Besuch einer internationalen Hackerkonferenz

OWASP Global AppSec Amsterdam

Willem L. Middelkoop
Sep. 27, 2019

Diesen Monat hatte ich das Glück, an der Global AppSec Amsterdam teilzunehmen, einer internationalen Konferenz für Hacker und Sicherheitsexperten. Es gab Präsentationen von ehemaligen Geheimdienstmitarbeitern, Bug-Bounty-Jägern, Akademikern und Softwareanbietern. Ich habe etwas über die neuesten Hacking-Techniken gelernt, interessante Leute getroffen und ein paar coole Retro-Spiele gespielt. Lesen Sie weiter für mehr.

OWASP Foundation und Global AppSec Amsterdam

Die OWASP Foundation ist eine gemeinnützige Organisation, die sich der Entwicklung von Tools, Dokumentation, Foren und Konferenzen rund um die Software-Sicherheit wid-

met. OWASP ist besonders, weil es frei von kommerziellem Druck ist und keiner Technologiefirma angeschlossen ist. Sie befürworten die Betrachtung der Anwendungssicherheit als ein Problem von Menschen, Prozessen und Technologien, da die effektivsten Ansätze zur Anwendungssicherheit Verbesserungen in all diesen Bereichen umfassen. Mehr über OWASP finden Sie auf `https://www.owasp.org`.

Die Global AppSec-Veranstaltungen werden auf der ganzen Welt organisiert. Diesen September fand eine solche Veranstaltung in meiner Heimatstadt Amsterdam statt. Schauen Sie sich ihren Terminplan an, um herauszufinden, ob OWASP auch in Ihre Stadt kommt.

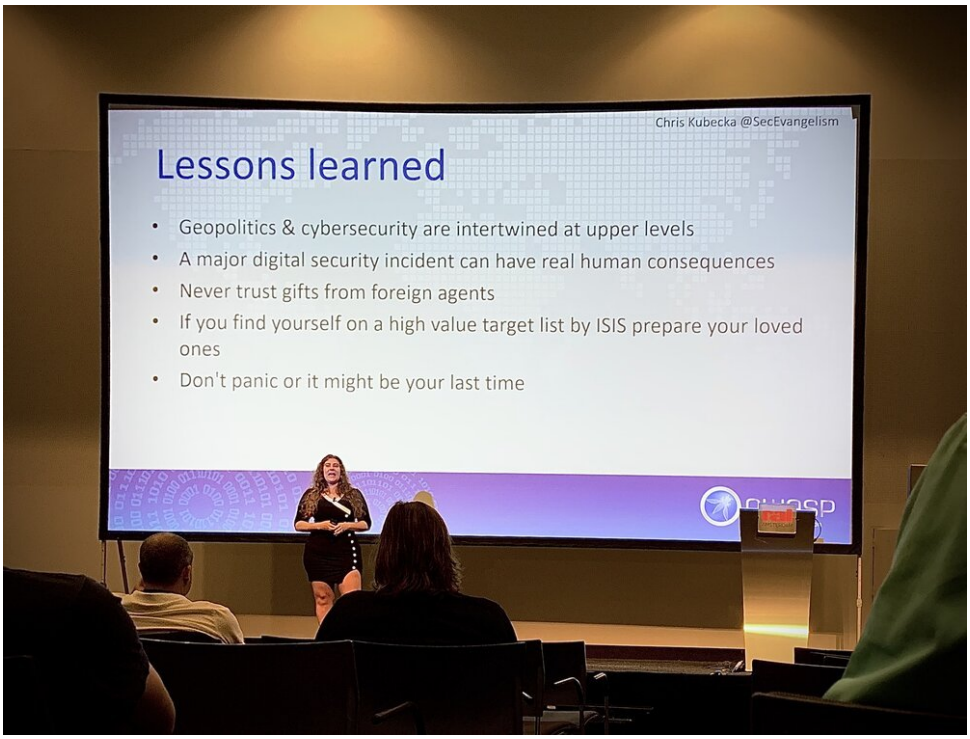
Global AppSec-Amsterdam

Wenn Cybersicherheit real wird: Terroristen ausschalten

Eine der beeindruckendsten Geschichten wurde von Chris Kubecka erzählt, einer Frau, die für die US Air Force und das United States Space Command gearbeitet hat. Sie ist Computersicherheitsforscherin und Spezialistin für Cyberkriegsführung.

Keynote-Präsentation von Cyberkriegsspezialistin Chris Kubecka

Sie spricht über ihre Arbeit in der Königlich-Saudischen Botschaft in Den Haag. Es ist sehr interessant zu erfahren, wie die örtliche Polizei, das diplomatische Korps und Spezialagenten beteiligt waren, um letztendlich einen Bombenanschlag auf das Kurhaus in Scheveningen zu verhindern. Wenn man diese Geschichten hört, wird einem klar, dass nicht alles, was passiert, in den Nachrichten erscheint!



Lektionen im Umgang mit Terroristen

Kaffee und Spiele

Nach der Keynote über Terroristen, Cyberkriegsführung und Bombenanschläge war es Zeit für Kaffee und Spiele. Retro-Spiele zu spielen ist eine unterhaltsame Möglichkeit, andere Hacker auf der Konferenz zu treffen, da man ein offensichtliches gemeinsames Thema hat, über das man sprechen kann. Das ist nützlich, da die meisten IT-Experten ein wenig Hilfe brauchen, um das Eis zu brechen, wenn es um soziale Kontakte geht...

Kaffee und PONG auf der Videospielkonsole mit Röhrenmonitor

DuckHunt mit einem originalen Nintendo Zapper

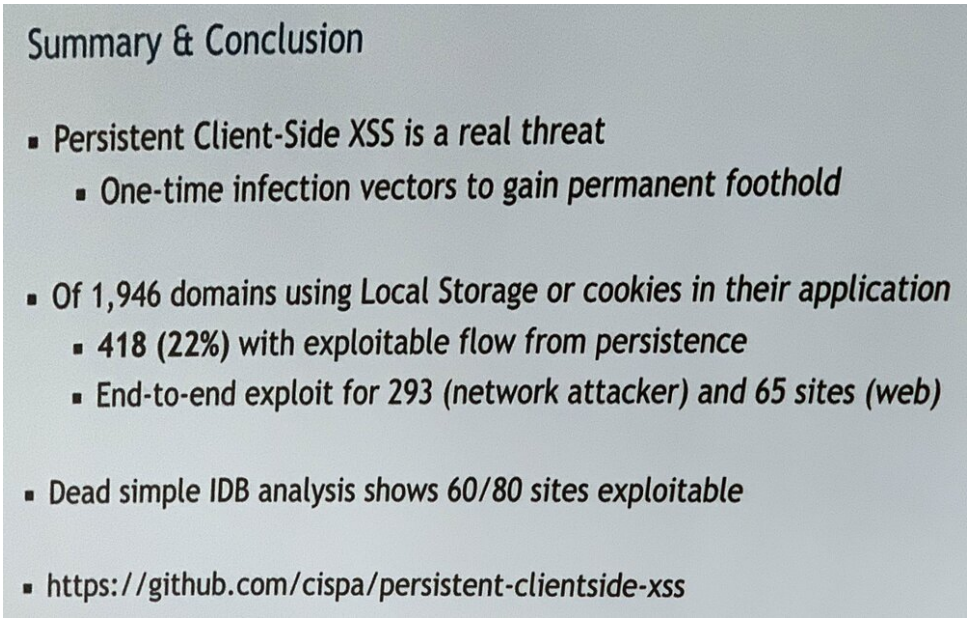
Erinnern Sie sich an die Tage, als dies Ihr durchschnittlicher Computer war - Achtung: die IBM Model M Tastatur... oh Mann!

Hacking-Techniken

Nach dem Kaffee gab es mehrere Sessions, an denen man teilnehmen konnte. Ich habe einige basierend auf meinen persönlichen Interessen und meiner Arbeit ausgewählt.

Persistentes clientseitiges XSS

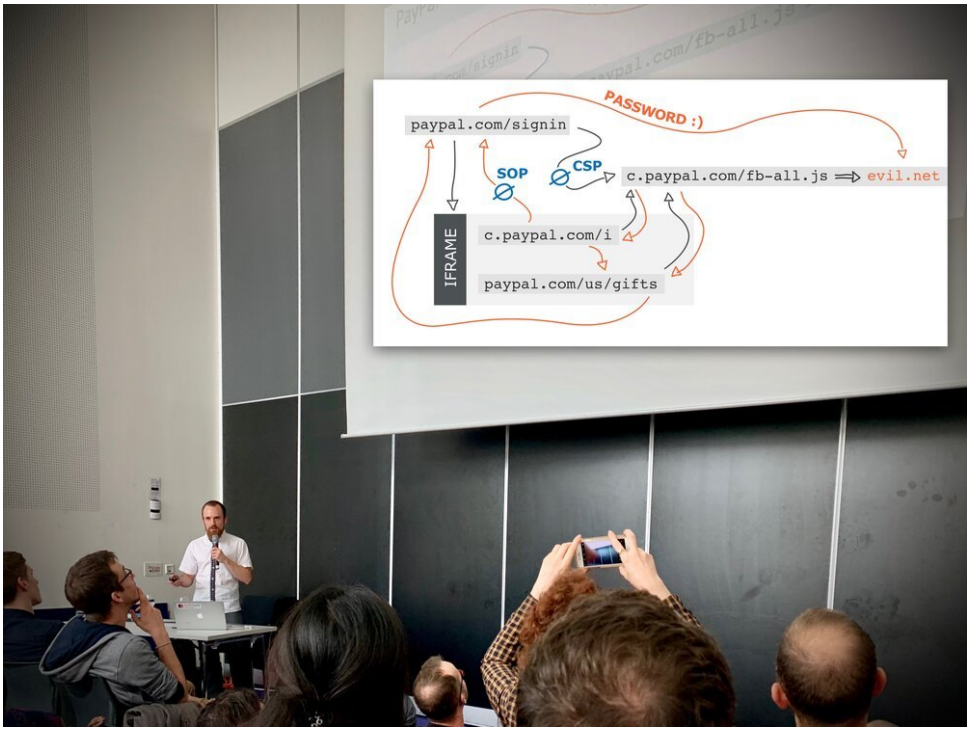
Einer der Vorträge, die ich besucht habe, befasste sich mit dem Angriff auf Websites mithilfe von Local Storage oder Cookies. Treffend "Don't trust the locals" genannt, war die Präsentation von Marius Steffens und Ben Stock sehr interessant. Ihre akademische Forschung ergab, dass viele Websites anfällig für Bedrohungen sind, die dauerhaft Fuß fassen!



Persistentes clientseitiges XSS ist eine echte Bedrohung - von Marius Steffens und Ben Stock

Hacking von PayPal mittels HTTP-Desync-Angriff

In seinem brillanten Vortrag beschreibt James Kettle seine Forschung zu einer der möglicherweise gefährlichsten Hacking-Techniken im modernen Web: HTTP Request Smuggling durch Desynchronisierung von HTTP-Anfragen. Diese Technik nutzt Schwachstellen aus, wenn eine Website ein Content Delivery Network (CDN), einen Web-Cache oder eine Web Application Firewall (WAF) verwendet. Es ist erstaunlich, davon zu erfahren, das zugrunde liegende Prinzip zu verstehen und zu lernen, wie man sich gegen diese Art von Angriff verteidigt.



James Kettle hackt PayPal - und erhält 38.900 $ an Prämien

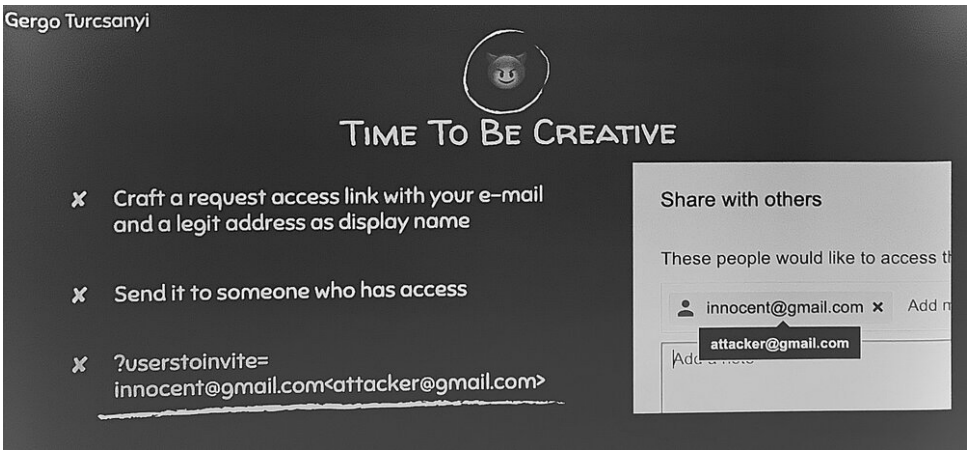
Hacking-Ökonomie: Was ist ein gehackter Account wert?

In einem weiteren interessanten Vortrag erklärt Jarrod Overson den Stand der Credential Stuffing Angriffe. Bei dieser Art von Angriff werden durchgesickerte Accountnamen und Passwörter auf verschiedenen Websites verwendet, was überraschend erfolgreich ist, da viele Leute dasselbe Passwort auf verschiedenen Websites verwenden. Er erklärt, wie man CAPTCHAS umgeht und wie Hacker ihre Malware dazu bringen, menschliches Verhalten für Betrug zu imitieren. Er kommt zu dem Schluss, dass Betrug ein menschliches Problem ist, kein technisches - angetrieben durch einfache Ökonomie: Es lohnt sich zu hacken!

Hacking von Renditen bei Investitionen zwischen 100 % im unteren Bereich und 150.000 % im oberen Bereich! (Von Jarrod Overson)

Hacker-Mentalität

In seinem Vortrag spricht Gergö Turcsányi darüber, wie er Kopfgeldjäger wurde. Er erklärt, dass man kein unglaublich begabter Mathematiker sein muss, um dies zu tun, alles, was man braucht, ist ein wenig Kreativität und etwas Zeit zum Herumstöbern. Schließlich führte ihn dies dazu, Google erfolgreich zu hacken!

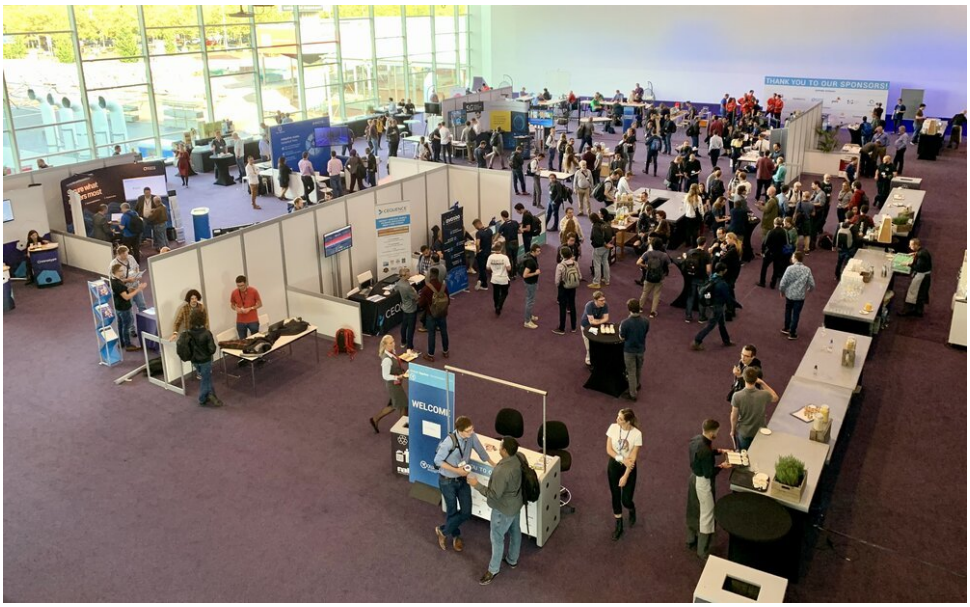


Google hacken - Wie ich Ihre Fotos von Google hätte stehlen können (Gergö Turcsányi)

Fazit

Der Besuch der Global AppSec war fantastisch! Es ist ein Privileg, andere Hacker zu treffen, von ihnen zu lernen und über Dinge zu hören, die man normalerweise nicht in den Nachrichten sieht.

Was auch immer man von einer Konferenz mitnimmt, es wird immer etwas geben, das man nicht erwartet hat zu lernen. Es ist dieses unerwartete Lernen, das den Besuch von Konferenzen sehr lohnenswert macht!



Global AppSec Amsterdam