Web开发-PHP应用&代码执行&命令注入&RCE安全&数据解析&引发函数&CVE审计



#知识点：  
1、安全开发-原生PHP-超级全局变量  
2、安全开发-原生PHP-代码审计案例  
---------------------------------------------  
0、安全开发-原生PHP-数据库通讯  
1、安全开发-原生PHP-身份验证技术  
2、安全开发-Cookie&Session&Token  
3、安全开发-原生PHP-代码审计案例  
---------------------------------------------  
1、安全开发-原生PHP-弱类型脆弱  
2、安全开发-原生PHP-函数&数据类型  
3、安全开发-原生PHP-代码审计案例  
---------------------------------------------  
1、安全开发-原生PHP-开发组件集合  
2、安全开发-原生PHP-模版引擎渲染  
3、安全开发-原生PHP-第三方编辑器  
---------------------------------------------  
1、安全开发-框架技术-ThinkPHP  
2、安全开发-框架安全-版本&写法  
3、安全开发-ThinkPHP-代码审计案例  
---------------------------------------------  
1、安全开发-原生PHP-文件安全操作  
2、安全开发-原生PHP-上传读取删除包含等  
3、安全开发-原生PHP-代码审计文件安全---------------------------------------------  
1、安全开发-原生PHP-RCE安全  
2、安全开发-原生PHP-代码执行&命令注入  
3、安全开发-原生PHP-代码审计案例  
  
#章节点：(待补充)  
#具体点：(待补充)

|  |  |  |
| --- | --- | --- |
| **类别** | **组件/框架** | **说明** |
| **[Web框架]** | Laravel | 现代化、功能全面的框架，适合大多数Web应用。 |
|  | Symfony | 高度模块化、功能强大的框架，适合复杂应用。 |
|  | CodeIgniter | 轻量级框架，适合快速开发。 |
|  | Zend Framework (Laminas) | 企业级框架，适合大规模应用，具有高扩展性和性能。 |
|  | Yii | 高性能框架，适合快速开发和大规模应用。 |
| **[数据库组件]** | Doctrine ORM | 强大的ORM工具，支持复杂的查询和映射。 |
|  | Eloquent ORM | Laravel内置ORM，简化数据库操作。 |
|  | PDO | PHP的数据库抽象层，支持多种数据库引擎。 |
|  | RedBeanPHP | 轻量级ORM，自动创建和管理数据库表。 |
| **[模板引擎]** | Twig | 灵活、现代的模板引擎，常用于Symfony项目。 |
|  | Blade | Laravel内置模板引擎，支持模板继承和控制结构。 |
|  | Smarty | 经典模板引擎，适合中大型项目。 |
|  | Mustache | 轻量级跨语言模板引擎，支持PHP、JavaScript等。 |
| **[路由组件]** | FastRoute | 高性能PHP路由库，适用于小型应用和API。 |
|  | AltoRouter | 轻量级路由库，适合小型项目，易于配置。 |
|  | Symfony Routing | Symfony的路由组件，适合复杂应用。 |
| **[认证与授权]** | OAuth2 Server PHP | 实现OAuth2协议的PHP库，适用于API认证。 |
|  | JWT (JSON Web Token) | 轻量级身份验证方案，适合API认证。 |
|  | PHP-Auth | 简单的用户认证库，适用于中小型Web应用。 |
| **[支付集成]** | Stripe PHP SDK | 集成Stripe支付功能，支持信用卡支付、订阅等。 |
|  | PayPal SDK for PHP | 集成PayPal支付功能，支持支付、退款等。 |
| **[邮件发送]** | PHPMailer | 功能强大的邮件发送库，支持SMTP、POP3等协议。 |
|  | SwiftMailer | 另一款流行的邮件发送库，支持多种邮件功能。 |
|  | Mailgun PHP SDK | Mailgun的官方SDK，用于通过Mailgun API发送邮件。 |
| **[文件管理]** | Flysystem | 文件存储抽象库，支持多种存储方式（如本地、Amazon S3、FTP等）。 |
|  | Symfony Filesystem | Symfony的文件系统组件，提供简单的文件操作API。 |
|  | Intervention Image | 图片处理库，支持裁剪、调整大小、水印等功能。 |
| **[缓存与性能]** | Redis | 内存数据存储系统，用于缓存、消息队列等，提升性能。 |
|  | Memcached | 内存缓存系统，适用于高并发应用。 |
|  | Symfony Cache | Symfony缓存组件，支持多种缓存后端。 |
|  | Laravel Cache | Laravel内置缓存系统，提升Web应用性能。 |
| **[日志管理]** | Monolog | 强大的日志库，支持多种日志渠道（如文件、数据库、邮件等）。 |
|  | Log4PHP | Apache Log4j的PHP实现，适用于复杂日志功能。 |
| **[任务队列]** | Laravel Queue | Laravel内置队列系统，支持延迟任务、异步处理。 |
|  | Resque | 基于Redis的任务队列库，适用于异步任务处理。 |
|  | RabbitMQ | 开源消息代理服务，用于任务调度和消息传递。 |
| **[WebSocket与实时通信]** | Ratchet | 用于实现WebSocket服务，适合在线聊天、实时通信。 |
|  | Swoole | 高性能协程框架，支持WebSocket、TCP、UDP等协议，适用于高并发实时应用。 |
| **[测试与调试]** | PHPUnit | PHP标准单元测试框架，广泛用于自动化测试。 |
|  | Xdebug | PHP调试工具，支持堆栈跟踪、性能分析、断点调试等功能。 |
| **[富文本编辑器]** | **KindEditor** | 一个轻量级且功能丰富的富文本编辑器，支持图片上传、插入视频等，适用于PHP开发的Web项目。 |
|  | **TinyMCE** | 开源的富文本编辑器，支持多种格式的文本编辑，插件丰富，易于集成。 |
|  | **CKEditor** | 高度可定制的富文本编辑器，支持图片、文件上传、富文本格式化等功能，广泛用于Web项目中。 |
|  | **Froala Editor** | 轻量级、现代的富文本编辑器，支持图像处理、视频嵌入、内嵌富文本等，适合复杂的Web应用。 |
|  | **Quill** | 开源富文本编辑器，功能强大、轻量级，支持图片、视频、格式设置等功能，适合单页面应用。 |
|  | **Summernote** | 基于jQuery的轻量级富文本编辑器，支持文本格式化、图片上传等，适合中小型Web项目。 |
|  | **Trumbowyg** | 轻量级的富文本编辑器，功能简单但支持基本的文本编辑、图片上传、视频插入等。 |
|  | **Redactor** | 现代的富文本编辑器，功能丰富，支持图片、文件上传等，适合多种Web应用。 |
| **[图片上传组件]** | **Dropzone.js** | 支持拖拽上传和多文件上传的JavaScript库，易于与PHP集成，常用于图片、文件上传功能。 |
|  | **FilePond** | 高度可定制的文件上传库，支持图片预览、验证、上传进度等，适合需要精美上传功能的Web项目。 |
|  | **Fine Uploader** | 支持多种文件上传方式的组件，支持多文件上传、拖拽上传，支持PHP处理后台。 |
|  | **Plupload** | 支持多种文件上传方式（包括HTML5和Flash），可以与PHP后台集成，广泛用于Web应用中。 |
| **[图片处理组件]** | **ImageMagick** | 强大的图像处理库，支持图像格式转换、剪裁、旋转、加水印等多种功能，适用于PHP处理图像。 |
|  | **GD Library** | PHP内置图像处理库，支持图像创建、缩放、裁剪、色调调整等功能。 |
|  | **Intervention Image** | PHP图像处理库，支持裁剪、缩放、加水印等，易于与Laravel集成。 |

演示案例：

* WEB开发-原生PHP-超级全局变量
* WEB开发-原生PHP-代码审计案例
* WEB开发-原生PHP-通讯数据库
* WEB开发-Cookie&Session&Token
* WEB开发-身份验证-代码审计案例
* WEB开发-弱类型&函数-特性安全
* WEB开发-数据对比-代码审计案例
* WEB开发-Smarty模版&插件编辑器
* WEB开发-模版&插件-代码审计案例
* WEB开发-框架技术-ThinkPHP
* WEB开发-ThinkPHP-代码审计案例
* WEB开发-文件安全-上传下载读取
* WEB开发-文件安全-删除遍历包含
* WEB开发-文件安全-代码审计案例

#代码执行  
PHP 提供代码执行 (Code Execution) 类函数主要是为了方便研发人员处理各类数据，然而当研发人员不能合理使用这类函数时或使用时未考虑安全风险，则很容易被攻击者利用执行远程恶意的PHP代码，威胁到系统的安全。  
eval，assert，preg\_replace，create\_function等  
https://www.yisu.com/ask/52559195.html  
https://www.jb51.net/article/264470.htm  
  
容易导致代码执行的 PHP 函数  
assert()  
pcntl\_exec()  
array\_fi lter()  
preg\_replace  
array\_map()  
require()  
array\_reduce()  
require\_once()  
array\_diff\_uassoc()  
register\_shutdown\_function()  
array\_diff\_ukey()  
register\_tick\_function()  
array\_udiff()  
set\_error\_handler()  
array\_udiff\_assoc()  
shell\_exec()  
array\_udiff\_uassoc()  
stream\_fi lter\_register()  
array\_intersect\_assoc()  
system()  
array\_intersect\_uassoc()  
usort()  
array\_uintersect()  
uasort()  
array\_uintersect\_assoc()  
uksort()  
array\_uintersect\_uassoc()  
xml\_set\_character\_data\_handler()  
array\_walk()  
xml\_set\_default\_handler()  
array\_walk\_recursive()  
xml\_set\_element\_handler()  
create\_function()  
xml\_set\_end\_namespace\_decl\_handler()  
escapeshellcmd()  
xml\_set\_external\_entity\_ref\_handler()  
exec()  
xml\_set\_notation\_decl\_handler()  
include  
xml\_set\_processing\_instruction\_handler()  
include\_once()  
xml\_set\_start\_namespace\_decl\_handler()  
ob\_start()  
xml\_set\_unparsed\_entity\_decl\_handler()  
  
#命令执行  
为了方便处理相关应用场景的功能，PHP系统中提供命令执行类函数，如 exec()、system() 等。当研发人员不合理地使用这类函数，同时调用的变量未考虑安全因素时，容易被攻击者利用执行不安全的命令调用。  
exec，system，passthru，popen，shell\_exec，pcntl\_exec，`等  
  
#代码审计案例  
1、Yccms 代码执行  
https://mp.weixin.qq.com/s/4i4MLsNAlMuLjySBc\_rySw  
2、CmsEasy 代码执行  
https://xz.aliyun.com/t/2577  
3、BJCMS 命令执行  
https://blog.csdn.net/qq\_44029310/article/details/125860865  
4、WBCE 命令执行  
https://developer.aliyun.com/article/1566395  
5、D-Link 命令执行  
https://xz.aliyun.com/t/2941  
6、安恒明御安全网关  
https://blog.csdn.net/smli\_ng/article/details/128301954

涉及资源：[资源下载地址](https://docs.qq.com/doc/DQ3Z6RkNpaUtMcEFr)