**Weekly Status**

**What We Did This Past Week**

We worked on a first draft of the revised outline, as a first step for coming up with a plan for a call for volunteers.

**A First Proposed Revised Outline**

A first proposed revised outline is below. Questions/Suggestions? Email the list and let’s discuss!

Introduction
Approach
Acknowledgements
Getting Started

- Injecting Security-Related Considerations Into Your Design
- Identifying Key Business Risks
- Defining Application and Environment Components
- Defining Component Business and Security Functions
- Performing Threat Modeling

Adding Security Controls Into Your Solution Stack

- Mapping the Top Ten to ASVS
- Understanding Enterprise Security API (ESAPI) Design Patterns
- Building Out Your Enterprise Security API
- Training Your Developers On Your Enterprise Security API

Web Application Security Design Guidelines

D1. Security Architecture
D2. Authentication
D3. Session Management
D4. Access Control
D5. Input Validation

D5.2 Verify that a positive validation pattern is defined and applied to all input.

D5.2.1 Define a positive validation pattern for all input
D5.2.1.1 Input identification worksheet
D5.2.1.2 Input syntax and semantics worksheet

D5.2.2 Apply a positive validation pattern to all input
D5.2.2.1 Solution stack checklist
D5.2.2.2 Development team checklist
D5.2.2.3 See also

D6. Output Encoding/Escaping
D7. Cryptography
D8. Error Handling and Logging
D9. Data Protection
D10. Communication Security
D11. HTTP Security
D12. Security Configuration
D13. Malicious Code Search
D14. Internal Security

Glossary
Where To Go From Here

**Where To Go From Here**

OWASP is the premier site for Web application security. The OWASP site hosts many projects, forums, blogs, presentations, tools, and papers. Additionally, OWASP hosts two major Web application security conferences per year, and has over 80 local chapters. The OWASP web site can be found here.

**Questions or comments? E-mail Mike Boberski**

*Weekly status template version 2.1*