(ISC)²

SECURITY CONGRESS | LATIN AMERICA 2015

Patrocinador Platinum:

DELL

Patrocinadores Gold:

Deloitte. Level (3) BLUE COAT

Parceria e Organização:

(ISC)² SEMINÁRIOS Valor ECONÔMICO mci

(ISC)²

SECURITY CONGRESS | LATIN AMERICA 2015

Application Security Challenges for Startups

Anderson Dadario

Who am I

I’m a little point that knows a little about few things in life. Founder of Gauntlet.io and FindMyNinja.io :)

01.

“IF YOU WANT TO PREDICT THE FUTURE, LOOK AT THE YOUNG”

WALDEZ LUDWIG

Why Security for Startups Matters

- In China, 49 tech startups per day are created
- On Product Hunt, 10~30 products are launched every day
- On Angel.co, approximately 28 new startups are registered every day
- **They may be your tomorrow's vendors**

02.

“OPTIMIZE FOR SPEED OVER SCALABILITY/CLEAN CODE”

STARTUP CLASS

Security Isn't A Huge Concern

- It's not taught on startup classes *although there is a very good reason for this*
- Angel.co jobs doesn't include Security Engineer as a searchable title
- Even security startups don't hire full time security engineers

03.

“INNOVATION IS SAYING NO TO 1,000 THINGS.”

STEVE JOBS

How Startups Stay Focused

- Delegate **everything** to cloud vendors
- Rapid interactions between product owner and development personnel
- Reuse whatever piece of code/server images/etc found on the internet which will result in faster deliveries *and low cost*

04.

“TRUST, BUT VERIFY.”

SUZANNE MASSIE

Least Common Mechanism

Top Vendors

- GitHub
- Amazon Web Services
- Google Apps (Mail)
- Trello
- Slack
- Stripe
- Dropbox

Tools

- Cutting-edge MVC Frameworks
- Software Libraries
- OS/Container Images
- OS packages

05.

“SECURITY FOR BROKEN THINGS ARE WORTHLESS”

ANDERSON DADARIO

(ISC)² SECURITY CONGRESS | LATIN AMERICA 2015

Beyond OWASP Top 10

- Subdomain Takeover
  - Leftover CNAME entries
- Debug mode in production (yes, is common)
- Protocol Handling Abuse and SSRF
  - Lack of whitelistening protocols when parsing URLs, so **gopher**, **javascript** and **file** are commonly used to exploit applications

Startup Security Summary

- High Trust on Vendors and New Frameworks
  - I.e., SQL Injection and XSS usually are mitigated
- High Risk of Security Misconfiguration
  - E.g., Patreon put a debugger on production
- High Risk of exploits on uncommon tasks
  - E.g., Pocket copy webpage body from a client input URL and show its contents

06.

“WHEN YOU’RE A CARPENTER MAKING A BEAUTIFUL CHEST OF DRAWERS, YOU’RE NOT GOING TO USE A PIECE OF PLYWOOD ON THE BACK (...)”

STEVE JOBS

Takeaways

For Vendors

- Reduce startup's time to go to market (e.g., AWS Lambda);
- Support SSO on trusted providers, e.g., Google because of Google Apps;
- Take security **seriously.**

For Startups

- Don't pick any vendor/tool. Consider their security, because it's your security too;
- Add Security to your SDLC;
- Don't need to hire a infosec guy fulltime at first, but hire on demand when needed at least.

Thank you

Anderson Dadario, CISSP, CSSLP
Twitter @andersonmvd
Slides available on my blog http://dadario.com.br/slides
Founder of Gauntlet.io and FindMyNinja.io

References [1-2]

- **LSBF - 49 new tech start-ups per day coming from China's Silicon Valley**
  http://www.lsbf.org.uk/blog/news/enterpreneurs-startups/new-tech-startups-coming-from-chinas-silicon-valley/81403
- **Google Web Cache since 28 set. 2015 01:38:32 GMT**
  http://webcache.googleusercontent.com/search?q=cache:W3V8baOB5dUJ:https://angel.co/companies+&cd=3&hl=pt-BR&ct=clnk&gl=br&client=ubuntu
- **Angel.co - Jobs**
  https://angel.co/jobs
- **SANS - 2015 - State Application Security**
  https://www.sans.org/reading-room/whitepapers/analyst/2015-state-application-security-closing-gap-35942
- **Business Insider - Here's Why Starbucks Is The Only Office Entrepreneurs Need**
  http://www.businessinsider.com/why-starbucks-is-the-only-office-you-need-2014-5

References [2-2]

- **How Patreon got hacked – Publicly exposed Werkzeug Debugger**
  http://labs.detectify.com/post/130332638391/how-patreon-got-hacked-publicly-exposed-werkzeug
- **Multiple Vulnerabilities in Pocket**
  https://www.gnu.gl/blog/Posts/multiple-vulnerabilities-in-pocket/
- **Neglected DNS records exploited to takeover subdomains**
  http://yassineaboukir.com/blog/neglected-dns-records-exploited-to-takeover-subdomains/