- 会话（Session）安全
- 文件系统安全
- 数据库安全
- 错误报告
-
- 使用 Register Globals
- 用户提交的数据
- 魔术引号
- 隐藏 PHP 。php 改名

PHP安全分类：

1. SQL注入 （防注入）
2. XSS攻击
3. CSRF攻击

默认地，PHP 对所有的 GET、POST 和 COOKIE 数据自动运行 addslashes()。所以您不应对已转义过的字符串使用 addslashes()，因为这样会导致双层转义。遇到这种情况时可以使用函数 get_magic_quotes_gpc() 进行检测。

1、命令注入(Command Injection)
2、eval注入(Eval Injection)
3、客户端脚本攻击(Script Insertion)
4、跨网站脚本攻击(Cross Site Scripting, XSS)
5、SQL注入攻击(SQL injection)
6、跨网站请求伪造攻击(Cross Site Request Forgeries, CSRF)
7、Session 会话劫持(Session Hijacking)
8、Session 固定攻击(Session Fixation)
9、HTTP响应拆分攻击(HTTP Response Splitting)
10、文件上传漏洞(File Upload Attack)
11、目录穿越漏洞(Directory Traversal)
12、远程文件包含攻击(Remote Inclusion)
13、动态函数注入攻击(Dynamic Variable Evaluation)
14、URL攻击(URL attack)
15、表单提交欺骗攻击(Spoofed Form Submissions)
16、HTTP请求欺骗攻击(Spoofed HTTP Requests)