ESTUDIOS DE SEGURIDAD DE APLICACIONES WEB

Autor: José Luis Roca Blázquez
Directora: Milagros Fernández Gavilanes

I. INTRODUCCIÓN Y CONTEXTO

La seguridad en sistemas de información y comunicaciones es actualmente un factor de vital importancia para el correcto funcionamiento de estados, instituciones públicas y empresas privadas, afectando también de manera directa a ciudadanos de cualquier país desarrollado. En el mundo de los sistemas de información y para la provisión de una enorme cantidad de servicios se utiliza tecnología web. Las aplicaciones web, actualmente muy usadas y extendidas, son la cara visible de una cantidad ingente de servicios proporcionados por administraciones públicas y el sector empresarial a "clientes" de diversa naturaleza (otras estructuras de la administración, empresas, ciudadanos, servicios automatizados, etc.). Por ese motivo y por su necesidad de exposición constante y pública, las aplicaciones web constituyen un posible punto de entrada de ataque a los sistemas que las sustentan, ataques que pueden implicar violaciones de seguridad de diversa índole (vulneración de la confidencialidad de la información, denegación de servicio, instalación de *malware* persistente para enviar información al exterior de forma secreta o para instalar *malware* adicional…).

Las aplicaciones web tienen una serie de características que hacen que se les deba prestar una atención preferente, ya que en su interior albergan un conjunto de tecnologías muy diversas, cada una de las cuales es susceptible de contener algún tipo de error y vulnerabilidad. Las posibilidades de atacar un servicio web se multiplican cuanto mayor es el número de tecnologías usadas, pero no solo es este el posible origen de vulnerabilidades dado que las arquitecturas utilizadas, los diseños realizados y las implementaciones finales son fuentes de vectores de entrada a posibles atacantes. Una mala implementación de alguna función o una lógica de negocio errónea pueden provocar ataques de robo o modificación de datos, secuestro de información, ejecución remota de código, etc.

Así pues, las aplicaciones web, debido a la amplia extensión en su uso y a las características comentadas, se convierten en uno de los principales objetivos de agentes que intentan vulnerar su seguridad para conseguir una variedad de pretensiones.

Realizar un estudio de seguridad de una aplicación web no es tarea trivial. Es necesario tener conocimientos avanzados en diversos campos relacionados con los sistemas informáticos y las comunicaciones. También resulta imprescindible conocer metodologías adecuadas que permitan llevar a cabo los estudios de seguridad con un mínimo de orden, rigor y criterio. En el presente Trabajo se analizan diversos aspectos

relacionados con los estudios de seguridad de aplicaciones web, y se proponen posibles líneas de investigación futuras en ese campo.

II. DESARROLLO Y RESULTADOS

El desarrollo de este Trabajo de Fin de Máster (TFM) comprende 2 partes. En la primera se ha hecho un análisis del estado actual del mundo de la seguridad de aplicaciones web, incluyendo metodologías publicadas para realizar dichos estudios de seguridad. Esta parte incluye la definición de algunos conceptos básicos en ese campo, un análisis de las tendencias actuales en lo referente al desarrollo web — mencionando arquitecturas y tecnologías—, un repaso de posibles amenazas a las que están expuestas las aplicaciones web, algunos estudios y trabajos realizados hasta el momento respecto al tema del Trabajo y herramientas usadas habitualmente.

En la segunda parte se han aplicado los conocimientos adquiridos para ponerlos en práctica en un laboratorio virtual con varias máquinas de prueba que contienen servicios web de varios tipos con distintas vulnerabilidades. En particular se han usado las herramientas descritas en la primera parte, y se ha explicado su funcionamiento, indicando cómo se manejan y cómo se extrae información de ellas, de tal manera que se pueda dar una idea suficiente de su utilidad, aunque sin intentar realizar un manual completo de su manejo. Se ha seguido una secuencia idéntica a la que seguiría cualquier profesional para hacer un estudio de seguridad de un sistema de servicios web. En particular, se han ejecutado los pasos en el orden lógico y habitual, descubriendo primero la infraestructura existente, obteniendo la mayor información posible sobre tal infraestructura, analizando las posibles vulnerabilidades en función de la información obtenida y posibilitando la explotación de dichas vulnerabilidades de la manera que se desee (para obtener información, infiltrarse de manera temporal o permanente en el sistema, hacer denegaciones de servicio, alterar y falsear información…). En todos los pasos se han ido obteniendo informes intermedios que, eventualmente, se acabarían fundiendo en un informe final.

Se han llevado a cabo las dos primeras fases de las pruebas de seguridad habituales, es decir, la de recopilación de información y la de descubrimiento de vulnerabilidades. No se ha llevado a cabo la fase de explotación de vulnerabilidades, por quedar fuera de los objetivos del presente Trabajo.

Como resultado de la parte práctica de este Trabajo sobre el laboratorio de máquinas virtuales se han obtenido resultados interesantes. Se han descubierto diferentes vulnerabilidades que son típicas de los servidores que albergan aplicaciones web, y para ello se han empleado herramientas de distinto tipo: por una parte, herramientas sencillas pero muy potentes que requieren una preparación y ejecución minuciosa y suponen un proceso manual muy controlado por el profesional de la seguridad. Por otra parte, se han usado aplicaciones más completas que reúnen funcionalidades de las herramientas sencillas y facilitan el trabajo, aunque hasta cierto punto esconden demasiado los procesos internos realizados y hacen que se pierda la visión general de la ejecución de los estudios de seguridad de aplicaciones web. En conjunto se ha seguido todo el

proceso de descubrimiento de información y de vulnerabilidades y se ha explicado paso a paso cómo se ha ejecutado, lo cual debe ayudar a dar una idea de cómo se realizan los estudios de seguridad objetos de estudio de este Trabajo.

III. CONCLUSIONES

Se ha constatado que el estudio de seguridad de un servicio web contempla muchísimos aspectos y requiere conocimientos de muchos campos de las comunicaciones y sistemas de información. Para realizar tales estudios existen por una parte herramientas individuales que llevan a cabo parte de las distintas fases, y que, no obstante, tienen capacidades bastante potentes, y por otra parte *suites* más complejas que reúnen las funcionalidades de varias herramientas individuales.

No existe una guía completa y clara sobre cómo realizar estudios de seguridad de aplicaciones web. Hay distintas metodologías que abarcan estudios y auditorías y que proporcionan marcos y guías de trabajo, pero no una lista clara de pasos a seguir, con una secuencia de acciones e indicaciones sobre qué hacer en cualquier estudio de seguridad. A pesar de la existencia de *suites* integradas que realizan muchas acciones y facilitan el trabajo, siempre es necesaria la intervención humana para analizar los resultados que se van obteniendo y para decidir en cada momento qué hacer en función de tales resultados. Por ello resulta complicado hacer una lista de pasos y acciones completa y universal. También resulta difícil automatizar completamente todo el proceso.

Actualmente las técnicas de inteligencia artificial y *machine learning* están en pleno desarrollo, y no es descartable que en futuro puedan emplearse para los estudios de seguridad de aplicaciones web. Hay formas de hacer que las máquinas aprendan con la experiencia, igual que hace un humano. Se podrían alimentar los sistemas de inteligencia artificial con las bases de datos de las últimas vulnerabilidades, con miles de casos de sistemas explotados, con los pasos seguidos por los profesionales en sus estudios y con los propios *exploits* existentes, para que aprendieran de todo ello. Es posible que finalmente se llegara a tener un sistema que pudiera realizar el trabajo de un profesional actual, e incluso que fuera capaz de detectar vulnerabilidades que pasarían desapercibidas a seres humanos que hicieran esa tarea. En cualquier caso, se podrían usar en el futuro técnicas híbridas en las que intervengan seres humanos y sistemas de inteligencia artificial.