Manejo de la sesión

Sesión Hijacking

Un atacante logra extraer la cookie de sesión. Se puede obtener aprovechando las siguientes vulnerabilidades:

- Transmión de cookie por texto plano a través de medios inseguros
- Fijación de la sesión
- Inyección de javascript

Esto se puede mitigar tomando las siguientes medidas:

- No transmitir cookies a través de medios inseguros, usar HTTPS
- No permitir el acceso desde javascript a la cookie de sesión con el atributo HTTPOnly
- Hacer que la sesión caduque para evitar que la cookie pueda ser usada indefinidamente.

Session Fixation

Se trata de una vulnerabilidad que consiste en que el atacante consigue que el usuario se identifique con un identificador de sesión que el propio atacante ha generado. Suele seguir los siguientes pasos:

1. El atacante accede a la pagina de inicio de sesión
2. El servidor crea un identificador de sesión y se lo asigna a esa sesión
3. El atacante logra que la víctima abra una URL con el identificador de sesión que ha obtenido previamente

```
http://acme.com/<script>document.cookie=”sessionid=863F3D316”;</script>
http://acme.com/<meta http-equiv=Set-Cookie content=”sessionid=863F3D316”>
```

1. La victima usa dicho enlace para autenticarse, usando el identificador de sesión del atacante.
2. La victima usa sus credenciales y la sesión pasa a ser una autenticada
3. El atacante puede realizar acciones a nombre de la victima a conocer su identificador de sesión.

Para prevenir este tipo de ataques lo que se suele hacer es generar una nueva cookie de sesión cada vez que el usuario se autentica, de esta forma la cookie de sesión del atacante queda anulada tras la nueva autenticación.

Reescritura de URL

Muchos servidores envía en ID de sesión a través de la url de la siguiente forma:

```
http://www.acme.com/account.html;jsessionid=863F3D316
```

Esto se considera una vulnerabilidad, ya que hace que se pueda obtener la sesión por sustracción.

Esto se puede paliar evitando que este identificador de sesión pueda estar en la cabecera, debe ser tratado como si fuera una contraseña.