Application Level Security in a Public Library: A Case Study

Richard Thomchick, Tonia San Nicolas-Rocca

Information Technology and Libraries, ISSN 2163-5226, Vol. 37, n. 4, 2018, p. 107-118

La privacidad de los usuarios es fundamental para los bibliotecarios, pero las nuevas tecnologías han supuesto que aparezcan nuevos desafíos para su protección. Hypertext Transport Protocol Secure (HTTPS) permite una comunicación segura a través de internet, pero en la práctica se ha demostrado que un hacker puede sabotearlo para conseguir los datos que busca. Este artículo analiza la implantación de sistemas HTTPS en aplicaciones de bibliotecas y sugiere formas en las que puedan evaluar y mejorar la seguridad y privacidad de sus usuarios. Para ello se utiliza una combinación de métodos heurísticos y automatizados que sirvieron para detectar vulnerabilidades en el sistema de una biblioteca universitaria de Estados Unidos. Los resultados mostraron que las debilidades de las aplicaciones de la web eran susceptibles de ser usadas por atacantes que podrían poner en peligro la seguridad de los usuarios. Lo primero que se detectó es que el protocolo HTTPS no se utiliza en toda la web, sino que debe ser introducido manualmente. Dentro de HTTPS también se pueden encontrar contenidos sin encriptar, por lo que también pueden ser fácilmente manipulados. El análisis también descubrió que la política de cookies de la biblioteca es incorrecta y permite que sean utilizadas para hackear sesiones. Transport Layer Security (TLS) es un protocolo para asegurar las comunicaciones en la web. La biblioteca no lo tiene implementado, por lo que la seguridad, privacidad e integridad de los datos de los usuarios pueden

verse afectadas. Los resultados del análisis son claros, pero debería hacerse un estudio más amplio en distintas bibliotecas para conocer el estado real de la cuestión.

Resumen elaborado por Antonio Rodríguez Vela