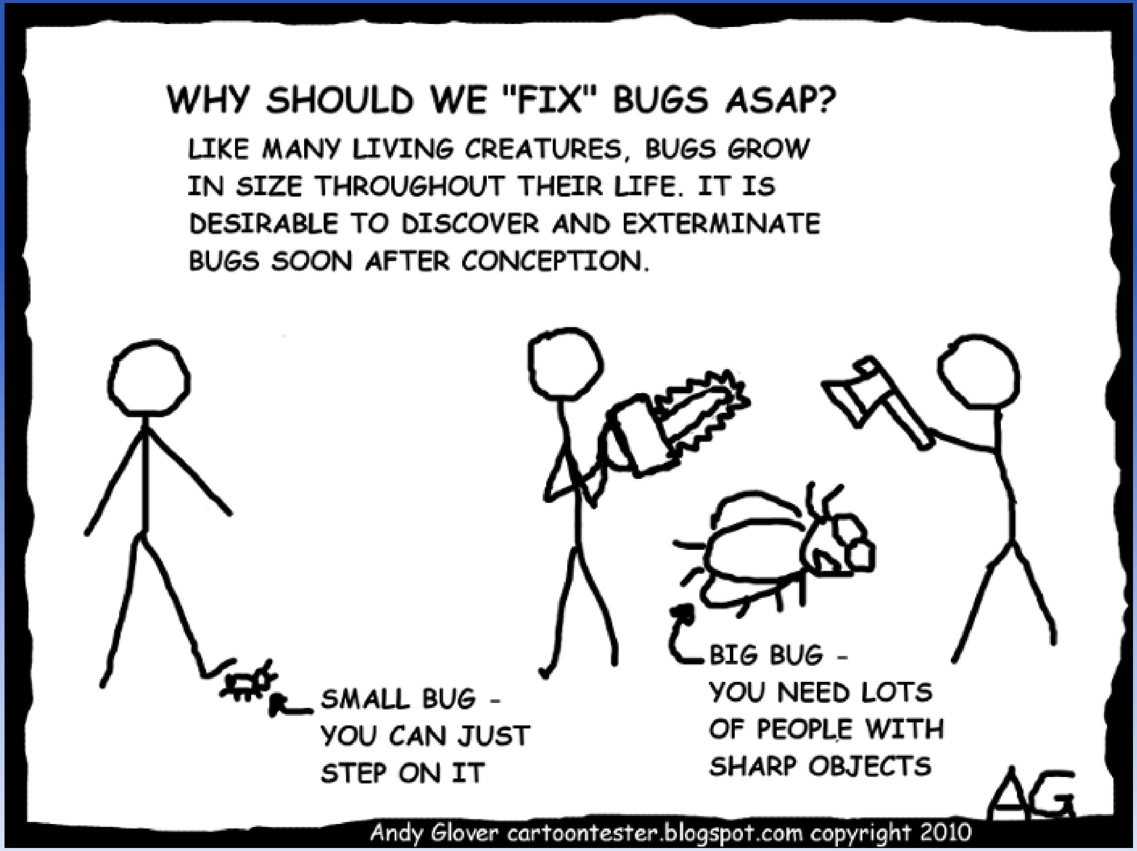
CS 493
Secure Software Systems

Ch 10 Application Review and Testing


WHY SHOULD WE "FIX" BUGS ASAP?
LIKE MANY LIVING CREATURES, BUGS GROW IN SIZE THROUGHOUT THEIR LIFE. IT IS DESIRABLE TO DISCOVER AND EXTERMINATE BUGS SOON AFTER CONCEPTION.
SMALL BUG - YOU CAN JUST STEP ON IT
BIG BUG - YOU NEED LOTS OF PEOPLE WITH SHARP OBJECTS
AG

Andy Glover cartoontester.blogspot.com copyright 2010

Dr. Williams Central Connecticut State University

Objectives

- Code review
- Assembling a penetration testing team
- System vulnerability scanning
- Assessing likely attack vectors
- Penetration testing assessment

Goals

- Identify objectives for penetration testing in a system.
- Scan a system for vulnerabilities.
- Perform a code review.
- Assemble a penetration testing team.
- Prioritize revisions based on penetration testing results.

Static Analysis

There are two types of attacks on a system that should be performed:

- Attacks at rest and attacks in action.
- Attacking or probing the system at rest is called **static analysis.**

Static Analysis

The following items are the primary interests in a static system review:

- **SQL injection locations**
- **Unvalidated input**
- **Authentication/authorization gaps**
- **Sensitive data mishandling**
- **Code access**
- **Ignoring exceptions**
- **Data access**
- **Cryptography misuse/mismanagement**
- **Unsafe code**
- **Misconfiguration**
- **Threading**
- **Undocumented public interfaces**

Dynamic Analysis

- The next phase of the analysis is to look at the system in action (**dynamic analysis**) and try to compromise it; this is the active penetration testing exercise.
- The first step in this process is to determine the best candidates from the vulnerability map for extracting information or sending the system into an unpredictable or shutdown state.

Casing the Joint

- Using tools for port scanning, public information about the system, and network traffic analysis internally is called **network auditing**.
- The next step is to get a picture of the path from the user to the application.
- **Network mapping** is the next goal; this is where you will determine live hosts, routers, and servers to establish a picture of the network topology.

Casing the Joint

- **Port scanning** is the next area of consideration in the network mapping operation.
- **Vulnerability scanning** is the use of an automated tool to assess where a likely break-in or misuse can occur.
- The vulnerabilities identified in this phase, together with the attack maps and mitigation techniques constructed in the system documentation, should be the primary vectors of attack against the system.

Never Stop at One

- The important element in penetration testing is that the more testing that is completed, the more robust the resulting system will be against attack.
- The more holes you find in the system now, the fewer you will encounter when the system is deployed in the production environment.
- Translating unknown vulnerabilities to known vulnerabilities is the key to this task.

Hardening the System

The breakdown of these categories is as follows:

1. **Prevent**
2. **Protect**
3. **Respond**
4. **Recover**

THE CASE PROJECT—TESTING PLAN

Given this configuration, the penetration test plan should include the following items:

- Attempt to gain administrative access with default log-in credentials
- Attempt to compromise the database or extract additional information via SQL injection
- Attempt to locate user accounts and break passwords to access the system
- Determine if the latest version of Flash is truly required for the full site or if older exploitable versions are permitted
- View the source of the pages for any coded secrets or additional functionality that is not documented
- Attempt to break the authentication mechanisms used in the mobile site and compare the level of authentication required for that end against the full site
- Attempt to overrun input on the app version and try to proceed with a transaction past any error messages
- Try to directly access pages discovered via successful log-in

Summary

- Penetration testing is a necessary element of producing and maintaining secure software.
- The environment for the penetration testing should be as close to the live environment as possible.
- The penetration testing team may be hired externally or they may be part of the organization.

In class exercises revisited

Bob’s Pizza Shack

In groups consider this scenario

Bob is a small business owner of Bob’s Pizza Shack and wants to create a website to allow online credit card delivery orders

Given this configuration, the penetration test plan should include the following items:

Alice’s Online Bank

In groups consider this scenario

- Alice opens Alice’s Online Bank (AOB)
  - Internal use bank employees
  - Interoperates with another bank
  - Interacts with customers
    - Web
    - Mobile app

Given this configuration, the penetration test plan should include the following items:

Location based social media app

In groups consider this scenario Open source group wants to create a mobile app to allow groups to communicate/find each other in public demonstrations/protests

- – Communication internet, as well as, P2P (WiFi/Bluetooth) in case internet cut off – so if person you want to contact is on other side of crowd and no internet as long as P2P network can be established with app can reach somebody outside your immediate vicinity via the P2P network
- – Should be able to communicate securely messages and images to people you identify within your group (group as whole or direct)
- – Should be able to share GPS location with people in group (group as whole or direct)

- Given this configuration, the penetration test plan should include the following items: