A++

Cookies encriptadas

María Victoria Calbet González
Marta Ramírez González
David Romero Esparraga
Jesús Ortiz Calleja
Guillermo Alcalá Gamero
Juan Carlos Utrilla Martín

Contenido

Las cookies de las tarjetas de crédito han sido encriptadas para mantener los datos de los usuarios seguros.

1. Procedimiento

Para realizar esta labor, se guardan los datos en cadenas de caracteres (tipo String en Java) y posteriormente, de almacenan en un array de bytes.

Una vez hecho eso se puede aplicar cualquier método criptográfico. En este caso se ha optado por un método de implementación propia para evitar excepciones inesperadas.

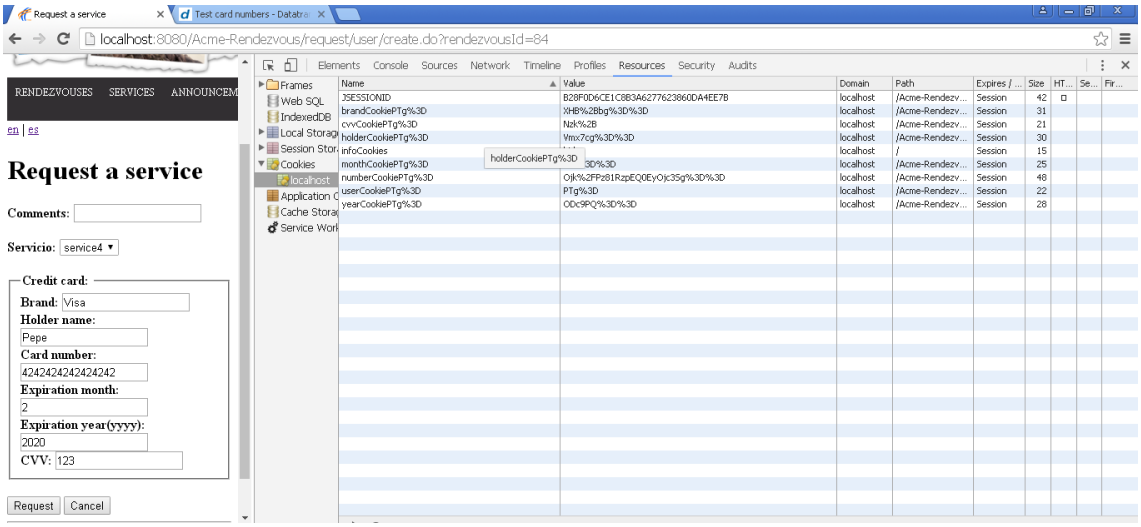
Dicho método consiste en recorrer el array de bytes y sumarle a cada byte un número pseudoaleatorio distinto. Este número es generado con un objeto de la clase Random de java.util, siendo inicializado con una semilla, en este caso la id del usuario. De esta forma, la secuencia de números es siempre la misma y se puede usar en el proceso de desencriptado. No es un método criptográfico muy robusto pero cumple su cometido. Quizás usando una semilla independiente del id del usuario o usando otro generador de números pseudoaleatorios.

Una vez encriptado, para evitar problemas de codificación con Java, se pasa el array de bytes a base64. Después, el nuevo array de bytes se transforma en un String, y por último, por compatibilidad con las cookies, los caracteres se codifican en un formato compatible con las URL usando la clase URLEncoder.

Así se ha procedido para encriptar. El desencriptado es un proceso análogo. Empezando desde el final; se decodifican los caracteres en formato URL con URLDecoder, se decodifica el String obtenido en un array de bytes usando base64, aplicar el método criptográfico de foma inversa, si antes se sumaban los número pseudoaleatorios, ahora se restan, obteniendo así el array de bytes desencriptado y por último, se transforman en el String que contiene los datos originales de forma inteligible.

Cabe destacar que aunque Spring tiene unas anotaciones para leer las cookies del navegador como parámetros en los métodos de los controladores, este método decodifica los caracteres de URL antes de tiempo provocando algunos fallos, por lo que se ha optado por leer las cookies usando la clase HttpServletRequest, además de usar HttpServletResponse para mandarlas, pues Spring no ofrece ningún mecanismo extra para enviar las cookies al navegador.

Para poder cargar en las cookies los datos de las tarjetas de crédito de varios usuarios, al nombre de los parámetros se ha añadido al final el id del usuario. De esa forma, cada uno de ellos tiene un nombre diferente e identificable.



La implementación de las cookies, así como el encriptado y desencriptado puede ser encontrado en el controlador RequestUserController.