Design Before Building
We create Threat Models on Completed Designs

What About *During* Design?
Design Patterns are Used During Design
Core J2EE Patterns are Used Extensively
Project: Analyze Patterns

Use to Implement:
- Synchronization Tokens as Anti-CSRF Mechanism
- Page-level Authorization

Avoid:
- XSLT and XPath Vulnerabilities
- XML Denial of Service
- Disclosure of Information in Soap Faults
- Publishing WSDL files

Diagram:
- Client delegates to ApplicationController
- ApplicationController invokes Target
- Target provides View
- Mapper resolves
- Mapper uses Map
- Avoid: Unhandled Commands
- Avoid: Unauthorized Commands
Project Goals

- Analyze patterns for security pitfalls to avoid
- Determine how patterns can implement security controls
- Provide advice portable to most frameworks
Not Overlapping
**Uses**

- Designing new web application frameworks
- Designing new apps that use the patterns
- Source code review of existing apps
- Runtime assessment of existing apps
- Integrate with threat modeling of new or existing apps
Analysis

Avoid

Relying Only on a Blacklist Validation Filter

Developers often use blacklists in filters as their only line of defense against input attacks such as Cross Site Scripting (CSS) because of errors in canonicalization and character encoding. In order to sufficiently protect against such attacks, do not rely on a blacklist validation filter as the sole means of protection; also validate input with strict whitelists on all input and output at every sink.

Use to Implement:
- Input validation
- Page-Level authorization
- Session Management
- Audit Logging

Avoid:
- Relying Only on Blacklist Validation
- Output Encoding in Filter
- Overly Generous Whitelist Validation
- XML Denial of Service
- Logging Arbitrary HTTP Parameters
public class MyFilter implements Filter {

    public void doFilter(ServletRequest request,
                          ServletResponse response,
                          FilterChain chain)
        throws IOException, ServletException {

        // implement blacklist filter
        // ...

        chain.doFilter();
    }
}
Design Analysis (This Project)  Control Implementation (ESAPI)  Verification (Static / Runtime Scan)
You Can Help ...

...Tell Developers

CC Flickr User wili hybrid
Our Dream:

- New web application framework idea
- Design-time security analysis
- Secure-by-default web application framework