www.pandoralabs.net

PANDORA
SECURITY LABS

Expert Advice. Experience Advantage.
Proactive Security Solutions Through Cutting-Edge Research.

Introduction To Web Application Testing

By @isaacsabas

PANDORA
SECURITY LABS

Expert Advice. Experience Advantage.
Proactive Security Solutions Through Cutting-Edge Research.

www.pandoralabs.net

We are a Security-as-a-Service company

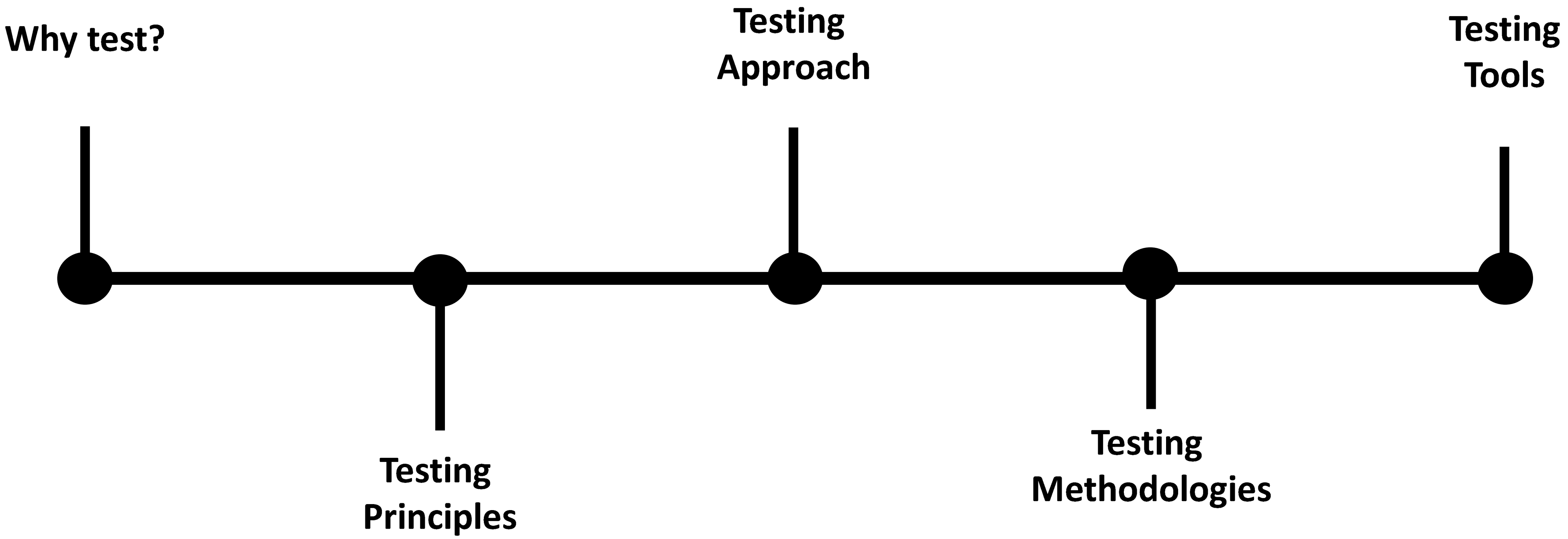
Providing businesses with on-demand threat detection & intelligence capabilities to secure their IT infrastructure, 24x7.

We Make IT Secure

An Introduction To:

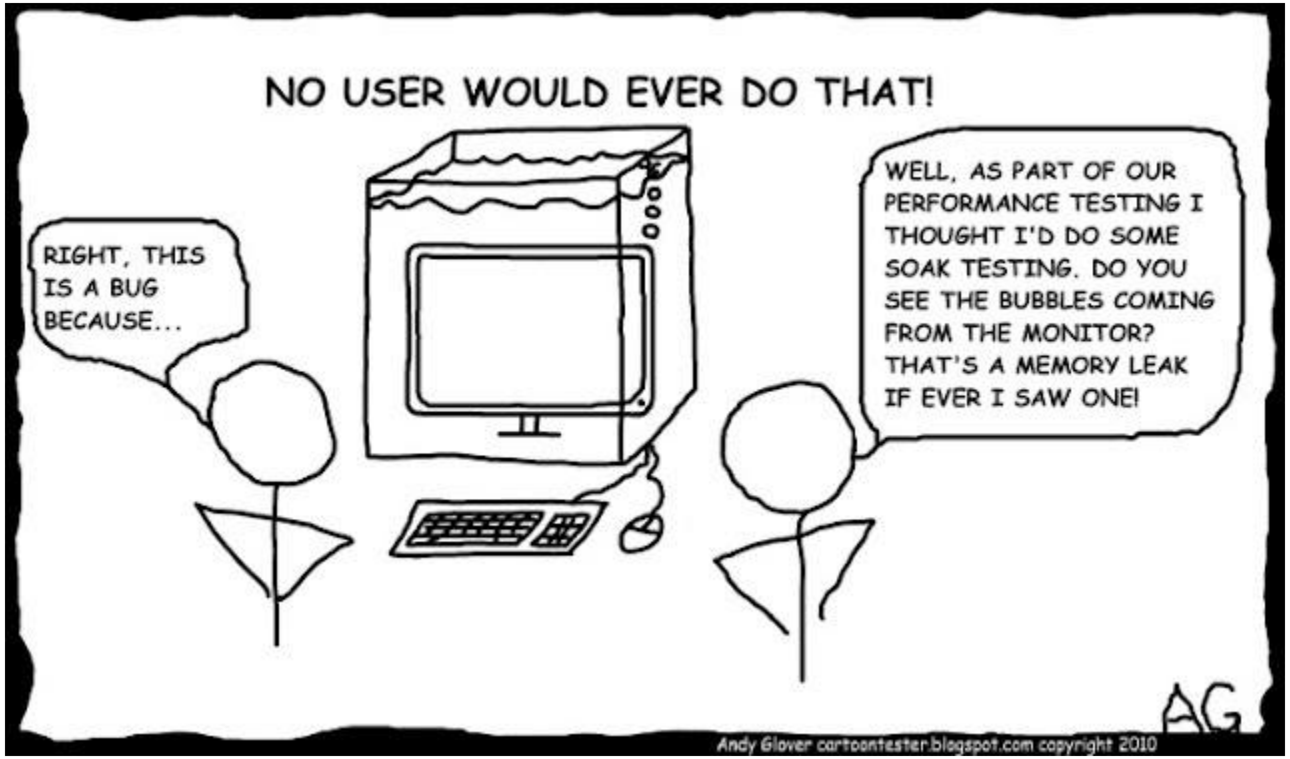
Web Application Testing

#pandorasecurity



Discussion Flow

What we will be discussing today


NO USER WOULD EVER DO THAT!
RIGHT, THIS IS A BUG BECAUSE...
WELL, AS PART OF OUR PERFORMANCE TESTING I THOUGHT I'D DO SOME SOAK TESTING. DO YOU SEE THE BUBBLES COMING FROM THE MONITOR? THAT'S A MEMORY LEAK IF EVER I SAW ONE!
AG

Andy Glover cartoontester.blogspot.com copyright 2010

Why Test?

We always begin with the “why”.

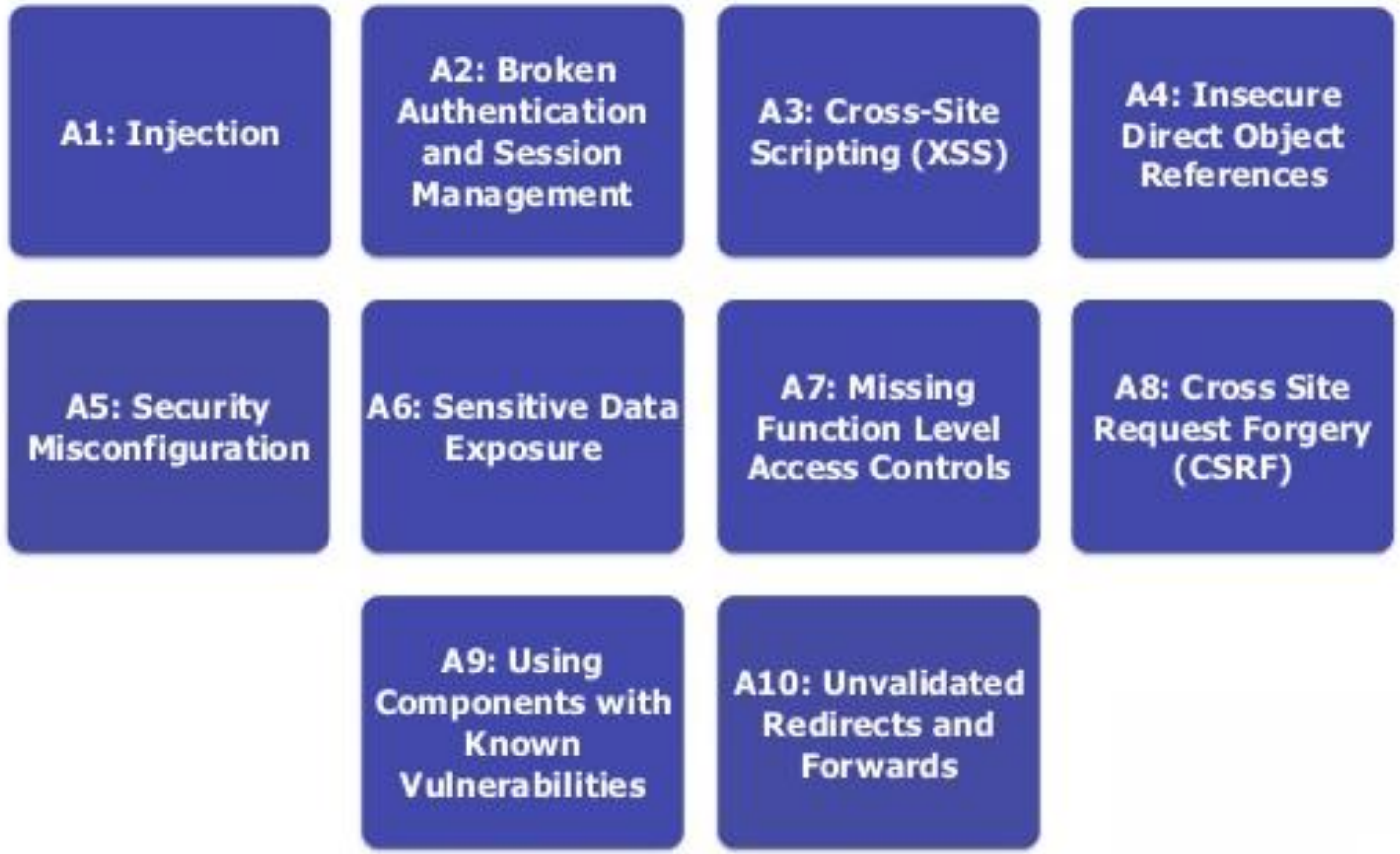
Items You Want to Test For

- Data loss or corruption
- Data theft
- Unauthorized access
- Denial of Service
- System Compromise

It's the web app, and all its components.

OWASP

Open Web Application Security Project



A1: Injection

A2: Broken Authentication and Session Management

A3: Cross-Site Scripting (XSS)

A4: Insecure Direct Object References

A5: Security Misconfiguration

A6: Sensitive Data Exposure

A7: Missing Function Level Access Controls

A8: Cross Site Request Forgery (CSRF)

A9: Using Components with Known Vulnerabilities

A10: Unvalidated Redirects and Forwards

Testing Principles

- There Is No Silver Bullet
- Think Strategically, Not Tactically
- Test Early and Test Often
- Understand the Scope of Security
- Understand the Subject
- Use the Right Tools
- The Devil is in the Details
- Document the Test Results

Testing Approach

1. Manual Inspections & Reviews
2. Threat Modeling
3. Code Review
4. Penetration Testing

1. Manual Inspection & Reviews

- Manual inspections can also include inspection of technology decisions such as architectural designs.
- Advantages:
  - Requires no supporting technology
  - Can be applied to a variety of situations
  - Flexible
  - Promotes teamwork
  - Early in the SDLC
- Disadvantages:
  - Can be time consuming
  - Supporting material not always available
  - Requires significant human thought and skill to be effective

2. Threat Modeling

- This approach involves:
  - Decomposing the application
  - Defining and classifying the assets
  - Exploring potential vulnerabilities
  - Exploring potential threats
  - Creating mitigation strategies
- Advantages:
  - Practical attacker's view of the system
  - Flexible
  - Early in the SDLC
- Disadvantages:
  - Relatively new technique
  - Good threat models don’t automatically mean good software

3. Code Review

- Source code review is the process of manually checking the source code of a web application for security issues. Many serious security vulnerabilities cannot be detected with any other form of analysis or testing.
- Advantages:
  - Completeness and effectiveness
  - Accuracy
  - Fast (for competent reviewers)
- Disadvantages:
  - Requires highly skilled security developers
  - Can miss issues in compiled libraries
  - Cannot detect run-time errors easily
  - The source code actually deployed might differ from the one being analyzed

4. Penetration Testing

- Penetration testing is essentially the “art” of testing a running application remotely to find security vulnerabilities, without knowing the inner workings of the application itself.
- Advantages:
  - Can be fast (and therefore cheap)
  - Requires a relatively lower programming skill-set than source code review
  - Tests the code that is actually being exposed
- Disadvantages:
  - Too late in the SDLC
  - Front impact testing only.

Different Types of Frameworks

- OWASP WAS Testing Cheat Sheet
- OWASP Testing Guide v4
- OWASP ASVS (Application Security Verification Standard)
- OSSTMM(Open Source Security Testing Methodology Manual)

Reporting Vulnerabilities

- When reporting security test data the best practice is to include the following information:
  - The categorization of each vulnerability by type
  - The security threat that the issue is exposed to
  - The root cause of security issues (e.g., security bugs, security flaw)
  - The testing technique used to find the issue
  - The remediation of the vulnerability (e.g., the countermeasure)
  - The severity rating of the vulnerability (High, Medium, Low and/or CVSS score)

Different Types of Tools

- Scanners
  - OWASP Zap
  - BurpSuite
  - Nikto
  - OWTF
  - W3af
  - Arachni
- Brute Forcers
  - THC Hydra
- Proxies
  - OWASP ZAP
  - BurpSuite
  - Paros
  - WebScarab
- Paid Vulnerability Scanners
  - Nessus
  - Qualys
  - Acunetix
  - AppSec

#pandorasecurity

HOW TO SPOT A TESTER IN THE MAKING
In the early years...
• TRY & BREAK THINGS
OH, A MOBILE! I'LL COVER IT WITH SALIVA TO ANNOY DADDY!
• USE TOOLS TO MAKE LIFE EASIER
LOOK DADDY. WITH 3 CRAYONS I CAN DRAW MUCH QUICKER
As infants or juniors...
• QUESTION AMBIGUITY
BUT MUMMY, HOW DID THE BABY GET INTO YOUR TUMMY IN THE FIRST PLACE?
• CHECK BOUNDARIES
MUM, IS IT OK IF I THROW STONES AT CARS DRIVING BY?
And young adults...
•HIGHLIGHT INCONSISTENCY
IT'S NOT FAIR! JEFF HAS MORE ICE-CREAM THAN ME!
•TEST LOGIC
IF METHANE IS FLAMMABLE, AND MY TRUMPS CONTAIN METHANE. CAN I LIGHT MY TRUMPS?
AG
Andy Glover cartoontester.blogspot.com Copyright 2011

Becoming A Tester

TIME FOR

Q&A

Introduction To Web Application Testing

An Introduction To:

Web Application Testing

www.pandoralabs.net

PANDORA
SECURITY LABS

Expert advice. Experience advantage.
Proactive Security Solutions Through Cutting-Edge Research.

OWASP TOP 10: #1 Injection

By @isaacsabas