Web开发-PHP应用&鉴别修复&AI算法&流量检测&PHP.INI&通用过滤&内置函数



#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  
---------------------------------------------  
1、安全开发-原生PHP-PHP.INI安全  
2、安全开发-原生PHP-全局文件&单函数  
3、安全开发-原生PHP-流量检测&AI算法  
  
#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
* WEB开发-修复方案-PHP.INI配置
* WEB开发-修复方案-单函数&全局文件
* WEB开发-修复方案-流量检测&AI算法

#通用-PHP.INI设置  
参考：  
https://www.yisu.com/ask/28100386.html  
https://blog.csdn.net/u014265398/article/details/109700309  
https://www.cnblogs.com/xiaochaohuashengmi/archive/2011/10/23/2222105.html  
安全模式 safe\_mode 命令执行函数会被禁用  
\*路径访问 open\_basedir 限制文件操作安全（遍历等）  
\*禁用函数 disable\_function 升级版安全模式，自定义限制函数  
\*魔术引号转义 magic\_quotes\_gpc 同理下面的sql过滤第一个函数  
数据库访问次数 max\_connections 防止数据库爆破  
禁用远程执行 allow\_url\_include allow\_url\_fopen远程包含开关等  
\*安全会话管理 session.cookie\_httponly session.cookie\_secure  
防止跨站脚本攻击（XSS）和中间人攻击（MITM）  
  
#引用-全局文件  
1、关键内容检测（黑白名单）  
文件上传，SQL注入，XSS跨站等  
演示：文件上传，SQL注入，XSS跨站  
2、模仿流量检测（基于规则或AI算法）  
演示：Python Flask+PHP Curl+训练大模型  
客户端请求数据 -> 中间件搭建平台 -> 服务器代码文件处理  
客户端请求数据 -> WAF或流量监控 （规则，AI模型算法）-> 正常数据 -> 中间件搭建平台 -> 服务器代码文件处理  
客户端请求数据 -> WAF或流量监控 （规则，AI模型算法）-> 异常数据 -> 截止  
  
#代码-内置函数  
检测：数据的类型差异，数据的固定内容  
gettype()获取变量的类型  
is\_float()检测变量是否是浮点型  
is\_bool()检测变量是否是布尔型  
is\_int()检测变量是否是整数  
is\_null()检测变量是否为NULL  
is\_numeric()检测变量是否为数字或数字字符串  
is\_object()检测变量是否是一个对象  
is\_resource()检测变量是否为资源类型  
is\_scalar()检测变量是否是一个标量  
is\_string()检测变量是否是字符串  
is\_array()检测变量是否是数组  
filter\_var()使用特定的过滤器过滤一个变量  
FILTER\_SANITIZE\_STRING 过滤器可以过滤HTML标签和特殊字符  
FILTER\_SANITIZE\_NUMBER\_INT 过滤器可过滤非整数字符  
FILTER\_SANITIZE\_URL 过滤器用于过滤URL中的非法字符   
FILTER\_VALIDATE\_EMAIL 过滤器来验证电子邮件地址的有效性  
演示：filter\_var() is\_numeric() is\_string()等  
  
1、SQL注入过滤：  
Addslashes()返回字符串，该字符串为了数据库查询语句等的需要在某些字符前加上了反斜线。这些字符是单引号()、双引号(”)、反斜线()与NULL字符)。  
stripslashes()反引用一个引用字符串,如果magic\_quotes\_sybase项开启，反斜线将被去除，但是两个反斜线将会被替换成一个。  
addcslashes()返回字符串，该字符串在属于参数charlist列表中的字符前都加上了反斜线。  
stripcslashes()返回反转义后的字符串。可识别类似C语言的\n，r，…八进制以及十六进制的描述。  
mysql\_escape\_string()此函数并不转义%和\_。作用和mysql real escape\_string()基本一样  
mysql\_real\_escape\_string()调用mysql库的函数在以下字符前添加反斜杠:x00、\n、\r、\、x1a  
PHP魔术引号当打开时，所有的'(单引号)，”(双引号)，(反斜线)和NULL字符都会被自动加上一个反斜线进行转义。这和addslashes()作用完全相同。  
预编译机制  
演示：魔术引号，addslashes()，预编译等  
  
2、XSS跨站过滤：  
htmlspecialchars()函数把预定义的字符转换为HTML实体。  
strip\_tags()函数剥去字符串中的HTML、XML以及PHP的标签。  
演示：htmlspecialchars() strip\_tags()  
  
3、命令执行过滤  
escapeshellcmd()确保用户只执行一个命令用户可以指定不限数量的参数用户不能执行不同的命令  
escapeshellarg()确保用户只传递一个参数给命令用户不能指定更多的参数一个用户不能执行不同的命令  
  
4、其他漏洞过滤  
可参考AI答案或参数类型过滤等  
  
#防护-WAF产品  
见前面的课程

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