



build | integrate | secure

Jump-Start Your Application Security Knowledge: For the Network Security Guy Who Knows Nothing about Applications

Jeremiah Grossman
John B. Dickson, CISSP

Speaker's Backgrounds

- Jeremiah Grossman
 - *Founder & CTO of WhiteHat Security*
 - *World-renowned expert in Web security and founder of the Web Application Security Consortium (WASC)*
 - *Former information security officer at Yahoo!*
- John Dickson
 - *Denim Group Principal and career security professional*
 - *Assists CISO's build application security programs*
 - *Prior to Denim Group, was a information security consultant at SecureLogix, KPMG, Trident Data Systems, and US Air Force*

Company Backgrounds

- WhiteHat Security Background
 - *WhiteHat Security is the leading provider of website risk management solutions*
 - *WhiteHat serves hundreds of customers in e-commerce, financial services, information technology and healthcare including many of the Fortune 1000*
 - *WhiteHat Sentinel, the company's flagship product family, launched in 2003*
- Denim Group Background
 - *Denim Group is a professional services company that*
 - develops secure software
 - helps organizations assess and mitigate risk with existing software
 - provides training on best practices in software security
 - *WhiteHat Security's Premier Integration Partner*
 - Built Snort-Sentinel Integration for real-time application level blocking

“Houston we have a Problem”

- Throughout industry security officers are responsible for the security of applications
 - *If a breach occurs involving applications, who gets called first?*
 - *CIO's largely can't distinguish between web applications and the infrastructure in which applications reside*
 - *Rarely, if ever, do security manager have control of development efforts to remediate*
- It begs the question
 - *Why are development colleagues not on the “hot seat” as well?*
- Security professionals are rushing into the application security world
 - *New entrants into the field have less background knowledge in applications*
 - *Demand to increase for application-smart security professionals*

The Key Problem

Security officers worry about application vulnerabilities, but have little power to fix them...

Development managers have power to fix application vulnerabilities, but don't worry about them

Business Impact of this Problem

- Many Security professionals are ill-equipped to secure applications
 - *Difficulty analyzing application-level scan reports*
 - *Sometimes powerless to overcome development team objections*
 - *Network vulnerabilities get fixed relatively quickly – not the case for applications*
- WhiteHat Website Security Statistics Report
 - *82% of websites have had a HIGH, CRITICAL, or URGENT issue*
 - *Vulnerability time-to-fix metrics are not changing substantively, typically requiring weeks to months to achieve resolution*
 - *Security managers need to do a better job of managing or influencing the solution*

Results of Denim Group Survey

- 75% of security respondents did not know the likely outcome of the exploitation of a Cross-Site Scripting (XSS) vulnerability
- Nearly 70% did not know that modern development languages like Java and .NET could provide protection against buffer overflow vulnerabilities
- Nearly 50% thought developers could perform source code reviews in the requirements
- Nearly 70% of respondents could not identify that logical vulnerabilities involving authorization and authentication are typically more difficult to remediate than coding flaws such as Cross-Site Scripting (XSS) or buffer overflow vulnerabilities

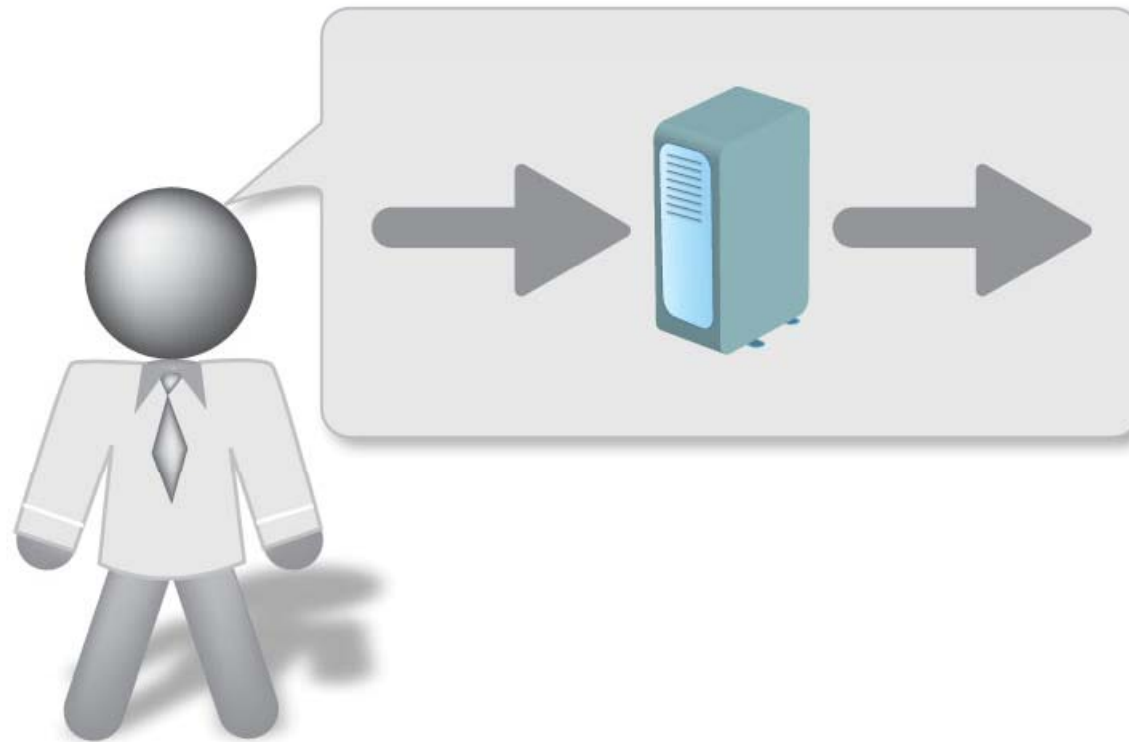
A Journey of 1,000 Miles Starts with one Step...

- Raise the bar on your knowledge of key aspects of software development, including:
 - *Key coding terms*
 - *software architecture terms*
 - *Different software development methodologies*
- Build up a dictionary of terms tailored to your environment
- Find a trusted development colleague to ask questions you wouldn't ask in a public meeting
- Understand what SDLC's their organization uses
 - *Different software development methodologies will drive how you want to introduce security practices to internal development teams*

Ask a Better Set of Questions!

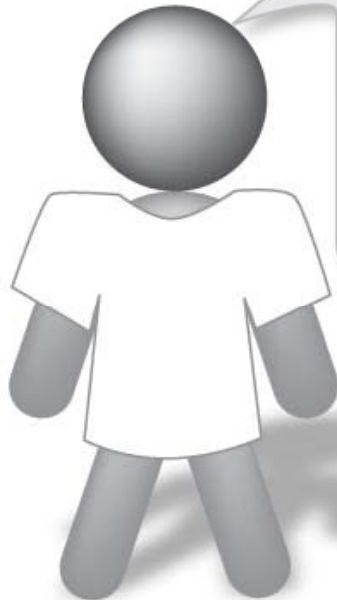
- Consider Participating in Threat Modeling Process
 - *A structured approach to understanding where vulnerabilities might exist in complex systems such as software applications*
 - *Enables security professionals to characterize risk and ask a more sophisticated set of questions to developers without diving to the level of application source code*
 - *Will help a non-coder think in more concrete terms by decomposing a complex application into its component pieces*

How Security Guys Think



securityTHINK

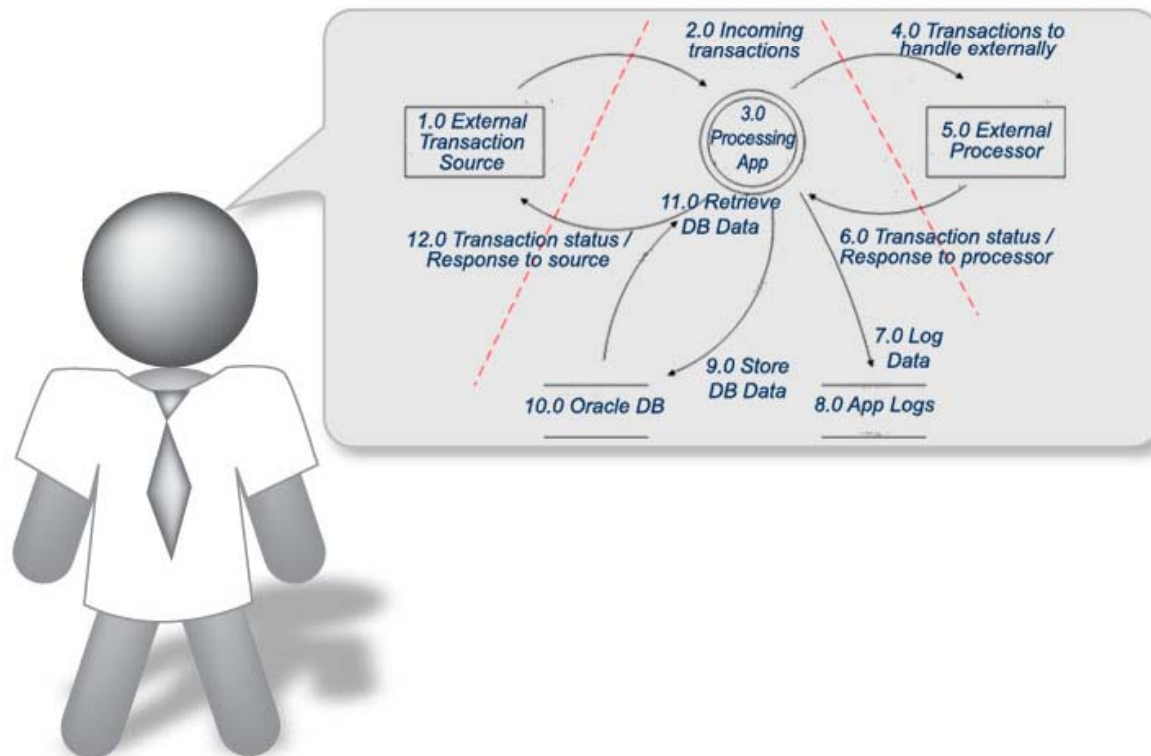
How Developers Think



```
} else if ((arg2) && (arg2.length > 0)){
    if ( cmd == "LMSGetValue") {
        testquestionsObj.SetVariable(arg2,
SC0GetValue(arg1));
    } else if ( cmd == "LMSGetLastError") {
        testquestionsObj.SetVariable(arg2,
SC0GetLastError(arg1));
    } else if ( cmd == "LMSGetErrorString")
    {
        testquestionsObj.SetVariable(arg2,
SC0GetLastError(arg1));
    } else if ( cmd == "LMSGetDiagnostic")
    {
        testquestionsObj.SetVariable(arg2,
SC0GetDiagnostic(arg1));
    } else {
        // for unknown LMSGetxxxx extension
        v = eval('g_objAPI.' + cmd + '(\\"' +
```

developer**THINK**

How Security Guys Should Think



idealTHINK

WhiteHat Sentinel – Snort Integration

- Denim Group developed technology based on the WhiteHat's open XML application programming interface (API), allowing for a seamless integration with Snort® to block website attacks
 - Highly accurate vulnerability information combined with an open XML API allows WhiteHat Sentinel data to be shared and employed within an organization's existing communications and reporting infrastructure
 - Integration supports both open source and commercial versions of IPS/IDS
 - Any IDS/IPS that imports these rules will work
- Sentinel customers can now use vulnerability data to quickly create ultra-targeted Snort rules
 - Expands capability of IPS to detect and block application layer attacks in real time
 - Fine-tunes Snort alerts and correlate findings to reduce noise
 - Leverages existing, deployed infrastructure
 - » 80% Fortune 100 use Snort
 - » No need to retrain employees or reconfigure networks



How the integration works:

- Implemented as a script, which when executed, will securely connect to the Sentinel open API to extract website's vulnerability details
 - Script translates downloaded data into Snort alert rules
 - Users apply rules to Snort IPS to alert on or block attacks
- Simple deployment
 - All Sentinel customers have access to Open XML API free of charge
- WhiteHat Open XML API also enables data exchange with:
 - Web Application Firewalls
 - Bug tracking systems
 - Security Information and Event Management systems

Contact Information

- Jeremiah Grossman
 - *jeremiah@whitehatsec.com*
 - *Twitter @jeremiahg*

www.whitehatsec.com

- John B. Dickson, CISSP
 - *john@denimgroup.com*
 - *Twitter @johnbdickson*

www.denimgroup.com