OWASP Broken Web Application Project

When Bad Web Apps are Good

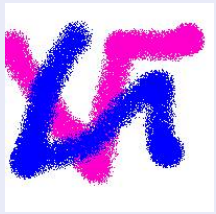
OWASP 中国

The Open Web Application Security Project

About Me

OWASP 中国
The Open Web Application Security Project

- Mordecai (Mo) Kraushar
- Director of Audit, CipherTechs
- OWASP Project Lead, Vicnum
- OWASP New York City chapter member



Assessing the assessor

OWASP 中国
The Open Web Application Security Project

Network Assessment

- Known methodologies
  - Reconnaissance
  - Discover
  - Fingerprint
  - Enumerate
  - Exploit
- Known tools
  - Nmap
  - Vulnerability Manager
  - Metasploit
- Known Goal
  - Shell
- Predictable Results

Web Application Assessment

- Methodology is uncertain*
- Assorted approaches
- Assorted tools exist to target the technical side of a web app*
- Assorted Goals
- Unpredictable Results*

* Getting better but still not as good as network assessments

Why the Difference?

OWASP 中国
The Open Web Application Security Project

Network Assessment

- Mature and stable TCP/IP protocols
- Well defended by network firewalls (usually)

Web Application Assessment

- New technologies are constantly emerging
  - Web Services
  - Mobile platforms
  - Different databases
- New CMS and Web frameworks
  - Ruby on Rails
  - Django (Python based)
  - Node.js
- Business logic
- Human element

Vulnerable Web Applications

OWASP 中国
The Open Web Application Security Project

- Many unintentional broken web applications ☺
- Many intentionally broken web applications
  - Different frameworks, languages, databases
  - Some available live, others to be downloaded and installed
- Several vendor provided apps exist
  - Test their product
- Training apps such as the OWASP WebGoat project
  - WebGoat originally written in J2EE now available on other platforms
  - An interactive teaching environment for web application security

Broken Web Application Project Goal

OWASP 中国
The Open Web Application Security Project

- Broken Web Applications are needed to know evil
  - Introduce people to the topic
  - Test web application scanner people
  - Test web application scanner products
  - Test source code analysis tools
  - Test web application firewalls
  - Collect evidence left by attackers
  - Develop business logic perspectives
  - Develop human element perspectives

Bad Web Apps Problems

OWASP 中国
The Open Web Application Security Project

- Some web sites are built on proprietary systems
- Back end databases may need licensing
- Can conflict with one another
- Can be difficult to install
- Should be set up in a secured and isolated environment

DISCLAIMER

OWASP 中国
The Open Web Application Security Project

OWASPBWA – A Virtual Machine that is a collection of broken web applications

!!! This VM has many serious security issues. We strongly recommend that you run it only on the "host only" or "NAT" network in the virtual machine settings !!!

OWASP BWA

OWASP 中国
The Open Web Application Security Project

- "Training Applications"
  - Web Goat (multiple platforms)
  - Damn Vulnerable Web Application
- "Real applications"
  - OWASP Vicnum project
  - Cyclone Transfers
- Older (broken) versions of real applications/frameworks such as WordPress and Joomla

Vicnum

OWASP 中国
The Open Web Application Security Project

- Flexible vulnerable web application useful to auditor's honing their web application security skills
- And anyone else needed a web security primer
- Based on games commonly used to kill time
- Used as a hacker challenge for several security events including http://www.appseceu.org/
- Available on Sourceforge
  - Guess the number (Guessnum)
  - Guess the word (Jotto)
  - Union Challenge
- Usually available live at http://vicnum.ciphertechs.com/

Demonstration of Vicnum

OWASP 中国
The Open Web Application Security Project

Two games to review in Vicnum

Guessnum - The computer will think of a three digit number with unique digits. After you attempt to guess the number, the computer will tell you how many of your digits match and how many are in the right position. Keeping on submitting three digit numbers until you have guessed the computer's number.

Jotto - The computer will think of a five letter word with unique letters. After you attempt to guess the word, the computer will tell you whether you guessed the word successfully, or how many of the letters in your guess match the computer's word. Keep on submitting five letter words until you have guessed the computer's word.

Where do we start?

What methodology?

What tools?

What are we after?

OWASP 中国
The Open Web Application Security Project

Demo of Vicnum

- Guessnum
- Jotto

Some OWASP tools to use:

- Zap
- DirBuster
- JBroFuzz

- Are input fields sanitized?
  - Cross site scripting attacks
    - GET
    - POST
  - SQL injections
- URL manipulation
- Backdoors in the application
- Administration and Authentication issues
- The question of state
- Encryption and encoding issues
- Business logic and the human element

Vicnum Review

OWASP 中国
The Open Web Application Security Project

- Did we find all the technical problems?
- Did we find non technical problems?

Cyclone Transfers

OWASP 中国
The Open Web Application Security Project

- Ruby on Rails Framework
- Available on github
  - git://github.com/fridaygoldsmith/bwa_cyclone_transfers.git
- A fictional money transfer service, that consists of multiple vulnerabilities including:
  - mass assignment vulnerability
  - cross site scripting
  - sql injections
  - file upload weaknesses
  - session management issues

OWASP 中国
The Open Web Application Security Project

Demo of Cyclone Transfers

Cyclone Review

OWASP 中国
The Open Web Application Security Project

- Did we find all the technical problems?
- Did we find non technical problems?
- Mass assignment allows Rails web apps to set many attributes at once
  - Rails is *convention-heavy* and certain fields like :admin, and :public_key are easily guessable
  - curl -d "user[email]=mo@abc.com&user[password]=password&user[password_confirmation]=password&user[name]=mo&user[admin]=true" localhost/cyclone/users
  - Many Rails based web sites were exploited in 2012 were exploited via the mass assignment vulnerability

Technical Issues in Web Hacking

OWASP 中国
The Open Web Application Security Project

- Hacking a network is different than hacking a web app
- Similarities do exist in certain areas
  - Cryptography checking
  - Credential attacks
  - Tools exist for scanning, fuzzing ….
- But major technical challenges exist
  - A request/response protocol where state is always an issue
  - How do you know you have found every vulnerability?
  - How do you know you have blocked every attack?

Non Technical Issues in Web Hacking

OWASP 中国
The Open Web Application Security Project

- Ultimately web pages are set up by application programmers meeting a business requirement
- Data works its way into web sites that might be difficult for a tool or a security analyst to evaluate
  - Comments might contain inappropriate data
  - URL fields can be manipulated and might show unintended web pages
  - URL parameters can also be guessed and may leak information
  - Hidden fields in form fields can be viewed and manipulated
  - Fields might be guessed
- How can we prepare hackers for the non technical piece of an assessment?

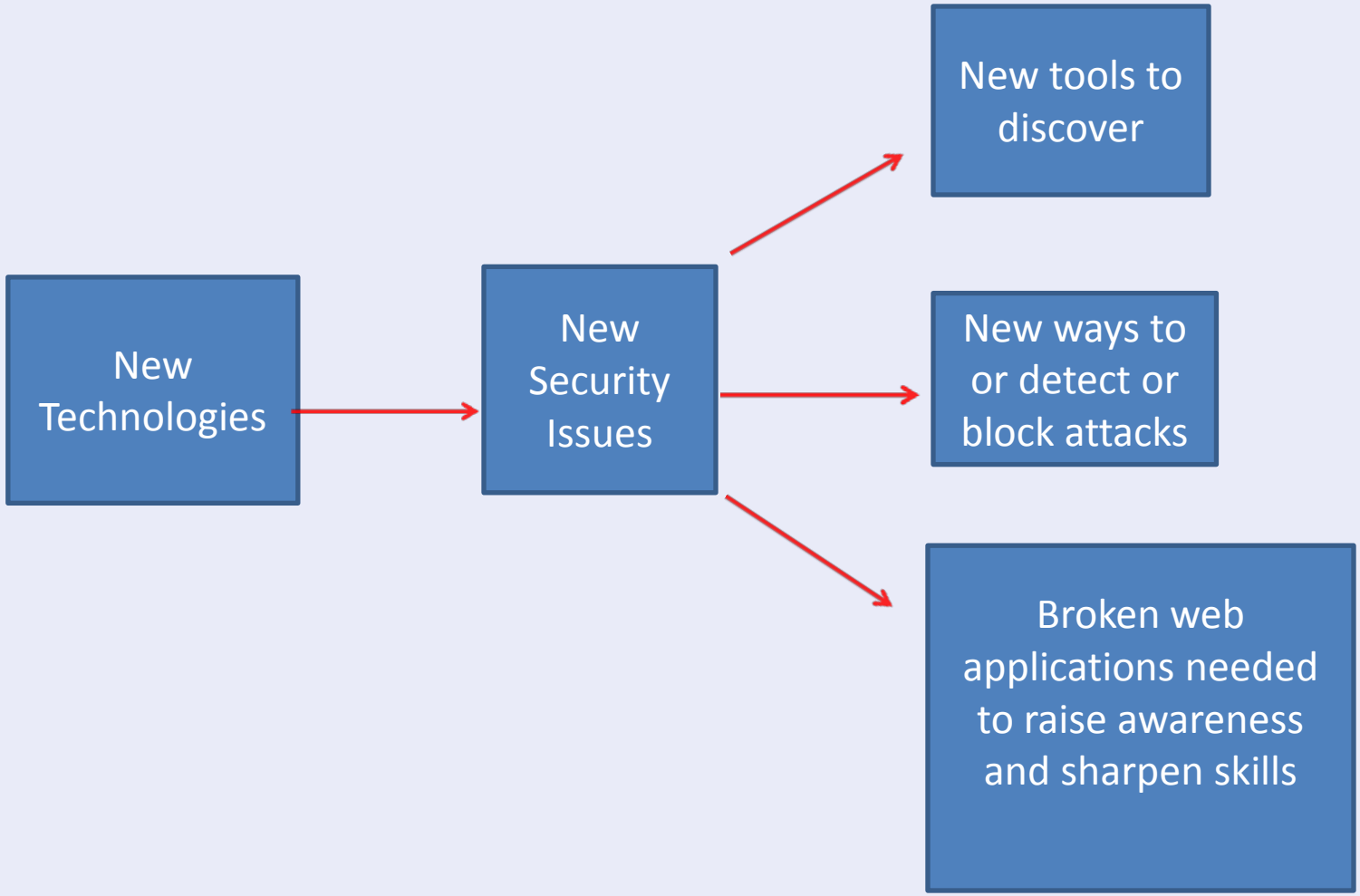
Some Political Questions

OWASP 中国
The Open Web Application Security Project

- Should web app security be done by network security?
- What kind of assessment?
  - Black Box
  - Gray Box
  - White Box
- How do you make sure that the latest web update is secure?
- Who is responsible for securing the app?
  - Network team
  - Application developer
  - Security team
- How does one remediate?
  - Code fix
  - Firewall block
- Manage the risk

Going Forward

OWASP 中国
The Open Web Application Security Project



Questions and Review

OWASP 中国
The Open Web Application Security Project

https://www.owasp.org/index.php/OWASP_Broken_Web_Applications_Project

@owaspbwa

@fridaygoldsmith

http://vicnum.ciphertechs.com
http://cyclone.ciphertechs.com

mo@ciphertechs.com

More Questions?

OWASP 中国
The Open Web Application Security Project

http://appsecusa.org/2013/