DBAPP Security
安恒信息

OWASP TOP 10介绍及安全开发编程概述

杭州安恒信息技术有限公司

安恒攻防实验室
DBAPP SecLab

目录

- OWASP TOP 10（2013）介绍
- 安全开发编程概述

OWASP TOP 10

DBAPPSecurity 安恒信息

OWASP TOP 10

- Injection(注入)
- Broken Authentication and session Manager（失效的认证和会话管理）
- XSS（跨站脚本）
- Insecure Direct Object References（不安全的直接对象引用）
- Security Misconfiguration（安全配置错误）
- Sensitive Data Exposure（敏感信息泄露）
- Missing Function Level Access Control（功能级访问控制缺失）
- CSRF（跨站请求伪造）
- Using Known Vulnerable Components（使用含有已知漏洞的组件）
- Unvalated Redirects and Forwards（未验证的重定向和转发）

目录

- OWASP TOP 10（2013）
- 安全开发编程概述

安全开发编程概述

DBAPPSecurity 安恒信息

安全设计

- 在安全设计阶段，特别加入以下两方面的考虑
  - 减少攻击界面。例如，对一个网络软件的设计，它需要监听那些网络端口，是否可以减少监听端口的数目？那些用户可以与这些端口建立连接，是否要加强身份验证?
  - 深层防御。底层模块的设计中，假设上层模块有可能出现安全漏洞。对传递的数据考虑进一步校验

安全开发编程概述

DBAPPSecurity 安恒信息

❖ 安全编程

- **独立、完整且集中的输入验证**

  创建并使用了独立的用户输入验证模块以完成对所有用户的输入校验，以此可带来：

  - ❑统一的输入检测策略
  - ❑统一的验证逻辑
  - ❑统一的错误验证处理
  - ❑降低升级和维护成本

安全开发编程概述

DBAPPSecurity 安恒信息

- **校验全部的程序输入**

  保证所有变量在使用之前都经过严格的校验，防止被污染的数据进入程序。

- **校验全部的输入长度**

  通过限制输入长度，可以有效的控制一些攻击使其不给系统带来过大的威胁：

  - SQL Inject
  - XSS
  - File Include
  - ……

安全开发编程概述

- **校验全部的输入类型**

  不同的程序所接收到的参数类型应严格区分并校验，对于非法的类型应有相关异常进行处理以防止其进入程序。

- **不使用任何方式验证失败的数据**

  当程序对某个数据校验失败时（如：校验数据类型），相关的异常处理程序应抛弃该数据并中断操作，而不应对数据进行任何的修复尝试。

- **对HTTP所有内容进行校验**

  除需对传统的HTTP GET、POST等数据进行严格校验外，还应对HTTP内所有可能使用到的字段进行校验，防止字段中包含恶意字符而污染程序，如：

  - Referer
  - Host
  - Cookie
  - ……

安全开发编程概述

- **校验向用户输出的数据**

  当程序通过查询后台数据库或其他方式从后台获取数据后，在将数据输出给用户前应对该数据进行校验，校验其中是否包含有非法字符、可执行客户端脚本等恶意信息。

- **使用安全的SQL查询方式**

  在进行SQL查询时，必须使用安全的查询方式，如：Prepared Statement，以避免查询语句中由用户恶意插入SQL语句所带来的风险。

- **禁止使用JavaScript进行任何校验**

  由于JavaScript为客户端脚本，因此任何试图使用JavaScript对用户数据进行校验的行为都可能被用户构造的本地脚本所绕过，因此，所有校验工作应由服务端程序完成而不是客户端。

安全开发编程概述

- **使用安全、统一的编码或转义方式**

  创建并使用独立、统一的编码或转移方式，而且编码或转移中，至少应包含对以下类别数据的编码或转移：

  - 可能造成SQL注入的数据，如：分号、单引号等
  - 可能造成XSS的数据，如：script、javascript等

- **设定有安全的权限边界**

  所有的程序都应清楚的了解到自己能做什么，而在其所能做的范围之外，均属于其权限边界之外，应严格禁止对其权限之外的任何操作。

- **校验被调用的后台命令**

  若程序需要调用后台可执行程序，则在调用时，应通过使用完整路径或对程序进行HASH校验等方式保证程序的调用正确。

安全开发编程概述

- **校验被调用的文本或配置文件**

  若程序需要调用后台文本或配置文件，则在调用前，应相对文件或配置文件的完整性和有效性进行检查，以确保读入的文本或配置文件是正确可用的。

- **确保程序所记录的日志可控**

  若程序需要记录额外的操作日志等信息，应保证这些日志中的某些或全部内容不来自用户输入，否则用户可能通过外部恶意提交信息的方式填充日志。

DBAPP Security
安恒信息

谢谢！

安恒攻防实验室
DBAPP SecLab