The CERN
WhiteHat Challenge

CERN Computer Security Team

Objective/Purpose

- Identify weaknesses in CERN-hosted software applications
  - Particular focus on (web) applications visible to the Internet (and being constantly probed by [White|Grey|Black]Hats)
  - Automatic tools don't discover everything
  - Phase space is just too big for a small team
- Team up with external universities
  - Current potential partners: students of cyber-security classes of U Florida, Polytechnique Montreal, HEIG VD, FH St. Pölten
  - Set up of a MoU with the corresponding professor/university
- Team up with YOU?
  - Dedicated training courses on penetration testing
  - Coordination, i.e. definition of application and scope, via the Computer Security Team

Rules of Engagement

- You must be enlisted with a participating university or with CERN and have signed the Rules of Engagement
- You must communicate the application to be tested, a schedule, and the source IPs to the Compute Security Team
  - For internal tests, you must seek explicit approval
- You must not violate any [U|ISP|nat'l] regulations
- You must keep traffic minimal and not impact network stability
- You must not alter or delete any webpage, account, data, or other any information hosted at CERN
- You must stop as soon as a vulnerability is found
- You must report all findings to Computer.Security@cern.ch

Why should you join?

- **Real-life hands-on training** on operational services
  - Reconnaissance/scanning, probing/poking, pen'testing, reporting
  - No mock-ups, no OWASP/WebGoat training pages, …
- Good opportunity to **learn security assessment tools**
- **Excellent semester project** to a BSc/MSc curriculum
- Definitive **enhancer of your CV**
- Risks?
  - You might just probe the level of your expertise and not find anything…
- And for CERN:
  Ultimate improvement of CERN's software applications!