The PHP Lifecycle

Yahoo! . 惠新宸

Tel : 86111

Mail: xinchen.hui@alibaba-inc.com

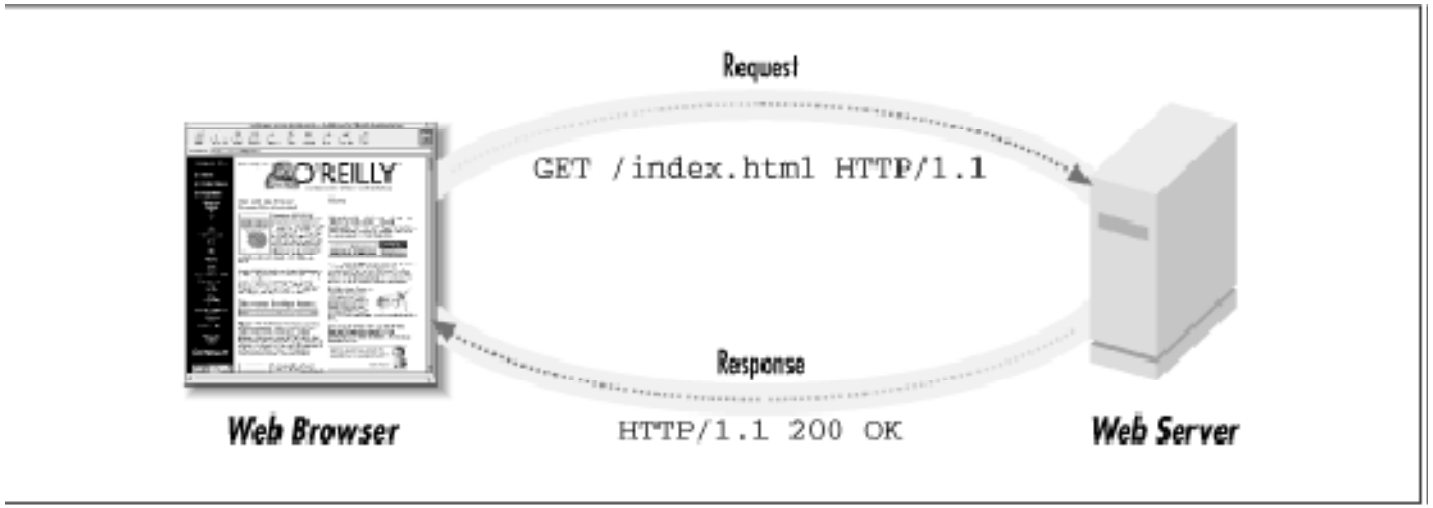
YAHOO! 中国雅虎

Summary

- B/S(HTTP Request Cycle)
- Apache Life Cycle
- Apache Parse Request Cycle
- PHP Life Cycle
- Cooperating with Apache
- PHP Parse/Execute Process
- Now We Can…

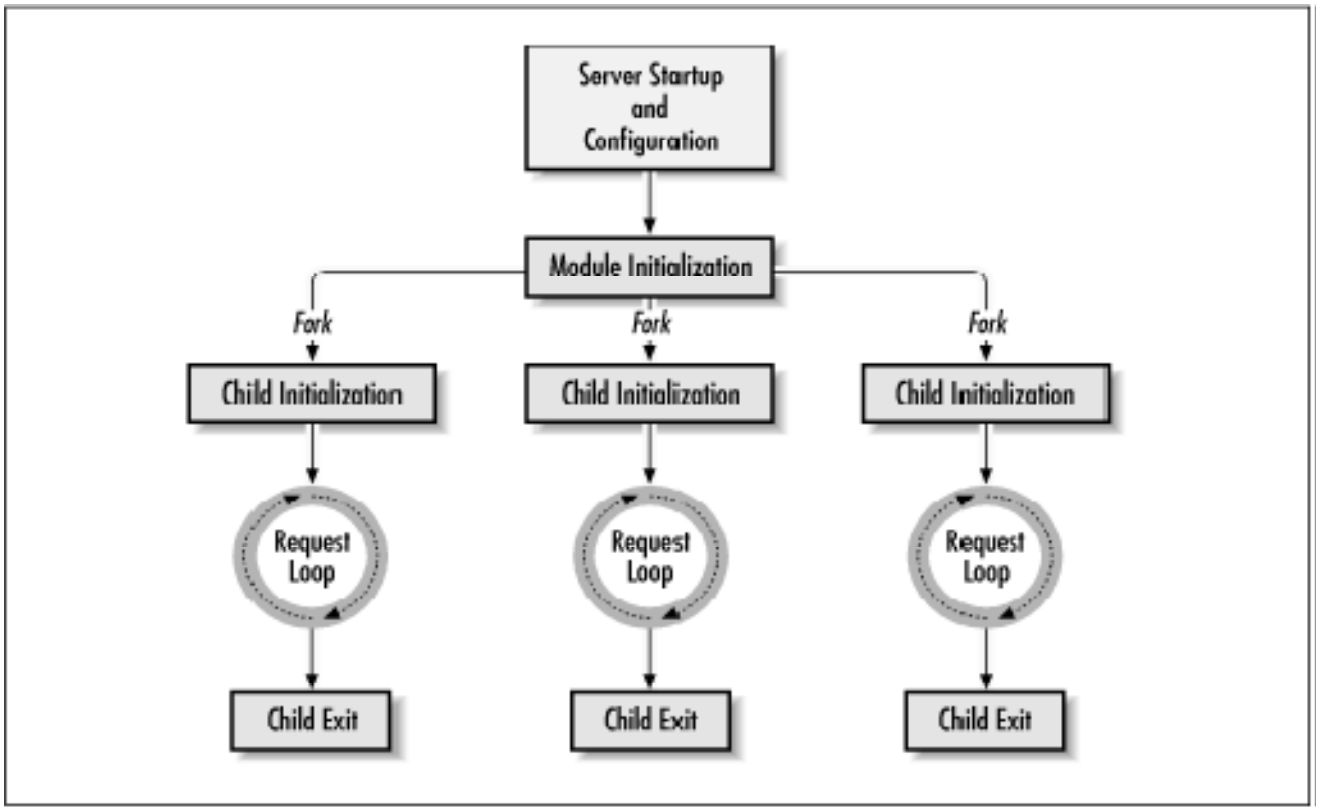
Linux/Unix + Apache 1.3x + PHP 5.x

B/S

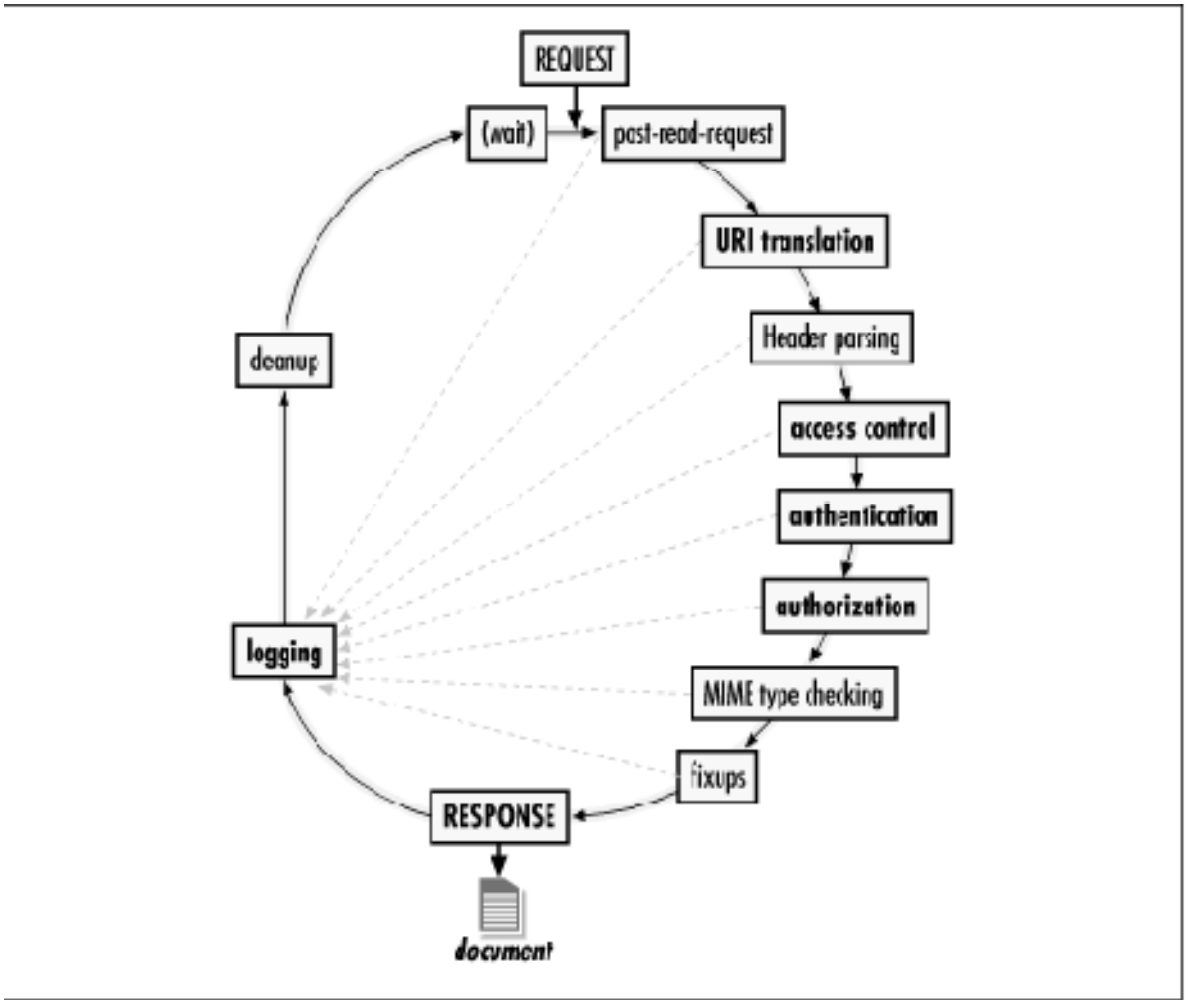


1. Client Request
2. Server Parse Requst and Send Response
3. Client interpret Responded Text/HTML/Json etc…

Apache Life Cycle

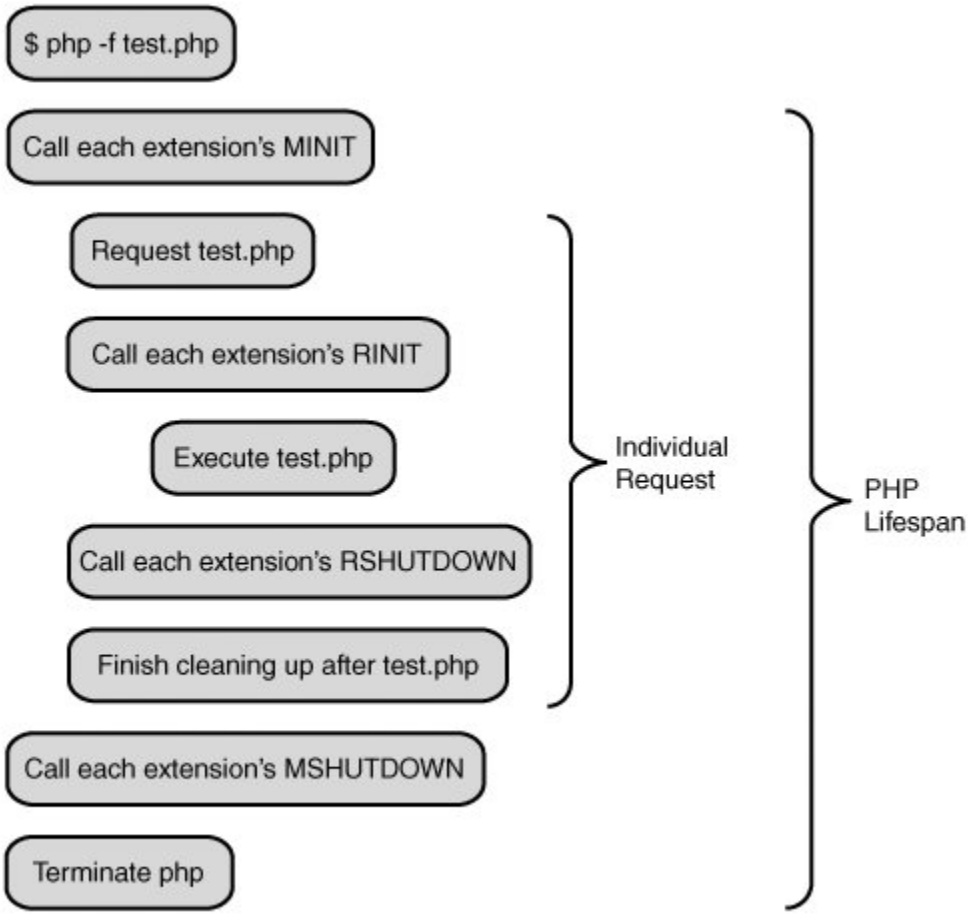


Apache Parse Request Cycle



PHP Life Cycle

- In command line mode(CLI)



PHP Life Cycle con’t

- PHP_MODULE_ENTRY(php_mysql.c 215行)

```
/* {{{ mysql_module_entry
 */
zend_module_entry mysql_module_entry = {
    STANDARD_MODULE_HEADER,
    "mysql",
    mysql_functions,
    ZEND_MODULE_STARTUP_N(mysql), //MINIT_FUNCTION
    PHP_MSHUTDOWN(mysql),
    PHP_RINIT(mysql),
    PHP_RSHUTDOWN(mysql),
    PHP_MINFO(mysql),
    "1.0",
    PHP_MODULE_GLOBALS(mysql),
    PHP_GINIT(mysql),
    NULL,
    NULL,
    STANDARD_MODULE_PROPERTIES_EX
};
/* }}} */
```

PHP Life Cycle con’t

- PHP_MINIT_FUNCTION(php_mysql.c 378行)

```
/* {{{ PHP_MINIT_FUNCTION
 */
ZEND_MODULE_STARTUP_D(mysql)
{
    REGISTER_INI_ENTRIES();
    le_result = zend_register_list_destructors_ex(_free_mysql_result, NULL, "mysql result", module_number);
    le_link = zend_register_list_destructors_ex(_close_mysql_link, NULL, "mysql link", module_number);
    le_plink = zend_register_list_destructors_ex(NULL, _close_mysql_plink, "mysql link persistent", module_number);
    Z_TYPE(mysql_module_entry) = type;

    REGISTER_LONG_CONSTANT("MYSQL_ASSOC", MYSQL_ASSOC, CONST_CS | CONST_PERSISTENT);
    REGISTER_LONG_CONSTANT("MYSQL_NUM", MYSQL_NUM, CONST_CS | CONST_PERSISTENT);
    REGISTER_LONG_CONSTANT("MYSQL_BOTH", MYSQL_BOTH, CONST_CS | CONST_PERSISTENT);
    REGISTER_LONG_CONSTANT("MYSQL_CLIENT_COMPRESS", CLIENT_COMPRESS, CONST_CS | CONST_PERSISTENT);
#if MYSQL_VERSION_ID >= 40000
    REGISTER_LONG_CONSTANT("MYSQL_CLIENT_SSL", CLIENT_SSL, CONST_CS | CONST_PERSISTENT);
#endif
    REGISTER_LONG_CONSTANT("MYSQL_CLIENT_INTERACTIVE", CLIENT_INTERACTIVE, CONST_CS | CONST_PERSISTENT);
    REGISTER_LONG_CONSTANT("MYSQL_CLIENT_IGNORE_SPACE", CLIENT_IGNORE_SPACE, CONST_CS | CONST_PERSISTENT);

    return SUCCESS;
}
/* }}} */
```

PHP Life Cycle con’t

- PHP_RINIT_FUNCTION(php_mysql.c 473行)

```
/* {{{ PHP_RINIT_FUNCTION
 */
PHP_RINIT_FUNCTION(mysql)
{
    MySG(default_link)=-1;
    MySG(num_links) = MySG(num_persistent);
    /* Reset connect error/errno on every request */
    MySG(connect_error) = NULL;
    MySG(connect_errno) =0;
    MySG(result_allocated) = 0;
    return SUCCESS;
}
/* }}} */
```

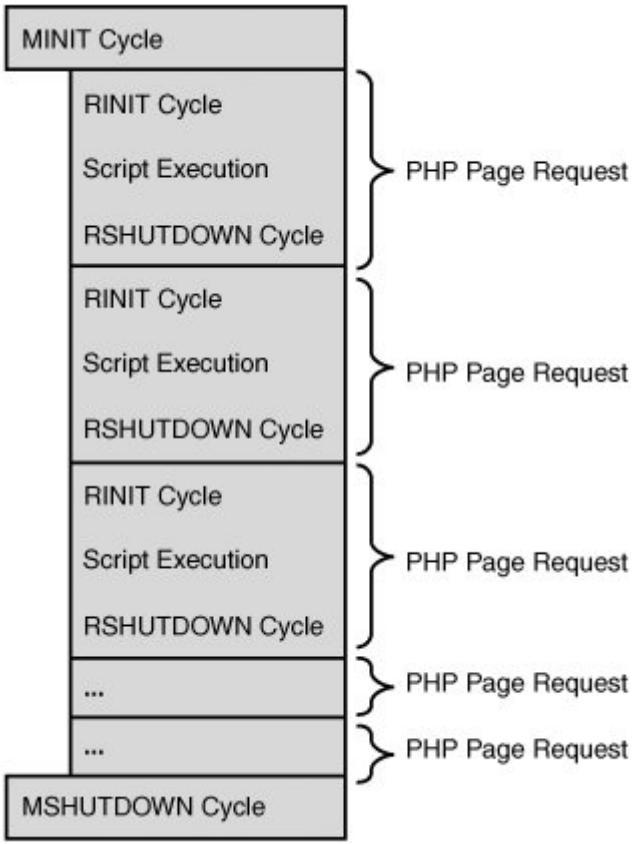
PHP Life Cycle con’t

- PHP_SHUTDOWNS(php_mysql.c 403行)

```
/* {{{ PHP_MSHUTDOWN_FUNCTION
 */
PHP_MSHUTDOWN_FUNCTION(mysql)
{
    UNREGISTER_INI_ENTRIES();
    return SUCCESS;
}
/* }}} */

+-- 13 lines: PHP_RINIT_FUNCTION----------------------------------------------------------------

/* {{{ PHP_RSHUTDOWN_FUNCTION
 */
PHP_RSHUTDOWN_FUNCTION(mysql)
{
    if (MySG(trace_mode)) {
        if (MySG(result_allocated)){
            php_error_docref("function.mysql-free-result" TSRMLS_CC, E_WARNING, "%lu result set(s
esult to free result sets which were requested using mysql_query()", MySG(result_allocated));
        }
    }

    if (MySG(connect_error)!=NULL) {
        efree(MySG(connect_error));
    }
    return SUCCESS;
}
/* }}} */
```

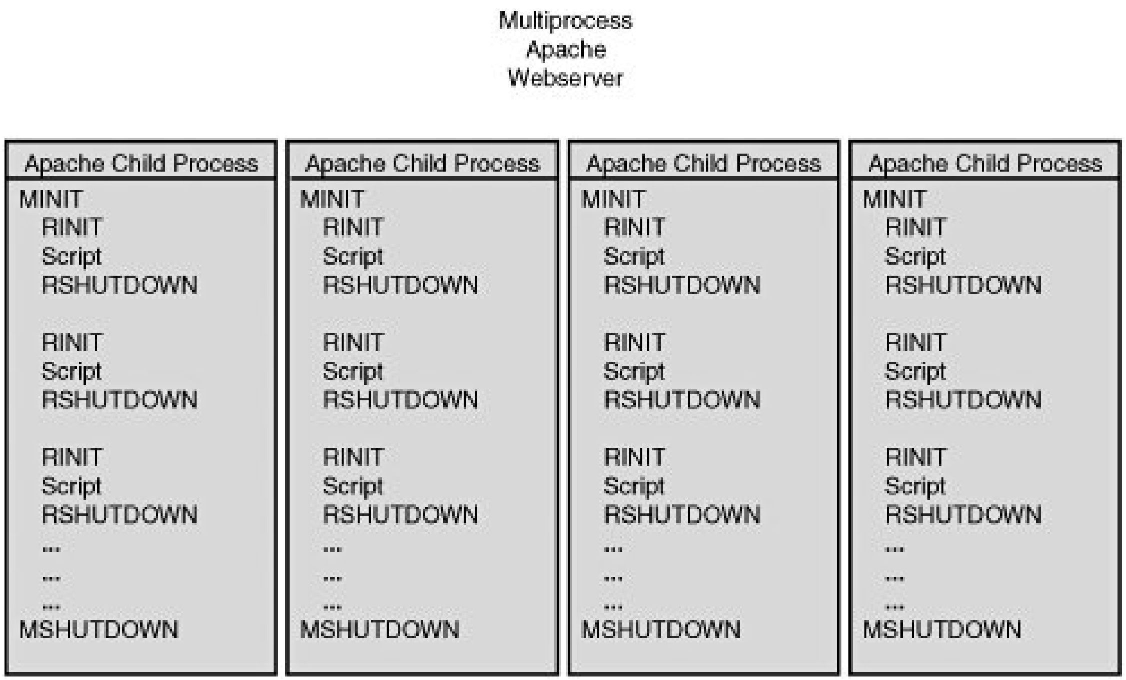
PHP Life Cycle con’t

- In DSO mode
  - Single process



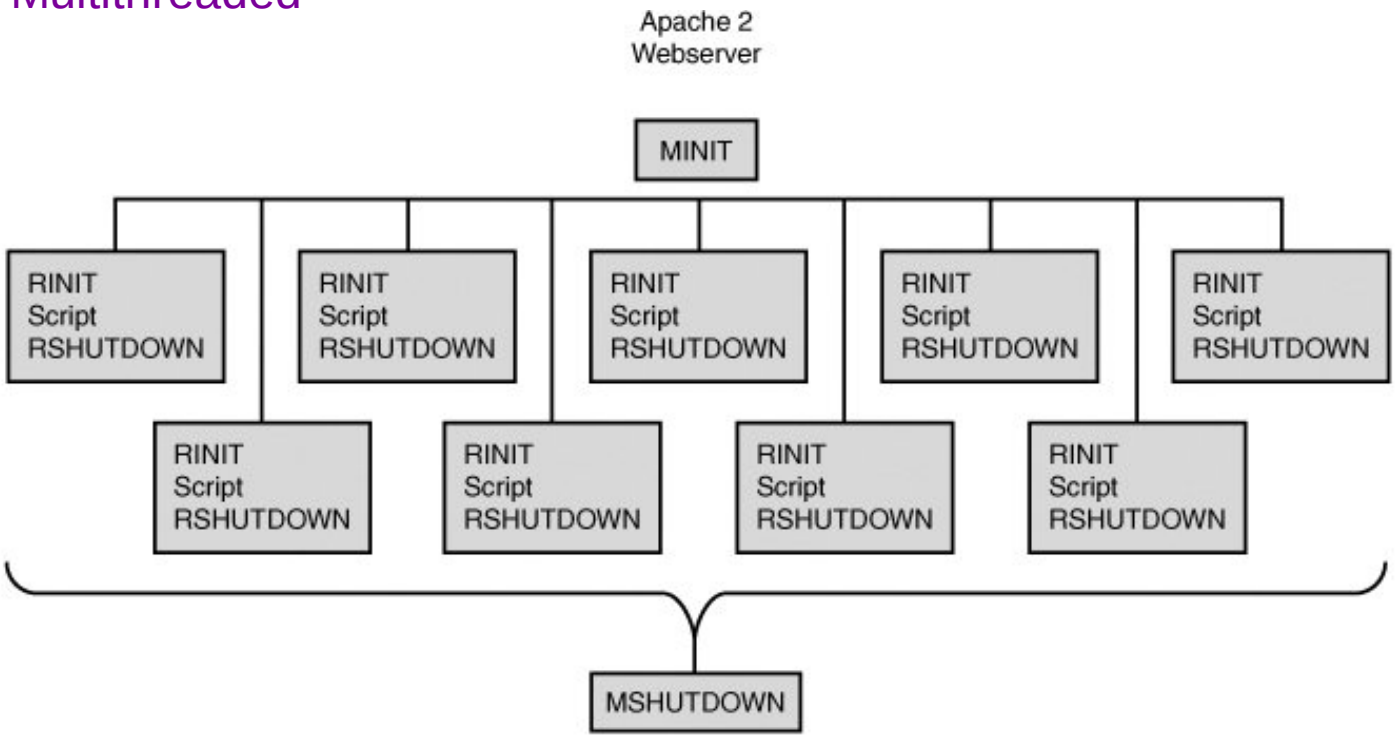
PHP Life Cycle con't

- In DSO mode
  - Multiprocess



PHP Life Cycle con’t

- In CGI mode
  - Multithreaded



Cooperation

- Apache 1.3x + PHP 5.x in DSO mode
- Dynamic Shared Objects (DSO)
  - mod_dso
    - src/modules/standard/mod_so.c 347行

```
static const command_rec so_cmds[] = {
    { "LoadModule", load_module, NULL, RSRC_CONF, TAKE2,
      "a module name and the name of a shared object file to load it from"},
    { "LoadFile", load_file, NULL, RSRC_CONF, ITERATE,
      "shared object file or library to load into the server at runtime"},
    { NULL }
};
```

Cooperation con’t

- Php Module注册Handler
  - mod_php5.c 963行

```
/* {{{ handler_rec php_handlers[]
 */
handler_rec php_handlers[] =
{
    {"application/x-httpd-php", send_parsed_php},
    {"application/x-httpd-php-source", send_parsed_php_source},
    {"text/html", php_xbithack_handler},
    {NULL}
};
/* }}} */
```

Cooperation con’t

- Php Module注册Handler
  - mod_php5.c 987行

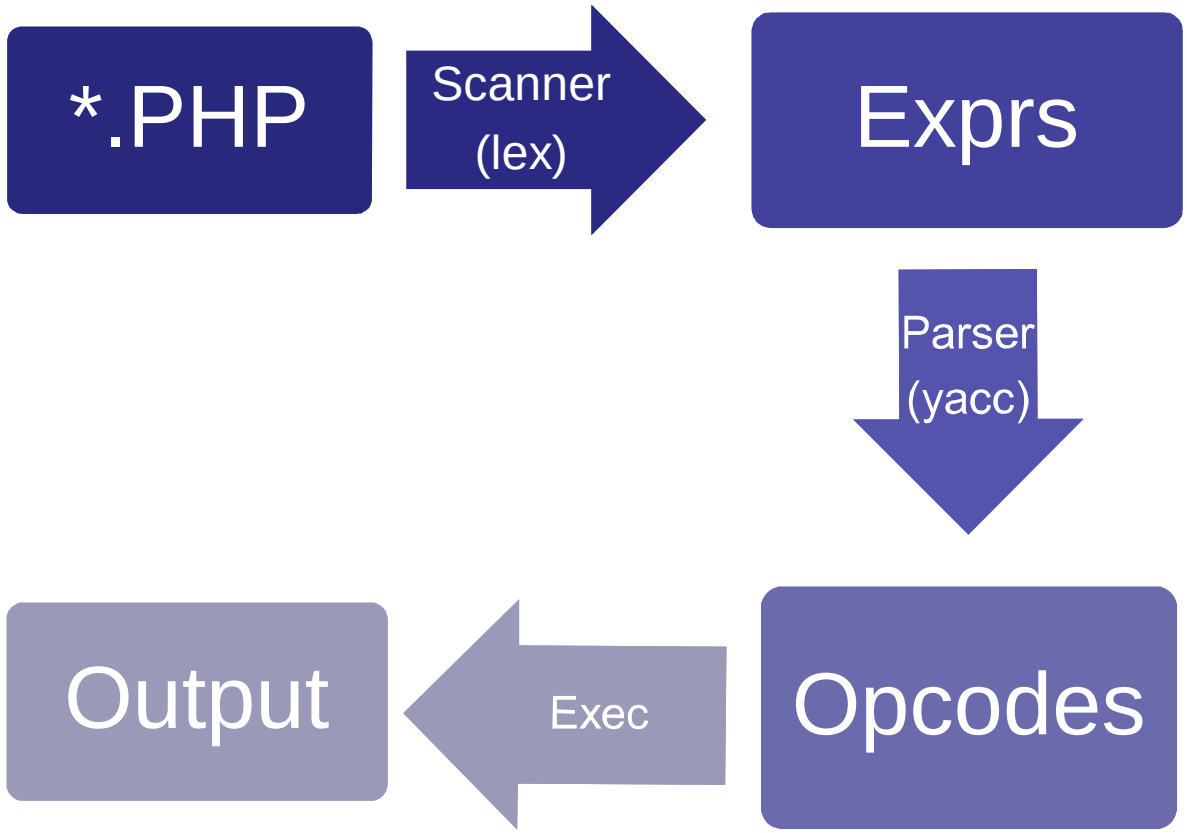
```
/* {{{ module MODULE_VAR_EXPORT php5_module
 */
module MODULE_VAR_EXPORT php5_module =
{
    STANDARD_MODULE_STUFF,
    php_init_handler,           /* initializer */
    php_create_dir,             /* per-directory config creator */
    php_merge_dir,              /* dir merger */
    NULL,                       /* per-server config creator */
    NULL,                       /* merge server config */
    php_commands,               /* command table */
    php_handlers,               /* handlers */
    NULL,                       /* filename translation */
    NULL,                       /* check_user_id */
    NULL,                       /* check auth */
    NULL,                       /* check access */
    NULL,                       /* type_checker */
    NULL,                       /* fixups */
    NULL                        /* logger */
#if MODULE_MAGIC_NUMBER >= 19970103
    , NULL                      /* header parser */
#endif
#if MODULE_MAGIC_NUMBER >= 19970719
    , NULL                      /* child_init */
#endif
#if MODULE_MAGIC_NUMBER >= 19970728
    , php_child_exit_handler        /* child_exit */
#endif
#if MODULE_MAGIC_NUMBER >= 19970902
    , NULL                      /* post read-request */
#endif
};
/* }}} */
```

Cooperation con’t

- http.conf

```
##### DO NO EDIT THIS FILE ####

LoadModule php5_module libexec/yapache_libphp5.so
AddType application/x-httpd-php .php
```

PHP Parse/Execute Process



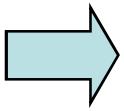
PHP Parse/Execute Process con't

- Scan(lex)
  - Zend/zend_language_scanner.c 3047行

```
ZEND_API zend_op_array *compile_file(zend_file_handle *file_handle, int type TSRMLS_DC){
        retval = op_array;
        ….
        return retval;}
```

  - Zend/zend_language_scanner.l

```
<?php
  $sum = 1 + 2;
  echo "1+2=".$sum;
?>
```

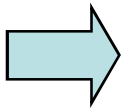


```
T_OPEN_TAG: '<?php '
=
T_LNUMBER: '1'
+
T_LNUMBER: '2'
T_ECHO: 'echo'
T_CONSTANT_ENCAPSED_STRI
NG: "1+2=".
T_CLOSE_TAG: '?>'
```

PHP Parse/Execute Process con’t

- Parse/Complie(yacc)
  - zend_language_parser.y

```
T_OPEN_TAG: '<?php '
=
T_LNUMBER: '1'
+
T_LNUMBER: '2'
T_ECHO: 'echo'
T_CONSTANT_ENCAPSED_STRI
NG: "1+2=".
T_CLOSE_TAG: '?>'
```



Opcode	Op1	Op2	Result
ADD	1	2	$tmp0
ASSIGN	$cv0(sum)	$tmp0	$var1
CONCAT	'1+2='	$cv0(sum)	$tmp2
ECHO	$tmp2		
RETURN	1		

PHP Parse/Execute Process con’t

- Execute
  - Zend/zend_execute.c

```
void (*zend_execute) (zend_op_array *op_array TSRMLS_DC);
```

- Zend_op_array
  - Zend/zend_compile.h

```
struct zend_op{
 opcode_handler_t   handler;
 znoderesult;
 znodeop1;
 znodeop2;
 ulongextended_value;
 uintlineno;
 zend_ucharopcode;
};
```

PHP Parse/Execute Process con't

- Execute
  - Zend/zend_opcode.c 428行

```
ZEND_API void *get_binary_op(int opcode)
{
    switch (opcode) {
        case ZEND_ADD:
        case ZEND_ASSIGN_ADD:
            return (void *) add_function;
            break;
        case ZEND_SUB:
        case ZEND_ASSIGN_SUB:
            return (void *) sub_function;
            break;
        case ZEND_MUL:
        case ZEND_ASSIGN_MUL:
            return (void *) mul_function;
```

A sample

- Clien Request

```
GET /index.php  HTTP/1.1
Host: localdev5.corp.cnb
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US;
rv:1.9.0.1) Gecko/2008070208 Firefox/3.0.1
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: ja,zh-cn;q=0.7,zh;q=0.3
Accept-Encoding: gzip,deflate
Accept-Charset: UTF-8,*
Keep-Alive: 300
Connection: keep-alive
```

A sample

- Server Pares
  - URI
  - User Auth
  - …
  - MIME type Check
    - application/x-httpd-http
  - Call handler
    - send_parsed_php(request_rec *)
    - Zend_execute_script(…..request_rec->filename);

A sample

- Zend/zend.c 1073 行

```
ZEND_API int zend_execute_scripts(int type TSRMLS_DC, zval **retval, int file_count, ...)
{
    va_list files;
    int i;
    zend_file_handle *file_handle;
    zend_op_array *orig_op_array = EG(active_op_array);
    zval *local_retval=NULL;

    va_start(files, file_count);
    for (i=0; i<file_count; i++) {
        file_handle = va_arg(files, zend_file_handle *);
        if (!file_handle) {
            continue;
        }
        EG(active_op_array) = zend_compile_file(file_handle, type TSRMLS_CC);
        if(file_handle->opened_path) {
```

A sample

- Index.php

```
<?php
    echo  2+3;
?>
```

A sample

- Zend_language_scanner.l 362行

```
ZEND_API zend_op_array *compile_file(zend_file_handle *file_handle, int type TSRMLS_DC)
{
        ......
        ......

        compiler_result = zendparse(TSRMLS_C);
```

- Zend_language_parse.c 62行

```
/* Substitute the variable and function names.  */
#define yyparse zendparse
#define yylex   zendlex
#define yyerror zenderror
#define yylval  zendlval
#define yychar  zendchar
#define yydebug zenddebug
#define yynerrs zendnerrs
```

A sample

- Parser
  - Zend_language_parse.y

```
    expr '^' expr   { zend_do_binary_op(ZEND_BW_XOR, &$$, &$1, &$3 TSRMLS_CC); }
    expr '.' expr   { zend_do_binary_op(ZEND_CONCAT, &$$, &$1, &$3 TSRMLS_CC); }
    expr '+' expr   { zend_do_binary_op(ZEND_ADD, &$$, &$1, &$3 TSRMLS_CC); }
    expr '-' expr   { zend_do_binary_op(ZEND_SUB, &$$, &$1, &$3 TSRMLS_CC); }
```

  - Zend_compile.c 258行

```
void zend_do_binary_op(zend_uchar op, znode *result, znode *op1, znode *op2 TSRMLS_DC)
{
    zend_op *opline = get_next_op(CG(active_op_array) TSRMLS_CC);

    opline->opcode = op;
    opline->result.op_type = IS_TMP_VAR;
    opline->result.u.var = get_temporary_variable(CG(active_op_array));
    opline->op1 = *op1;
    opline->op2 = *op2;
    *result = opline->result;
}
```

A sample

- Opcodes

```
$ sudo php -d vld.active=1 -r' echo 2+3;';
Password:
Branch analysis from position: 0
Return found
filename:       Command line code
function name:  (null)
number of ops:  4
compiled vars:  none
line     #  op                            fetch          ext  return  operands
-------------------------------------------------------------------------------
   1     0  ADD                                              ~0      2, 3
         1  ECHO                                                     ~0
         2  RETURN                                                   null
         3* ZEND_HANDLE_EXCEPTION
```

A sample

- Execute
- Output
- Server send Responds Text to Client.

Now We Can….

- 1, 服务器的Access log没有任何输出
- 2, 隐藏PHP文件类型
- 3, PHP出错的阶段
- 4, 编写PHP扩展
- 5, …

Documents

- 《Apache Server 源代码分析》
- 《Writing Apache Modules with Perl and C》
- 《Extending and Embedding PHP》
- 《PHP手册》：“Zend API：深入 PHP 内核”
- http://www.laruence.com

谢谢大家！