Het bezoeken van een internationale hackersconferentie

OWASP Global AppSec Amsterdam

Willem L. Middelkoop
27 sep. 2019

Deze maand had ik het geluk om Global AppSec Amsterdam bij te wonen, een internationale conferentie voor hackers en beveiligingsspecialisten. Er waren presentaties van voormalige geheim agenten, bounty hunters, academici en softwareleveranciers. Ik leerde over enkele van de nieuwste hacktechnieken, ontmoette interessante mensen en speelde een paar coole retro games. Lees verder voor meer.

OWASP Foundation en Global AppSec Amsterdam

De OWASP Foundation is een non-profitorganisatie die zich toelegt op het creëren van tools, documentatie, forums en conferenties rond softwarebeveiliging. OWASP is speciaal omdat het vrij is van commerciële druk en niet gelieerd is aan een technologiebedrijf.

Ze pleiten ervoor om applicatiebeveiliging te benaderen als een probleem van mensen, processen en technologie, omdat de meest effectieve benaderingen van applicatiebeveiliging verbeteringen in al deze gebieden omvatten. Meer over OWASP is te vinden op https://www.owasp.org.

De Global AppSec-evenementen worden over de hele wereld georganiseerd. Afgelopen september was er zo'n evenement in mijn woonplaats Amsterdam. Bekijk hun schema om te zien of OWASP ook naar jouw stad komt.

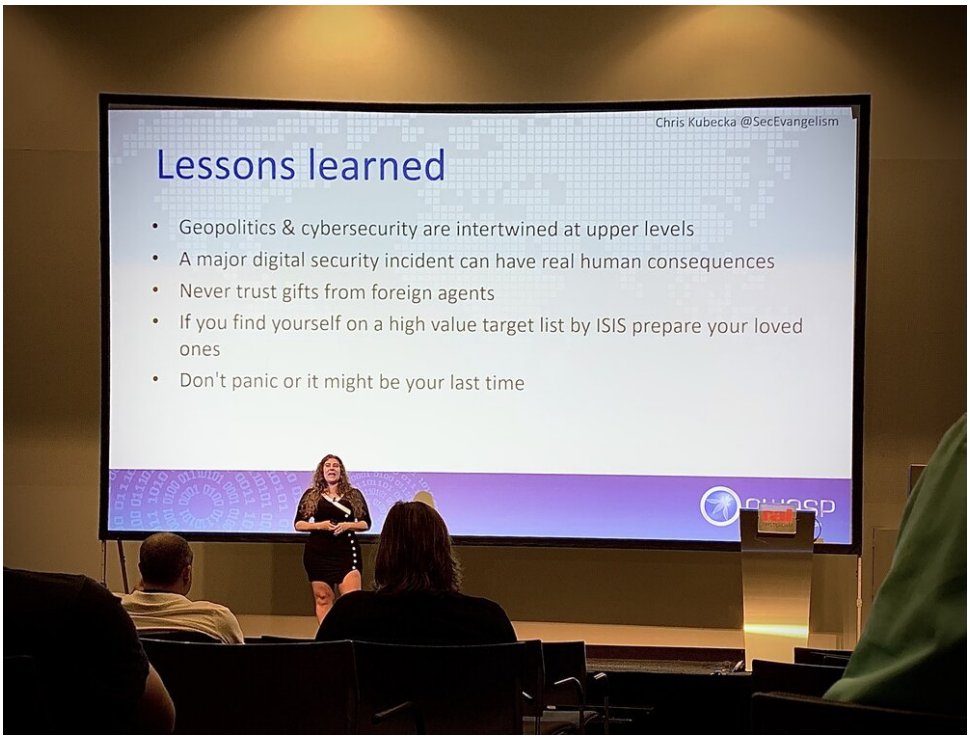
Global AppSec-Amsterdam

Wanneer cyberbeveiliging echt wordt: Terroristen uitschakelen

Een van de meest indrukwekkende verhalen werd verteld door Chris Kubecka, een vrouw die heeft gewerkt voor de Amerikaanse luchtmacht en het United States Space Command. Ze is een computerbeveiligingsonderzoeker en specialist in cyberoorlogvoering.

Keynote presentatie door cyberwarfare specialist, Chris Kubecka

Ze vertelt over haar werk bij de Koninklijke Saoedi-Arabische ambassade in Den Haag. Het is erg interessant om te horen hoe de lokale politie, het Corps Diplomatique en speciale agenten betrokken waren om uiteindelijk een bomaanslag op het Kurhaus in Scheveningen te voorkomen. Het is wanneer je deze verhalen hoort dat je je realiseert dat niet alles wat er gebeurt in het nieuws komt!



Lessen geleerd in de omgang met terroristen

Koffie en games

Na de keynote over terroristen, cyberoorlogvoering en bomaanslagen was het tijd voor koffie en games. Retro-games spelen is een leuke manier om andere hackers op de conferentie te ontmoeten, omdat je een duidelijk gemeenschappelijk onderwerp hebt om over te praten. Dat is handig, want de meeste IT-experts hebben een beetje hulp nodig om het ijs te breken als het gaat om socializen...

Koffie en PONG op de videospelconsole met CRT monitor

DuckHunt met een originele Nintendo zapper

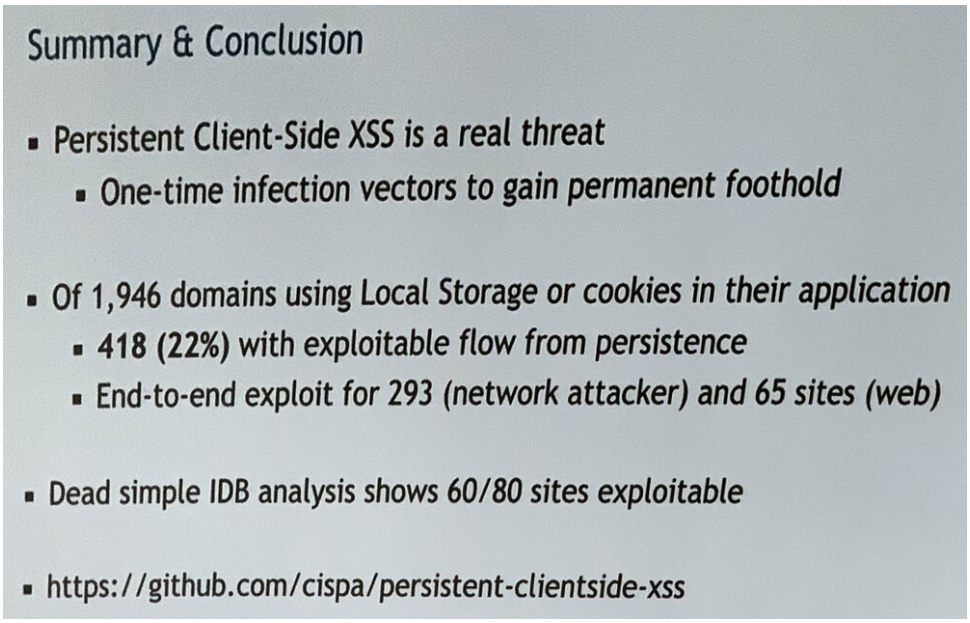
Herinner je je de dagen dat dit je gemiddelde computer was - let op: het IBM model M toetsenbord... oh boy!

Hacktechnieken

Na de koffie waren er verschillende sessies die je kon bijwonen. Ik heb er een paar geselecteerd op basis van mijn persoonlijke interesses en mijn werk.

Persistente Client-Side XSS

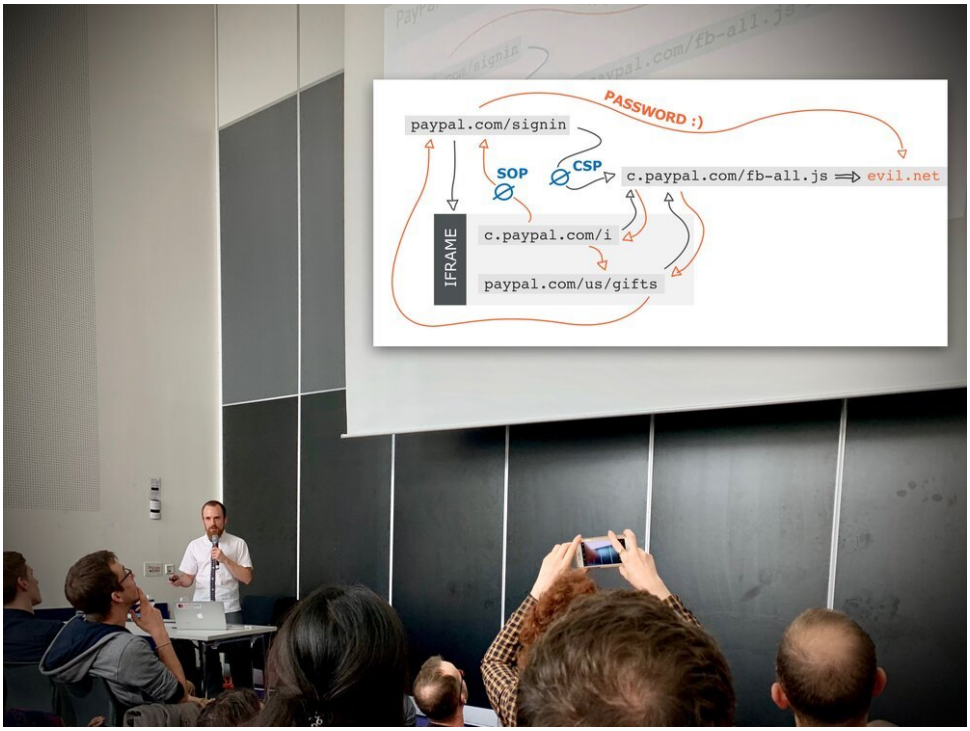
Een van de lezingen die ik bijwoonde ging over het aanvallen van websites met behulp van Local Storage of cookies. De presentatie van Marius Steffens en Ben Stock, toepasselijk genaamd "Don't trust the locals", was zeer interessant. Hun academisch onderzoek toonde aan dat veel websites kwetsbaar zijn voor bedreigingen die permanent voet aan de grond krijgen!



Persistente Client-Side XSS is een echte bedreiging - door Marius Steffens en Ben Stock

PayPal hacken met behulp van HTTP desync-aanval

In zijn briljante lezing beschrijft James Kettle zijn onderzoek naar mogelijk een van de gevaarlijkste hacktechnieken op het moderne web: HTTP Request Smuggling door HTTP-requests te desynchroniseren. Deze techniek maakt gebruik van kwetsbaarheden wanneer een website een content delivery network (CDN), een webcache of een web application firewall (WAF) gebruikt. Het is geweldig om hierover te leren, het onderliggende principe te begrijpen en te leren hoe je je tegen dit soort aanvallen kunt verdedigen.



James Kettle over het hacken van PayPal - $38.900 aan bounties verdiend

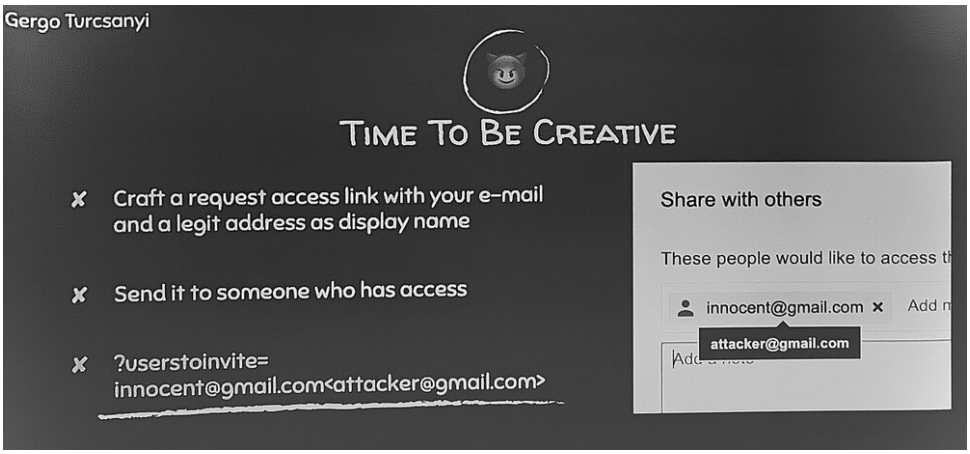
Hackeconomie: wat is een gehackt account waard?

In een andere interessante lezing legt Jarrod Overson de stand van zaken uit van credential stuffing aanvallen. Bij dit type aanval worden gelekte accountnamen en wachtwoorden op verschillende websites gebruikt, wat verrassend succesvol is omdat veel mensen hetzelfde wachtwoord op verschillende sites gebruiken. Hij legt uit hoe je CAPTCHAS kunt omzeilen en hoe hackers hun malware menselijk gedrag laten nabootsen voor fraude. Hij concludeert dat fraude een menselijk probleem is, geen technisch probleem - gedreven door eenvoudige economie: het is de moeite waard om te hacken!

Hacking rendementen op investeringen tussen 100% aan de lage kant en 150.000% aan de hoge kant! (Door Jarrod Overson)

Hackersmentaliteit

In zijn lezing vertelt Gergö Turcsányi hoe hij een bounty hunter werd. Hij legt uit dat je hiervoor geen ongelooflijk bevaardigd wiskundige hoeft te zijn, je hebt alleen een beetje creativiteit en wat tijd nodig om rond te snuffelen. Uiteindelijk leidde dit ertoe dat hij Google succesvol hackte!

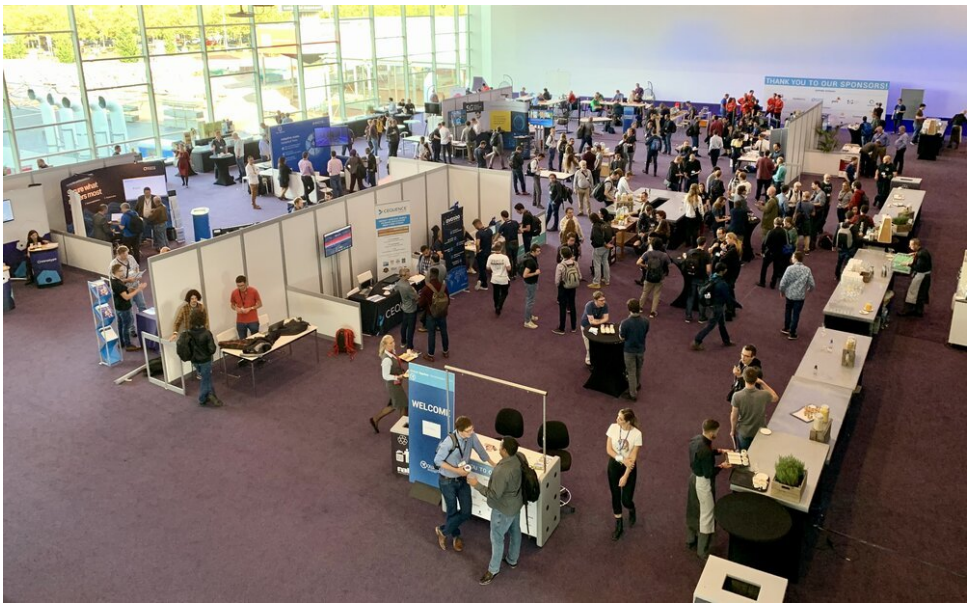


Hacking Google - Hoe ik je foto's van Google had kunnen stelen (Gergö Turcsányi)

Conclusie

Een bezoek aan Global AppSec was fantastisch! Het is een voorrecht om andere hackers te ontmoeten, van hen te leren en te horen over de dingen die je normaal gesproken niet in het nieuws ziet.

Wat je ook meeneemt van een conferentie, er zal altijd iets zijn dat je niet had verwacht te leren. Het is dit onverwachte leren dat het bezoeken van conferenties zeer de moeite waard maakt!



Global AppSec Amsterdam