OWASP, Part 2 of 4: Forgery and Phishing

page 1

Meet the expert: Mike Benkovich delivers technical presentations around the U.S. as a consultant, trainer, and former Developer Evangelist for Microsoft. He has worked in a variety of professional roles including architect, project manager, developer, and technical writer. Mike is also an author of two books, published by WROX Press and APress, that show developers how to get the most from their SQL databases. Since appearing in the 1994 Microsoft DevCast, Mike has presented technical information at seminars, conferences, and corporate boardrooms across America.

Prerequisites: This course is for users with experience with developing web applications using C# or other object oriented programming languages.

Runtime: 40:00

Course description: In this course you'll look at building secure applications from the mindset of the hacker and what a developer can do to avoid the front pages of the latest exploit. You will see examples of Cross-Site Forgery, how a phishing email works, the vulnerabilities of open source components, and also redirects from unvalidated links.

Course outline:

Cross-Site Request Forgery
- Introduction
- Cross-Site Request Forgery
- OWASP Threat Assessment
- Example
- Phishing Email Sent to User...
- Code Includes CSRF Hack
- CSRF
- Demo: CSRF
- Demo: Preventing CSRF
- Cross-Site Request Forgery
- Summary

Vulnerable Components
- Introduction
- Known Vulnerabilities
- Example: Apache CXF & Spring
- OWASP Threat Assessment
- Components Known Vulnerabilities
- Reality of Software Components
- Explained...
- Comps with Known Vulnerabilities
- Demo: Known Vulnerabilities
- Summary

Redirects
- Introduction
- Unvalidated Redirects
- Example
- Demo: Unvalidated Redirects
- Demo: Using Validation
- Unvalidated Redirects