About Quotium

• EU Based Enterprise Software Company
• New Generation Application Security
• Fortune 500 Customers – Banking, Insurance, Industry, Services, Healthcare & More…
• Headquartered in Paris
• Branches in London, New York, Israel
About Myself

• 10+ Years in Application Security
• Breaking and Building Web and Software
• Penetration Tester, Security Researcher, OWASP Contributor
• VP Product of Seeker
Agenda

• Evolution of Application Security
  – Ancient History (1990-1999)
  – Middle Ages (2000-2005)
  – Early Modern Ages (2006-2010)
  – Modern Ages (2011-2013)
Google Scholar - “Application Security”
Ancient Times (1990-1999)

Intel Launches the Pentium Processor
Java is First Released by Sun
Larry Page and Sergey Brin Build a Search Engine
Internet Reaches a Million Users

Application Security Experts Start to Emerge
Hackers Party, Deface and Start to get Jailed
Government Warns: Online Industry Lacks Protection
Ancient Times (1990-1999)

- Early Nineties – most of the talk still revolves around non-application Hacking
- Mid-Late Nineties – Starting to be Evident that Application Security is an Issue
- Application Hacks Begin to be Published
- First Application Security Oriented Companies Emerge
Ancient Times (1990-1999)

  – HFG (Hacking for Girlies)
  – Defacement
  – FOR MITNICK!
  – Targeting Reporter John Markoff and Others
Ancient Times (1990-1999)

<!-- Don't hate us because we nailed your girlfriend. -->

F1RST OFF, WE HAVE T0 SAY.. WE OWN YER DUMB ASS. 4ND R3MEMB3R, DUMB ASS 1S OFT3N CUTE 4SS. AND WE L1KE CUTE ASS. S3C0ND, TH3R3 AR3 S0 MANY L0S3RS H3R3, 1TZ HARD T0 P1CK WH1CH T0 1NSULT THE M0ST.

S1NC3 WE AR3 N0W INTERN3T TERR0RISTZ, W3 F1GURE WE SH0ULD DEMAND S0ME RANSOM OR SOMETHING. SO, PAY US 104 GIRLIEZ, 6 BILLION IN N3WSPAP3R SUBSCRI1PTIONZ, AND MAYBE A PR1NT1NG PR3SS 0R S0M3TH1NG. N0T L1K3 Y0U GUYS KN0W WHAT FA1R J0URNALIZM IS ANYWAY. DUMB WH0R3Z.
Ancient Times (1990-1999)

• New York Times Hack – Responses
  – Defacement was discovered by the editor
  – It must be an anomalous hole in the website
  – They performed a penetration test two years ago, maybe it was not enough
Ancient Times (1990-1999)

• More Action in the 90ies
  – Early Roots of Hacktivism (300 sites hacked in 1998)
  – FTC warns about lack of website security and privacy concerns (1997)
  – Sierra-Online Hack – “Sierra is bringing in a security expert to determine how the hack occurred and how to prevent it in the future.”
Ancient Times (1990-1999)

90ies Hacker
- Young
- Idealist
- Mostly Unorganized
- Looks up to Mitnick
- Varying Level of Skill
- Few set Goals

90ies Application Defender
- Mostly Inexistent
- Low Budget
- Beginning to get Recognition
- Mostly Low Level of Skill
- Mostly Unorganized
- Little Government Support
Middle Ages (2000-2004)

Dot-com bubble bursts
Apple Introduces the iPod
MySpace, LinkedIn, WordPress are Launched
Internet Population Surpasses 500 Million

Security Experts Start OWASP, WASC
Hackers form Anonymous and get Organized
Governments pass Acts and Regulations
Middle Ages (2000-2004)

- Application Security Begins to Gain Momentum, More Companies are Founded
- OWASP AppSec USA Takes Place in NYC
- First Edition of the Top Ten Project is Released
Middle Ages (2000-2004)

How To Hire a Security Consultant
Source: The Anti-Defamation League

Guidelines for Hiring a Security Contractor

Once a decision is made that your institution has short- or long-term security needs, it should be determined whether limited or complex security requirements are necessary.

ADL strongly recommends that each institution undertake security as a long-term, ongoing process. Depending on the nature and complexity of the institution, an assessment by security professionals might be required. To view the ADL guidelines, click here. For additional information contact your local ADL office.
Middle Ages (2000-2004)

- US Government Passes Sarbanes-Oxley
- International Standards Organization takes BS7799 and makes ISO17799
- Applications hosting Medical Data are required to HIPAA Compliance
- Payment Card Industry Issues PCI-DSS
Middle Ages (2000-2004)
Middle Ages (2000-2004)

Early 2000’s Hacker
- Still quite young
- Begins to understand a lot of money can be gained
- Starts to be more organized and targeted
- Idealistic & Hacktivistic
- Some good technologists, mostly script kiddies

Early 2000’s Application Defender
- Talks security in the SDLC
- Starts professional communities and helps governments design regulations
- Gets very technological and forms application security consulting and software companies
- Enjoys strong government support
Early Modern Ages
(2005-2010)

Nintendo Releases Wii
Amazon introduces the Kindle, Apple the iPhone
YouTube, Wikipedia, and LOLcats are Launched
Internet Reaches a Billion Users

Application Security is Trendy
Hackers Become Pop-Culture, not Sub-Culture
Governments & Businesses Dedicate more Resources
Watch out cyberworld!

Hairballs aren't the only things I hack!
Early Modern Ages (2005-2010)

• In 2007 the Die Hard 4 Movie Features a Cyber Attack on National Infrastructure
• Samy hits MySpace with a PXSS worm reaching over a million users within 20 hours
• Tsunami Hacker gets Convicted
Early Modern Ages (2005-2010)

- Also in 2007, a TJ Maxx hacker takes off with over 45 million credit card numbers (and is undetected for nearly half a year)
- 3 Years Later TJ Maxx Hacker also Admits to Hacking Barns & Noble, and more..
- TJ Maxx is a Big Milestone
Early Modern Ages (2005-2010)

• Enterprises have either already Established or are Establishing Application Security Testing Teams
• Enterprises Start to Understand Need for Routine Application Security Testing
• Experts talk about Change Management, Agile Development Security, and Ongoing Testing
Early Modern Ages (2005-2010)

Late 2000’s Hacker
- Government, crime organizations and individuals
- Motivated by ideals, money or fame (or all)
- Script kiddies trained by veterans
- Governments and crime organizations have extensive training programs

Late 2000’s Application Defender
- Thoroughly understands attackers and threats
- Helps achieve regulation and/or works for governments, consulting firms, businesses or security vendors
- In high demand, enjoys a very dynamic field
Modern Ages (2011-2013)

Apple makes Champagne iPhone
Elon Musk makes Cool Stuff

1.2 Billion mobile apps Downloaded at Christmas 2011
Number of Smart Phones Reaches 1 Billion

Application Security Turns to Mobile and Cyber
Hackers turn to Mobile and Cyber
Resources are allocated for Mobile and Cyber
Modern Ages (2011-2013)

• Application Security Shifting to Mobile and Cyber
Modern Ages (2011-2013)

- Some Enterprises talk about Advanced Persistent Threats
- Others still Fail to Create an Effective Application Security Testing Process
- 2011 is the Starting Year of the Big Hacks
Modern Ages (2011-2013)
Modern Ages (2011-2013)

- Attackers get Advanced and Persistent, more Sophisticated
- Hacktivism Strongly Affected by Arab Spring
- US Government Arrests 5 Ukrainians and Russians for Largest Hack in History

The group allegedly hacked NASDAQ, Visa, J.C. Penney, 7-Eleven and JetBlue, among other companies, from 2005 until early last year. The men are accused of illegally obtaining roughly 160 million credit and debit card numbers, and allegedly stealing more than $300 million from at least three of the companies they attacked.
Modern Ages (2011-2013)

- Countries turn on Each Other

News for **iran nuclear hack**

US Says **Iran Hacked Navy Computers**

*Wall Street Journal* - by Julian Barnes - 3 days ago

U.S. officials said **Iran hacked** unclassified Navy computers in recent ... with **Iran** over its **nuclear** program, show the depth and complexity of ...
Modern Ages (2011-2013)

2010’s Hacker
- Part of Global Cyber War
- Vast Amounts of Script-Kiddies with some Trained Individuals
- Organized (Anonymous, Lulzsec, Governments, Crime Organizations), Advanced and Persistent

2010’s Defender
- Talks Cyber and APTs, Understands the Landscape has changed
- Helps Organizations Achieve Security as part of SDLC
- A lot of Highly Trained Experts. Also Experts with 15 Years of Experience
Summary

• Application Security Evolved Following the World Technological Advancements
• Application Security Experts Emerged, got Organized (over 600 Registered to OWASP Israel 2013!)
• Governments Joined in on the Fun
• Hackers get Organized, but Keep sense of Humor
Summary

LOL. THE GOVERNMENT WAS LIKE

ANONYMOUS CAN'T HACK US
Thank You!

Questions?

Irene Abezgaucz
irene@quotium.com