Visita a una conferencia internacional de hackers

OWASP Global AppSec Ámsterdam

Willem L. Middelkoop
Sep. 27, 2019

Este mes tuve la suerte de asistir a Global AppSec Amsterdam, una conferencia internacional para hackers y especialistas en seguridad. Hubo presentaciones de exagentes de inteligencia, cazadores de recompensas, académicos y vendedores de software. Aprendí sobre algunas de las técnicas de hacking más recientes, conocí a gente interesante y jugué algunos juegos retro geniales. Sigue leyendo para más información.

Fundación OWASP y Global AppSec Amsterdam

La Fundación OWASP es una organización sin ánimo de lucro dedicada a crear herramientas, documentación, foros y conferencias en torno a la seguridad del software. OWASP

es especial porque está libre de presiones comerciales, no está afiliada a ninguna empresa de tecnología. Abogan por abordar la seguridad de las aplicaciones como un problema de personas, procesos y tecnología, porque los enfoques más efectivos para la seguridad de las aplicaciones incluyen mejoras en todas estas áreas. Se puede encontrar más información sobre OWASP en `https://www.owasp.org`.

Los eventos Global AppSec se organizan en todo el mundo. Este septiembre hubo un evento de este tipo en mi ciudad natal, Ámsterdam. Consulta su programa para saber si OWASP llega a tu ciudad.

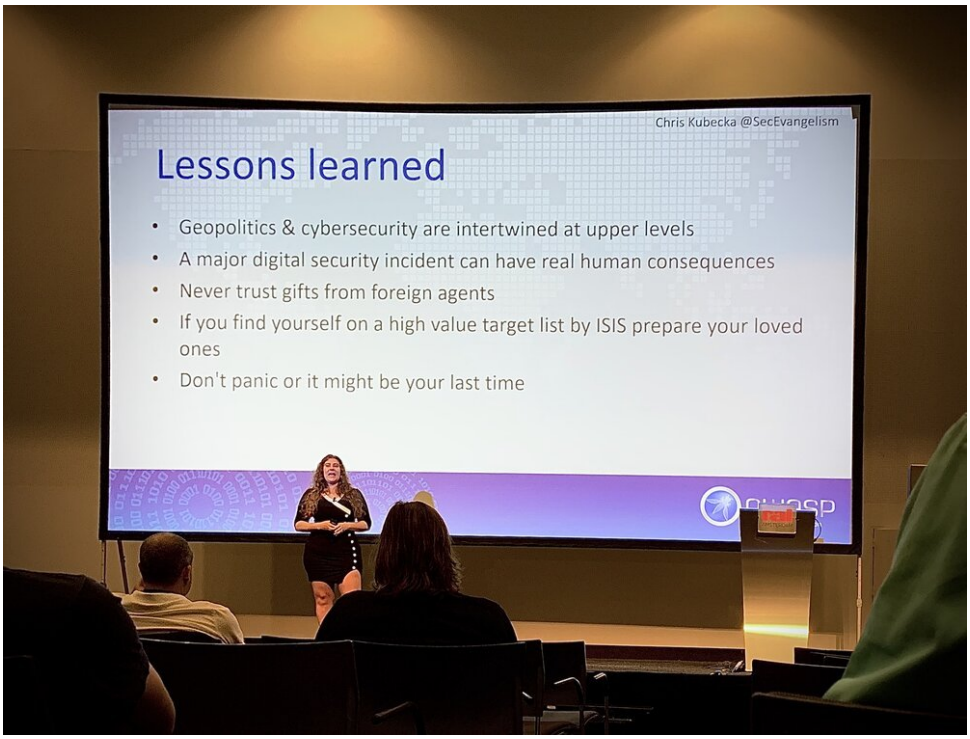
Global AppSec-Ámsterdam

Cuando la ciberseguridad se vuelve real: Aplastando terroristas

Una de las historias más impresionantes fue contada por Chris Kubecka, una mujer que ha trabajado para la Fuerza Aérea de los EE. UU. y el Comando Espacial de los Estados Unidos. Es investigadora de seguridad informática y especialista en guerra cibernética.

Presentación magistral del especialista en guerra cibernética, Chris Kubecka

Habla sobre su trabajo en la Embajada Real de Arabia Saudita en La Haya. Es muy interesante aprender cómo la policía local, el Cuerpo Diplomático y agentes especiales participaron para finalmente prevenir un ataque con bomba en el Kurhaus de Scheveningen. ¡Es cuando escuchas estas historias que te das cuenta de que no todo lo que sucede aparece en las noticias!



Lecciones aprendidas al tratar con terroristas

Café y juegos

Después de la charla magistral sobre terroristas, guerra cibernética y ataques con bombas, llegó el momento del café y los juegos. Jugar juegos retro es una forma divertida de conocer a otros hackers en la conferencia, ya que tendrás algo obvio en común de lo que hablar. Eso es útil, ya que la mayoría de los expertos en TI necesitan un poco de ayuda para romper el hielo cuando se trata de socializar...

Café y PONG en la videoconsola con monitor CRT

DuckHunt con una pistola Zapper original de Nintendo

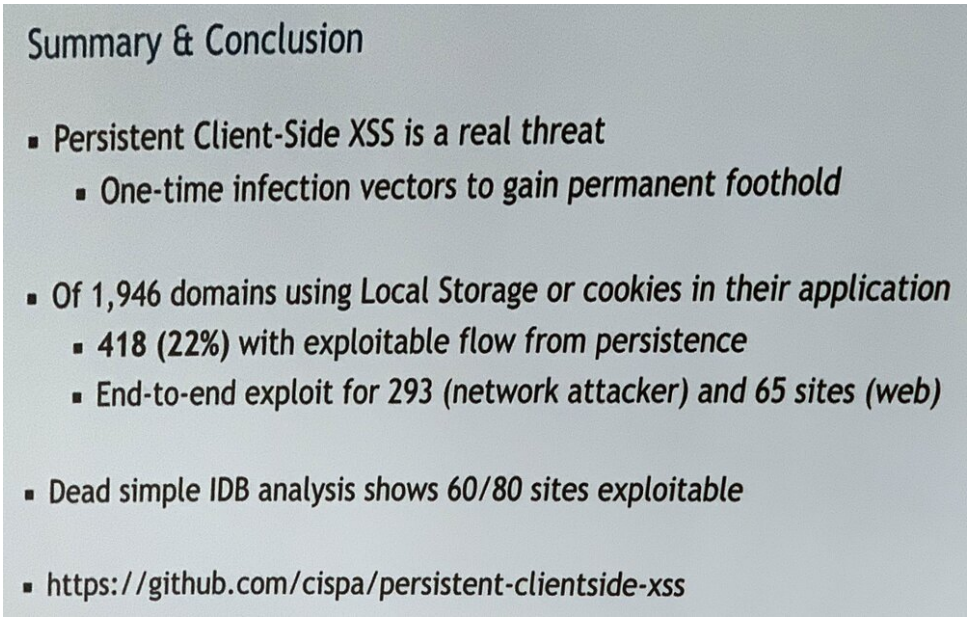
¿Recuerdas los días en que este era tu ordenador promedio? - nota: el teclado IBM modelo M... ¡vaya!

Técnicas de hacking

Después del café, hubo varias sesiones a las que se podía asistir. Seleccioné algunas en función de mis intereses personales y mi trabajo.

XSS persistente del lado del cliente

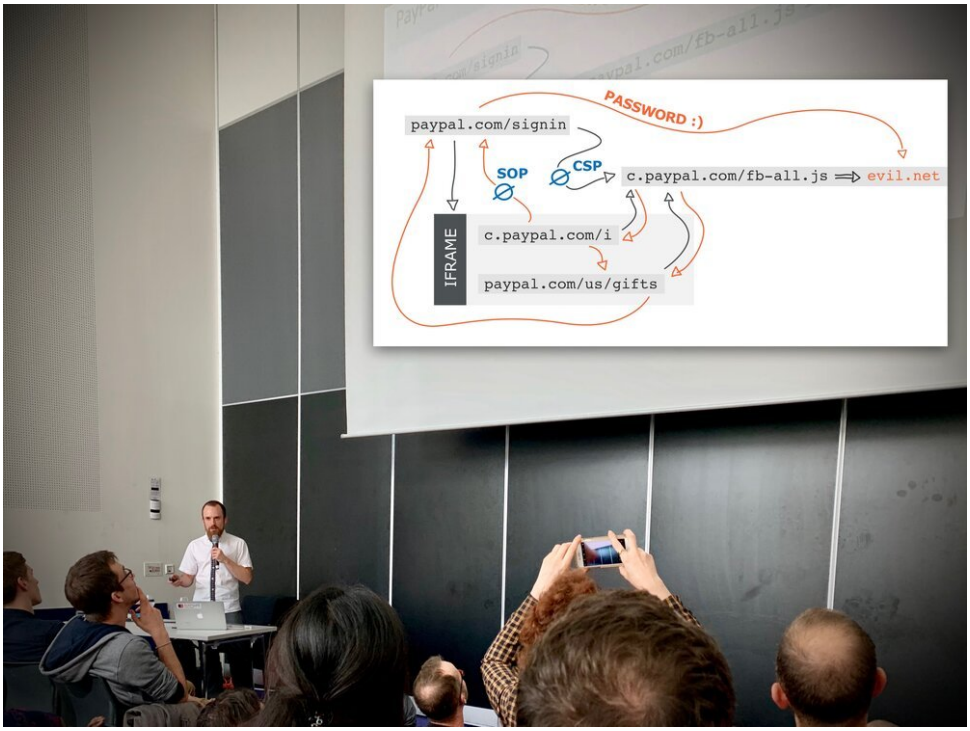
Una de las charlas a las que asistí trató sobre atacar sitios web utilizando almacenamiento local o cookies. Acertadamente llamada "No confíes en los locales", la presentación de Marius Steffens y Ben Stock fue muy interesante. ¡Su investigación académica reveló que muchos sitios web son vulnerables a amenazas que ganan un punto de apoyo permanente!



XSS persistente del lado del cliente es una amenaza real - por Marius Steffens y Ben Stock

Hackear PayPal usando un ataque de desincronización HTTP

En su brillante charla, James Kettle describe su investigación sobre posiblemente una de las técnicas de hacking más peligrosas en la web moderna: Ataque de desincronización HTTP por desincronización de solicitudes HTTP. Esta técnica utiliza vulnerabilidades cuando un sitio web utiliza una red de entrega de contenido (CDN), una caché web o un firewall de aplicaciones web (WAF). Es asombroso aprender sobre esto, comprender el principio subyacente y aprender a defenderse contra este tipo de ataque.



James Kettle sobre hackear PayPal - obteniendo $38,900 en recompensas

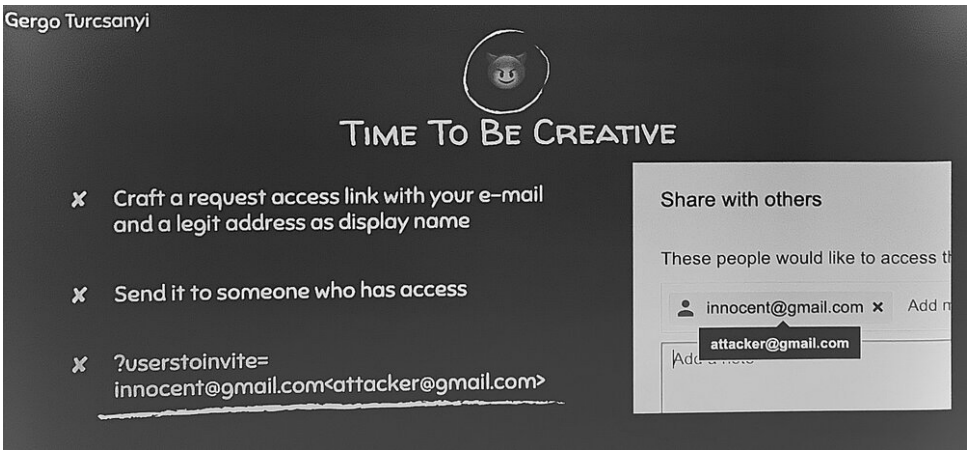
Economía del hacking: ¿cuánto vale una cuenta hackeada?

En otra charla interesante, Jarrod Overson explica el estado de los ataques de relleno de credenciales. Este tipo de ataque implica el uso de nombres de cuenta y contraseñas filtrados en diferentes sitios web, lo cual tiene un éxito sorprendente, ya que muchas personas usan la misma contraseña en diferentes sitios. Explica cómo evitar los CAPTCHAS y cómo los hackers hacen que su malware imite el comportamiento humano para cometer fraude. Concluye que el fraude es un problema humano, no técnico, impulsado por una simple economía: ¡vale la pena hackear!

¡Hackear las tasas de retorno de la inversión entre un 100% en el extremo inferior y un 150,000% en el extremo superior! (Por Jarrod Overson)

Mentalidad de hacker

En su charla, Gergö Turcsányi habla sobre cómo se convirtió en un cazador de recompensas. Explica que no necesitas ser un matemático increíblemente hábil para hacer esto, todo lo que necesitas es un poco de creatividad y algo de tiempo para investigar. ¡Eventualmente, esto lo llevó a hackear Google con éxito!

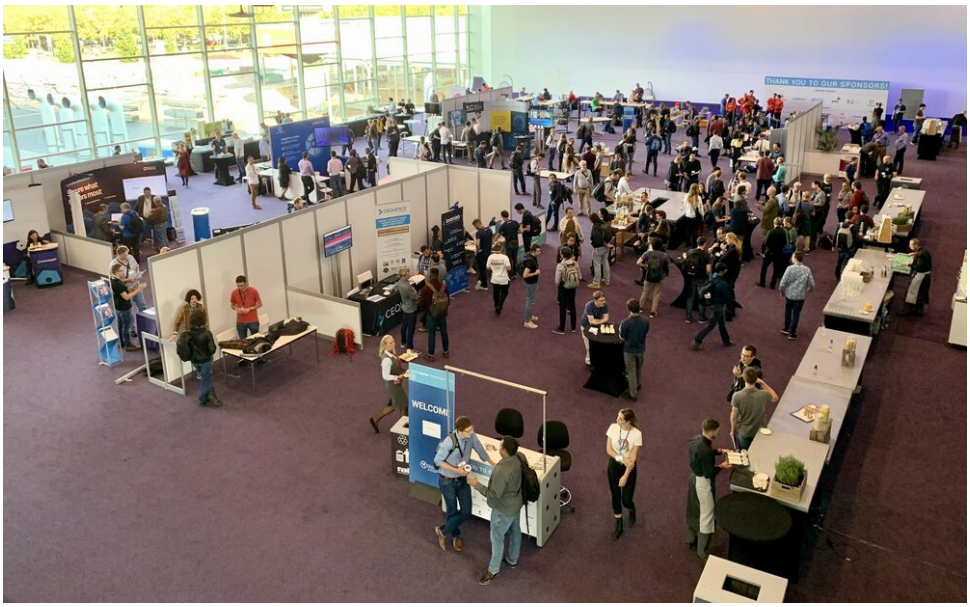


Hackeando Google - Cómo podría haber robado tus fotos de Google (Gergö Turcsányi)

Conclusión

¡Visitar Global AppSec fue fantástico! Es un privilegio conocer a otros hackers, aprender de ellos y escuchar sobre las cosas que normalmente no se ven en las noticias.

Independientemente de lo que te lleves de una conferencia, siempre habrá algo que no esperabas aprender. ¡Es este aprendizaje inesperado lo que hace que valga la pena el esfuerzo de asistir a conferencias!



Global AppSec Ámsterdam