State of Web Application Security

Ralph Durkee
Durkee Consulting, Inc.
Rochester ISSA & OWASP Chapters
rd@rd1.net

Ralph Durkee

- **Founder of Durkee Consulting** since 1996
- **Founder of Rochester OWASP** since 2004
- **President of Rochester ISSA chapter**
- **SANS Instructor** and course developer
- **SANS GIAC Certified** – GSEC, GCIH, GCIA, GSNA, GPEN
- CISSP Certified
- **Application Security**, development, auditing, PCI compliance, pen testing, Ethical Hacking , Auditing and consulting
- **CIS (Center for Internet Security)** – developed benchmark security standards – Apache, Linux, BIND DNS, OpenLDAP, FreeRadius, Unix, FreeBSD

Agenda

- OWASP Updates
- App Sec DC 2010
- State of Web Application Security
- Web Security Methods and Tools
- Open Discussion on the State and Future of Web Application Security
- References and Resources

OWASP

Open Web Application Security Project

- A volunteer group, a not-for-profit charitable organization
- Produces free, professional-quality, open-source documentation, tools, and standards
- Dedicated to helping organizations understand and improve the security of their web application.
- Facilitates conferences, local chapters, articles, papers, and message forums

See **www.OWASP.org/rochester** for the Rochester Chapter

OWASP Brief History

- Sept 2001 – Started
- 2004 Local Chapters Started, include the Rochester Chapter
- Nov 2008 – First Summit in 2008 Portugal - Major Changes
  - Many Working Sessions
  - Formed Global Committees
  - New Outreach program, Tools and Guidance
- Nov 2009 – Smaller 1day Summit
- Feb 2011 – Next Summit in Portugal

OWASP 2008 Summit

OWASP EU Summit Portugal

Over 80 application security experts from over 20 countries joined forces to identify, coordinate, and prioritize our 2009 efforts to create a more secure Internet.

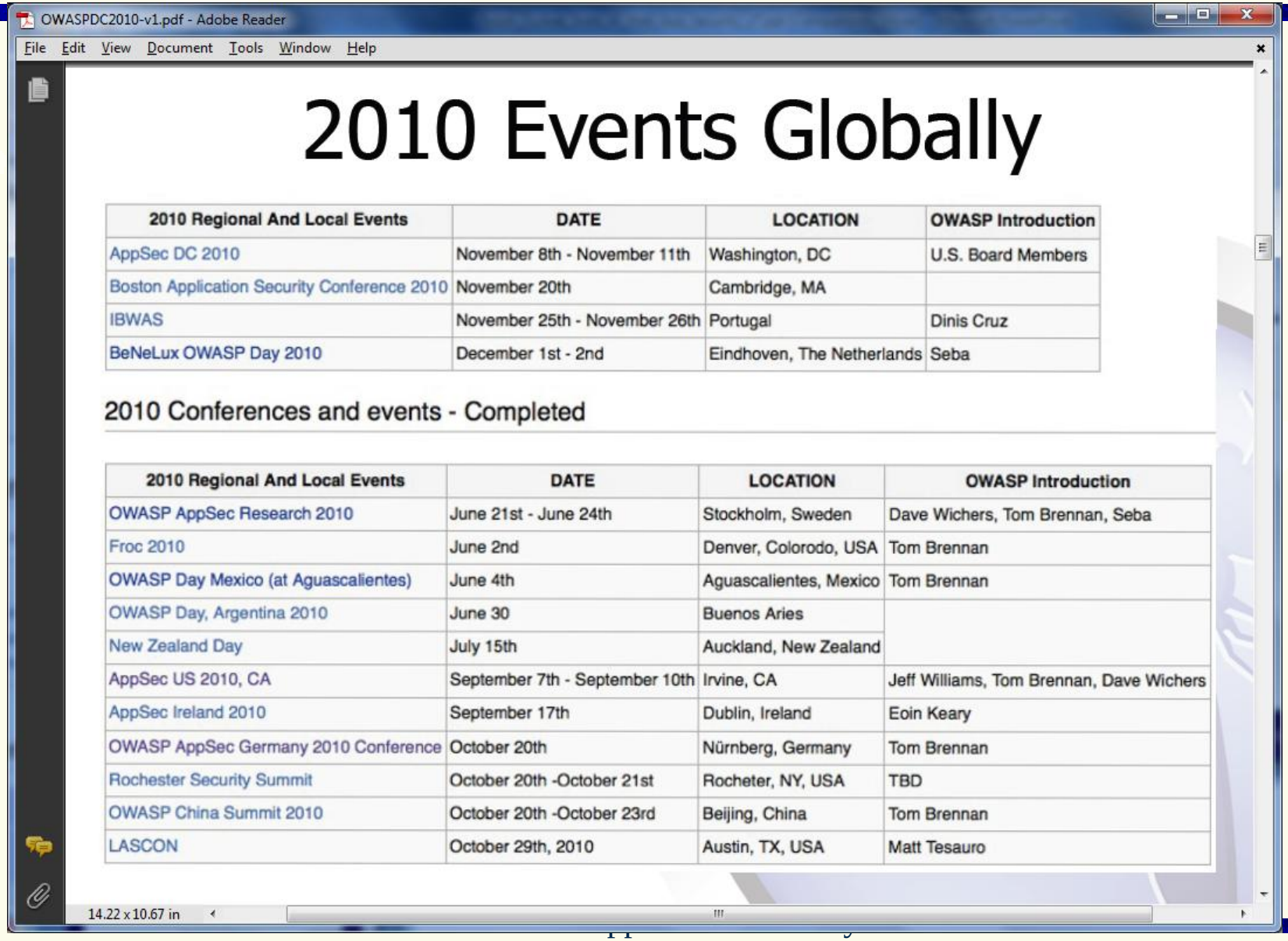
OWASP 2011 Summit

- Lots of anticipated work sessions
- Expected changes for OWASP
- Talk of new OWASP 4.0!

App Sec DC 2010

- Major App Sec Conference
- 2 Training Days and 2 Plenary Days
- 4 Parallel Tracks each days
- Plenty of great presentations
- RSS get's a major mention in the keynote
- Presentation slides available on-line

App Sec DC 2010 & RSS



App Sec DC 2010 – Highlights

H.....t.....t....p.......p....o....s....t

H.....t.....t....p.......p....o....s....t

Presented by

Onn Chee – OWASP Singapore Lead

Tom Brennan – OWASP Foundation

A new Layer 7 DoS attack

App Sec DC 2010 – Highlights H.....t.....t....p.......p....o....s....t

H.....t.....t....p.......p....o....s....t - Onn Chee & Tom Brennan

- New Denial Service Vulnerability
- Has some Similar to Slow Loris, but uses POST
- Very difficult to mitigate
- Affects All Web Applications that allow POST
- Vendors – Its a protocol flaw - no fix coming
- Followed by Workshop on slow HTTP Post DoS

App Sec DC 2010 – Highlights H.....t.....t....p.......p....o....s....t

- How it Works
- HTTP Post send with all the HTTP Headers
- Sending headers bypasses the IIS Slowloris mitigation which times out on the headers.
- Content-Length indicates size of the body
- Content is sent very slow and in small pieces.
- For Example 1 bytes per 110 seconds.
- Large servers easily brought down with only 20k connections

App Sec DC 2010 – Highlights
Closing the Gap

Closing the Gap: Analyzing the Limitations of Web Application Vulnerability Scanners

By

- David Shelly
- Randy Marchany
- Joseph Tront

Virginia Polytechnic Institute and State Univ.

App Sec DC 2010 – Highlights
Closing the Gap

Closing the Gap: Analyzing the Limitations of Web Application Vulnerability Scanners

- Examined Current State for Web App Scanners for accurately detecting:
  - SQL Injection
  - Cross-Site Scripting (XSS)
  - Session Management Flaws
- 6 Web App Vulnerability Scanners examined:
- Results Anonymized - not intended to compare products

App Sec DC 2010 – Highlights
Closing the Gap - Results Summary

Vulnerability Tested	Detected	Implemented	False Negatives
SQL-Inject Form	59.7%	12	40.3%
SQL-Inject Cookie	6.3%	8	93.7%
XSS Reflect	43.3%	10	56.7%
XSS Stored	11.1%	6	88.9%
XSS DOM-based	0%	1	100%
Session Predictable SID	20%	1	80%
Session Insecure Cookie	4.4%	9	95.6%

App Sec DC 2010 – Highlights
Closing the Gap – False Positives

Vulnerability Tested	Total Reported	Avg. Correct	False Positives
SQL-Inject False Positives	58	79.3%	20.7%
XSS – False Positives	36	86,1%	13.9%

App Sec DC 2010 –Highlights Power of Code Review

Power of Code Review

By Dave Wichers – Aspect Security & OWASP Board

- Compared Manual Code Review vs. Manual Web App Pen Test
- Demonstrated that many flaws are easier to find and verify with Code Review rather than with penetration testing.

App Sec DC 2010 –Highlights
Power of Code Review - Summary

Summary

- To find them?
  - Result: Similar, but slight edge to code review.
    - It's a MYTH that code review is way more expensive. If you have people with the right skills, its actually faster AND more effective
- To find exactly where they are in the app?
  - Result: Clear advantage to code review
- To verify we don't have them?
  - Result: Also clearly the advantage goes to code review

App Sec DC 2010 –Highlights Read the Label

Don’t Judge a Website by its Icon – Read the Label!

By Jeff William – Aspect Security & OWASP Chair

- Reviewed Impact of Consumer Labels on the industry
- Proposed Security Labels for Applications
- Addresses Issue of how do we make Software Security Visible.

State of Security
What is being Attacked?

- Major shifts in targets for Attacks
  - Web Applications
  - Client Browsers
  - Client E-mail
  - Combinations of all of the above
- Why the Change?
  - Attackers go for the easy targets
  - Broadband clients are very useful too

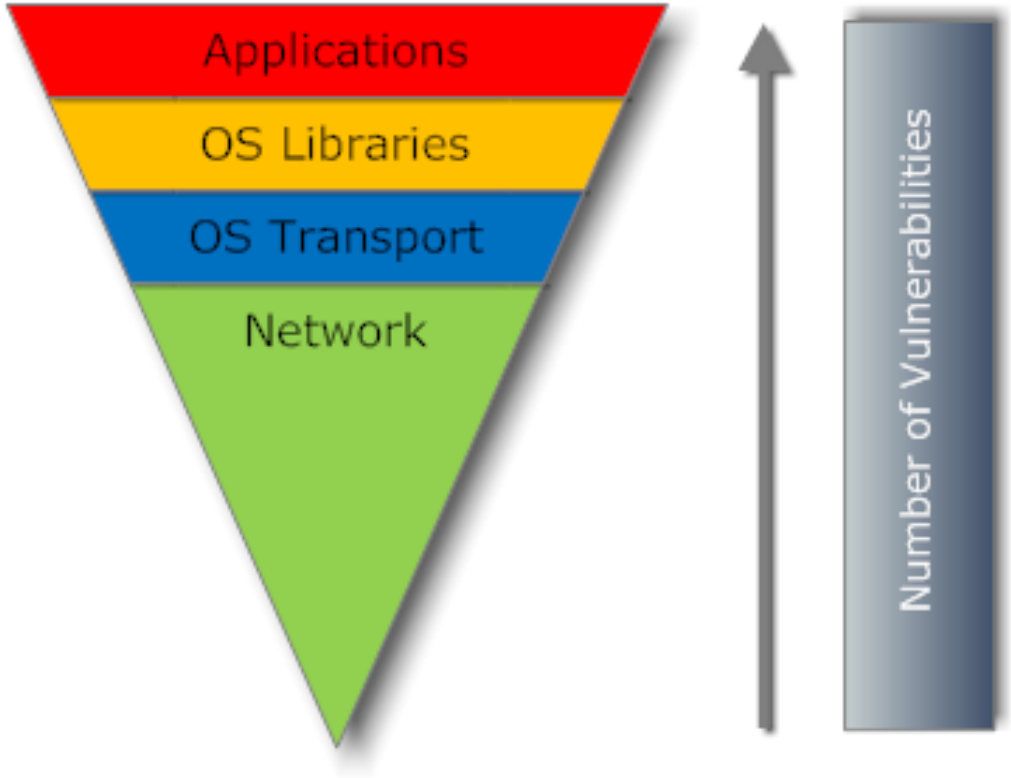
Web Application Vulnerabilities

Web Application Security is:

Traditional Layers	Traditional Security Controls
Network Protocols	Firewalls, Routers, Operating System IP Stack Configuration and Filtering, VPNs, and Vulnerability Scanners
Operating System	Operating System Patches and OS Configuration, Authentication, Authorization, Encryption, and Vulnerability Scanners
Commercial and Open Source Applications	Minimize Services, Application Configuration, Patches, Application Level Authentication Authorization, and Vulnerability Scanners
Custom Web Applications	Architecture, Design and Code Reviews, Application Scanners, Testing with Malicious Input

How Bad Is It? – SANS - Top Cyber Security Risks

- Sept 2009 Report with data from TippingPoint IPS and vulnerability data by Qualys.
- Web Applications have largest # of Vulnerabilities.



How Bad Is It? – More Reports

- Typically reports are **90-99% of Web Applications are Vulnerable**
- Privacy Rights Clearing House reports 93% of all data breaches involve Applications or Databases.
- Gartner reports 75% of attacks today are at the Application Level
- **90% of malware originates from legitimate websites** that have been hacked [Sophos July 2008]

How Bad Is It? - Verizon 2010 Data Breach Investigations Report

Attack Pathways

After being edged out in 2008 as the most-used path of intrusion, **web applications now reign supreme** in both the number of breaches and the amount of data compromised through this vector.

. . . **54% of breaches and 92% of records . . .**

Web applications have the rather unfortunate calling to be public-facing, dynamic, user-friendly, and secure all at the same time. Needless to say, it's a tough job.

http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf

How Bad Is It? – SANS @ RISK Vulnerability Reports

- Vulnerability Reports consistently report Web Applications with highest # of vulnerabilities.
- Example SANS @RISK Oct 2010

SANS @RISK Oct 2010	10/7	10/15	10/21	10/28	**Total**
Microsoft	3	14	11	0	**28**
Mac	0	0	0	1	**1**
Linux	4	10	4	2	**20**
Solaris	0	0	0	0	**0**
Network Device	0	0	2	0	**2**
Web Applications	28	7	15	9	**59**

Auditing Web Applications

Security Trends

- Vast Majority of Vulnerabilities are now found in the Web Applications
- The Criminals have shifted their focus to attacking Web Applications and Web clients

Audit Trends?

- Has Auditing adjusted to the changing threats?
- As Auditors are we focusing a majority of the effort where we find the greatest risks?
- Are check lists and automated scans effective for auditing custom in-house developed applications?

Auditing Web Applications Methods

In addition to check-list and network scans:

- Applications Vulnerability Scanners
- Web App Penetration Testing
- Security Code Reviews
- SDLC training and processes - Integrate Security throughout the Software Development Life Cycle
- Threat Modeling
- See **www.OWASP.org** for free resources on each

Web Application Code and Network Scanners

- **Web Application Scanners**
  - Different from Vulnerability scanners
  - Not as easy to use
  - High level of False Positives and False Negatives
- **Study by Stanford** [1]
  - Vulnerability detection rate averaged from 2% - 48% depending on vulnerability category
- **Study by MITRE** [2]
  - All tool vendors claims put together covered only 45% of over 600 CWE vulnerabilities studied.

OWASP ASVS - Application Security Verification Standard

Level 1 – Automated Verification

- Level 1A – Dynamic Scan (Partial Automated Verification)
- Level 1B – Source Code Scan (Partial Automated Verification)

Level 2 – Manual Verification

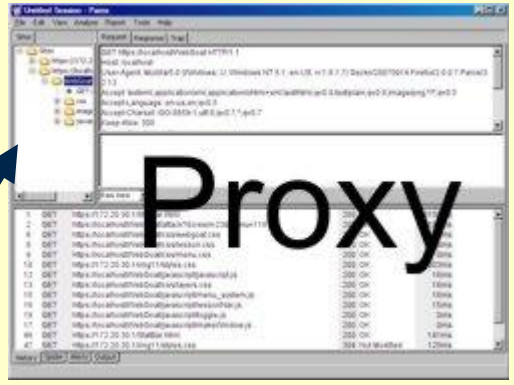
- Level 2A – Penetration Test (Partial Manual Verification)
- Level 2B – Code Review (Partial Manual Verification)

Level 3 – Design Verification (Includes Threat Modeling)

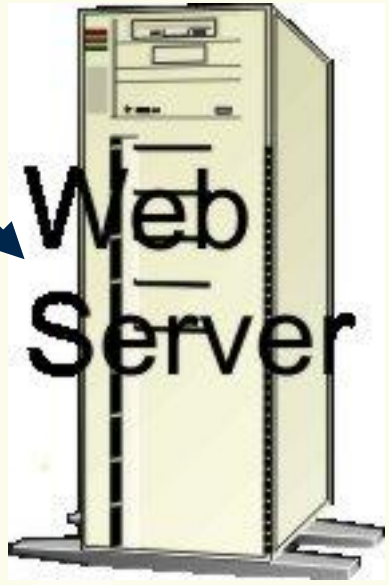
Level 4 – Internal Verification

Testing Web Applications with a Proxy

App. Tester or Attackers Computer



All request and responses may be analyzed and modified using the proxy!



Secure SDLC
Building Secure Web Applications

- Application vulnerabilities are NOT prevented by traditional security controls
- Application Security starts with the Architecture and Design
- Security can't be easily added on later without re-work
- Educate developers and testers on Web App Security.
- Perform application architecture and code reviews with security trained professionals.
- Integrate security into software development life cycle.
- Don't invent your own security controls
- **Design, Design, Design,** code**, Test, Test, Test**

Threat Risk Modeling

Looks at detailed architecture and design along with threat vectors, and abuse cases to identify vulnerabilities and analyze the risk.

Steps:

1. **Identify Security Objectives**
2. **Survey the Application**
3. **Decompose it**
4. **Identify Threats**
5. **Identify Vulnerabilities**

Discussion and Questions

Current State

- Are we making progress? And are we getting ahead of or keeping up with the threats?
- How has the risks changed?
- In what areas are we as an application security industry doing better, and where is improvement needed?

Discussion and Questions

Current State

- Are we making progress? And are we getting ahead of or keeping up with the threats?
- How has the risks changed?
- In what areas are we as an application security industry doing better, and where is improvement needed?
- Is the Application Software Industry a broken economy?

Discussion and Questions – Future State

Future State

- Where should we be headed?
- Are there major changes needed or helpful to "fix" the application security profession?

Resources – Rochester Non-Profit Groups

OWASP Rochester Chapter Information

http://www.OWASP.org/rochester

Rochester Security Summit Oct 2011

htttp://RochesterSecurity.org

Rochester ISSA Chapter

http://RochISSA.org

On-Line References

1. **State of The Art: Automated Black Box Web Application Vulnerability Testing - Stanford Computer Lab**
   http://www.owasp.org/images/2/28/Black_Box_Scanner_Presentation.pdf and
   http://theory.stanford.edu/~jcm/papers/pci_oakland10.pdf
2. **SAMATE and Evaluating Static Analysis Tools**
   http://hissa.nist.gov/~black/Papers/staticAnalyExper%20Ada%20Geneva%20Jun%20007.pdf
3. **Verizon 2010 Data Breach Investigations Report**
   http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf

On-Line Resources

SANS The Top Cyber Security Risks Sept 2009

http://www.sans.org/top-cyber-security-risks/

Washington Post - European Cyber-Gangs Target Small U.S. Firms

http://www.washingtonpost.com/wp-dyn/content/article/2009/08/24/AR2009082402272.html

Washington Post - PC Invader Costs Ky. County $415,000

http://voices.washingtonpost.com/securityfix/2009/07/an_odyssey_of_fraud_part_ii.html

IBM X-Force reports time from disclosure to exploit often less then 24 hours.

http://www.theregister.co.uk/2008/07/29/x_force_threat_report/print.html

Honetnet Project KYE: Fast-Flux Service Networks

http://honeynet.org/node/132

OWASP - Open Web Application Security Project

http://www.owasp.org/

Thank You!

Ralph Durkee
Durkee Consulting, Inc.
Rochester OWASP & ISSA Chapters
rd@rd1.net