OWASP ROI:

Optimize Security Spending using OWASP

Matt Tesauro
OWASP Global Projects
Committee Member
OWASP Live CD Project Lead
mtesauro@gmail.com

OWASP
Austin
Chapter

The OWASP Foundation
http://www.owasp.org

OWASP ROI:

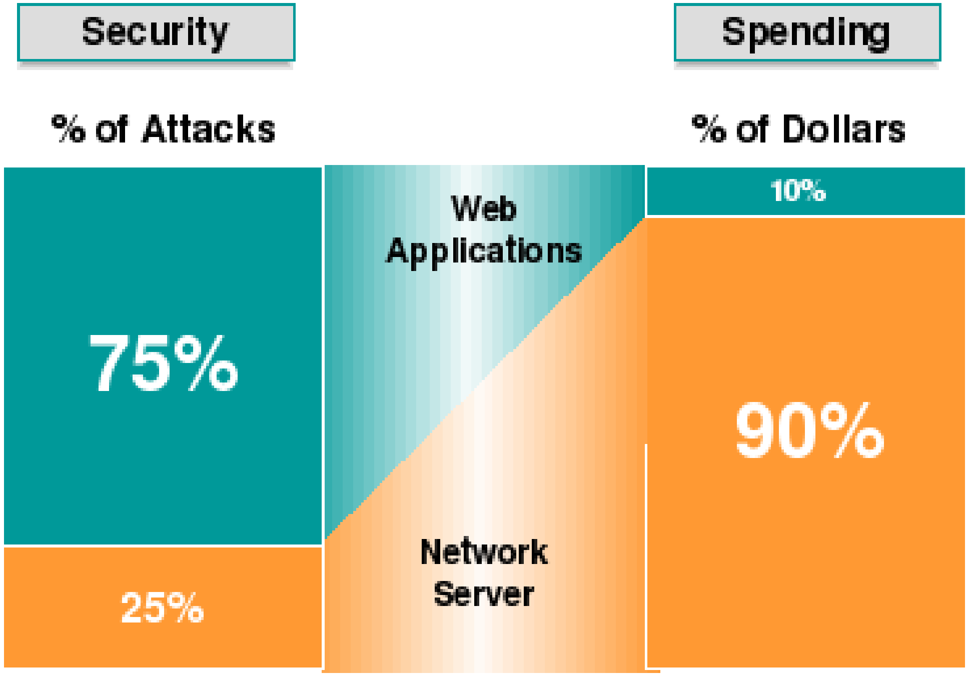
Optimize Security Spending with OWASP

- Introduction
- Case Study: U.S. Financial Institution
  - Mission and Goals of the Security Team
  - Before OWASP (How things ***were*** done)
  - With OWASP (How things ***are*** done)
  - OWASP in my career
- Projects you should probably know
  - Projects already mentioned
  - Projects you should probably know
  - Projects to keep you eye on

Who's this speaker anyway?

- Varied IT Background
  - Developer, DBA, Sys Admin, Pen Tester, Application Security Engineer
  - CISSP, CEH, RHCE, Linux+
- Long history with Linux and Open Source
  - First Linux install ~1998
  - DBA and Sys Admin was on open source
  - Contributor to many projects, leader of one
- Background in Economics and taught at the business school at Texas A&M University

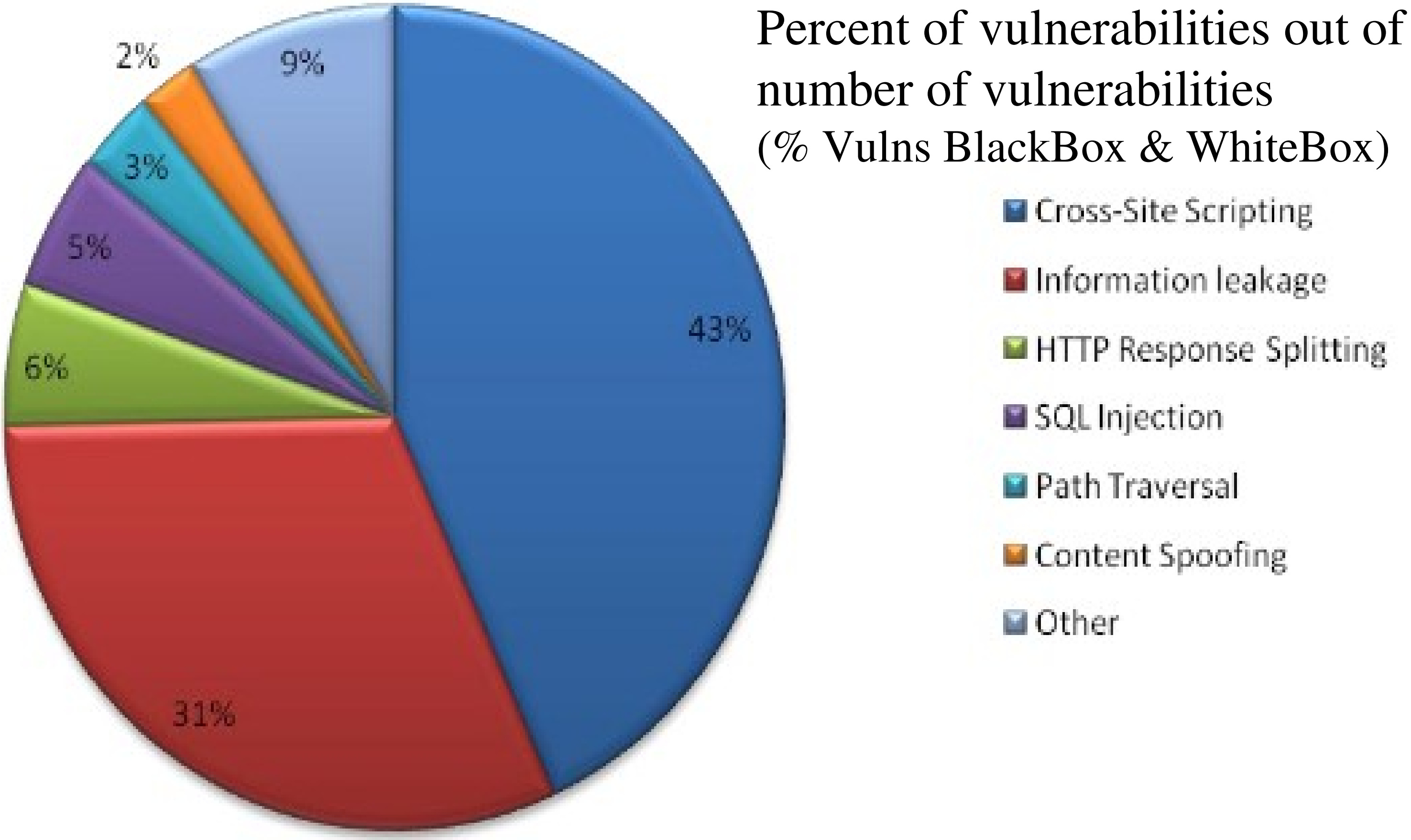
Spending Levels Today



2/3 of All Web Applications Are Vulnerable
Gartner

Sources: Gartner, Watchfire

What are the web attacks?



Percent of vulnerabilities out of total number of vulnerabilities
(% Vulns BlackBox & WhiteBox)

Source: WASC Web Application Security Statistics 2008
http://projects.webappsec.org/Web-Application-Security-Statistics

Case Study: U.S. Financial Company

- Company name will not be disclosed

  (We need a name for this company)

  UFS (Unidentified Financial Services)

USF: Company Overview

- Relative size
  - Among the largest 25 banks in the U.S.
  - Branches in many states in the U.S.
- General information
  - Company Type: Subsidiary of larger firm
  - Industry: Finance and Banking
  - Revenue: 2+ Billion USD (3.43+ Billion BRL)
  - Employees: 13,000+
  - Parent Company: ~$14 billion in revenue (24 billion BRL), ~$650 billion in assets (~1,114 Billion BRL) and ~110,000 employees

1 USD = 1.715 BRL

USF: IT Security

- The USF Security group
  - 8 IT Security Analysts (full-time employees)
- Mission and Goals
  - Compliance efforts
    - PCI DSS & SOx (Sarbanes-Oxley Act)
    - Compliance is a starting point for them. They aim for secure and get compliance along the way.
  - Assessment / security reviews of online assets
    - Online assets include multiple web applications
  - Traditional network based security services
  - Anti-Phishing efforts

USF: Before OWASP

- Fiscal Year 2007
- Web Application security reviews
  - Utilized only outside security firms
  - USF security group handled remediation tasks
  - Request for additional details on review findings represented additional costs
  - Average engagement cost: $8,000 per site
    13,720 BRL

    Web App Security reviews for 2007 = 30 sites
    or $240,000 total cost
    411,600 RBL

1 USD = 1.715 BRL

USF: With OWASP

- Fiscal Year 2008
- Web Application security reviews
  - Utilized only internal security analysts
    - Used the OWASP Testing Guide v2 plus WebScarab as their standard for testing web applications
    - Printed guide copies for all 8 analysts for $200 (343 BRL)
  - USF security group handles remediation tasks
  - Average engagement cost: $0 per site
    - Assumes salaries are a fixed cost
    - No new staff added for this effort
  - Assessed 48 sites in 2008

1 USD = 1.715 BRL

USF: With OWASP

Web App Security review costs:

2007 $240,000 (30 sites x $8,000/site)
411,600 BRL
2008 $200 for 48 sites (printing costs)
343 BRL
If 2008 didn't have OWASP:
$384,000 (48 sites x $8,000/site)
658,560 BRL
OWASP Savings = $383,800 in year 1
658,217 BRL

1 USD = 1.715 BRL

USF: The Pros with OWASP

- Cost reduction will continue past year 1
  - Accomplished more reviews at a lower cost
  - Time to assess should trend down
- Reports are standardized now
  - Different vendor = different reporting in prior years
  - Standard reporting = better trend analysis
- Increased Efficiency in remediation
  - Analysts better understand the reported findings
- Analysts can better address audit questions
  - Annual audits from Govn't & parent company
  - Federal auditors praised the “well developed internal review process”

USF: The Cons with OWASP

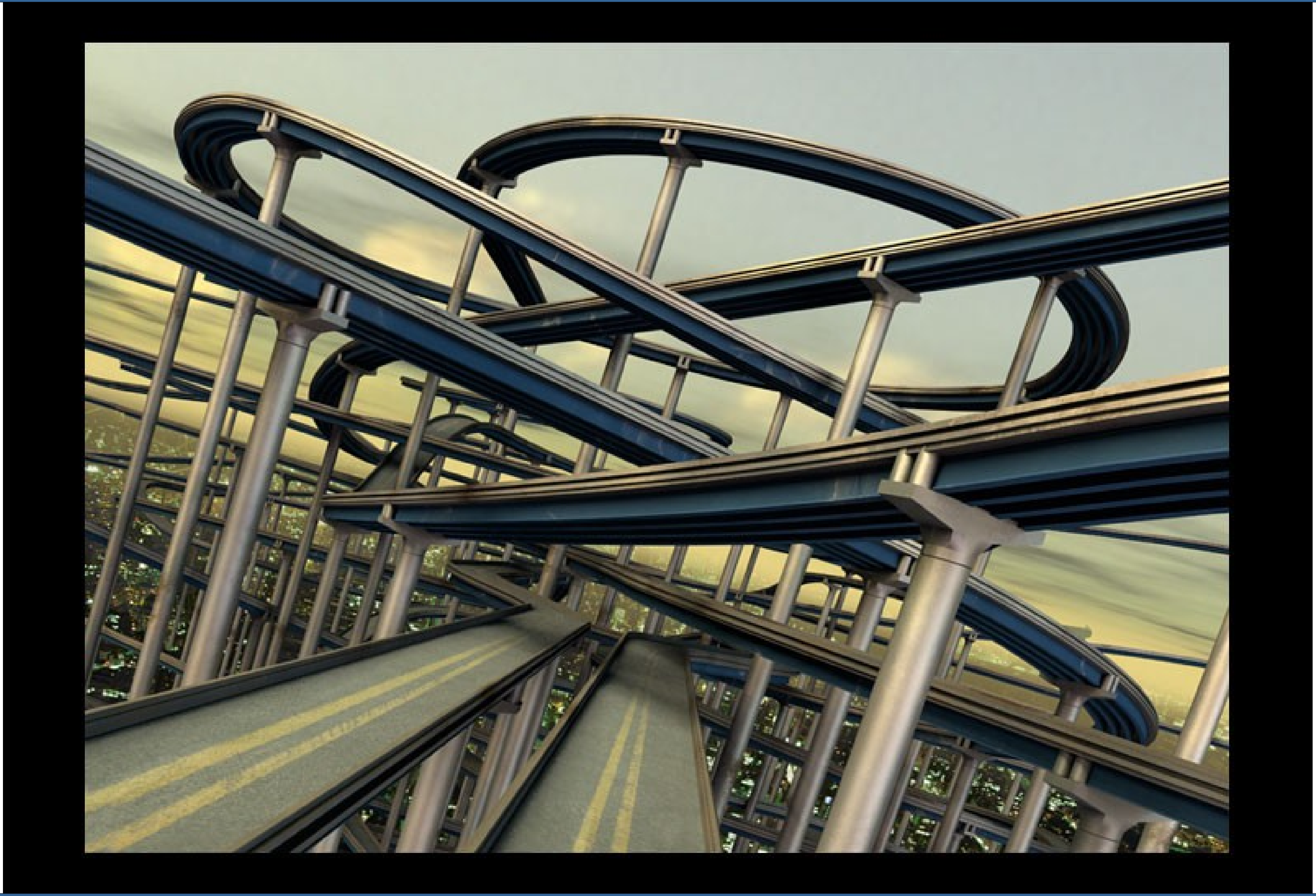
- Starting up the program was initially slow
  - Mid-year efficiency gains allowed them to surpass the 2007 review number in 2008
- Requires strong management support
  - Must accept the potential for a slow year 1
- At least one analyst must be familiar with application security to lead the effort
- Additional training is still needed for some USF analysts
  - Level out the skills of the analysts
  - One time cost of $15,000 to $25,000 for on-site, instructor based training (25,725 to 42,875 BRL)

1 USD = 1.715 BRL

Some Personal Anecdotes

- OWASP Projects used in my security career
  - OWASP WebGoat
    - How I first learned about application security
  - OWASP WebScarab
    - Used during many penetration test
  - OWASP Live CD
    - My current preferred App Sec testing environment
  - OWASP Testing Guide
    - Used in creating reports during security reviews
  - OWASP Legal Project
    - Utilized language from the project to add security language to our procurement process documents

Untangling the OWASP Projects knot



Projects you should probably know

Lets untangle the knot of OWASP Projects (120+)

- Review of those we've already mentioned
- Other good projects to know
- Things to keep your eye on

  For each project,

  - A brief description / overview
  - Suggestions on how it can help your security efforts
  - A link to the website

Note: These are projects that have the caught the speakers attention. It is possible, if not likely, that several great projects have been missed. My apologies to those projects.

OWASP Testing Guide

- Provides a “best practice” penetration framework and a “low level” penetration testing guide that describes techniques for testing web applications.
  - Version 3 is the latest and is a 349 page book
  - Tests split into 9 sub-categories with 66 controls to test
- Benefits
  - Ready made testing framework
  - Great categories and identifiers for reporting
  - Excellent to augment skills of analysts

http://www.owasp.org/index.php/Category:OWASP_Testing_Project

OWASP WebScarab

- WebScarab is a tool to analyze applications which communicate via HTTP/HTTPS. It is an intercepting proxy with numerous features
  - Proxy, Spider, Manual Intercept, Fragments, Search, Compare, Fuzzer, Session Analysis, Bandwidth simulator, scripting support, ...
  - WebScarab NG is a re-write of the original
- Benefits
  - Single tool which can cover the majority of manual testing needs
  - Scripting allows for customization

http://www.owasp.org/index.php/Category:OWASP_WebScarab_Project

OWASP WebGoat

- WebGoat is a deliberately insecure J2EE web application created by OWASP and designed to teach web application security lessons
- Benefits
  - Fantastic introduction to basic and more advanced application security concepts
  - Fully developed and complete web application that can tested safely and without legal worries
  - Detailed lesson solution hints
  - Runs on Windows/OS-X/Linux

http://www.owasp.org/index.php/Category:OWASP_WebGoat_Project

OWASP Live CD

- The OWASP Live CD collects some of the best open source security projects in a single environment. Web developers, testers and security professionals can boot from this Live CD and have access to a full security testing suite.
  - Virtual Box and VMware installs also available
  - 26 pre-configured and integrated tools
- Benefits
  - Web App Testing environment in one download
  - No need to gather and configure all the tools
  - Includes documentation also (OWASP Guides, etc)

http://www.owasp.org/index.php/Category:OWASP_Live_CD_Project

OWASP Legal Project

- The OWASP Legal Project helps software developers and their clients negotiate and capture important contractual terms and conditions related to the security of the software to be developed or delivered.
  - The Contract Annex provides a framework for determining how software security will be handled when developing software
- Benefits
  - Provides clear and complete language
  - Can (and should) tailor it to the business's needs

http://www.owasp.org/index.php/Category:OWASP_Legal_Project

Unveiling projects we've not seen yet...

OWASP Top Ten

- The OWASP Top Ten represents a broad consensus of what the most critical web application security flaws are.
  - Adopted by the Payment Card Industry (PCI)
  - Recommended as a best practice by many government and industry entities
- Benefits
  - Powerful awareness document for web application security
  - Great starting point and reference for developers

http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

OWASP ESAPI

- OWASP Enterprise Security API (ESAPI) is a free and open collection of all the security methods that a developer needs to build a secure web application.
  - API is fully documented and online
  - Implementations in multiple languages
- Benefits
  - Provides a great reference
  - Implementation can be adapted/used directly
  - Provides a benchmark to measure frameworks

http://www.owasp.org/index.php/Category:OWASP_Enterprise_Security_API

OWASP ASVS

- The OWASP Application Security Verification Standard (ASVS) defines a standard for conducting app sec verifications.
  - Covers automated and manual approaches for external testing and code review techniques
  - Recently created and already adopted by several companies and government agencies
- Benefits
  - Standardizes the coverage and level of rigor used to perform app sec assessments
  - Allows for better comparisons

http://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project

OWASP Open SAMM

- The Software Assurance Maturity Model (SAMM) is an open framework to help organizations formulate and implement a strategy for software security that is tailored to the specific risks facing the organization.
- Benefits
  - Evaluate your organization's existing software security practices
  - Build a balanced software security program in well-defined iterations.
  - Demonstrating concrete improvements

http://www.owasp.org/index.php/Category:OWASP_Software_Assurance_Maturity_Model_Project

OWASP Guides

- OWASP Testing Guide (already covered above)
- OWASP Code Review Guide
  - Documentation on the best practices for reviewing code
- OWASP Application Security Desk Reference
  - Reference volume of App Sec Fundamentals
- OWASP Development Guide (a bit old)
  - A massive document covering all aspects of web application and web service security
- OWASP AppSec FAQ Project
  - FAQ covering many app sec topics

OWASP AntiSamy

- OWASP AntiSamy is an API for ensuring user-supplied HTML/CSS is compliant within the applications rules.
  - API plus implementations
  - Java, .Net, Coldfusion, PHP (HTMLPurifier)
- Benefits
  - It helps you ensure that clients don't supply malicious code into your application
  - A safer way to allow for rich content from an application's users

http://www.owasp.org/index.php/Category:OWASP_AntiSamy_Project

OWASP CSRFGuard

- OWASP CSRFGuard utilizes request tokens to address Cross-Site Request Forgery. CSRF is an attack where the victim is tricked into interacting with a website where they are already authenticated.
  - Java, .Net and PHP implementations
  - CSRF is considered the app sec sleeping giant
- Benefits
  - Provides code to generate unique request tokens to mitigate CSRF risks

http://www.owasp.org/index.php/Category:OWASP_CSRFGuard_Project

Projects to keep your eye on

OWASP OpenPGP Extensions for HTTP

- OWASP OpenPGP Extensions for HTTP utilize PKI to enhance secure session management. OpenPGP signing is added to the HTTP protocol.
  - A server module plus a browser plugin exists.
- Benefits
  - Provides a PKI alternative to SSL/TLS for authentication and integrity
    - Allows for server to authenticate clients
    - Allows for clients to authenticate servers
    - Future enhancements will include encryption
    - Proposed as an IETF specification

http://www.owasp.org/index.php/Category:OWASP_OpenPGP_Extensions_for_HTTP_-_Enigform_and_mod_openpgp

OWASP Static Analysis tools

- OWASP Code Crawler
  - .Net static code review tool
  - Covers .Net and J2EE/Java languages
  - Companion for the OWASP Code Review Guide
- OWASP Orizon
  - Library + API + Reporting tools + GUI
  - Advanced but in its early stages
  - Working for Java – other languages planned
- OWASP Yasca
  - Command-line grep-based tool (HTML output)
  - Java, C/C++, JavaScript, .Net

OWASP Securing WebGoat using ModSecurity

- This project created a set of custom ModSecurity rulesets that augment the Core Set and protect WebGoat 5.2 from as many vulnerabilities as possible.
  - Very challenging to protect a purposely vulnerable application
  - Developed scripts (Lua) for ModSecurity as well as JavaScript injections
  - Really pushed the boundaries of what a WAF can do – even business logic issues
  - See OWASP Podcast #2 for an interview

http://www.owasp.org/index.php/Category:OWASP_Securing_WebGoat_using_ModSecurity_Project

OWASP Security Spending Benchmarks

- This project seeks to produce guidance and an industry accepted benchmark for justifying overall Web application security spending. The project will attempt to identify how many resources should go into various SDLC activities.
  - Produced its first report on March 2009
- Benefits
  - Produces some of the first (and only) metrics on application security spending
  - March report has a number of interesting findings

http://www.owasp.org/index.php/Category:OWASP_Security_Spending_Benchmarks

Other projects of interest

- OWASP Security Analysis of Core J2EE Design Patterns Project
  - Provides advice for J2EE patterns
  - What pattern needs what additional controls
- OWASP O2
  - Recently released from Ounce Labs
  - Static analysis + visualization
- OWASP Vicnum & OWASP Mutillidae
  - Vulnerable apps to demonstrate sec issues
  - Vicnum – lightweight app / Vicnum Game
  - Mutillidae – implements the OWASP Top 10

Conclusion

Almost anywhere you are in the SDLC, OWASP has something that can improve your security and lower your costs.

You just have to know where to look

Questions?

Bonus Material: http://pseudosec.com/

The **PseudoSec Security Challenge** offers a unique opportunity to test your web application security skills and problem solving ability by uncovering and exploiting vulnerabilities in a simulated corporate website. Whether you are a seasoned infosec professional or a novice interested in learning the tricks of the trade, the PseudoSec Security Challenge provides an exciting and educational resource for users of all experience levels.