OWASP 企业级安全应用程序接口工具包

功能强大,简单易用的安全控件

正如可以通过公钥基础设施（PKI）来帮助 web 应用程序和 web 服务实现诸如基于证书的认证，Web 应用和服务也可以通过 OWASP 的企业级安全控件来确保一些服务和应用程序免受攻击者的入侵。

最新的特征及改进

- 现在 OWASP ESAPI 拥有以下语言的版本：企业级 Java ,.NET,标准 ASP，ColdFusion/CFML, PHP, Python
- 企业级 Java 版本的 ESAPI 包含一个 web 应用程序防火墙（WAF），它可以给开发团队在修正错误的时候留有余地
- 所有语言版本的 ESAPI 组件工具箱都使用 BSD 许可证，你可以按照自己的需求使用或者修改 ESAPI，甚至将它集成到商用产品中。

不要试着自己编写安全控件！

重新为每个 WEB 应用或 WEB 服务编写安全控件通常非常浪费时间而且会产生大量新的安全漏洞。OWASP 企业级安全应用程序接口工具箱可帮助软件开发人员防范安全方面设计和实施中产生的缺陷。ESAPI 工具箱的结构非常简单---它的实质是一个类的集合，这些类封装了大多数应用程序所需的关键安全操作。ESAPI 旨在加固现有应用程序的安全，同时为进一步的开发打下坚实的基础。

计划之后再开始实施，避免返工...

安全测试、代码评审、渗透测试以及结构评审对他们自身而言并不是最终的目的。只有当架构师和开发者为修改代码做好准备并且将防范漏洞作为第一要务，否则有关安全的测试和分析很难提上日程。必须强调添加强健、简单的安全控件到你的解决方案中，并且从一开始就培训你的架构师和开发人员在执行安全测试、代码评审、渗透测试以及结构评审之前使用这些安全控件。

ESAPI 如何工作:

为了兼容不同的开发语言，OWASP ESAPI 的所有版本都基于相同的设计理念:

- OWASP ESAPI 包含了一系列的安全控件接口。这些接口定义了传入各种安全控件的参数类型，同时在这些接口中不包含针对某种应用的私有信息或逻辑控制.
- OWASP ESAPI 对于每个安全控件都有一个示例实现。这些示例实现中的处理逻辑并不是基于某个组织或者某种应用，他们之中也不包含针对某个组织或者某种应用的私有信息或逻辑控制。例如：基于字符串的输入验证.
- 你可以有选择的为自己定制对这些安全控件的实现，您或者您所在的组织可以在这些控件的实现的类中加入自己的应用逻辑。在这些类中也可以包含有您公司或者为您公司开发的专有的信息或应用逻辑，例如：企业级的身份认证.

从开发者的角度看 OWASP ESAPI 是如何工作的

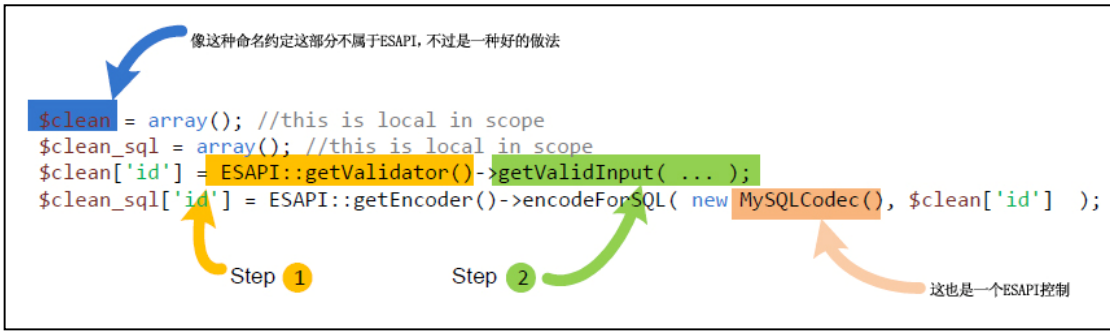
相关的 OWASP 项目:

- 了解最常见的 Web 应用程序漏洞：OWASP TOP 10
- 在你整合 ESAPI 后安全团队将为您测试什么：OWASP 应用安全验证标准（ASVS）
- 你怎样做才能有助于确保安全在构建时处于首要的位置：OWASP 合法性项目

如果您需要关于 OWASP ESAPI 的更多细节信息，请访问网站：
http://www.owasp.org/index.php/Category:OWASP_Enterprise_Security_API

弹指间调用安全控件!

ESAPI 的安全控件接口包含一个通常被称为定位器的 ESAPI 类。ESAPI 的定位器类在需要获取单个安全控件中的单例对象时被调用，这些安全控件往往是用来执行一些安全检查（如执行访问控制检查）或者是产生安全效用（如产生审计记录）。下面的例子说明了如何在输入验证和输出转义时防止 SQL 注入:



已包含的安全控件:

OWASP ESAPI 已经包含了下面安全控件的示例实现:

- 身份认证
- 访问控制
- 输入验证
- 输出编码/转义
- 密码
- 错误处理和日志
- 通信安全
- HTTP 安全
- 安全配置

OWASP
The Open Web Application Security Project

The Open Web Application Security Project (OWASP) is a worldwide free and open community focused on improving the security of application software. Our mission is to make application security "visible," so that people and organizations can make informed decisions about application security risks. Every-one is free to participate in OWASP and all of our materials are available under a free and open software license. The OWASP Foundation is a 501c3 not-for-profit charitable organization that ensures the ongoing availability and support for our work.