

<http://www.tehtri-security.com/en/trainings.php>

Description

Advanced PHP Hacking... Lot of people think they already know everything related to PHP and IT Security, because tons of tiny papers/exploits were released everywhere those years. Some just think that PHP should not be used, but the reality shows that it's a worldwide web language used either by individuals or by corporate teams (Facebook...).

Trying to cover large scale knowledge related to PHP and hacking is not that easy, because it deals with networks, systems, services, applications, code, end-users... Thanks to this training, you'll learn every needed concept to **become a master at PHP Security** thanks to the lectures, and you'll also master practical issues thanks to the lab hands-on exercises.

After this session, **you will really know how attackers work and move through PHP hax0ring** so that they can jump down to your networks. Pentesters or security staff will be able to improve their tools and methods. Sysadmins and network staff will be able to help at protecting their information system and at detecting evil behaviors. Of course, developers will avoid errors that might cost a lot.

Topics

Breaking into PHP environment:

- Reminder and introduction about PHP, web servers, SQL, etc.
- How to gather information (direct or indirect contacts with the target, search engine issue, versions/plugins/applications...)
- What kind of vulnerabilities can be found (LFI, RFI, SQL injection, execution, disclosure...)
- How to find vulnerabilities (code analysis, fuzzing, dynamic tests, manual or automatic issues... ***0days & exploits will be found and created during this training with the Instructor***)
- How to exploit the target and get different kind of accesses

Attack Activities:

- How to keep a remote control thanks to **backdoors** (PHP classical backdoors, socket reuse, /proc, adding or modifying files...)
- How to **bounce** elsewhere (PHP port/banner/vuln scanner, PHP worms, SQL bounce, FTP bounce, SSH bounce, PHP proxies, PHP mail sender/fetcher...)
- How to **explore** a compromised computer through a PHP control (file system, Posix issues, avoid local protections...)
- How to **escalate privileges** (exploits and TTY issues, file descriptors...)
- How to **abuse incoming clients** (clients-side attacks with mpack-like stuff, source code analysis of mafia fishing stuff caught on real honeypots with mailer/CB grabber...)
- How to **clean your fingerprints** (logs, errors, file descriptors issues, network issues, system issues, applications issues, SQL...)

Defense:

- How to (try to?) protect, contain, and detect evil PHP related activities through different layers:
 - Networks (NIDS, traffic monitoring, firewall, etc),
 - Systems (hardening, file system, user management, etc)
 - Applications (security patches, secure coding, hardened configuration, etc).

Hacking Simulation:

- This training will end with a final train through a **live step by step real hack simulation**. It will help students at coming back to hands-on exercises seen during the whole day, thanks to this complete action.

Prerequisites

- Basic experience with PHP, SQL and HTTP. No stress: minimum needed knowledge will be reminded and explained at the beginning of the Dojo
- TCP/IP (IPv4) to connect your laptop to the hands-on lab
- Experience of Windows or Unix-like operating systems

Prerequisite material

- Students need a laptop (any OS welcome) with:
 - Clients: SSH, FTP, and web browser (Latest Firefox suggested with those plug-ins: Live HTTP Header, Cookie Monster, Header Spy, Modify Headers, Tamper Data...)
 - Services: a minimum local web server (recent Apache with PHP/Mysql enabled, like a local LAMP/WAMP architecture)
 - Shell tools and scripting languages (Instructor will use python, bash, curl, netcat, wget, etc). Windows end-users should install Cygwin.