Ethical Hacking for Web Application

Karen Elizabeth Salazar Carpio
Universidad Mayor de San Andrés
Carrera de Informática
Análisis y Diseño de Sistemas de Información
sc_eliza@hotmail.com

RESUMEN

Hacking Ético consiste en un testeo de seguridad controlada en los sistemas informáticos de una empresa, de la misma forma que lo haría un intruso o pirata informático pero de forma ética, previa autorización de un convenio de confidencialidad por escrito. El resultado es un informe donde se identifican los sistemas en los que se ha logrado penetrar y la información confidencial y/o secreta conseguida.

Los sitios web se han convertido en el talón de Aquiles de la seguridad informática, los atacantes están intensamente enfocados en atacar aplicaciones web para así infectar las máquinas de los usuarios finales y están poniendo a las empresas en contra de sus propios clientes en sus constantes esfuerzos por robar datos personales de los consumidores.

Términos Generales

Hackers éticos, vulnerabilidad en los sistemas de ciertas entidades.

Palabras Clave

Seguridad, aplicaciones, web, hacker

1. INTRODUCCION

Durante el proceso de pruebas de seguridad de una aplicación web, se suele tener la falsa concepción de que la revisión automatizada es eficiente y efectiva, es así como muchos testers y pentesters suelen anteponer y priorizar los resultados devueltos por scanners de vulnerabilidades en aplicaciones web sobre la inspección manual, con esto no se pretende de ninguno modo desestimar la labor que desempeñan dichas herramientas como scanners y frameworks de penetración, solamente que es necesario comprender que dichas herramientas tienen sus propias limitaciones y que no se puede esperar que una utilidad que ha sido creada para aplicaciones genéricas funcione del mismo modo para aplicaciones con un alto nivel de personalización. Dadas estas premisas, está claro que el uso de las herramientas no es suficiente para afrontar el reto que implica desplegar una aplicación web segura, es necesario que la persona responsable y el equipo involucrado tenga conocimientos de las técnicas sobre el testing de una aplicación web.

2. ANATOMIA DE UNA APLICACIÓN WEB

Una aplicación web típica se ilustra en el siguiente diagrama (Véase Fig. 1). Los componentes mostrados pueden residir en la misma computadora, o más a menudo en distintas computadoras que existan en distintos lugares dentro de una red.

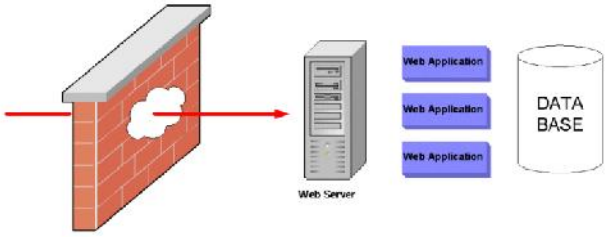

Figura 1. Arquitectura típica para una aplicación web

Una vez que se ha tomado la decisión de permitir el acceso HTTP(Hypertext Transfer Protoco o Protocolo de Transferencia de Hipertexto) al servidor web, muy poco se puede hacer para evitar que un atacante intentar "hackear" la aplicación web.

Los ataques a las aplicaciones Web se realizan sobre HTTP y se consideran aceptables para el tráfico de firewall / filtro. La introducción de SSLv2(es un Protocolo Criptográfico o de cifrado que se utiliza para dar conexiones seguras “no interceptables” en Internet) no hace nada para impedir los ataques y da al atacante la comodidad.

3. MOTIVACIONES PARA EL HACKING DE APLICACIONES WEB

Es importante señalar algunas de las características de las aplicaciones web que las hacen tan atractivas para los atacantes.

Ubicuidad:
Las aplicaciones web están en casi todas partes hoy en día y siguen extendiéndose rápidamente a través de redes públicas y privadas. Para los hackers de aplicaciones web la probabilidad de encontrar una aplicación "jugosa" y vulnerable es cada vez mayor.

Anonimato:
El Internet todavía tiene muchas regiones no catalogadas o auditadas, y es bastante fácil para lanzar ataques con poco o sin temor de ser rastreado. El rastro del Web Hacking, en particular, es de fácil lavado (y a menudo sin darse cuenta) a través de proxys HTTP/S que son abundantes en la Red. Hackers sofisticados enrutan cada solicitud a través de un proxy diferente para hacer las cosas aún más difíciles de rastrear. Sin duda, ésta sigue siendo la razón principal para la proliferación del hacking malicioso, ya que el anonimato protege al atacante de uno de los principales factores de disuasión en el mundo físico (es decir, ser atrapado y castigado).

Incapacidad de los Firewalls:
El HTTP/S entrante (puertos 80 y 443) es permitido por todos los cortafuegos o firewalls. Es un comportamiento necesario para poder recibir las solicitudes de los navegadores clientes. Inclusive esto seguirá sucediendo a pesar de que cada vez más aplicaciones emigren a la Web.

Código personalizado:
Con la proliferación de plataformas para facilitar el desarrollo web como ASP.NET y LAMP (Linux / Apache / MySQL / PHP), una gran parte de las aplicaciones web son ensambladas por desarrolladores que tienen poca o ninguna experiencia previa en seguridad de aplicaciones.

4. PAGAR PARA HACKEAR SU PROPIA APLICACIÓN O SITIO WEB

Para poner a prueba un sistema de seguridad, los hackers éticos utilizan los mismos métodos que sus hermanos maliciosos (Véase Fig. 2), pero los problemas descubiertos se informan a su cliente en lugar de aprovecharse de ellos.

Figura 2. Web Hacking

Los servicios de Ethical Hacking de Aplicaciones Web son:

- ✓ Identificar vulnerabilidades resultado de errores de diseño y programación de Aplicaciones Web.
- ✓ Conocer las debilidades de sus aplicaciones Web, cuya vulneración puede ocasionar daños de alto impacto para su negocio.
- ✓ Obtener un plan de acción para la remediación de sus vulnerabilidades, clasificadas según su nivel de riesgo.
- ✓ Obtener informes técnicos libres de falsos positivos, sustentados con la evidencia obtenida durante el proceso de evaluación.
- ✓ Certificar el pase a producción de sus aplicaciones Web[3].

Un ejemplo de las miles que existen es la empresa Veracode[4] realiza tanto el análisis de código estático, dinámico y encuentra las vulnerabilidades de seguridad, tales como el código malicioso o cifrado suficientes que puedan dar lugar a violaciones de seguridad.

5. HACKERS DESARROLLARON APLICACIONES WEB

La aplicación denominada *Civicmap*, los jóvenes Juan Sebastián Duque, Juan Camilo Bejarano, Gustavo Núñez y Henry Rodríguez (Vease Fig. 3), fueron escogidos como ganadores de la 'Hackathon', una actividad organizada por el Banco Mundial y el Gobierno, en la que por más de 28 horas cien jóvenes desarrollaron ideas como esta, reunidos en el Centro Cultural de Cali, Colombia el lunes 6 de mayo del 2013.[6]

Figura 3. Ganadores de "Hackathon"

El grupo ganador de la final será llevado a Londres a una feria de emprendimiento empresarial. En total se desarrollaron nueve aplicaciones en Cali, con temáticas como movilidad, seguridad y cultura.

La escogida en segundo lugar fue una aplicación llamada *Ciclomundo*, que informa a los ciclistas sobre cuáles son las calles más seguras para transitar con sus bicicletas y en qué lugares hay parqueaderos para sus vehículos. "Destacamos mucho que es una idea que promueve un hábito saludable como es andar en bicicleta", aseguró Johanna Pimiento, directora de Gobierno en Línea a nivel nacional. Otra de las aplicaciones desarrolladas por los jóvenes es 'Taxi seguro', que busca que mediante un 'botón de pánico' los taxistas puedan reportar a la Policía un atraco, y a su vez, que los usuarios puedan calificar el servicio brindado por un conductor.

.

6. CONCLUSIÓN

En el mundo de la seguridad de las aplicaciones, el hacking ético en línea toma la forma de pruebas de penetración. "Las pruebas de penetración" se realizan en escenarios tan realistas como sea posible para asegurar los resultados de reproducir fielmente lo que un intruso podría potencialmente alcanzar. La comprensión de los factores de motivación para el Hacking de la Aplicaciones Web conducirá a una perspectiva mucho más clara de las defensas que deben ser adoptadar para mitigar el riesgo.

Lo importante es que la gente que sea experta en ciertos temas, utilice su talento para cosas buenas, porque hay muchas problemáticas que hoy se pueden resolver con aplicaciones informáticas.

7. REFERENCIAS

[1] *Hacking Ético para aplicaciones Web*. Autor: TalSoft TS S.R.L. Disponible en: http://www.talsoft.com.ar/index.php/servicios/seguridad-informatica/testeo-de-seguridad-para-aplicaciones-web

[2] *Motivaciones para el Hacking de Aplicaciones*. Autor: Mauro Maulini R. Disponible en: http://www.e-securing.com/novedad.aspx?id=83

[3] *Ethical Hacking de Aplicaciones Web*. Autor: BINAR10. Disponible en: http://binar10.com/pentest/pentest-webapp

[4] *Veracode secures the world's software*. Autor: VERACODE. Disponible en: http://www.veracode.com/#

[5] *Web Application Hacking*. SensePost Research. Disponible en: research@sensepost.com

[6] Hackers desarrollaron aplicaciones web para solucionar problemas de ciudad. Disponible en: http://www.elpais.com.co/elpais/cali/noticias/hackers