PHP有自己的PHPGDB

如果想用调试器执行一个可执行文件， 在用gcc编译时必须加上-g选项：

1. 创建符号表，符号表包含了程序中使用的变量名称的列表。

2. 关闭所有的优化机制，以便程序执行过程中严格按照原来的C代码进行。

有时会遇到一种很特殊的调试需求，对当前正在运行的其它进程进行调试（正是我今天遇到的情形）。这种情况有可能发生在那些无法直接在调试器中运行的进程身上，例如有的进程 只能在系统启动时运行。另外如果需要对进程产生的子进程进行调试的话，也只能采用这种方式。GDB可以对正在执行的程序进行调度，它允许开发人员中断程序 并查看其状态，之后还能让这个程序正常地继续执行。

gdb xxx 进入gdb shell

start/run 运行程序

list 查看载入程序的源文件

break 行号或函数名或条件

attach "PID" 调试指定pid的进程

info reg 显示寄存器信息

多线程调试：

info thread 查看当前进程的线程。

info threads 显示当前可调式的所有线程，gdb会为每一个线程分配ID

thread <ID> 切换调试的线程为指定ID的线程。

break file.c:100 thread all 在file.c文件第100行处为所有经过这里的线程设置断点。

set scheduler-locking[off|on|step] off 不锁定任何线程，也就是所有线程都执行，这是默认值。on 只有当前被调试线程会执行。step表示在单步执行的时候，只有当前线程会执行。

插件支持：

PEDA 全称是Python Exploit Development Assistance for GDB

pip install peda