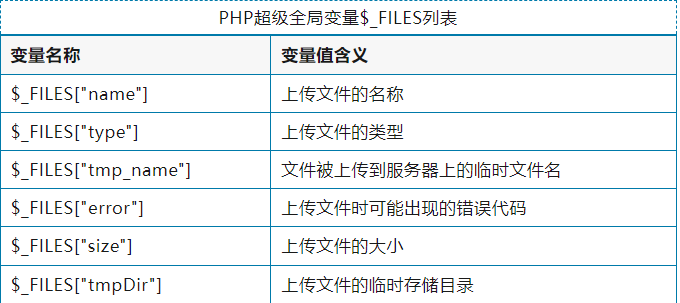
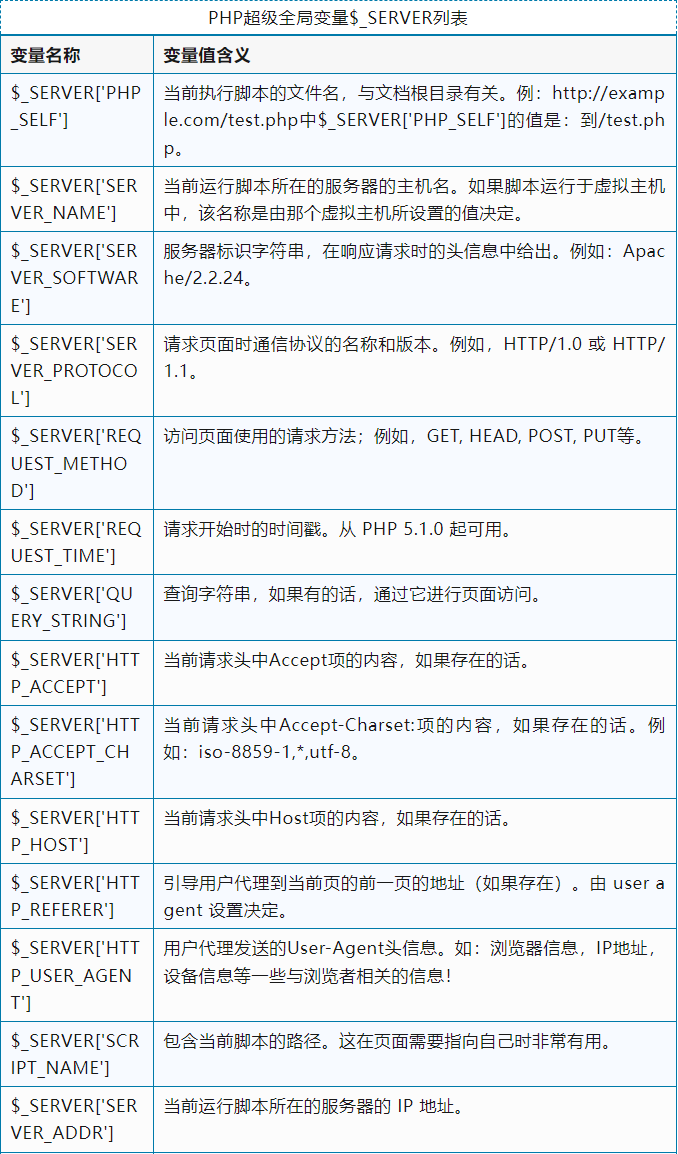
Web开发-PHP应用&原生语法&全局变量&数据接受&身份验证&变量覆盖&任意上传



#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  
  
#章节点：(待补充)  
#具体点：(待补充)







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

DW + PHPStorm + PhpStudy + Navicat Premium  
DW : HTML&JS&CSS开发  
PHPStorm : 专业PHP开发IDE  
PhpStudy ：Apache MYSQL环境  
Navicat Premium: 全能数据库管理工具  
参考：https://tutorials.wcode.net/php  
  
变量覆盖安全：  
$GLOBALS：这种全局变量用于在PHP脚本中的任意位置访问全局变量  
  
数据接收安全：  
$\_REQUEST：$\_REQUEST 用于收集 HTML 表单提交的数据。  
$\_POST：广泛用于收集提交method="post" 的HTML表单后的表单数据。  
$\_GET：收集URL中的发送的数据。也可用于提交表单数据(method="get")   
$\_ENV：是一个包含服务器端环境变量的数组。  
$\_SERVER：这种超全局变量保存关于报头、路径和脚本位置的信息。  
  
文件上传安全：  
$\_FILES：文件上传且处理包含通过POST方法上传给当前脚本的文件内容。  
  
身份验证安全：  
$\_COOKIE：是一个关联数组，包含通过cookie传递给当前脚本的内容。  
本地客户端浏览器存储  
$\_SESSION：是一个关联数组，包含当前脚本中的所有session内容。  
目标服务端存储，存储记录的数据  
  
代码审计应用：  
1、DuomiCMS变量覆盖  
找变量覆盖代码->找此文件调用->  
选择利用覆盖Session->找开启Session文件覆盖  
参考：https://blog.csdn.net/qq\_59023242/article/details/135080259  
/interface/comment.php?\_SESSION[duomi\_admin\_id]=10&\_SESSION[duomi\_group\_id]=1&\_SESSION[duomi\_admin\_name]=zmh  
  
2、YcCms任意文件上传  
找文件上传代码->找此文件调用->找函数调用->过滤type用mime绕过  
参考：https://zhuanlan.zhihu.com/p/718742254  
?a=call&m=upLoad send

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