php代码审计基础篇

第2课 环境配置

PHP环境搭建

phpstudy

https.//www.xp.cn/download.html

该程序包集成最新的Apache+PHP+MySQL+phpMyAdmin+ZendOptimizer,一次性安装，无须配置即可使用，是非常方便、好用的PHP调试环境.该程序不仅包括PHP调试环境，还包括了开发工具、开发手册等.总之学习PHP只需一个包

phpstudy适合多种系统操作，并且支持IIS和Nginx,phpstudy程序包集中了很多php版本的编写语言，运行速度也是很快的

- Sublime Text
- http://www.sublimetext.com/3
- phpstorm
- https://www:jetbrains.com/phpstorm/
- 辅助工具
- burp

seay代码审计工具

·这是一款基于C#语言开发的一款针对PHP代码安全性审计的系统主要运行于Windows系统上。这款软件能够发现SQL注入、代码执行、命令执行、文件包含、文件上传、绕过转义防护、拒绝服务、XSS跨站、信息泄露、任意URL跳转等漏洞

RIPS

·RIPS是一个用PHP编写的源代码分析工具，它使用了静态分析技术，能够自动化地挖掘PHP源代码潜在的安全漏洞。渗透测试人员可以直接容易的审阅分析结果，而不用审阅整个程序代码。由于静态源代码分析的限制，漏洞是否真正存在，仍然需要代码审阅者确认。RIPS能够检测XSS,SQL注入，文件泄露，Header Injection漏洞等

php配置文件关键讲解

•php.ini

•在php启动时被读取，对于服务器模块版本的php,仅在web服务器启动时读取一次。对于cgi和cli版本，每次调用都会读取。还可以在httpd.conf中覆盖php.ini的值，以进行更灵活的配置：

•.user.ini

•此类文件自PHP5.3.0起，PHP支持基于每个目录的htaccess风格的INI文件。此类文件仅被CGI/FastCGI SAPI处理。此功能使得PECL的htscanner扩展作废。如果使用Apache,则用htaccess文件有同样效果。在.user.ini风格的INI文件中只有具有PHP_INI_PERDIR和PHP_INI__USER模式的INI设置可被识别。当使用PHP作为Apache模块时，也可以用Apache的配置文件(例如httpd.conf)和.htaccess文件中的指令来修改PHP的配置设定。需要有“AllowOverride Options”或AllowOverride All"权限才可以。

•语法

•设置指令格式directive =value

•指令名direvtive是大小写敏感的INI文件中的表达式仅使用：位运算符、逻辑非、圆括号，

•|位或、&位与、~位非、1逻辑非布尔标志用On表示打开，用Off表示关闭。

php配置文件关键讲解

- regster giohabs =off启用全局变量
- short open tag =On短标签
- magic_quotes gpc =off魔术引号
- safe_mode =off安全模式
- safe_mode_exec_dir =/var/www/html安全模式下执行程序主目录
- disable_functions
- allow urlLinclude =off是否允许包含远程文件
- allow_urLopen =on是否允许打开远程文件
- upload tmp_dir =文件上传临时目录
- file_uploads =on upload_max_filesize =8M设置上传及最大上传文件大小
- open_basedir =E:\WWW
- display_errors =on内部错误选项

- cms搭建
- 白
- MVC架构
- MVC是一种软件开发框架、MVC将程序分为三个部分：模型层(M)、视图层(V)和控制层(C)。对不同的层进行分层管理和控制，方便程序的修改和扩展.在PHP中使用MVC框架，可以实现了分层、分类开发，实现了web的分离，使前端代码与后端分离，某一层的调整，不会对另一层的代码和逻辑造成影响，使用MVC开发框架更加方便程序的扩展，使开发的代码整体更加清晰
- 白+黑
- 敏感关键字回溯参数，查找可控变量，功能点定向审计

谢谢观赏