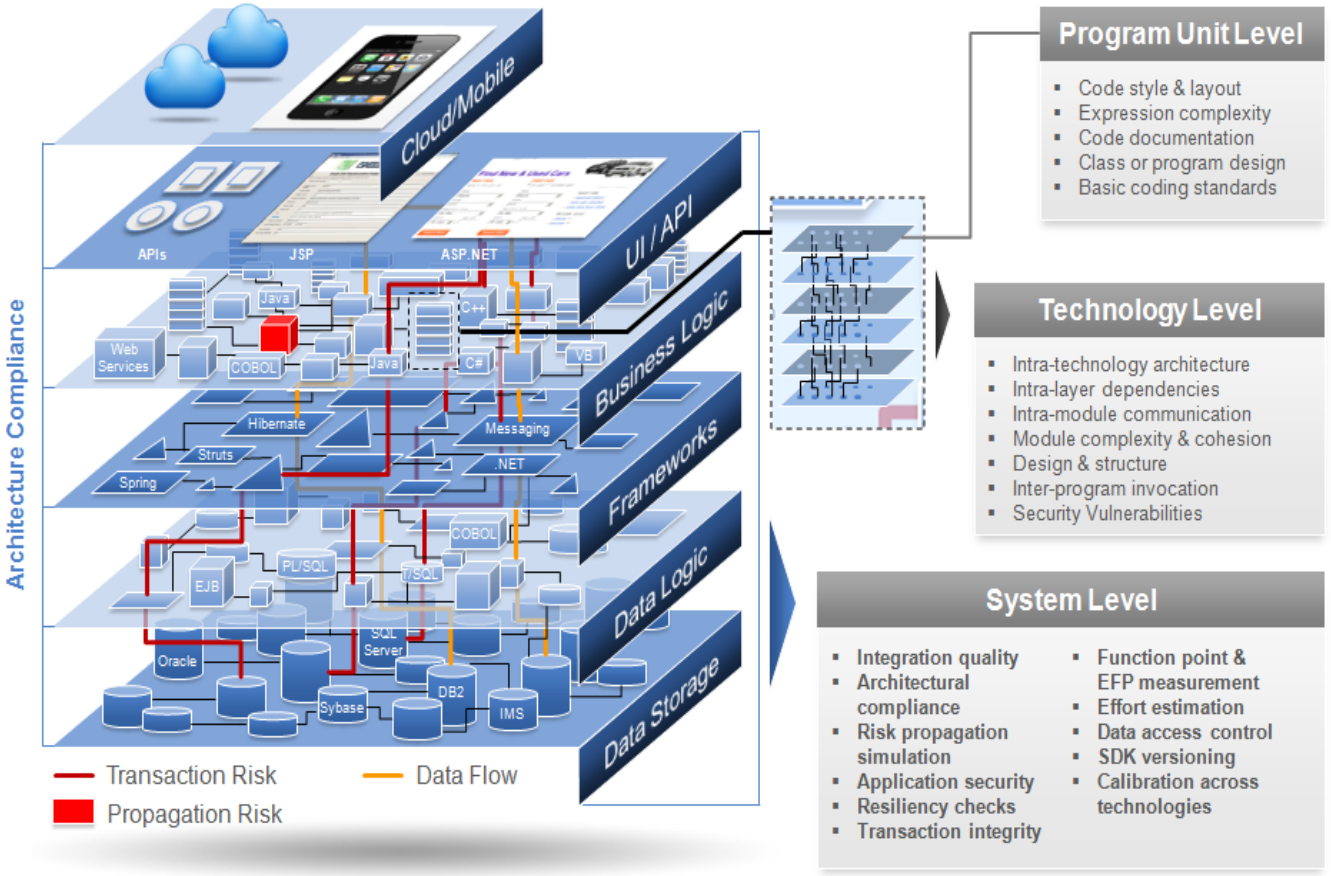
Application Security is Easy Right?

Trying to learn App Sec

- I came up the old fashioned way:
  - Help Desk
  - PC Tech
  - Systems Administrator
  - Network Administrator
- Moved into IT Security
  - Intrusion Analyst
  - Penetration Tester
- The way nature intended….

Pentesting Starting Moving Away From The Network

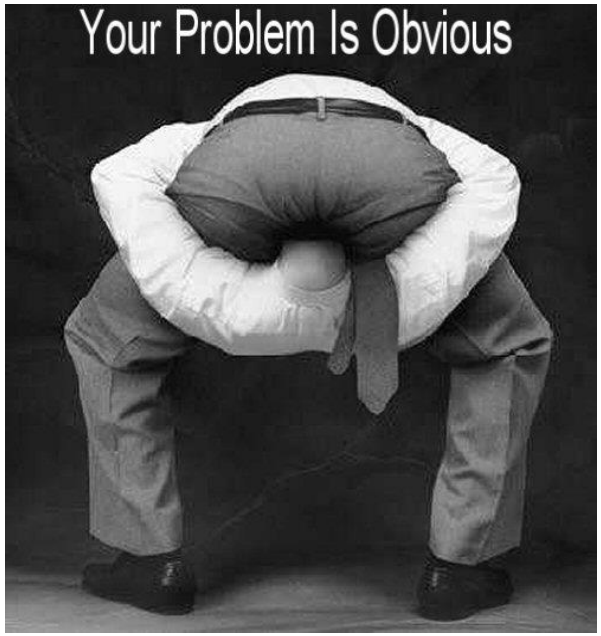
- Pentesting started shifting away from the network….
  - Network and Systems
  - Web App
  - Mobile App
  - Cloud
  - Mashups
  - Source Code
- Easy right?
- Houston….



I Felt Lost In The App Sec

I DON'T KNOW HOW TO PROGRAM

- A lot of computer scientists will be familiar with programming concepts such as:
  - Turing's Primitives
  - Programming Logic
  - Data Structures and Algorithms
  - Object Oriented Programming
- If you are like me then none of this stuff makes any sense to you
- I don't understand any of this stuff, and don't plan on trying
- I'm regular working stiff – so that means that I like:
  - Alcohol
  - Sports
  - Barbequing

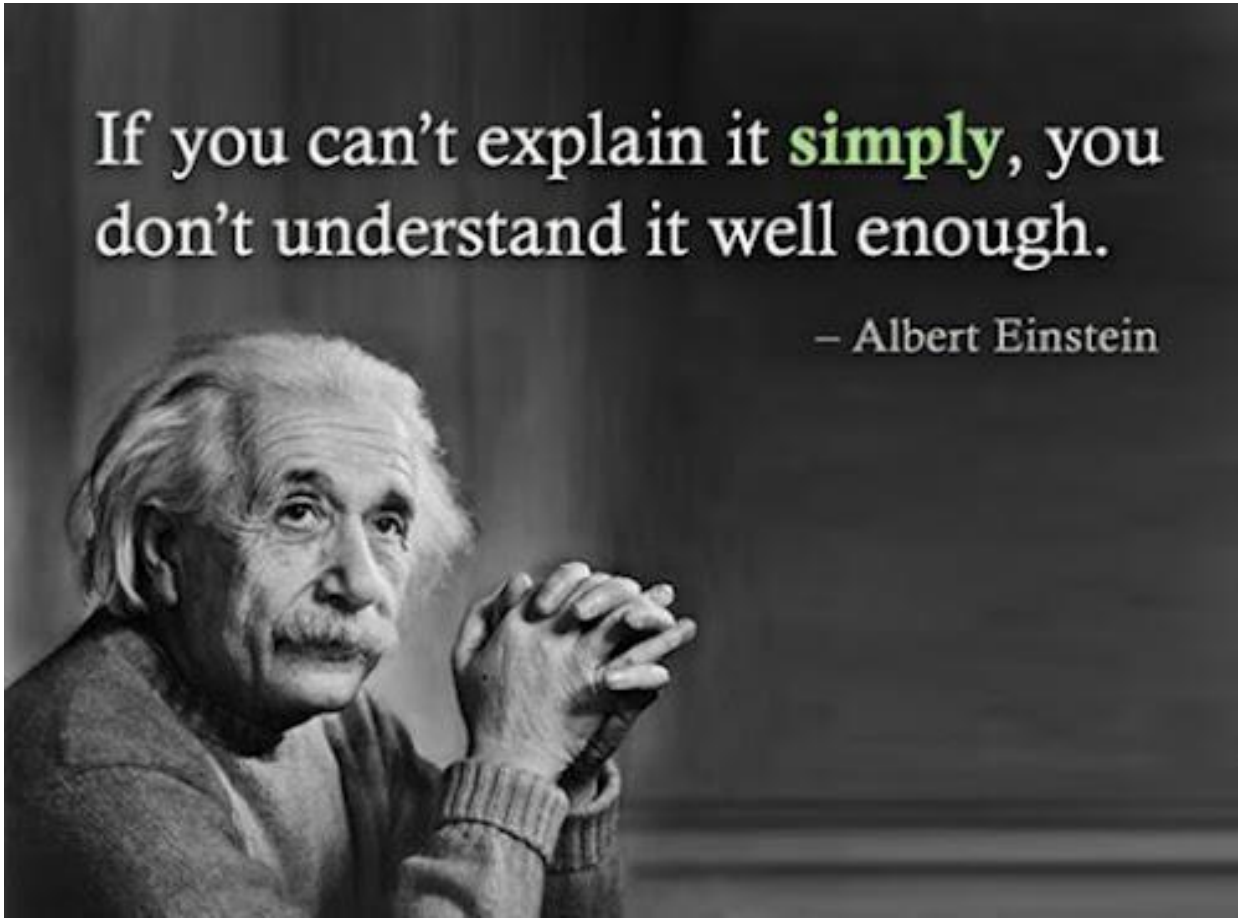


OWASP Confused Me More

- OWASP Testing Guide
- https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents

I Needed Something Simple I Could Do

- **A process to follow**
- **A methodology to use**
- **It has to be simple**



3 Simple Questions

1. Is it talking to a DB?
   - Is there parameter passing – if yes…
   - Insert a single quote

2. Can I or someone else see what I type?
   - Is there a forum, blog, guestbook, contact us page, feedback form, instant messenger/chat – if yes...
   - Insert <script>alert('xss')</script>

3. Does it reference a file?
   - Is it talking about a file on the local file system – if yes…
   - Insert ../../../../../../etc/passwd, ../../../../../../etc/passwd%00
   - ../../../../../../windows/win.ini, ../../../../../../windows/win.ini%00

Let’s drive

Everything I’m doing today can be found at:

- http://pastebin.com/ka5PvLp8

I use pastebin to allow you to follow me and just copy/paste the commands I type

So you can just just open up Firefox and follow along

What About Tools

Once you have a methodology then you can start with simple firefox addons:

ShowIP
https://addons.mozilla.org/en-US/firefox/addon/showip/

Server Spy
https://addons.mozilla.org/en-US/firefox/addon/server-spy/

FoxyProxy
https://addons.mozilla.org/en-US/firefox/addon/foxyproxy-standard/

Tamper Data
https://addons.mozilla.org/en-US/firefox/addon/tamper-data/

Firebug
https://addons.mozilla.org/en-US/firefox/addon/firebug/

A good list of web app testing add ons for Firefox:
https://addons.mozilla.org/en-us/firefox/collections/adammuntner/webappsec/

What About Free/Low Cost Tools

Once you are comfortable with the firefox addons, then I think you can move on to the proxies:

Burp Suite
https://portswigger.net/burp/download.html

Zap
https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

Fiddler
http://www.telerik.com/fiddler

Charles Proxy
http://www.charlesproxy.com/

What About Commercial Tools

Once you are comfortable with the firefox addons, then I think you can move on to the proxies:

IBM AppScan
http://www-03.ibm.com/software/products/en/appscan

HP WebInspect
http://www8.hp.com/us/en/software-solutions/webinspect-dynamic-analysis-dast/

Acunetix
https://www.acunetix.com/vulnerability-scanner/

Comparison of the scanners
http://sectoolmarket.com/price-and-feature-comparison-of-web-application-scanners-unified-list.html

I built one (shameless plug)

Web Scanner Pro (YES IT IS FREE and cheap):
http://strategicsec.com/products/webscannerpro/

You don’t need to be a Web App expert to use the product

You don’t need to be a programmer to understand the reports

You don’t need to be a compliance expert to demonstrate your due diligence

Contact Me....

Toll Free: **1-844-458-1008**

Email: joe@strategicsec.com

Twitter: http://twitter.com/j0emccray

LinkedIn: http://www.linkedin.com/in/joemccray