The OWASP Foundation is excited to present:

OWASP **GLOBAL** CAPTURE THE FLAG COMPETITION

Powered by: The Irish Honeynet Project

Sponsored by:

What is CTF?

A CTF challenge is a dedicated competition in computer security. The Irish Honeynet design CTF challenges to be an educational exercise to give participants experience in securiing machines, as well as conducting and reacting to the sort of attacks found in the real world. The winners of the CTF challenges need to be well versed in the skills of reverse-engineering, network sniffing, protocol analysis, system administration, programming, and cryptanalysis ... just for starters.

How will it work?

The event will open mid August in Hamburg, Germany at OWASP AppSec EU and will run until mid November 2013. The prizes will be awarded and presented at OWASP AppSec USA in New York city. The CTF games will be knock-out based; each week new challenges will be launched for the security community to solve

The challenges will range in difficulty from entry level to expert. All challenges are written by technical and knowledge based experts in partnership with the world of industry and academia. Levels are designed to take between 5 minutes and 3 hours to solve, depending on the difficulty rating.

The more complex the challenge, the more points the player will score. The winner will be the player with the most points at the end of the games.

The games will be accessible 6 days a week.

The Honeynet team will light up social media like Twitter to encourage dialogue between players and creators to drop game clues, and announce bonus levels

The Irish Honeynet are a not-for-profit volunteer organization. They are a small group of talented IT security professionals who believe in the importance of Internet security. Their project is run with the support of the Technical University of Ireland. A honeynet is a network of high interaction honeypots that simulate a production network and are configured such that all activity is monitored, recorded and desreetly regulated. The attack data aquired as part of the honeynet program will be used to distil current attack trends.