SektionEins
http://www.sektioneins.de

PHP Security Crash Course

Stefan Esser <stefan.esser@sektioneins.de>

June 2009 - Amsterdam

Who I am?

Stefan Esser

- from Cologne / Germany
- Informationsecurity since 1998
- PHP Core Developer since 2001
- Month of PHP Bugs and Suhosin
- Head of Research and Development at SektionEins GmbH

Agenda

- Introduction
- Security Problems and Solutions
    - XSS
    - CSRF
    - SQL Injection
    - Session Management
    - PHP Code Inclusion / Evaluation

Part I

Introduction

Introduction

- Input to web-applications can be arbitrary manipulated
- Many security problems arise from misplaced trust in user input - but not all
- malfunction in case of
  - unexpected variables
  - unexpected data-types
  - unexpected lengths
  - unexpected characters / ranges

Filter Input and Escape Output

What is Input? (I)

- $_GET - URL variables
- $_POST - form data
- $_COOKIE - cookies
- $_REQUEST - mixture of GPC ***(unknown source)***
- $_FILES - uploaded files
- $_SERVER - HTTP headers / URL / querystring
- $_ENV - environment

What is Input? (II)

➡ don't forget other inputs like

- result of database queries
- result of shell commands
- result of web services
- or results of other external data sources

What is Filtering?

- removing all unknown / unexpected variables
- removing illegal input
  - casting to expected data-types
  - removing illegal characters
  - cutting overlong input
- **attention:** repairing illegal input can be dangerous
- Mantra does not make a difference to **validation**

What is Validation?

- Validation of user input against expected
  - data-types
  - lengths
  - characters / ranges
- Blocking / Ignoring illegal input

What is Output?

- every output of the web-application
  - HTML, JSON, ...
  - HTTP headers
- but also over communication with subsystems
  - Database
  - UNIX Shell (-commands)
  - Filesystem (filenames)

What is Escaping?

- „escaping“ wrongly used in the Mantra
- „escaping“ normally means disarming subsystem specific meta characters
- Mantra means every kind of preparation for output

Questions ?