

Session E33 – Web Site Gray Box Testing

By Bob Grill

Topic Summary

The root cause of Web Site Application Vulnerabilities is either in the code or the supporting infrastructure configuration. Often the code is tested through stimulus / response testing. This type of testing is called Black Box, Penetration Testing, Outside In Testing, or Hacking, because the server side code syntax is not known. The tester simply makes educated guesses, trying to get a response that satisfies their hypothesis. This type of testing is haphazard, time consuming and often leaves vulnerabilities undiscovered. White Box testing has traditionally been a review of the source code. With thousands of lines of code, this method is also plagued with shortcomings such as ignoring dynamic HTML, overlooking infrastructure, extremely time consuming, and simply missing vulnerabilities due to the volume of code to review.

This presentation focuses on how to configure web servers and application servers to prevent application vulnerabilities. This type of testing is somewhere in-between white (inside out) and black box (outside in) testing, so it has been coined gray box testing. However, gray box testing falls into the "inside out" category. Specific configurations covered will include; session management; cookies; HTTP methods, Object and file access, Java Bean and Servlet security settings. The scope will be limited to security related configuration settings that directly impact browser based applications typically on port 80 or 443 and does not include administration. The methods outlined in this presentation have been submitted for consideration as OWASP Testing Standards.