Sobre las cookies

Las cookies de credit card han sido encriptadas para mantener los datos de los usuarios seguros.

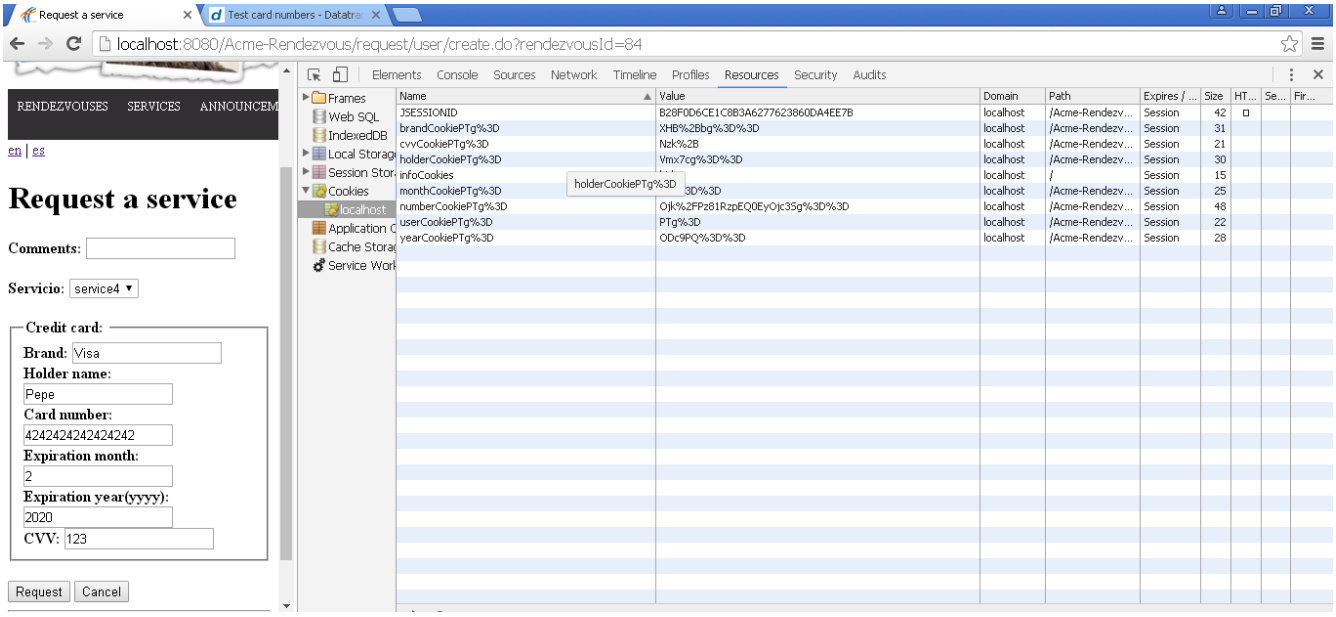
Para ello se pasan los datos a String y de ahí a array de bytes. Una vez hecho eso se puede aplicar cualquier método criptográfico; en este caso se ha optado por un método de implementación propia para evitar excepciones inesperadas, dicho método consiste en recorrer el array de bytes y sumarle a cada 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 usar otra semilla y generador de números aleatorios lo mejoraría.

Una vez encriptado, para evitar problemas de codificación con Java, se pasa el array de bytes a base64, 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, que desase lo anteriormente enumerado en orden inverso. Empezando desde el final; decodificar los caracteres en formato URL con URLDecoder, decodificar el String obenido 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 credit card de varios usuarios, al nombre de los parámetros se ha añadido al final la id del usuario, de esa forma cada uno de ellos tiene un nombre diferenciado e identificable.



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