Visiting an international hackers conference

OWASP Global AppSec Amsterdam

Willem L. Middelkoop
Sep. 27, 2019

This month I was lucky enough to attend Global AppSec Amsterdam, an international conference for hackers and security specialists. There were presentations from former intelligence agents, bounty hunters, academics and software vendors. I learned about some of the newest hacking techniques, met with interesting people and played some cool retro games. Read along for more.

OWASP Foundation and Global AppSec Amsterdam

The OWASP Foundation is a not-for-profit organisation dedicated to create tools, documentation, forums and conferences around software security. OWASP is special because

it's free from commercial pressure, it is not affiliated with any technology company. They advocate approaching application security as a people, process and technology problem because the most effective approaches to application security include improvements in all of these areas. More about OWASP can be found on https://www.owasp.org.

The Global AppSec events are organised all over the world. This September there was such an event in my hometown Amsterdam. Check their schedule to find out if OWASP is coming to your town.

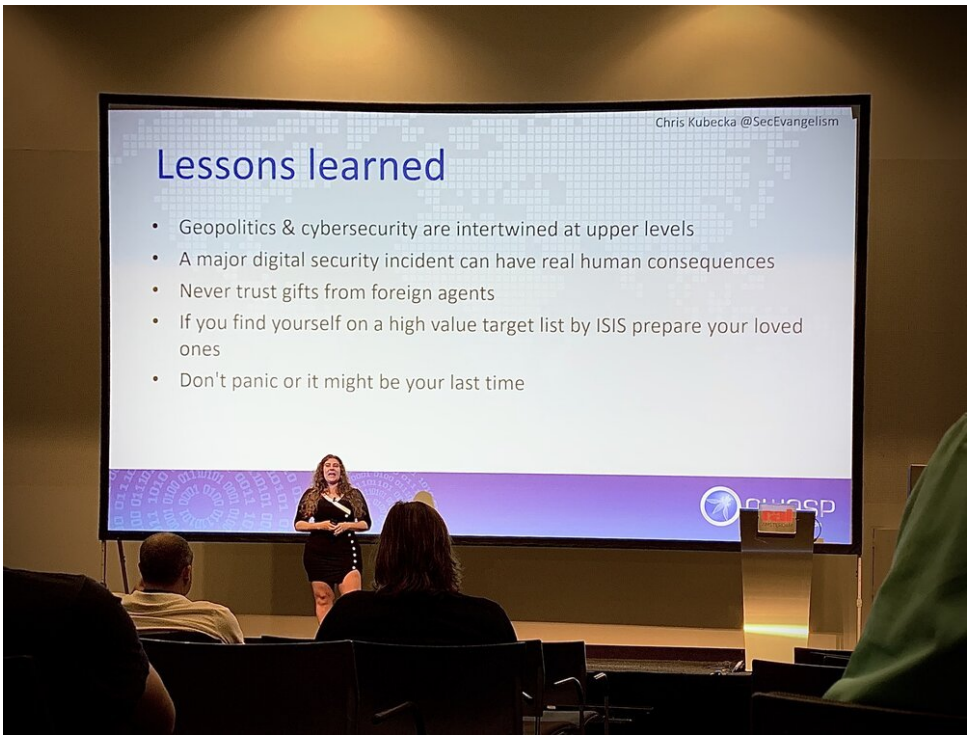
Global AppSec-Amsterdam

When cyber security gets real: Squashing Terrorists

One of the most impressive stories was told by Chris Kubecka, a woman wo has worked for the US Air Force and United States Space Command. She is a computer security researcher, and cyberwarfare specialist.

Keynote presentation by cyberwarfare specialist, Chris Kubecka

She talks about her work at the Royal Saudi Arabian Embassy in The Hague. It's very interesting to learn about how the local police, the Diplomatic Corps and special agents were involved to ultimately prevent a bomb attack on the Kurhaus in Scheveningen. It's when you hear these stories that you realise that not everything that happens gets featured on the news!



Lessons learned from dealing with terrorists

Coffee and games

After the keynote about terrorists, cyberwarfare and bomb attacks it was time for some coffee and games. Playing retro games is a fun way to meet other hackers on the conference as you'll have an obvious shared thing to talk about. That's useful as most IT-experts need a little help breaking the ice when it comes to socialising...

Coffee and PONG on the video-sports console with CRT monitor

DuckHunt with an original Nintendo zapper

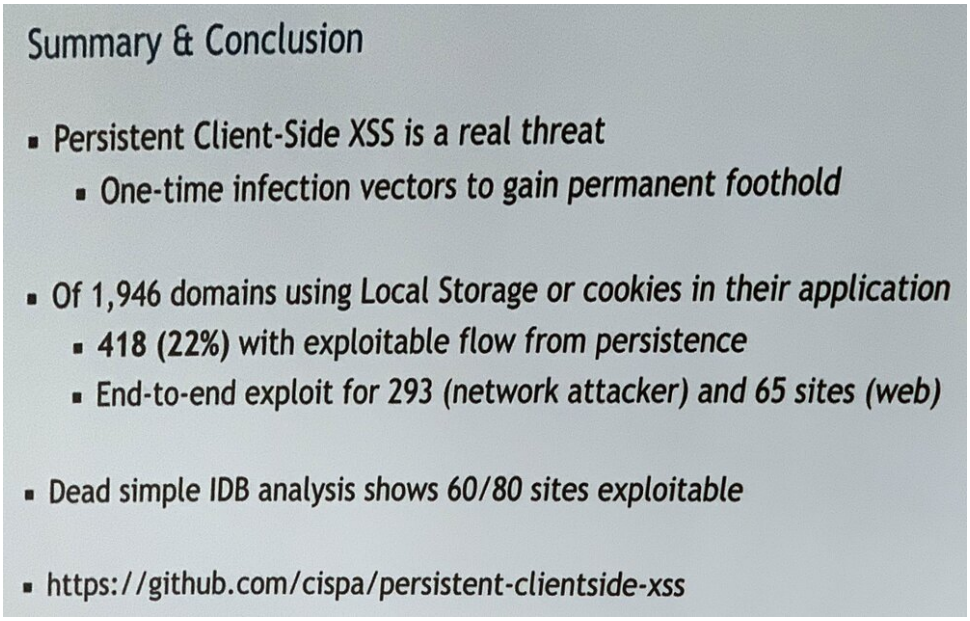
Remember the days that this was your average computer - note: the IBM model M keyboard... oh boy!

Hacking techniques

After coffee there were several sessions that you could attend. I selected a few based on my personal interests and my work.

Persistent Client-Side XSS

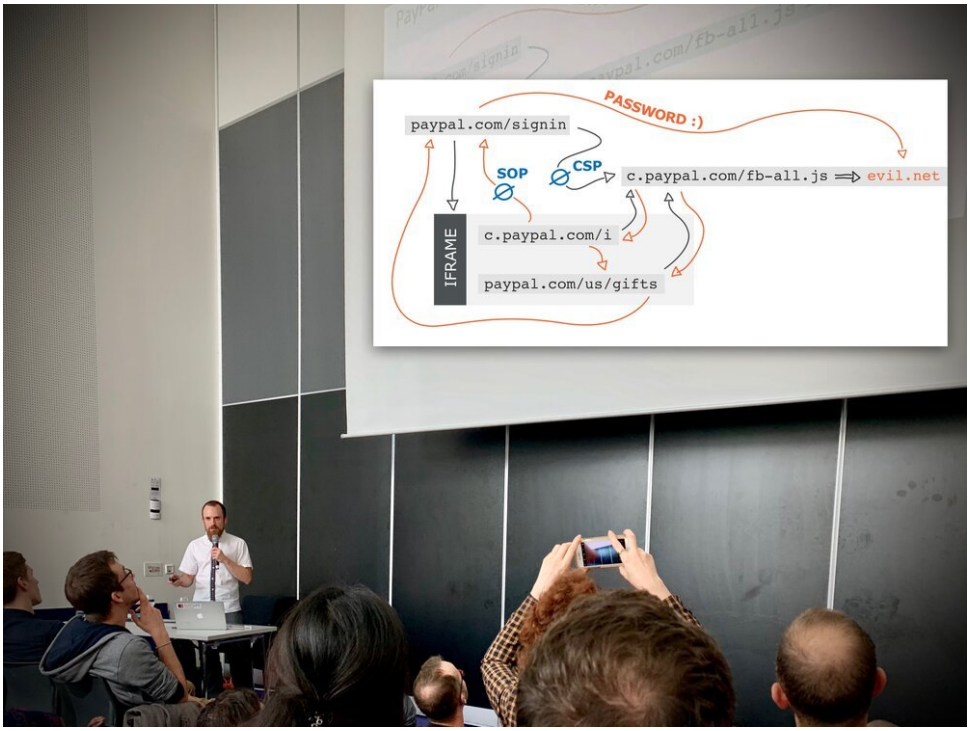
One of the talks I attended involved attacking websites using Local Storage or cookies. Aptly named "Don't trust the locals", the presentation from Marius Steffens and Ben Stock was very interesting. Their academic research revealed that many websites are vulnerable for threats gaining a permanent foothold!



Persistent Client-Side XSS is a real threat - by Marius Steffens and Ben Stock

Hacking PayPal using HTTP desync attack

In his brilliant talk James Kettle describes his research on possibly one of the most dangerous hacking techniques on the modern web: HTTP Request Smuggling by desyncing HTTP requests. This technique uses vulnerabilities when a website uses a content delivery network (CDN), a web cache or a web application firewall (WAF). It's amazing to learn about this, to understand the underlying principle and to learn how to defend against this kind of attack.



James Kettle on hacking PayPal - gaining $38,900 in bounties

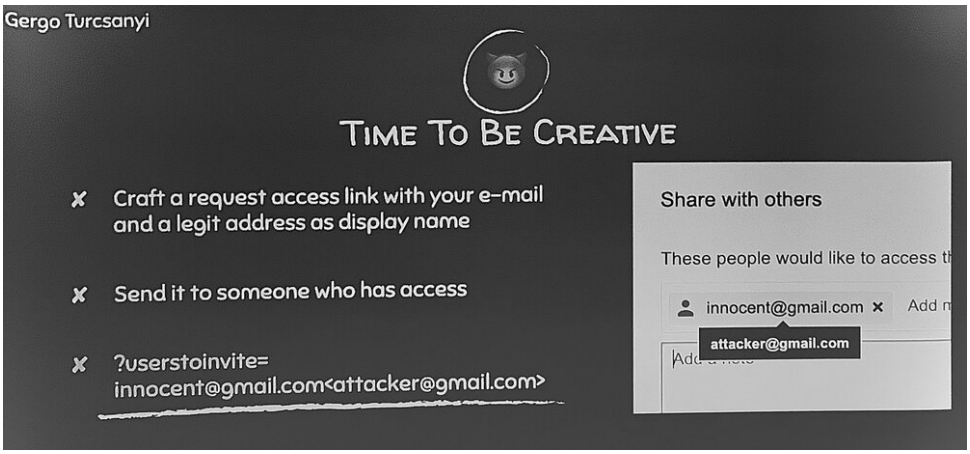
Hacking economics: what's an hacked account worth?

In another interesting talk Jarrod Overson explains the state of credential stuffing attacks. This type of attack involves using leaked account names and passwords on different websites, which is surprisingly successful as a lot of people use the same password on different sites. He explains how to bypass CAPTCHAS and how hackers make their malware mimic human behaviour for fraud. He concludes that fraud is a human problem, not a technical one - driven by simple economics: it's worth hacking!

Hacking return rates on investment between 100% on the low end and 150,000% on the high end! (By Jarrod Overson)

Hacker's mindset

In his talk, Gergö Turcsányi talks about how he became a bounty hunter. He explains that you don't need to be an incredibly skilled mathematician to do this, all you need is a little creativity and some time to time to poke around. Eventually, this led him to successfully hack Google!

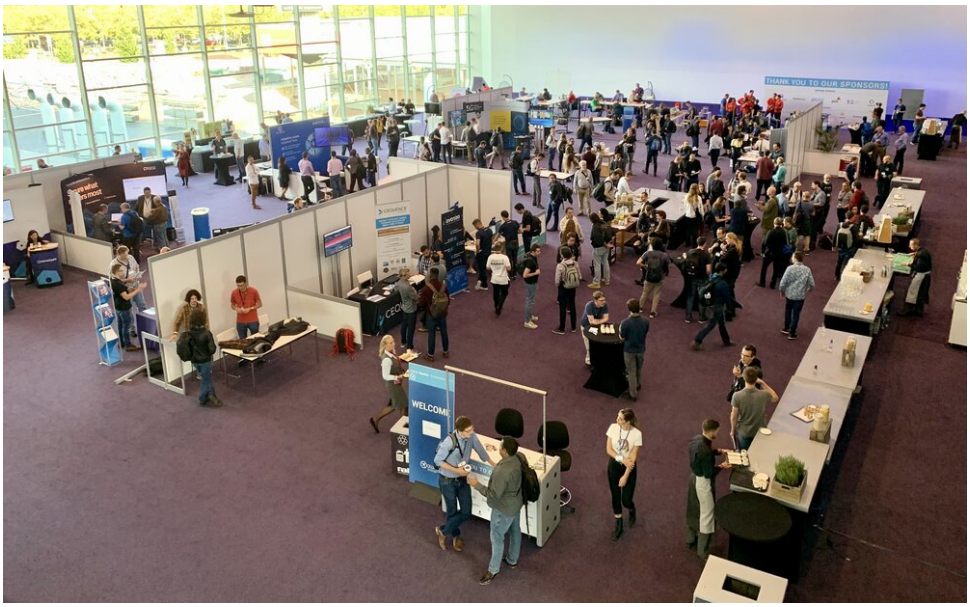


Hacking Google - How I could have stolen your photos from Google (Gergö Turcsányi)

Conclusion

Visiting Global AppSec was fantastic! It's a privilege to meet other hackers, learn from them and hear about the things you normally won't see on the news.

Whatever you take away from a conference, there will always be something that you didn't expect to learn. It's this unexpected learning that makes visiting conferences very much worth the effort!



Global AppSec Amsterdam