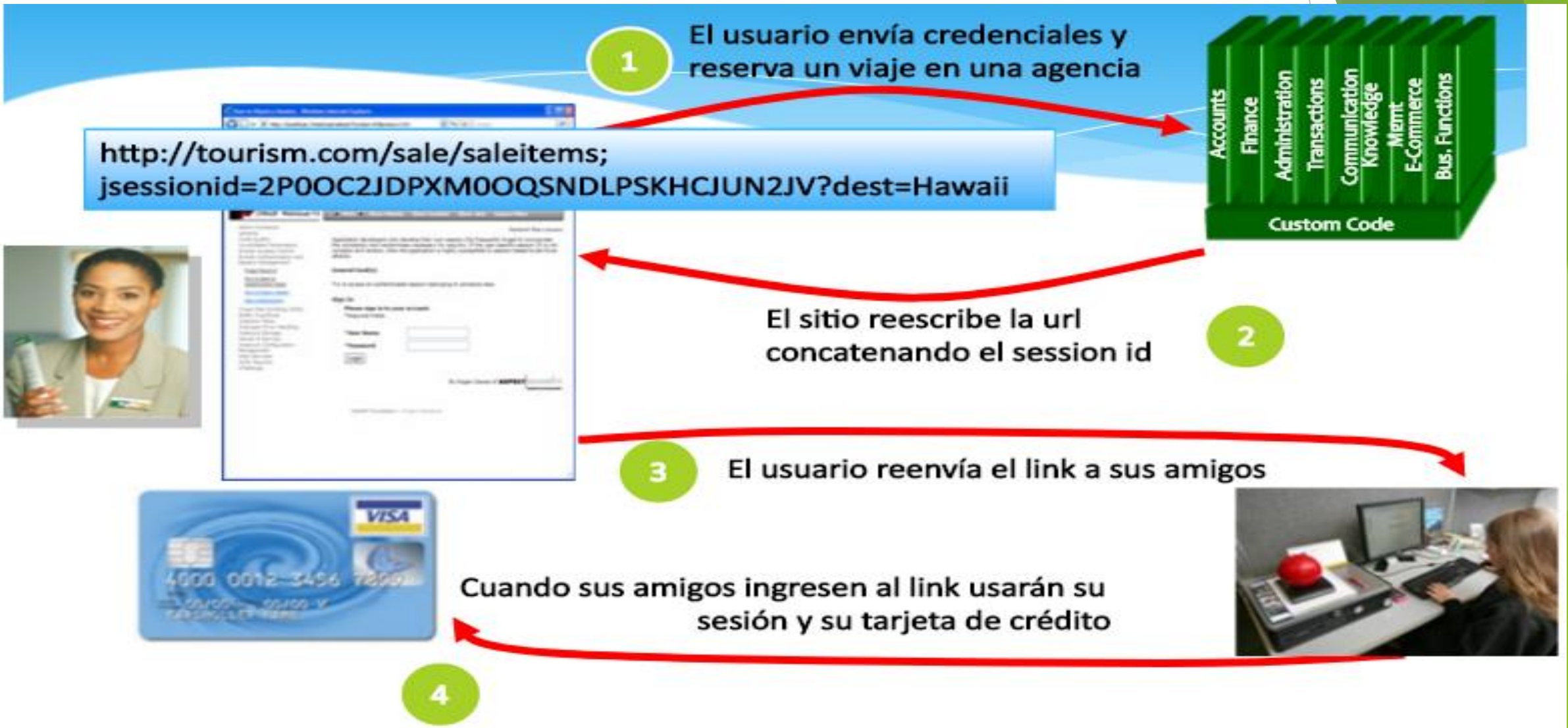
PÉRDIDA DE AUTENTICACIÓN
Y
GESTIÓN DE SESIONES

INTRODUCCIÓN

- La **autenticación** es el proceso de verificación que hace un individuo.
- La identificación debe ser única.
- Para acceder, el usuario necesita proporcionar información privada.
- La **gestión de sesiones** es un proceso mediante el cual un servidor mantiene el estado de una entidad que interactúa con él.
- Los ataques de la pérdida de autenticación y gestión de sesiones son ataques anónimos con la intención de tratar de recuperar (robar) información personal.
- **Motivo:** las credenciales de una cuenta y los tokens de las sesiones no suelen estar protegidos adecuadamente.

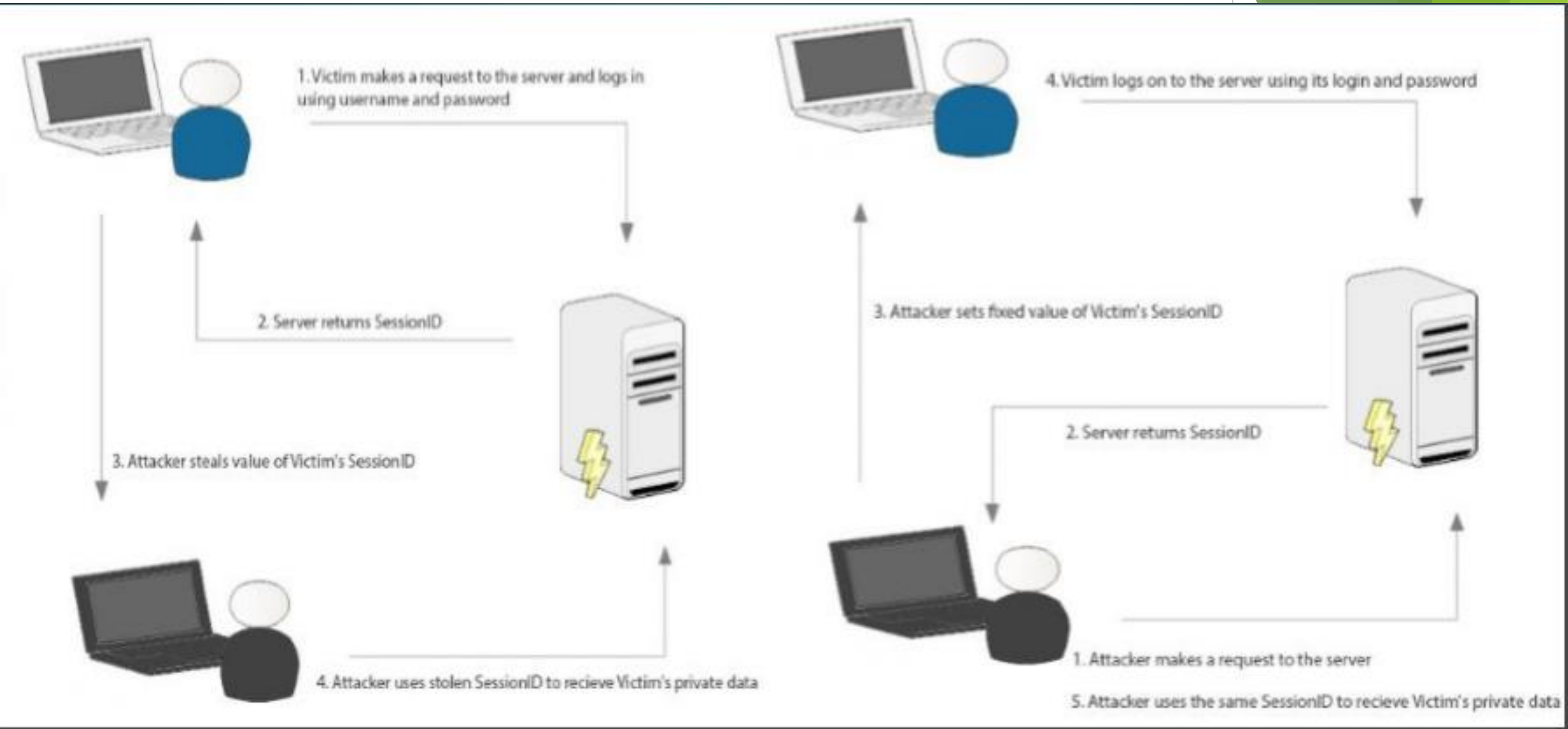
EJEMPLO DE PÉRDIDA DE AUTENTICACIÓN



¿Cuándo soy vulnerable?

- Cuando se almacena credenciales cifradas de los usuarios.
- Si es posible adivinar o sobrescribir las credenciales a través de funciones débiles de gestión de sesión.
- Si los identificadores (ID) de sesión son expuestos en la URL.
- Cuando los identificadores (ID) de sesión, las sesiones de usuarios o los tokens de autenticación no expiran.
- ID son vulnerables a ataques de fijación de la sesión.

Método de ataque



EJEMPLOS DE ATAQUES

*Por fuerza bruta

-Proceso automatizado de ensayo y error:

- Adivinar el nombre de usuario, contraseña, número de tarjeta de crédito, etc. De una persona.
- El sistema envía un valor y espera respuesta, luego intenta con otro y así sucesivamente.
- Extractos de la base de datos.

-Muchos sistemas permiten el uso de contraseñas débiles:

- Un atacante utiliza un diccionario de palabras.
- Genera miles de contraseñas incorrectas.
- Cuando acierta la contraseña, accede.

*Por fuerza bruta

Ejemplo:

Username ▪ Emmanuel

Passwords ▪ 1234567, qwertz, asdfgh, abcd, ...

[pet names], [birthdays], [car names], [dictionary].

Usernames▪ Emmanuel, Jan, Eric, Guenter,...

Password ▪ 12345678

*Por sesión de detección

-El atacante tiene la posibilidad de escuchar el tráfico a través del nivel de IP (sniffer).

-El cliente se conecta al servidor HTTP 'www.mysite.com'

- Visita una página que contiene un formulario de inicio de sesión (url es HTTPS).
- Recibe una cookie que contiene su ID de sesión.
- Envía sus credenciales cifradas (HTTPS).

-El atacante recibe la siguiente información:

- Session ID
- Ve que el usuario ha enviado sus credenciales. (usando una conexión encriptada)

-El atacante puede utilizar la cookie para ser reconocido como un usuario!

*Ataque de repetición

-Es una forma de ataque de red en el que una transmisión de datos válida, se reproduce de manera maliciosa.

-EJEMPLO 1: la víctima quiere logearse en un sitio web. Envía su nombre de usuario y contraseña. El sitio web lo verifica. Si un atacante puede escuchar la información, lo transfiere mediante sniffer (sin cifrar) /troyano (cifrado). Luego puede iniciar sesión en el sistema usando los datos.

-EJEMPLO 2: Alice quiere probar su identidad a Bob. Bob solicita la contraseña de Alice como prueba de identidad; mientras tanto Eve está “husmeando” la conversación y guarda la contraseña. Después del intercambio entre Bob y Alice, Eve se conecta a Bob. Cuando se le pide la prueba de identidad, Eve envía la contraseña de Alice, obteniendo así el acceso.

*Ataque de fijación de sesión

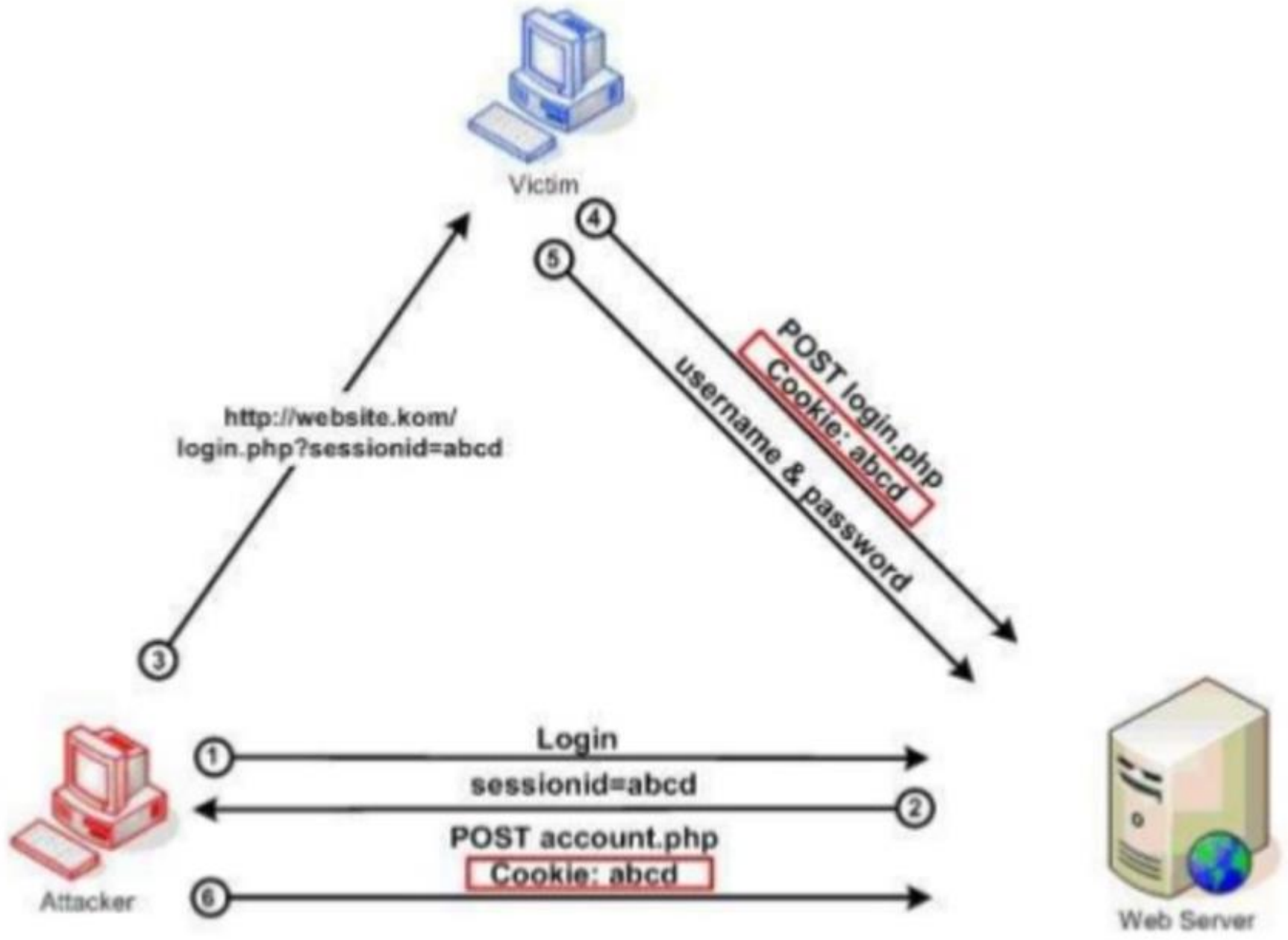
-Los ataques de fijación de sesión intentan un sistema que permite a una persona 'fijar' la identificación de otra persona.

-La mayoría de estos ataques están basados en web y dependen de los identificadores de sesión que se aceptan desde URLs o datos POST.

-El atacante utiliza alguna técnica común para ello:

- Parámetro URL
- Campo de formulario oculto
- Cookies

Ejemplo


Victim
4
5
POST login.php
Cookie: abcd
username & password
http://website.kom/
login.php?sessionid=abcd
3
Attacker
1
Login
sessionid=abcd
2
POST account.php
Cookie: abcd
6
Web Server

*Secuestro de sesión (Session Hijacking)

-Predicción de credenciales/sesiones

- El atacante deduce o adivina el ID de la sesión.
- El atacante puede usar un sitio web con los privilegios de la víctima.

-Los derechos se almacenan en una sesión, solo se utiliza el identificador de sesión para vincular el navegador y su sesión.

- HTTP es sin sesión.
- La información no aparece en cara solicitud.

-Adivinando el ID de sesión, permite al atacante ser el usuario.

-El token de sesión podría verse comprometido de diferentes maneras:

- Token de sesión predecible.
- Sesión de inhalación (session sniffing).
- Los ataques del lado del cliente.

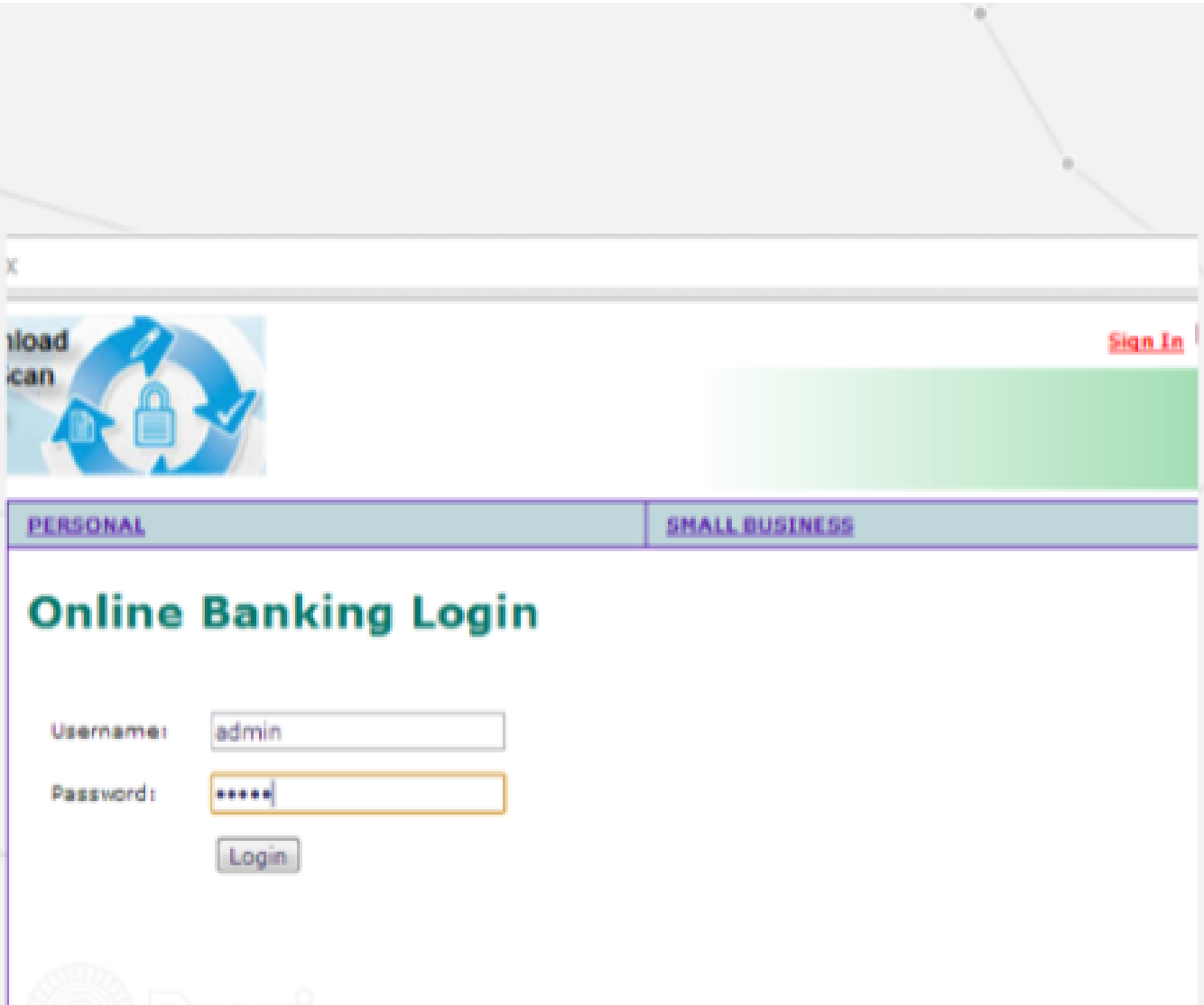
Ejemplo


Session ID = ACF3D35F216AAEFC
Victim
Web Server
Sniffing a legitim session
Attacker

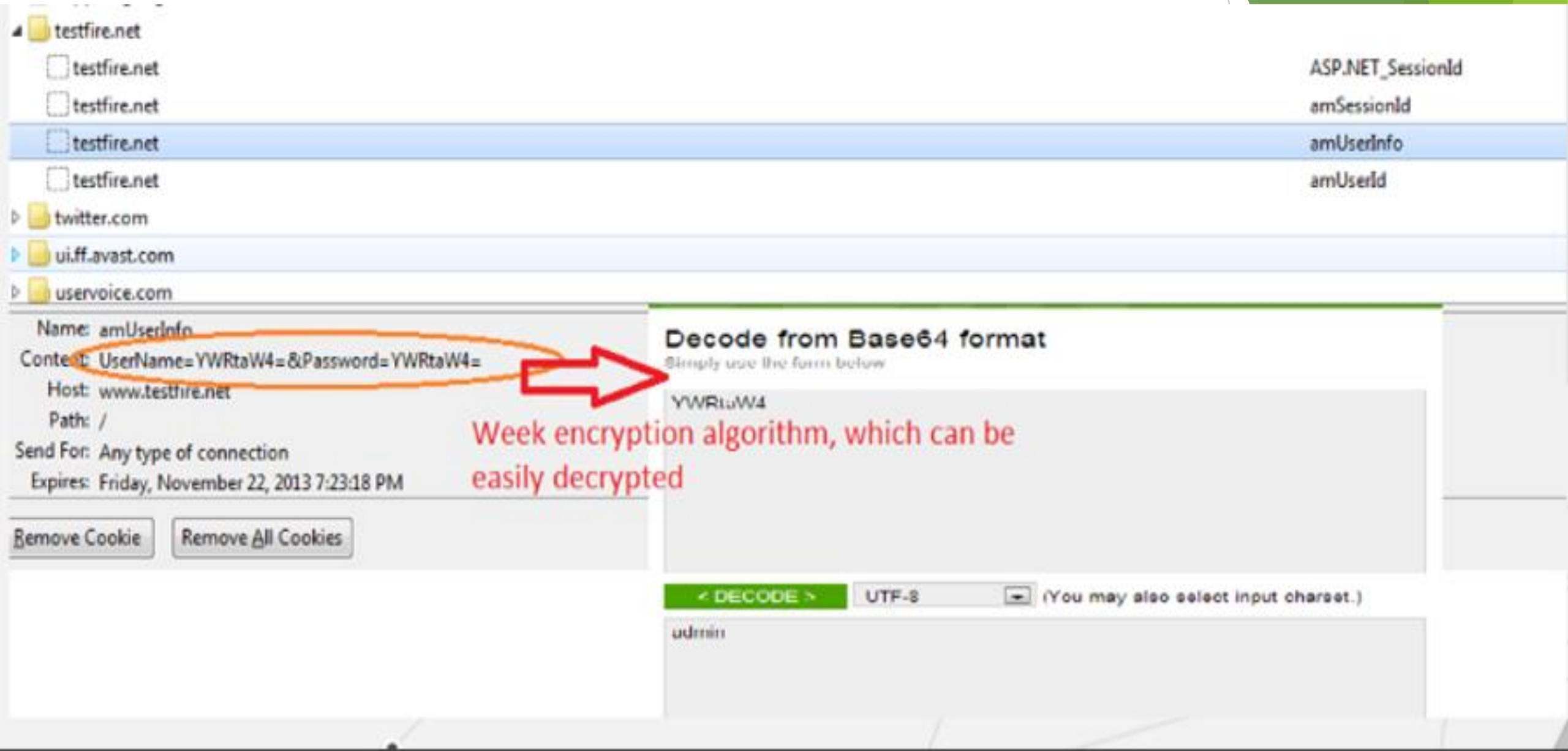

Session ID = ACF3D35F216AAEFC
Victim
Web Server
Session ID = ACF3D35F216AAEFC

OTROS EJEMPLOS

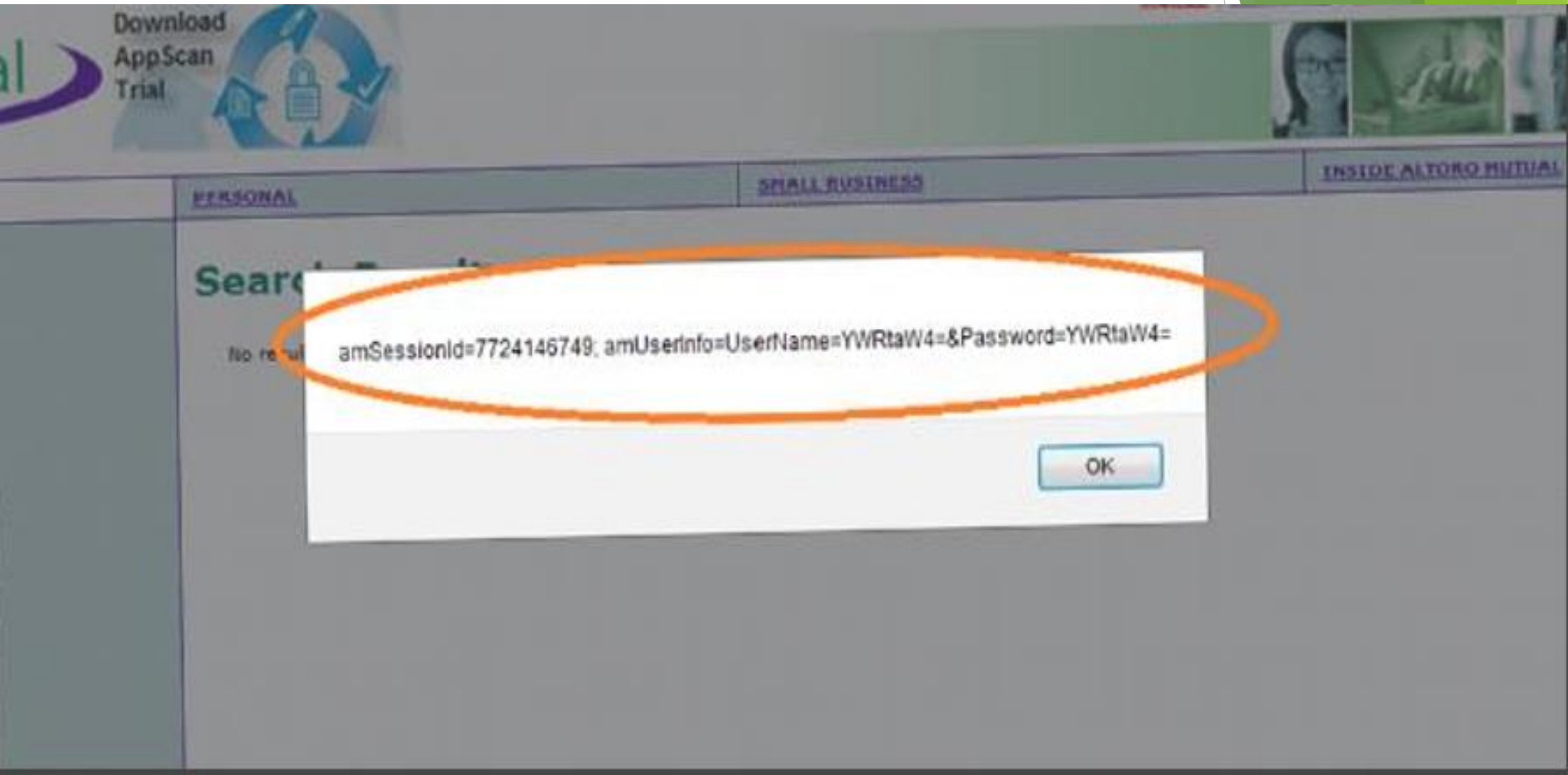
1. Credenciales débiles



2. Mecanismos débiles de encriptación



3. Debilidad ante ataques XSS



Mecanismos de Protección

- Mantener la IP y el explorador en la sesión. Esto permite chequear que los valores no cambien durante la misma sesión.
- Solicitar re-login para áreas y funcionalidades sensibles.
- Regenerar SessionID luego de un login exitoso sobre SSL.
- Utilizar SSL en toda la aplicación.

¿Cómo Protegernos?

- Usar SSL exclusivamente para todo acceso autenticado.
- Encriptar todas las credenciales y tokens para almacenarlos.
- No exponer datos sensibles en URLs o registros.
- Utilizar un único mecanismo de autentificación.
- Ser cuidadoso con el envío de contraseñas a direcciones de correo.
- Limitar o eliminar el uso de cookies para la autentificación o gestión de sesiones.
- No aceptar ID de sesión nuevos, preestablecidos o inválidos en URLs o peticiones.
- Crear una nueva sesión tras la autentificación o cambio de nivel de privilegio.