We politely ask for 2 grace periods for this project and apologize for any inconvenience caused by our delay.

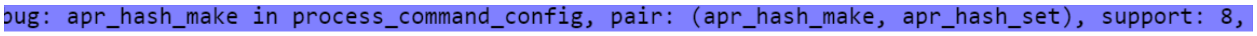
CS510: Project2

Chufeng Gao gao513@purdue.edu
Meng-Chieh Lin lin1055@purdue.edu

Part 1 (b). Many bugs generated by our detection tool turn out to be false positives. The first reason is that the default algorithm does not expand scopes and check the partners in them during the detecting process, which results in many misclassified to appm ear wseeithout some of their ”partners”. But in fact, they are paired.

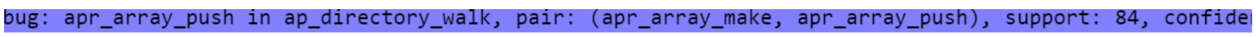
The second reason is that some of the reported ”bugs” are intentionally designed by developers for some purposes, meaning those ”bugs” should be treated as normal practices.

The pairs we want to discuss are (apr_hash_make, apr_hash_set) and (apr_array_make, apr_array_push). For the first pair, one of corresponding bug reports is below



```
ug: apr_hash_make in process_command_config, pair: (apr_hash_make, apr_hash_set), support: 8,
```

which indicates that *apr_hash_make* is unpaired in function *process_command_config*. However, when expanding the functions called in *process_command_config*, we find that function *apr_hash_set* is called in function *ap_add_module_commands* which is in the function *rebuild_conf_hash* called in *process_command_config*. In other words, *apr_hash_make* is paired with *apr_hash_set* if the default algorithm expands functions into second level. For the second pair, the one of corresponding bug reports is below



```
bug: apr_array_push in ap_directory_walk, pair: (apr_array_make, apr_array_push), support: 84, confide
```

which implies that function *apr_array_push* is unpaired in function *ap_directory_walk*. However, if we expand *ap_directory_walk*, it is not difficult to find that function *prep_walk_cache*, which is called in *ap_directory_walk*, calls function *apr_array_make* in its body. Therefore, we consider this bug report as a false positive with the same reason.

Part 1 (c). Our algorithms applies the concept, Inter-Procedural Analysis, to expand scopes when detection bugs with a given level parameter. To avoid misunderstanding, we call the functions, including scopes, in the example listed in page 2 of project2 functions here.

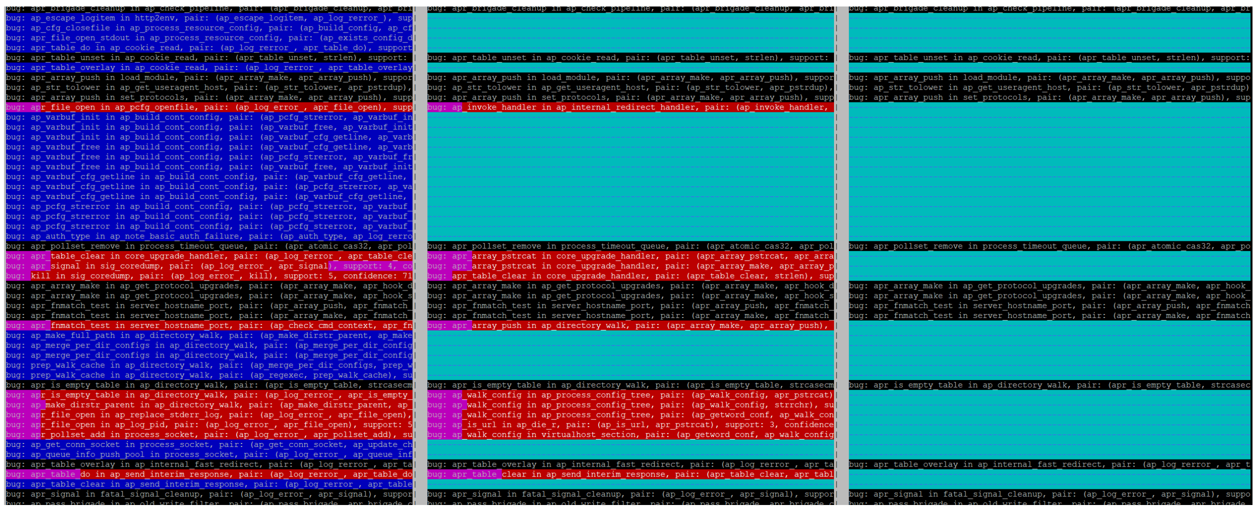
There are two process when we can perform function inline(expansion of scopes). One is the process when we are counting supports and calculating confidences. The other is the process when we are detecting bugs using the pairing assumption inferred from the counted supports and confidences. If we perform function inline during the counting process, the result could be unpredictable since the expansion process both increases method support and pair support. Therefore, we choose only to expand scopes during the detection process.

We develop two algorithms and compare them with default one(we use the algorithm give in part a as a baseline). After calculating all supports and confidences and generating a map which contains pairs that should appear, our first algorithm detects bugs by expanding any functions that involve other functions while reserving those expanded functions. Different from our first algorithm, the second one expands those functions without keeping them while detecting bugs.

Take scopeX{A(); B(); C(); D()} as an example, if we expand it in a non-reservation fashion, it will look as A(); B(); C(); D(). If we expand it in a reservation fashion, it will look as {scopeX(); A(); B(); C(); D();}

Below are the experiments we examine [1] on three algorithms: likely-invariants (*LI*), expansion-involved likely-invariants with scope (*EILIS*), and expansion-involved likely-invariants without scope (*EILI*).

The following figures always show the result of the three algorithms from left to right in the order of *EILI*(Remove scope after expansion), *LI*(Baseline, no expansion performed), and *EILIS*(Reserve scope after expansion). The level in following figures are just for *EILI* and *EILIS*.



```
bug: apr_brigade_cleanup in ap_check_pipeline, pair: (apr_brigade_cleanup, apr_bri
bug: ap_escape_logitem in http2env, pair: (ap_escape_logitem, ap_log_rerror_), sup
bug: ap_cfg_closefile in ap_process_resource_config, pair: (ap_build_config, ap_cf
bug: apr_file_open_stdout in ap_process_resource_config, pair: (ap_exists_config_d
bug: apr_table_do in ap_cookie_read, pair: (ap_log_rerror_, apr_table_do), support
bug: apr_table_unset in ap_cookie_read, pair: (apr_table_unset, strlen), support:
bug: apr_table_overlay in ap_cookie_read, pair: (ap_log_rerror_, apr_table_overlay
bug: apr_array_push in load_module, pair: (apr_array_make, apr_array_push), suppor
bug: ap_str_tolower in ap_get_useragent_host, pair: (ap_str_tolower, apr_pstrdup),
bug: apr_array_push in set_protocols, pair: (apr_array_make, apr_array_push), supp
bug: apr_file_open in ap_pcfg_openfile, pair: (ap_log_error_, apr_file_open), supp
bug: ap_varbuf_init in ap_build_cont_config, pair: (ap_pcfg_strerror, ap_varbuf_in
bug: ap_varbuf_init in ap_build_cont_config, pair: (ap_varbuf_free, ap_varbuf_init
bug: ap_varbuf_init in ap_build_cont_config, pair: (ap_varbuf_cfg_getline, ap_varb
bug: ap_varbuf_free in ap_build_cont_config, pair: (ap_varbuf_cfg_getline, ap_varb
bug: ap_varbuf_free in ap_build_cont_config, pair: (ap_pcfg_strerror, ap_varbuf_fr
bug: ap_varbuf_free in ap_build_cont_config, pair: (ap_varbuf_free, ap_varbuf_init
bug: ap_varbuf_cfg_getline in ap_build_cont_config, pair: (ap_varbuf_cfg_getline,
bug: ap_varbuf_cfg_getline in ap_build_cont_config, pair: (ap_pcfg_strerror, ap_va
bug: ap_varbuf_cfg_getline in ap_build_cont_config, pair: (ap_varbuf_cfg_getline,
bug: ap_pcfg_strerror in ap_build_cont_config, pair: (ap_pcfg_strerror, ap_varbuf_
bug: ap_pcfg_strerror in ap_build_cont_config, pair: (ap_pcfg_strerror, ap_varbuf_
bug: ap_pcfg_strerror in ap_build_cont_config, pair: (ap_pcfg_strerror, ap_varbuf_
bug: ap_auth_type in ap_note_basic_auth_failure, pair: (ap_auth_type, ap_log_rerro
bug: apr_pollset_remove in process_timeout_queue, pair: (apr_atomic_cas32, apr_pol
bug: apr_table_clear in core_upgrade_handler, pair: (ap_log_rerror_, apr_table_cle
bug: apr_signal in sig_coredump, pair: (ap_log_error_, apr_signal), support: 4, co
bug: kill in sig_coredump, pair: (ap_log_error_, kill), support: 5, confidence: 71
bug: apr_array_make in ap_get_protocol_upgrades, pair: (apr_array_make, apr_hook_d
bug: apr_array_make in ap_get_protocol_upgrades, pair: (apr_array_make, apr_hook_s
bug: apr_fnmatch_test in server_hostname_port, pair: (apr_array_push, apr_fnmatch_
bug: apr_fnmatch_test in server_hostname_port, pair: (apr_array_make, apr_fnmatch_
bug: apr_fnmatch_test in server_hostname_port, pair: (ap_check_cmd_context, apr_fn
bug: ap_make_full_path in ap_directory_walk, pair: (ap_make_dirstr_parent, ap_make
bug: ap_merge_per_dir_configs in ap_directory_walk, pair: (ap_merge_per_dir_config
bug: ap_merge_per_dir_configs in ap_directory_walk, pair: (ap_merge_per_dir_config
bug: prep_walk_cache in ap_directory_walk, pair: (ap_merge_per_dir_configs, prep_w
bug: prep_walk_cache in ap_directory_walk, pair: (ap_regexec, prep_walk_cache), su
bug: apr_is_empty_table in ap_directory_walk, pair: (apr_is_empty_table, strcasecm
bug: apr_is_empty_table in ap_directory_walk, pair: (ap_log_rerror_, apr_is_empty_
bug: ap_make_dirstr_parent in ap_directory_walk, pair: (ap_make_dirstr_parent, ap_
bug: apr_file_open in ap_replace_stderr_log, pair: (ap_log_error_, apr_file_open),
bug: apr_file_open in ap_log_pid, pair: (ap_log_error_, apr_file_open), support: 5
bug: apr_pollset_add in process_socket, pair: (ap_log_error_, apr_pollset_add), su
bug: ap_get_conn_socket in process_socket, pair: (ap_get_conn_socket, ap_update_ch
bug: ap_queue_info_push_pool in process_socket, pair: (ap_log_error_, ap_queue_inf
bug: apr_table_overlay in ap_internal_fast_redirect, pair: (ap_log_rerror_, apr_ta
bug: apr_table_do in ap_send_interim_response, pair: (ap_log_rerror_, apr_table_do
bug: apr_table_clear in ap_send_interim_response, pair: (ap_log_rerror_, apr_table
bug: apr_signal in fatal_signal_cleanup, pair: (ap_log_error_, apr_signal), suppor
bug: ap_pass_brigade in ap_old_write_filter, pair: (ap_pass_brigade, apr_brigade_c
```

```
bug: apr_brigade_cleanup in ap_check_pipeline, pair: (apr_brigade_cleanup, apr_bri
bug: apr_table_unset in ap_cookie_read, pair: (apr_table_unset, strlen), support:
bug: apr_array_push in load_module, pair: (apr_array_make, apr_array_push), suppor
bug: ap_str_tolower in ap_get_useragent_host, pair: (ap_str_tolower, apr_pstrdup),
bug: apr_array_push in set_protocols, pair: (apr_array_make, apr_array_push), supp
bug: ap_invoke_handler in ap_internal_redirect_handler, pair: (ap_invoke_handler,
bug: apr_pollset_remove in process_timeout_queue, pair: (apr_atomic_cas32, apr_pol
bug: apr_array_pstrcat in core_upgrade_handler, pair: (apr_array_pstrcat, apr_arra
bug: apr_array_pstrcat in core_upgrade_handler, pair: (apr_array_make, apr_array_p
bug: apr_table_clear in core_upgrade_handler, pair: (apr_table_clear, strlen), sup
bug: apr_array_make in ap_get_protocol_upgrades, pair: (apr_array_make, apr_hook_d
bug: apr_array_make in ap_get_protocol_upgrades, pair: (apr_array_make, apr_hook_s
bug: apr_fnmatch_test in server_hostname_port, pair: (apr_array_push, apr_fnmatch_
bug: apr_fnmatch_test in server_hostname_port, pair: (apr_array_make, apr_fnmatch_
bug: apr_array_push in ap_directory_walk, pair: (apr_array_make, apr_array_push),
bug: apr_is_empty_table in ap_directory_walk, pair: (apr_is_empty_table, strcasecm
bug: ap_walk_config in ap_process_config_tree, pair: (ap_walk_config, apr_pstrcat)
bug: ap_walk_config in ap_process_config_tree, pair: (ap_walk_config, strrchr), su
bug: ap_walk_config in ap_process_config_tree, pair: (ap_getword_conf, ap_walk_con
bug: ap_is_url in ap_die_r, pair: (ap_is_url, apr_pstrcat), support: 3, confidence
bug: ap_walk_config in virtualhost_section, pair: (ap_getword_conf, ap_walk_config
bug: apr_table_overlay in ap_internal_fast_redirect, pair: (ap_log_rerror_, apr_ta
bug: apr_table_clear in ap_send_interim_response, pair: (apr_table_clear, apr_tabl
bug: apr_signal in fatal_signal_cleanup, pair: (ap_log_error_, apr_signal), suppor
bug: ap_pass_brigade in ap_old_write_filter, pair: (ap_pass_brigade, apr_brigade_c
```

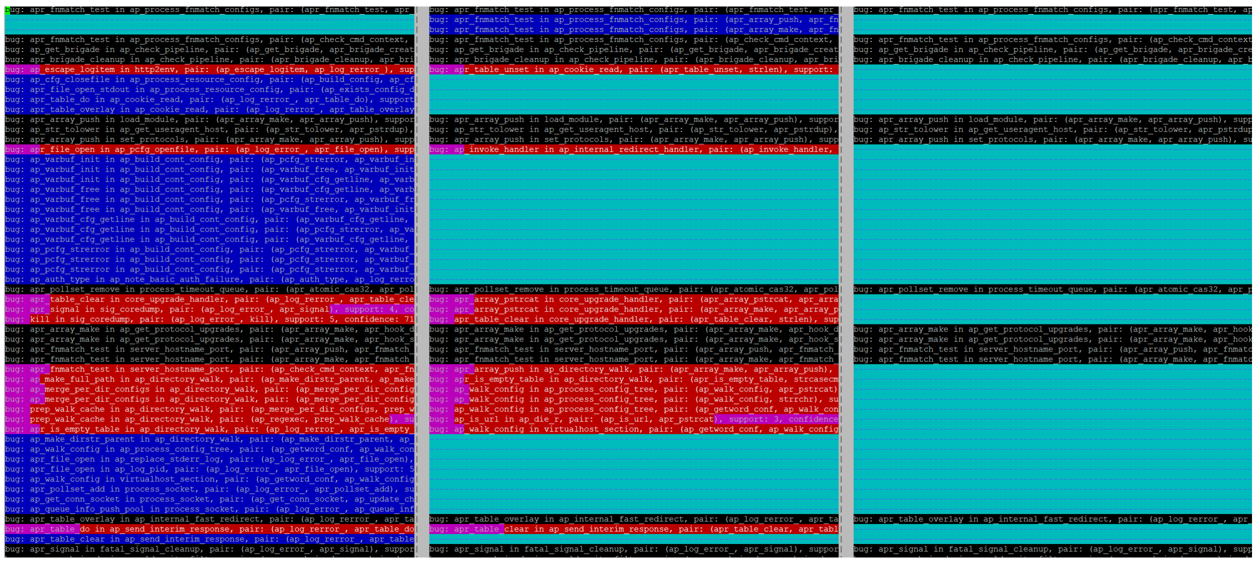
```
bug: apr_brigade_cleanup in ap_check_pipeline, pair: (apr_brigade_cleanup, apr_br
bug: apr_table_unset in ap_cookie_read, pair: (apr_table_unset, strlen), support:
bug: apr_array_push in load_module, pair: (apr_array_make, apr_array_push), suppo
bug: ap_str_tolower in ap_get_useragent_host, pair: (ap_str_tolower, apr_pstrdup)
bug: apr_array_push in set_protocols, pair: (apr_array_make, apr_array_push), sup
bug: apr_pollset_remove in process_timeout_queue, pair: (apr_atomic_cas32, apr_po
bug: apr_array_make in ap_get_protocol_upgrades, pair: (apr_array_make, apr_hook_
bug: apr_array_make in ap_get_protocol_upgrades, pair: (apr_array_make, apr_hook_
bug: apr_fnmatch_test in server_hostname_port, pair: (apr_array_push, apr_fnmatch
bug: apr_fnmatch_test in server_hostname_port, pair: (apr_array_make, apr_fnmatch
bug: apr_is_empty_table in ap_directory_walk, pair: (apr_is_empty_table, strcasec
bug: apr_table_overlay in ap_internal_fast_redirect, pair: (ap_log_rerror_, apr_t
bug: apr_signal in fatal_signal_cleanup, pair: (ap_log_error_, apr_signal), suppo
bug: ap_pass_brigade in ap_old_write_filter, pair: (ap_pass_brigade, apr_brigade_
```

Figure 1: Support = 3, Confidence = 65, Level = 2

In Figure 1, we can see that *EILI*(Expansion with scopes no reserved) performs even worse than *LI*. Because the expanded functions do not remain after expansion, pairs that contain those expanded scopes are incorrectly consider as a bug. For *EILIS*(Expansion with scopes reserved), it behaves better than other two algorithms. The reason is that it digs deep into nested functions to find any possible contained pairs, which leads to better results in the end. Obviously, the assumption can be proved from the number of detected

[1]To run our algorithm, just add an argument, level, after argument T_CONFIDENCE

bugs. The bugs detected by each algorithm are 415(scope not reserved after expansion), 253(baseline), and 200(scope reserved after expansion) respectively. More experimental results are listed below.



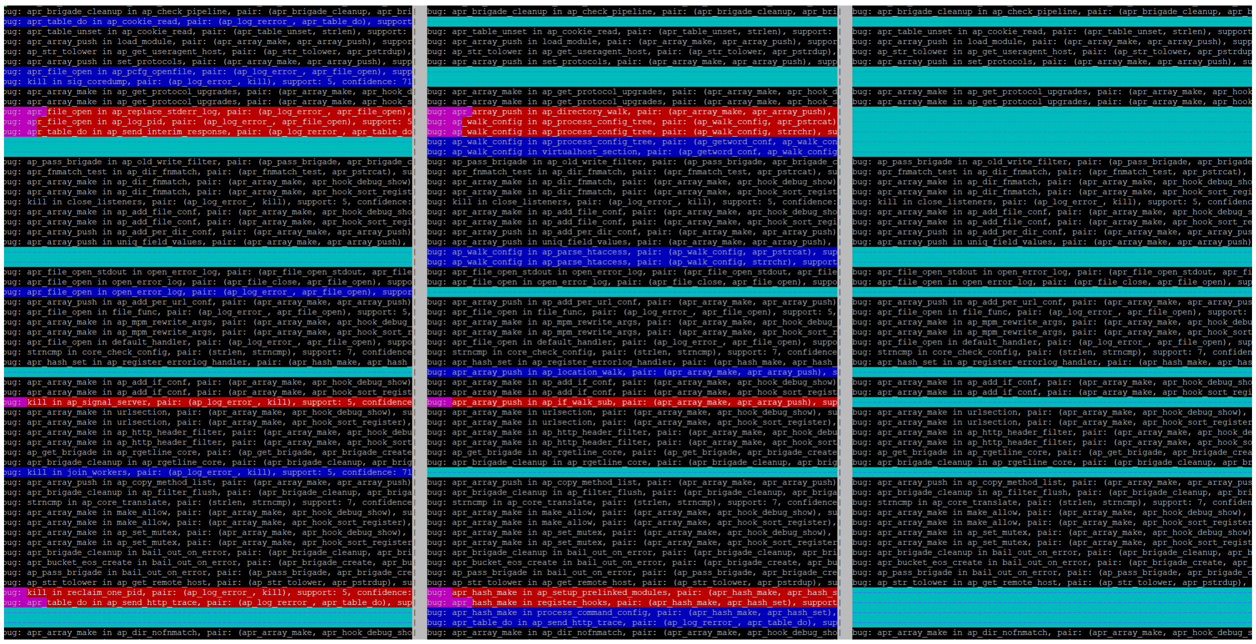
```
bug: apr_fnmatch_test in ap_process_fnmatch_configs, pair: (apr_fnmatch_test, apr_
bug: apr_fnmatch_test in ap_process_fnmatch_configs, pair: (ap_check_cmd_context,
bug: ap_get_brigade in ap_check_pipeline, pair: (ap_get_brigade, apr_brigade_creat
bug: apr_brigade_cleanup in ap_check_pipeline, pair: (apr_brigade_cleanup, apr_bri
bug: ap_escape_logitem in http2env, pair: (ap_escape_logitem, ap_log_rerror_), sup
bug: ap_cfg_closefile in ap_process_resource_config, pair: (ap_build_config, ap_cf
bug: apr_file_open_stdout in ap_process_resource_config, pair: (ap_exists_config_d
bug: apr_table_do in ap_cookie_read, pair: (ap_log_rerror_, apr_table_do), support
bug: apr_table_overlay in ap_cookie_read, pair: (ap_log_rerror_, apr_table_overlay
bug: apr_array_push in load_module, pair: (apr_array_make, apr_array_push), suppor
bug: ap_str_tolower in ap_get_useragent_host, pair: (ap_str_tolower, apr_pstrdup),
bug: apr_array_push in set_protocols, pair: (apr_array_make, apr_array_push), supp
bug: apr_file_open in ap_pcfg_openfile, pair: (ap_log_error_, apr_file_open), supp
bug: ap_varbuf_init in ap_build_cont_config, pair: (ap_pcfg_strerror, ap_varbuf_in
bug: ap_varbuf_init in ap_build_cont_config, pair: (ap_varbuf_free, ap_varbuf_init
bug: ap_varbuf_init in ap_build_cont_config, pair: (ap_varbuf_cfg_getline, ap_varb
bug: ap_varbuf_free in ap_build_cont_config, pair: (ap_varbuf_cfg_getline, ap_varb
bug: ap_varbuf_free in ap_build_cont_config, pair: (ap_pcfg_strerror, ap_varbuf_fr
bug: ap_varbuf_free in ap_build_cont_config, pair: (ap_varbuf_free, ap_varbuf_init
bug: ap_varbuf_cfg_getline in ap_build_cont_config, pair: (ap_varbuf_cfg_getline,
bug: ap_varbuf_cfg_getline in ap_build_cont_config, pair: (ap_pcfg_strerror, ap_va
bug: ap_varbuf_cfg_getline in ap_build_cont_config, pair: (ap_varbuf_cfg_getline,
bug: ap_pcfg_strerror in ap_build_cont_config, pair: (ap_pcfg_strerror, ap_varbuf_
bug: ap_pcfg_strerror in ap_build_cont_config, pair: (ap_pcfg_strerror, ap_varbuf_
bug: ap_pcfg_strerror in ap_build_cont_config, pair: (ap_pcfg_strerror, ap_varbuf_
bug: ap_auth_type in ap_note_basic_auth_failure, pair: (ap_auth_type, ap_log_rerro
bug: apr_pollset_remove in process_timeout_queue, pair: (apr_atomic_cas32, apr_pol
bug: apr_table_clear in core_upgrade_handler, pair: (ap_log_rerror_, apr_table_cle
bug: apr_signal in sig_coredump, pair: (ap_log_error_, apr_signal), support: 4, co
bug: kill in sig_coredump, pair: (ap_log_error_, kill), support: 5, confidence: 71
bug: apr_array_make in ap_get_protocol_upgrades, pair: (apr_array_make, apr_hook_d
bug: apr_array_make in ap_get_protocol_upgrades, pair: (apr_array_make, apr_hook_s
bug: apr_fnmatch_test in server_hostname_port, pair: (apr_array_push, apr_fnmatch_
bug: apr_fnmatch_test in server_hostname_port, pair: (apr_array_make, apr_fnmatch_
bug: apr_fnmatch_test in server_hostname_port, pair: (ap_check_cmd_context, apr_fn
bug: ap_make_full_path in ap_directory_walk, pair: (ap_make_dirstr_parent, ap_make
bug: ap_merge_per_dir_configs in ap_directory_walk, pair: (ap_merge_per_dir_config
bug: ap_merge_per_dir_configs in ap_directory_walk, pair: (ap_merge_per_dir_config
bug: prep_walk_cache in ap_directory_walk, pair: (ap_merge_per_dir_configs, prep_w
bug: prep_walk_cache in ap_directory_walk, pair: (ap_regexec, prep_walk_cache), su
bug: apr_is_empty_table in ap_directory_walk, pair: (ap_log_rerror_, apr_is_empty_
bug: ap_make_dirstr_parent in ap_directory_walk, pair: (ap_make_dirstr_parent, ap_
bug: ap_walk_config in ap_process_config_tree, pair: (ap_getword_conf, ap_walk_con
bug: apr_file_open in ap_replace_stderr_log, pair: (ap_log_error_, apr_file_open),
bug: apr_file_open in ap_log_pid, pair: (ap_log_error_, apr_file_open), support: 5
bug: ap_walk_config in virtualhost_section, pair: (ap_getword_conf, ap_walk_config
bug: apr_pollset_add in process_socket, pair: (ap_log_error_, apr_pollset_add), su
bug: ap_get_conn_socket in process_socket, pair: (ap_get_conn_socket, ap_update_ch
bug: ap_queue_info_push_pool in process_socket, pair: (ap_log_error_, ap_queue_inf
bug: apr_table_overlay in ap_internal_fast_redirect, pair: (ap_log_rerror_, apr_ta
bug: apr_table_do in ap_send_interim_response, pair: (ap_log_rerror_, apr_table_do
bug: apr_table_clear in ap_send_interim_response, pair: (ap_log_rerror_, apr_table
bug: apr_signal in fatal_signal_cleanup, pair: (ap_log_error_, apr_signal), suppor
```

```
bug: apr_fnmatch_test in ap_process_fnmatch_configs, pair: (apr_fnmatch_test, apr_
bug: apr_fnmatch_test in ap_process_fnmatch_configs, pair: (apr_array_push, apr_fn
bug: apr_fnmatch_test in ap_process_fnmatch_configs, pair: (apr_array_make, apr_fn
bug: apr_fnmatch_test in ap_process_fnmatch_configs, pair: (ap_check_cmd_context,
bug: ap_get_brigade in ap_check_pipeline, pair: (ap_get_brigade, apr_brigade_creat
bug: apr_brigade_cleanup in ap_check_pipeline, pair: (apr_brigade_cleanup, apr_bri
bug: apr_table_unset in ap_cookie_read, pair: (apr_table_unset, strlen), support:
bug: apr_array_push in load_module, pair: (apr_array_make, apr_array_push), suppor
bug: ap_str_tolower in ap_get_useragent_host, pair: (ap_str_tolower, apr_pstrdup),
bug: apr_array_push in set_protocols, pair: (apr_array_make, apr_array_push), supp
bug: ap_invoke_handler in ap_internal_redirect_handler, pair: (ap_invoke_handler,
bug: apr_pollset_remove in process_timeout_queue, pair: (apr_atomic_cas32, apr_pol
bug: apr_array_pstrcat in core_upgrade_handler, pair: (apr_array_pstrcat, apr_arra
bug: apr_array_pstrcat in core_upgrade_handler, pair: (apr_array_make, apr_array_p
bug: apr_table_clear in core_upgrade_handler, pair: (apr_table_clear, strlen), sup
bug: apr_array_make in ap_get_protocol_upgrades, pair: (apr_array_make, apr_hook_d
bug: apr_array_make in ap_get_protocol_upgrades, pair: (apr_array_make, apr_hook_s
bug: apr_fnmatch_test in server_hostname_port, pair: (apr_array_push, apr_fnmatch_
bug: apr_fnmatch_test in server_hostname_port, pair: (apr_array_make, apr_fnmatch_
bug: apr_array_push in ap_directory_walk, pair: (apr_array_make, apr_array_push),
bug: apr_is_empty_table in ap_directory_walk, pair: (apr_is_empty_table, strcasecm
bug: ap_walk_config in ap_process_config_tree, pair: (ap_walk_config, apr_pstrcat)
bug: ap_walk_config in ap_process_config_tree, pair: (ap_walk_config, strrchr), su
bug: ap_walk_config in ap_process_config_tree, pair: (ap_getword_conf, ap_walk_con
bug: ap_is_url in ap_die_r, pair: (ap_is_url, apr_pstrcat), support: 3, confidence
bug: ap_walk_config in virtualhost_section, pair: (ap_getword_conf, ap_walk_config
bug: apr_table_overlay in ap_internal_fast_redirect, pair: (ap_log_rerror_, apr_ta
bug: apr_table_clear in ap_send_interim_response, pair: (apr_table_clear, apr_tabl
bug: apr_signal in fatal_signal_cleanup, pair: (ap_log_error_, apr_signal), suppor
```

```
bug: apr_fnmatch_test in ap_process_fnmatch_configs, pair: (apr_fnmatch_test, ap
bug: apr_fnmatch_test in ap_process_fnmatch_configs, pair: (ap_check_cmd_context
bug: ap_get_brigade in ap_check_pipeline, pair: (ap_get_brigade, apr_brigade_cre
bug: apr_brigade_cleanup in ap_check_pipeline, pair: (apr_brigade_cleanup, apr_b
bug: apr_array_push in load_module, pair: (apr_array_make, apr_array_push), supp
bug: ap_str_tolower in ap_get_useragent_host, pair: (ap_str_tolower, apr_pstrdup
bug: apr_array_push in set_protocols, pair: (apr_array_make, apr_array_push), su
bug: apr_pollset_remove in process_timeout_queue, pair: (apr_atomic_cas32, apr_p
bug: apr_array_make in ap_get_protocol_upgrades, pair: (apr_array_make, apr_hook
bug: apr_array_make in ap_get_protocol_upgrades, pair: (apr_array_make, apr_hook
bug: apr_fnmatch_test in server_hostname_port, pair: (apr_array_push, apr_fnmatc
bug: apr_fnmatch_test in server_hostname_port, pair: (apr_array_make, apr_fnmatc
bug: apr_table_overlay in ap_internal_fast_redirect, pair: (ap_log_rerror_, apr_
bug: apr_signal in fatal_signal_cleanup, pair: (ap_log_error_, apr_signal), supp
```

Figure 2: Support = 3, Confidence = 65, Level = 5

In Figure 2, the bugs detected by each algorithm are 436, 253, and 180 respectively. As the level of expansion increases, the number of false positives decreases.



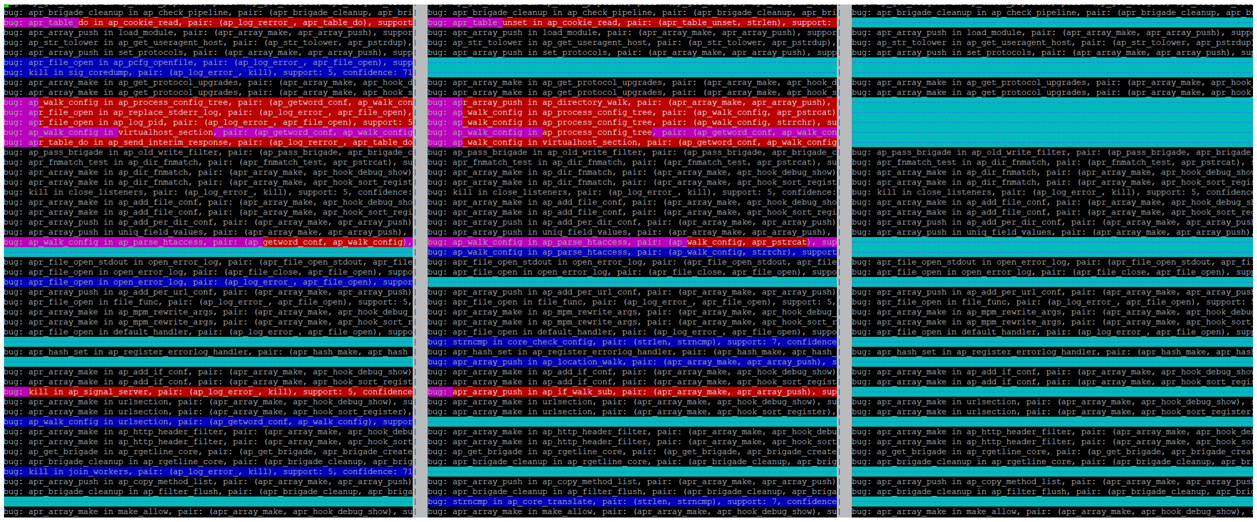
```
bug: apr_brigade_cleanup in ap_check_pipeline, pair: (apr_brigade_cleanup, apr_bri
bug: apr_table_do in ap_cookie_read, pair: (ap_log_rerror_, apr_table_do), support
bug: apr_table_unset in ap_cookie_read, pair: (apr_table_unset, strlen), support:
bug: apr_array_push in load_module, pair: (apr_array_make, apr_array_push), suppor
bug: ap_str_tolower in ap_get_useragent_host, pair: (ap_str_tolower, apr_pstrdup),
bug: apr_array_push in set_protocols, pair: (apr_array_make, apr_array_push), supp
bug: apr_file_open in ap_pcfg_openfile, pair: (ap_log_error_, apr_file_open), supp
bug: kill in sig_coredump, pair: (ap_log_error_, kill), support: 5, confidence: 71
bug: apr_array_make in ap_get_protocol_upgrades, pair: (apr_array_make, apr_hook_d
bug: apr_array_make in ap_get_protocol_upgrades, pair: (apr_array_make, apr_hook_s
bug: apr_file_open in ap_replace_stderr_log, pair: (ap_log_error_, apr_file_open),
bug: apr_file_open in ap_log_pid, pair: (ap_log_error_, apr_file_open), support: 5
bug: apr_table_do in ap_send_interim_response, pair: (ap_log_rerror_, apr_table_do
bug: ap_pass_brigade in ap_old_write_filter, pair: (ap_pass_brigade, apr_brigade_c
bug: apr_fnmatch_test in ap_dir_fnmatch, pair: (apr_fnmatch_test, apr_pstrcat), su
bug: apr_array_make in ap_dir_fnmatch, pair: (apr_array_make, apr_hook_debug_show)
bug: apr_array_make in ap_dir_fnmatch, pair: (apr_array_make, apr_hook_sort_regist
bug: kill in close_listeners, pair: (ap_log_error_, kill), support: 5, confidence:
bug: apr_array_make in ap_add_file_conf, pair: (apr_array_make, apr_hook_debug_sho
bug: apr_array_make in ap_add_file_conf, pair: (apr_array_make, apr_hook_sort_regi
bug: apr_array_push in ap_add_per_dir_conf, pair: (apr_array_make, apr_array_push)
bug: apr_array_push in uniq_field_values, pair: (apr_array_make, apr_array_push),
bug: apr_file_open_stdout in open_error_log, pair: (apr_file_open_stdout, apr_file
bug: apr_file_open in open_error_log, pair: (apr_file_close, apr_file_open), suppo
bug: apr_file_open in open_error_log, pair: (ap_log_error_, apr_file_open), suppor
bug: apr_array_push in ap_add_per_url_conf, pair: (apr_array_make, apr_array_push)
bug: apr_file_open in file_func, pair: (ap_log_error_, apr_file_open), support: 5,
bug: apr_array_make in ap_mpm_rewrite_args, pair: (apr_array_make, apr_hook_debug_
bug: apr_array_make in ap_mpm_rewrite_args, pair: (apr_array_make, apr_hook_sort_r
bug: apr_file_open in default_handler, pair: (ap_log_error_, apr_file_open), suppo
bug: strncmp in core_check_config, pair: (strlen, strncmp), support: 7, confidence
bug: apr_hash_set in ap_register_errorlog_handler, pair: (apr_hash_make, apr_hash_
bug: apr_array_make in ap_add_if_conf, pair: (apr_array_make, apr_hook_debug_show)
bug: apr_array_make in ap_add_if_conf, pair: (apr_array_make, apr_hook_sort_regist
bug: kill in ap_signal_server, pair: (ap_log_error_, kill), support: 5, confidence
bug: apr_array_make in urlsection, pair: (apr_array_make, apr_hook_debug_show), su
bug: apr_array_make in urlsection, pair: (apr_array_make, apr_hook_sort_register),
bug: apr_array_make in ap_http_header_filter, pair: (apr_array_make, apr_hook_debu
bug: apr_array_make in ap_http_header_filter, pair: (apr_array_make, apr_hook_sort
bug: ap_get_brigade in ap_rgetline_core, pair: (ap_get_brigade, apr_brigade_create
bug: apr_brigade_cleanup in ap_rgetline_core, pair: (apr_brigade_cleanup, apr_brig
bug: kill in join_workers, pair: (ap_log_error_, kill), support: 5, confidence: 71
bug: apr_array_push in ap_copy_method_list, pair: (apr_array_make, apr_array_push)
bug: apr_brigade_cleanup in ap_filter_flush, pair: (apr_brigade_cleanup, apr_briga
bug: strncmp in ap_core_translate, pair: (strlen, strncmp), support: 7, confidence
bug: apr_array_make in make_allow, pair: (apr_array_make, apr_hook_debug_show), su
bug: apr_array_make in make_allow, pair: (apr_array_make, apr_hook_sort_register),
bug: apr_array_make in ap_set_mutex, pair: (apr_array_make, apr_hook_debug_show),
bug: apr_array_make in ap_set_mutex, pair: (apr_array_make, apr_hook_sort_register
bug: apr_brigade_cleanup in bail_out_on_error, pair: (apr_brigade_cleanup, apr_bri
bug: apr_bucket_eos_create in bail_out_on_error, pair: (apr_brigade_create, apr_bu
bug: ap_pass_brigade in bail_out_on_error, pair: (ap_pass_brigade, apr_brigade_cre
bug: ap_str_tolower in ap_get_remote_host, pair: (ap_str_tolower, apr_pstrdup), su
bug: kill in reclaim_one_pid, pair: (ap_log_error_, kill), support: 5, confidence:
bug: apr_table_do in ap_send_http_trace, pair: (ap_log_rerror_, apr_table_do), sup
bug: apr_array_make in ap_dir_nofnmatch, pair: (apr_array_make, apr_hook_debug_sho
```

```
bug: apr_brigade_cleanup in ap_check_pipeline, pair: (apr_brigade_cleanup, apr_bri
bug: apr_table_unset in ap_cookie_read, pair: (apr_table_unset, strlen), support:
bug: apr_array_push in load_module, pair: (apr_array_make, apr_array_push), suppor
bug: ap_str_tolower in ap_get_useragent_host, pair: (ap_str_tolower, apr_pstrdup),
bug: apr_array_push in set_protocols, pair: (apr_array_make, apr_array_push), supp
bug: apr_array_make in ap_get_protocol_upgrades, pair: (apr_array_make, apr_hook_d
bug: apr_array_make in ap_get_protocol_upgrades, pair: (apr_array_make, apr_hook_s
bug: apr_array_push in ap_directory_walk, pair: (apr_array_make, apr_array_push),
bug: ap_walk_config in ap_process_config_tree, pair: (ap_walk_config, apr_pstrcat)
bug: ap_walk_config in ap_process_config_tree, pair: (ap_walk_config, strrchr), su
bug: ap_walk_config in ap_process_config_tree, pair: (ap_getword_conf, ap_walk_con
bug: ap_walk_config in virtualhost_section, pair: (ap_getword_conf, ap_walk_config
bug: ap_pass_brigade in ap_old_write_filter, pair: (ap_pass_brigade, apr_brigade_c
bug: apr_fnmatch_test in ap_dir_fnmatch, pair: (apr_fnmatch_test, apr_pstrcat), su
bug: apr_array_make in ap_dir_fnmatch, pair: (apr_array_make, apr_hook_debug_show)
bug: apr_array_make in ap_dir_fnmatch, pair: (apr_array_make, apr_hook_sort_regist
bug: kill in close_listeners, pair: (ap_log_error_, kill), support: 5, confidence:
bug: apr_array_make in ap_add_file_conf, pair: (apr_array_make, apr_hook_debug_sho
bug: apr_array_make in ap_add_file_conf, pair: (apr_array_make, apr_hook_sort_regi
bug: apr_array_push in ap_add_per_dir_conf, pair: (apr_array_make, apr_array_push)
bug: apr_array_push in uniq_field_values, pair: (apr_array_make, apr_array_push),
bug: ap_walk_config in ap_parse_htaccess, pair: (ap_walk_config, apr_pstrcat), sup
bug: ap_walk_config in ap_parse_htaccess, pair: (ap_walk_config, strrchr), support
bug: apr_file_open_stdout in open_error_log, pair: (apr_file_open_stdout, apr_file
bug: apr_file_open in open_error_log, pair: (apr_file_close, apr_file_open), suppo
bug: apr_array_push in ap_add_per_url_conf, pair: (apr_array_make, apr_array_push)
bug: apr_file_open in file_func, pair: (ap_log_error_, apr_file_open), support: 5,
bug: apr_array_make in ap_mpm_rewrite_args, pair: (apr_array_make, apr_hook_debug_
bug: apr_array_make in ap_mpm_rewrite_args, pair: (apr_array_make, apr_hook_sort_r
bug: apr_file_open in default_handler, pair: (ap_log_error_, apr_file_open), suppo
bug: strncmp in core_check_config, pair: (strlen, strncmp), support: 7, confidence
bug: apr_hash_set in ap_register_errorlog_handler, pair: (apr_hash_make, apr_hash_
bug: apr_array_push in ap_location_walk, pair: (apr_array_make, apr_array_push), s
bug: apr_array_make in ap_add_if_conf, pair: (apr_array_make, apr_hook_debug_show)
bug: apr_array_make in ap_add_if_conf, pair: (apr_array_make, apr_hook_sort_regist
bug: apr_array_push in ap_if_walk_sub, pair: (apr_array_make, apr_array_push), sup
bug: apr_array_make in urlsection, pair: (apr_array_make, apr_hook_debug_show), su
bug: apr_array_make in urlsection, pair: (apr_array_make, apr_hook_sort_register),
bug: apr_array_make in ap_http_header_filter, pair: (apr_array_make, apr_hook_debu
bug: apr_array_make in ap_http_header_filter, pair: (apr_array_make, apr_hook_sort
bug: ap_get_brigade in ap_rgetline_core, pair: (ap_get_brigade, apr_brigade_create
bug: apr_brigade_cleanup in ap_rgetline_core, pair: (apr_brigade_cleanup, apr_brig
bug: apr_array_push in ap_copy_method_list, pair: (apr_array_make, apr_array_push)
bug: apr_brigade_cleanup in ap_filter_flush, pair: (apr_brigade_cleanup, apr_briga
bug: strncmp in ap_core_translate, pair: (strlen, strncmp), support: 7, confidence
bug: apr_array_make in make_allow, pair: (apr_array_make, apr_hook_debug_show), su
bug: apr_array_make in make_allow, pair: (apr_array_make, apr_hook_sort_register),
bug: apr_array_make in ap_set_mutex, pair: (apr_array_make, apr_hook_debug_show),
bug: apr_array_make in ap_set_mutex, pair: (apr_array_make, apr_hook_sort_register
bug: apr_brigade_cleanup in bail_out_on_error, pair: (apr_brigade_cleanup, apr_bri
bug: apr_bucket_eos_create in bail_out_on_error, pair: (apr_brigade_create, apr_bu
bug: ap_pass_brigade in bail_out_on_error, pair: (ap_pass_brigade, apr_brigade_cre
bug: ap_str_tolower in ap_get_remote_host, pair: (ap_str_tolower, apr_pstrdup), su
bug: apr_hash_make in ap_setup_prelinked_modules, pair: (apr_hash_make, apr_hash_s
bug: apr_hash_make in register_hooks, pair: (apr_hash_make, apr_hash_set), support
bug: apr_hash_make in process_command_config, pair: (apr_hash_make, apr_hash_set),
bug: apr_table_do in ap_send_http_trace, pair: (ap_log_rerror_, apr_table_do), sup
bug: apr_array_make in ap_dir_nofnmatch, pair: (apr_array_make, apr_hook_debug_sho
```

```
bug: apr_brigade_cleanup in ap_check_pipeline, pair: (apr_brigade_cleanup, apr_b
bug: apr_table_unset in ap_cookie_read, pair: (apr_table_unset, strlen), support
bug: apr_array_push in load_module, pair: (apr_array_make, apr_array_push), supp
bug: ap_str_tolower in ap_get_useragent_host, pair: (ap_str_tolower, apr_pstrdup
bug: apr_array_push in set_protocols, pair: (apr_array_make, apr_array_push), su
bug: apr_array_make in ap_get_protocol_upgrades, pair: (apr_array_make, apr_hook
bug: apr_array_make in ap_get_protocol_upgrades, pair: (apr_array_make, apr_hook
bug: ap_pass_brigade in ap_old_write_filter, pair: (ap_pass_brigade, apr_brigade
bug: apr_fnmatch_test in ap_dir_fnmatch, pair: (apr_fnmatch_test, apr_pstrcat),
bug: apr_array_make in ap_dir_fnmatch, pair: (apr_array_make, apr_hook_debug_sho
bug: apr_array_make in ap_dir_fnmatch, pair: (apr_array_make, apr_hook_sort_regi
bug: kill in close_listeners, pair: (ap_log_error_, kill), support: 5, confidenc
bug: apr_array_make in ap_add_file_conf, pair: (apr_array_make, apr_hook_debug_s
bug: apr_array_make in ap_add_file_conf, pair: (apr_array_make, apr_hook_sort_re
bug: apr_array_push in ap_add_per_dir_conf, pair: (apr_array_make, apr_array_pus
bug: apr_array_push in uniq_field_values, pair: (apr_array_make, apr_array_push)
bug: apr_file_open_stdout in open_error_log, pair: (apr_file_open_stdout, apr_fi
bug: apr_file_open in open_error_log, pair: (apr_file_close, apr_file_open), sup
bug: apr_array_push in ap_add_per_url_conf, pair: (apr_array_make, apr_array_pus
bug: apr_file_open in file_func, pair: (ap_log_error_, apr_file_open), support:
bug: apr_array_make in ap_mpm_rewrite_args, pair: (apr_array_make, apr_hook_debu
bug: apr_array_make in ap_mpm_rewrite_args, pair: (apr_array_make, apr_hook_sort
bug: apr_file_open in default_handler, pair: (ap_log_error_, apr_file_open), sup
bug: strncmp in core_check_config, pair: (strlen, strncmp), support: 7, confiden
bug: apr_hash_set in ap_register_errorlog_handler, pair: (apr_hash_make, apr_has
bug: apr_array_make in ap_add_if_conf, pair: (apr_array_make, apr_hook_debug_sho
bug: apr_array_make in ap_add_if_conf, pair: (apr_array_make, apr_hook_sort_regi
bug: apr_array_make in urlsection, pair: (apr_array_make, apr_hook_debug_show),
bug: apr_array_make in urlsection, pair: (apr_array_make, apr_hook_sort_register
bug: apr_array_make in ap_http_header_filter, pair: (apr_array_make, apr_hook_de
bug: apr_array_make in ap_http_header_filter, pair: (apr_array_make, apr_hook_so
bug: ap_get_brigade in ap_rgetline_core, pair: (ap_get_brigade, apr_brigade_crea
bug: apr_brigade_cleanup in ap_rgetline_core, pair: (apr_brigade_cleanup, apr_br
bug: apr_array_push in ap_copy_method_list, pair: (apr_array_make, apr_array_pus
bug: apr_brigade_cleanup in ap_filter_flush, pair: (apr_brigade_cleanup, apr_bri
bug: strncmp in ap_core_translate, pair: (strlen, strncmp), support: 7, confiden
bug: apr_array_make in make_allow, pair: (apr_array_make, apr_hook_debug_show),
bug: apr_array_make in make_allow, pair: (apr_array_make, apr_hook_sort_register
bug: apr_array_make in ap_set_mutex, pair: (apr_array_make, apr_hook_debug_show)
bug: apr_array_make in ap_set_mutex, pair: (apr_array_make, apr_hook_sort_regist
bug: apr_brigade_cleanup in bail_out_on_error, pair: (apr_brigade_cleanup, apr_b
bug: apr_bucket_eos_create in bail_out_on_error, pair: (apr_brigade_create, apr_
bug: ap_pass_brigade in bail_out_on_error, pair: (ap_pass_brigade, apr_brigade_c
bug: ap_str_tolower in ap_get_remote_host, pair: (ap_str_tolower, apr_pstrdup),
bug: apr_array_make in ap_dir_nofnmatch, pair: (apr_array_make, apr_hook_debug_s
```

Figure 3: Support = 5, Confidence = 70, Level = 2

In Figure 3, the bugs detected by each algorithm are 117, 118, and 101 respectively.



```
bug: apr_brigade_cleanup in ap_check_pipeline, pair: (apr_brigade_cleanup, apr_bri
bug: apr_table_do in ap_cookie_read, pair: (ap_log_rerror_, apr_table_do), support
bug: apr_array_push in load_module, pair: (apr_array_make, apr_array_push), suppor
bug: ap_str_tolower in ap_get_useragent_host, pair: (ap_str_tolower, apr_pstrdup),
bug: apr_array_push in set_protocols, pair: (apr_array_make, apr_array_push), supp
bug: apr_file_open in ap_pcfg_openfile, pair: (ap_log_error_, apr_file_open), supp
bug: kill in sig_coredump, pair: (ap_log_error_, kill), support: 5, confidence: 71
bug: apr_array_make in ap_get_protocol_upgrades, pair: (apr_array_make, apr_hook_d
bug: apr_array_make in ap_get_protocol_upgrades, pair: (apr_array_make, apr_hook_s
bug: ap_walk_config in ap_process_config_tree, pair: (ap_getword_conf, ap_walk_con
bug: apr_file_open in ap_replace_stderr_log, pair: (ap_log_error_, apr_file_open),
bug: apr_file_open in ap_log_pid, pair: (ap_log_error_, apr_file_open), support: 5
bug: ap_walk_config in virtualhost_section, pair: (ap_getword_conf, ap_walk_config
bug: apr_table_do in ap_send_interim_response, pair: (ap_log_rerror_, apr_table_do
bug: ap_pass_brigade in ap_old_write_filter, pair: (ap_pass_brigade, apr_brigade_c
bug: apr_fnmatch_test in ap_dir_fnmatch, pair: (apr_fnmatch_test, apr_pstrcat), su
bug: apr_array_make in ap_dir_fnmatch, pair: (apr_array_make, apr_hook_debug_show)
bug: apr_array_make in ap_dir_fnmatch, pair: (apr_array_make, apr_hook_sort_regist
bug: kill in close_listeners, pair: (ap_log_error_, kill), support: 5, confidence:
bug: apr_array_make in ap_add_file_conf, pair: (apr_array_make, apr_hook_debug_sho
bug: apr_array_make in ap_add_file_conf, pair: (apr_array_make, apr_hook_sort_regi
bug: apr_array_push in ap_add_per_dir_conf, pair: (apr_array_make, apr_array_push)
bug: apr_array_push in uniq_field_values, pair: (apr_array_make, apr_array_push),
bug: ap_walk_config in ap_parse_htaccess, pair: (ap_getword_conf, ap_walk_config),
bug: apr_file_open_stdout in open_error_log, pair: (apr_file_open_stdout, apr_file
bug: apr_file_open in open_error_log, pair: (apr_file_close, apr_file_open), suppo
bug: apr_file_open in open_error_log, pair: (ap_log_error_, apr_file_open), suppor
bug: apr_array_push in ap_add_per_url_conf, pair: (apr_array_make, apr_array_push)
bug: apr_file_open in file_func, pair: (ap_log_error_, apr_file_open), support: 5,
bug: apr_array_make in ap_mpm_rewrite_args, pair: (apr_array_make, apr_hook_debug_
bug: apr_array_make in ap_mpm_rewrite_args, pair: (apr_array_make, apr_hook_sort_r
bug: apr_file_open in default_handler, pair: (ap_log_error_, apr_file_open), suppo
bug: apr_hash_set in ap_register_errorlog_handler, pair: (apr_hash_make, apr_hash_
bug: apr_array_make in ap_add_if_conf, pair: (apr_array_make, apr_hook_debug_show)
bug: apr_array_make in ap_add_if_conf, pair: (apr_array_make, apr_hook_sort_regist
bug: kill in ap_signal_server, pair: (ap_log_error_, kill), support: 5, confidence
bug: apr_array_make in urlsection, pair: (apr_array_make, apr_hook_debug_show), su
bug: apr_array_make in urlsection, pair: (apr_array_make, apr_hook_sort_register),
bug: ap_walk_config in urlsection, pair: (ap_getword_conf, ap_walk_config), suppor
bug: apr_array_make in ap_http_header_filter, pair: (apr_array_make, apr_hook_debu
bug: apr_array_make in ap_http_header_filter, pair: (apr_array_make, apr_hook_sort
bug: ap_get_brigade in ap_rgetline_core, pair: (ap_get_brigade, apr_brigade_create
bug: apr_brigade_cleanup in ap_rgetline_core, pair: (apr_brigade_cleanup, apr_brig
bug: kill in join_workers, pair: (ap_log_error_, kill), support: 5, confidence: 71
bug: apr_array_push in ap_copy_method_list, pair: (apr_array_make, apr_array_push)
bug: apr_brigade_cleanup in ap_filter_flush, pair: (apr_brigade_cleanup, apr_briga
bug: apr_array_make in make_allow, pair: (apr_array_make, apr_hook_debug_show), su
```

```
bug: apr_brigade_cleanup in ap_check_pipeline, pair: (apr_brigade_cleanup, apr_bri
bug: apr_table_unset in ap_cookie_read, pair: (apr_table_unset, strlen), support:
bug: apr_array_push in load_module, pair: (apr_array_make, apr_array_push), suppor
bug: ap_str_tolower in ap_get_useragent_host, pair: (ap_str_tolower, apr_pstrdup),
bug: apr_array_push in set_protocols, pair: (apr_array_make, apr_array_push), supp
bug: apr_array_make in ap_get_protocol_upgrades, pair: (apr_array_make, apr_hook_d
bug: apr_array_make in ap_get_protocol_upgrades, pair: (apr_array_make, apr_hook_s
bug: apr_array_push in ap_directory_walk, pair: (apr_array_make, apr_array_push),
bug: ap_walk_config in ap_process_config_tree, pair: (ap_walk_config, apr_pstrcat)
bug: ap_walk_config in ap_process_config_tree, pair: (ap_walk_config, strrchr), su
bug: ap_walk_config in ap_process_config_tree, pair: (ap_getword_conf, ap_walk_con
bug: ap_walk_config in virtualhost_section, pair: (ap_getword_conf, ap_walk_config
bug: ap_pass_brigade in ap_old_write_filter, pair: (ap_pass_brigade, apr_brigade_c
bug: apr_fnmatch_test in ap_dir_fnmatch, pair: (apr_fnmatch_test, apr_pstrcat), su
bug: apr_array_make in ap_dir_fnmatch, pair: (apr_array_make, apr_hook_debug_show)
bug: apr_array_make in ap_dir_fnmatch, pair: (apr_array_make, apr_hook_sort_regist
bug: kill in close_listeners, pair: (ap_log_error_, kill), support: 5, confidence:
bug: apr_array_make in ap_add_file_conf, pair: (apr_array_make, apr_hook_debug_sho
bug: apr_array_make in ap_add_file_conf, pair: (apr_array_make, apr_hook_sort_regi
bug: apr_array_push in ap_add_per_dir_conf, pair: (apr_array_make, apr_array_push)
bug: apr_array_push in uniq_field_values, pair: (apr_array_make, apr_array_push),
bug: ap_walk_config in ap_parse_htaccess, pair: (ap_walk_config, apr_pstrcat), sup
bug: ap_walk_config in ap_parse_htaccess, pair: (ap_walk_config, strrchr), support
bug: apr_file_open_stdout in open_error_log, pair: (apr_file_open_stdout, apr_file
bug: apr_file_open in open_error_log, pair: (apr_file_close, apr_file_open), suppo
bug: apr_array_push in ap_add_per_url_conf, pair: (apr_array_make, apr_array_push)
bug: apr_file_open in file_func, pair: (ap_log_error_, apr_file_open), support: 5,
bug: apr_array_make in ap_mpm_rewrite_args, pair: (apr_array_make, apr_hook_debug_
bug: apr_array_make in ap_mpm_rewrite_args, pair: (apr_array_make, apr_hook_sort_r
bug: apr_file_open in default_handler, pair: (ap_log_error_, apr_file_open), suppo
bug: strncmp in core_check_config, pair: (strlen, strncmp), support: 7, confidence
bug: apr_hash_set in ap_register_errorlog_handler, pair: (apr_hash_make, apr_hash_
bug: apr_array_push in ap_location_walk, pair: (apr_array_make, apr_array_push), s
bug: apr_array_make in ap_add_if_conf, pair: (apr_array_make, apr_hook_debug_show)
bug: apr_array_make in ap_add_if_conf, pair: (apr_array_make, apr_hook_sort_regist
bug: apr_array_push in ap_if_walk_sub, pair: (apr_array_make, apr_array_push), sup
bug: apr_array_make in urlsection, pair: (apr_array_make, apr_hook_debug_show), su
bug: apr_array_make in urlsection, pair: (apr_array_make, apr_hook_sort_register),
bug: apr_array_make in ap_http_header_filter, pair: (apr_array_make, apr_hook_debu
bug: apr_array_make in ap_http_header_filter, pair: (apr_array_make, apr_hook_sort
bug: ap_get_brigade in ap_rgetline_core, pair: (ap_get_brigade, apr_brigade_create
bug: apr_brigade_cleanup in ap_rgetline_core, pair: (apr_brigade_cleanup, apr_brig
bug: apr_array_push in ap_copy_method_list, pair: (apr_array_make, apr_array_push)
bug: apr_brigade_cleanup in ap_filter_flush, pair: (apr_brigade_cleanup, apr_briga
bug: strncmp in ap_core_translate, pair: (strlen, strncmp), support: 7, confidence
bug: apr_array_make in make_allow, pair: (apr_array_make, apr_hook_debug_show), su
```

```
bug: apr_brigade_cleanup in ap_check_pipeline, pair: (apr_brigade_cleanup, apr_bi
bug: apr_array_push in load_module, pair: (apr_array_make, apr_array_push), suppo
bug: ap_str_tolower in ap_get_useragent_host, pair: (ap_str_tolower, apr_pstrdup
bug: apr_array_push in set_protocols, pair: (apr_array_make, apr_array_push), sup
bug: apr_array_make in ap_get_protocol_upgrades, pair: (apr_array_make, apr_hook
bug: apr_array_make in ap_get_protocol_upgrades, pair: (apr_array_make, apr_hook
bug: ap_pass_brigade in ap_old_write_filter, pair: (ap_pass_brigade, apr_brigade
bug: apr_fnmatch_test in ap_dir_fnmatch, pair: (apr_fnmatch_test, apr_pstrcat),
bug: apr_array_make in ap_dir_fnmatch, pair: (apr_array_make, apr_hook_debug_sho
bug: apr_array_make in ap_dir_fnmatch, pair: (apr_array_make, apr_hook_sort_regi
bug: kill in close_listeners, pair: (ap_log_error_, kill), support: 5, confidence
bug: apr_array_make in ap_add_file_conf, pair: (apr_array_make, apr_hook_debug_sh
bug: apr_array_make in ap_add_file_conf, pair: (apr_array_make, apr_hook_sort_re
bug: apr_array_push in ap_add_per_dir_conf, pair: (apr_array_make, apr_array_push
bug: apr_array_push in uniq_field_values, pair: (apr_array_make, apr_array_push),
bug: apr_file_open_stdout in open_error_log, pair: (apr_file_open_stdout, apr_fi
bug: apr_file_open in open_error_log, pair: (apr_file_close, apr_file_open), sup
bug: apr_array_push in ap_add_per_url_conf, pair: (apr_array_make, apr_array_push
bug: apr_file_open in file_func, pair: (ap_log_error_, apr_file_open), support:
bug: apr_array_make in ap_mpm_rewrite_args, pair: (apr_array_make, apr_hook_debu
bug: apr_array_make in ap_mpm_rewrite_args, pair: (apr_array_make, apr_hook_sort
bug: apr_file_open in default_handler, pair: (ap_log_error_, apr_file_open), sup
bug: apr_hash_set in ap_register_errorlog_handler, pair: (apr_hash_make, apr_hash
bug: apr_array_make in ap_add_if_conf, pair: (apr_array_make, apr_hook_debug_sho
bug: apr_array_make in ap_add_if_conf, pair: (apr_array_make, apr_hook_sort_regi
bug: apr_array_make in urlsection, pair: (apr_array_make, apr_hook_debug_show),
bug: apr_array_make in urlsection, pair: (apr_array_make, apr_hook_sort_register)
bug: apr_array_make in ap_http_header_filter, pair: (apr_array_make, apr_hook_de
bug: apr_array_make in ap_http_header_filter, pair: (apr_array_make, apr_hook_so
bug: ap_get_brigade in ap_rgetline_core, pair: (ap_get_brigade, apr_brigade_crea
bug: apr_brigade_cleanup in ap_rgetline_core, pair: (apr_brigade_cleanup, apr_br
bug: apr_array_push in ap_copy_method_list, pair: (apr_array_make, apr_array_push
bug: apr_brigade_cleanup in ap_filter_flush, pair: (apr_brigade_cleanup, apr_bri
bug: apr_array_make in make_allow, pair: (apr_array_make, apr_hook_debug_show),
```

Figure 4: Support = 5, Confidence = 70, Level = 5

In Figure 4, the bugs detected by each algorithm are 119, 118, and 95 respectively. In conclusion, our first algorithm, *EILIS*, performs the best among the three in eliminating false positives. By the way, we also try the algorithm of expanding functions while counting supports and confidences, but the result varies in a huge range. Therefore, we no more provide any experiment results here.

Part 1 (d). Since there is little ground truth data of project 2, we choose not to refer to any published paper for other potential solutions. Instead, we derive our own way to reduce the false positives. To further enhance the algorithm introduced in part1(c), we create an algorithm, *EILISP*. Based on *EILIS*, we analyze the ”partner list” we acquired for each function after counting the supports and comparing supports and confidences to the corresponding thresholds. We use the ”partner list” to help determine whether the function call is a bug by calculating the ratio of missing partners.

Take the following case as an example.

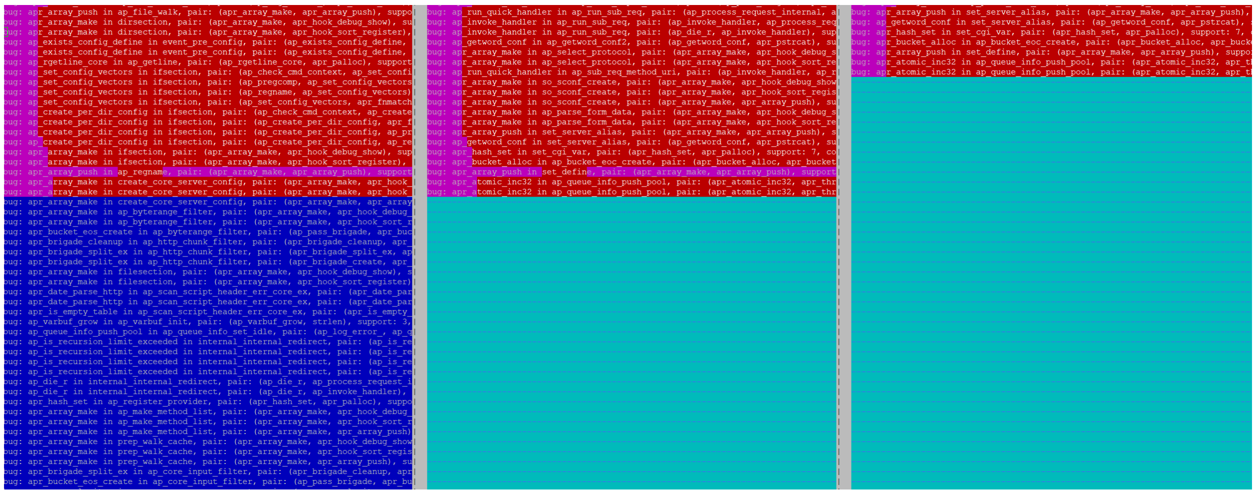
function	partners
A	B,C,D,E

```
void K(){
    A(); B(); C(); D();
}
```

After building the partner list for function A, we calculate the ratio mentioned above after expanding functions. The ratio in this case is 1/4 since only E does not appear in node K. If the achieved ratio is lower than the unpaired ratio threshold passed as an argument into the program, we assume the A appearing without B is not a bug.

The intuition here is that when A appears without B, the cause could be that the function B is missing here instead of function A is redundant. If most partners of A appear in this function node, we can assume there should be a function call of A here. Thus the reason of A unpaired with B here is that the develop forgets to call B in the function node.

The results of algorithms showed below are always in the order as: *LI*(Baseline), *EILIS*(Expansion with scope reserved), and *EILISP*(Expansion with scope reserved and enhanced with unpaired partner ratio). The ratio argument is only applied on *EILISP*.



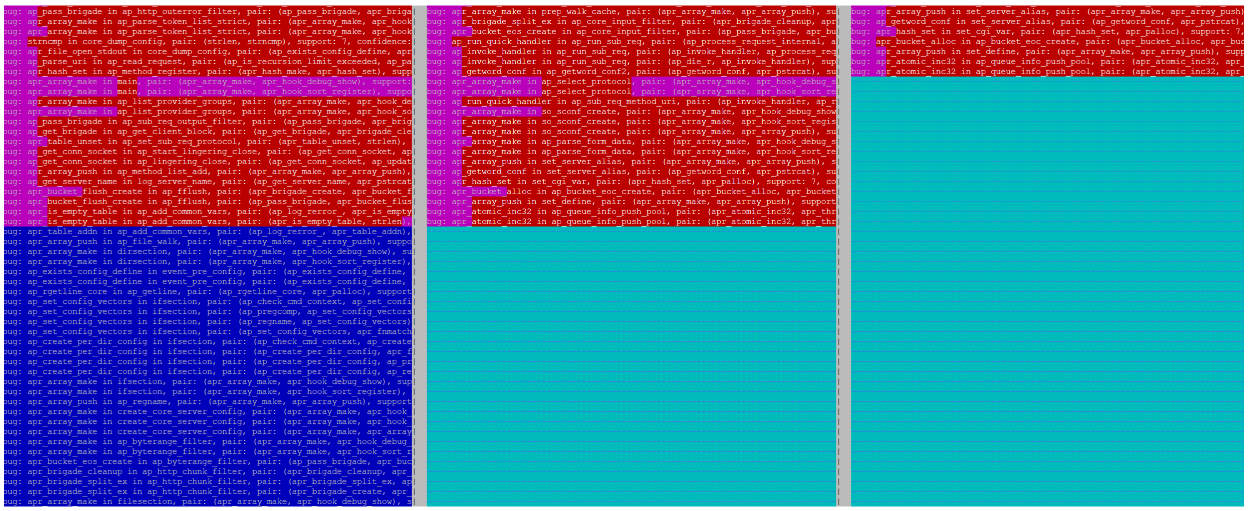
```
bug: apr_array_push in ap_file_walk, pair: (apr_array_make, apr_array_push), suppo
bug: apr_array_make in dirsection, pair: (apr_array_make, apr_hook_debug_show), su
bug: apr_array_make in dirsection, pair: (apr_array_make, apr_hook_sort_register),
bug: ap_exists_config_define in event_pre_config, pair: (ap_exists_config_define,
bug: ap_exists_config_define in event_pre_config, pair: (ap_exists_config_define,
bug: ap_rgetline_core in ap_getline, pair: (ap_rgetline_core, apr_palloc), support
bug: ap_set_config_vectors in ifsection, pair: (ap_check_cmd_context, ap_set_confi
bug: ap_set_config_vectors in ifsection, pair: (ap_pregcomp, ap_set_config_vectors
bug: ap_set_config_vectors in ifsection, pair: (ap_regname, ap_set_config_vectors)
bug: ap_set_config_vectors in ifsection, pair: (ap_set_config_vectors, apr_fnmatch
bug: ap_create_per_dir_config in ifsection, pair: (ap_check_cmd_context, ap_create
bug: ap_create_per_dir_config in ifsection, pair: (ap_create_per_dir_config, apr_f
bug: ap_create_per_dir_config in ifsection, pair: (ap_create_per_dir_config, ap_pr
bug: ap_create_per_dir_config in ifsection, pair: (ap_create_per_dir_config, ap_re
bug: apr_array_make in ifsection, pair: (apr_array_make, apr_hook_debug_show), sup
bug: apr_array_make in ifsection, pair: (apr_array_make, apr_hook_sort_register),
bug: apr_array_push in ap_regname, pair: (apr_array_make, apr_array_push), support
bug: apr_array_make in create_core_server_config, pair: (apr_array_make, apr_hook_
bug: apr_array_make in create_core_server_config, pair: (apr_array_make, apr_hook_
bug: apr_array_make in create_core_server_config, pair: (apr_array_make, apr_array
bug: apr_array_make in ap_byterange_filter, pair: (apr_array_make, apr_hook_debug_
bug: apr_array_make in ap_byterange_filter, pair: (apr_array_make, apr_hook_sort_r
bug: apr_bucket_eos_create in ap_byterange_filter, pair: (ap_pass_brigade, apr_buc
bug: apr_brigade_cleanup in ap_http_chunk_filter, pair: (apr_brigade_cleanup, apr_
bug: apr_brigade_split_ex in ap_http_chunk_filter, pair: (apr_brigade_split_ex, ap
bug: apr_brigade_split_ex in ap_http_chunk_filter, pair: (apr_brigade_create, apr_
bug: apr_array_make in filesection, pair: (apr_array_make, apr_hook_debug_show), s
bug: apr_array_make in filesection, pair: (apr_array_make, apr_hook_sort_register)
bug: apr_date_parse_http in ap_scan_script_header_err_core_ex, pair: (apr_date_par
bug: apr_date_parse_http in ap_scan_script_header_err_core_ex, pair: (apr_date_par
bug: apr_is_empty_table in ap_scan_script_header_err_core_ex, pair: (apr_is_empty_
bug: ap_varbuf_grow in ap_varbuf_init, pair: (ap_varbuf_grow, strlen), support: 3,
bug: ap_queue_info_push_pool in ap_queue_info_set_idle, pair: (ap_log_error_, ap_q
bug: ap_is_recursion_limit_exceeded in internal_internal_redirect, pair: (ap_is_re
bug: ap_is_recursion_limit_exceeded in internal_internal_redirect, pair: (ap_is_re
bug: ap_is_recursion_limit_exceeded in internal_internal_redirect, pair: (ap_is_re
bug: ap_is_recursion_limit_exceeded in internal_internal_redirect, pair: (ap_is_re
bug: ap_die_r in internal_internal_redirect, pair: (ap_die_r, ap_process_request_i
bug: ap_die_r in internal_internal_redirect, pair: (ap_die_r, ap_invoke_handler),
bug: apr_hash_set in ap_register_provider, pair: (apr_hash_set, apr_palloc), suppo
bug: apr_array_make in ap_make_method_list, pair: (apr_array_make, apr_hook_debug_
bug: apr_array_make in ap_make_method_list, pair: (apr_array_make, apr_hook_sort_r
bug: apr_array_make in ap_make_method_list, pair: (apr_array_make, apr_array_push)
bug: apr_array_make in prep_walk_cache, pair: (apr_array_make, apr_hook_debug_show
bug: apr_array_make in prep_walk_cache, pair: (apr_array_make, apr_hook_sort_regis
bug: apr_array_make in prep_walk_cache, pair: (apr_array_make, apr_array_push), su
bug: apr_brigade_split_ex in ap_core_input_filter, pair: (apr_brigade_cleanup, apr
bug: apr_bucket_eos_create in ap_core_input_filter, pair: (ap_pass_brigade, apr_bu
```

```
bug: ap_run_quick_handler in ap_run_sub_req, pair: (ap_process_request_internal, a
bug: ap_invoke_handler in ap_run_sub_req, pair: (ap_invoke_handler, ap_process_req
bug: ap_invoke_handler in ap_run_sub_req, pair: (ap_die_r, ap_invoke_handler), sup
bug: ap_getword_conf in ap_getword_conf2, pair: (ap_getword_conf, apr_pstrcat), su
bug: apr_array_make in ap_select_protocol, pair: (apr_array_make, apr_hook_debug_s
bug: apr_array_make in ap_select_protocol, pair: (apr_array_make, apr_hook_sort_re
bug: ap_run_quick_handler in ap_sub_req_method_uri, pair: (ap_invoke_handler, ap_r
bug: apr_array_make in so_sconf_create, pair: (apr_array_make, apr_hook_debug_show
bug: apr_array_make in so_sconf_create, pair: (apr_array_make, apr_hook_sort_regis
bug: apr_array_make in so_sconf_create, pair: (apr_array_make, apr_array_push), su
bug: apr_array_make in ap_parse_form_data, pair: (apr_array_make, apr_hook_debug_s
bug: apr_array_make in ap_parse_form_data, pair: (apr_array_make, apr_hook_sort_re
bug: apr_array_push in set_server_alias, pair: (apr_array_make, apr_array_push), s
bug: ap_getword_conf in set_server_alias, pair: (ap_getword_conf, apr_pstrcat), su
bug: apr_hash_set in set_cgi_var, pair: (apr_hash_set, apr_palloc), support: 7, co
bug: apr_bucket_alloc in ap_bucket_eoc_create, pair: (apr_bucket_alloc, apr_bucket
bug: apr_array_push in set_define, pair: (apr_array_make, apr_array_push), support
bug: apr_atomic_inc32 in ap_queue_info_push_pool, pair: (apr_atomic_inc32, apr_thr
bug: apr_atomic_inc32 in ap_queue_info_push_pool, pair: (apr_atomic_inc32, apr_thr
```

```
bug: apr_array_push in set_server_alias, pair: (apr_array_make, apr_array_push),
bug: ap_getword_conf in set_server_alias, pair: (ap_getword_conf, apr_pstrcat),
bug: apr_hash_set in set_cgi_var, pair: (apr_hash_set, apr_palloc), support: 7,
bug: apr_bucket_alloc in ap_bucket_eoc_create, pair: (apr_bucket_alloc, apr_bucke
bug: apr_array_push in set_define, pair: (apr_array_make, apr_array_push), suppo
bug: apr_atomic_inc32 in ap_queue_info_push_pool, pair: (apr_atomic_inc32, apr_th
bug: apr_atomic_inc32 in ap_queue_info_push_pool, pair: (apr_atomic_inc32, apr_th
```

Figure 5: Support = 3, Confidence = 65, Level = 2, ratio = 40

In Figure 5, the bugs detected by each algorithm are 253, 200, and 188 respectively.



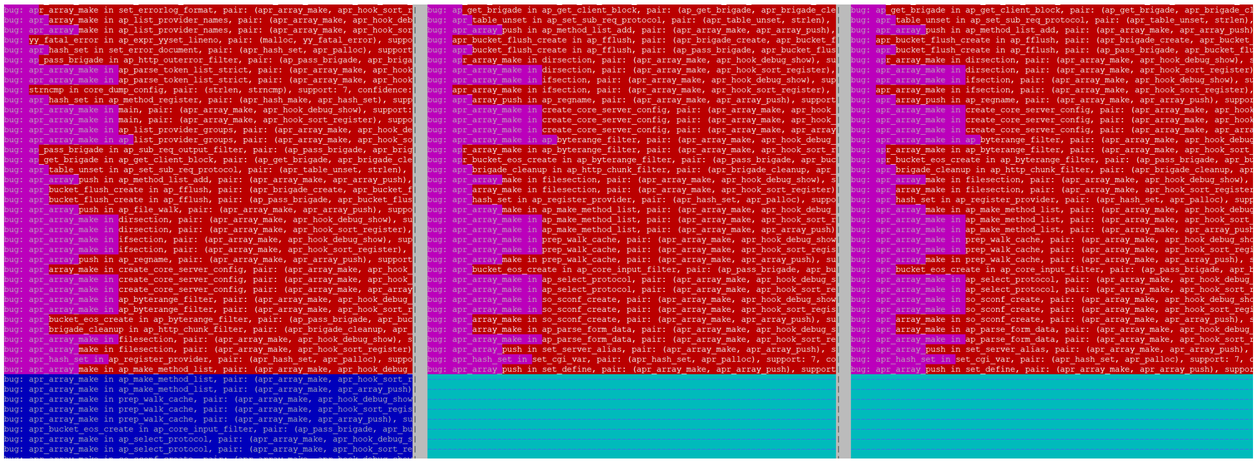
```
bug: ap_pass_brigade in ap_http_outerror_filter, pair: (ap_pass_brigade, apr_briga
bug: apr_array_make in ap_parse_token_list_strict, pair: (apr_array_make, apr_hook
bug: apr_array_make in ap_parse_token_list_strict, pair: (apr_array_make, apr_hook
bug: strncmp in core_dump_config, pair: (strlen, strncmp), support: 7, confidence:
bug: apr_file_open_stdout in core_dump_config, pair: (ap_exists_config_define, apr
bug: ap_parse_uri in ap_read_request, pair: (ap_is_recursion_limit_exceeded, ap_pa
bug: apr_hash_set in ap_method_register, pair: (apr_hash_make, apr_hash_set), supp
bug: apr_array_make in main, pair: (apr_array_make, apr_hook_debug_show), support:
bug: apr_array_make in main, pair: (apr_array_make, apr_hook_sort_register), suppo
bug: apr_array_make in ap_list_provider_groups, pair: (apr_array_make, apr_hook_de
bug: apr_array_make in ap_list_provider_groups, pair: (apr_array_make, apr_hook_so
bug: ap_pass_brigade in ap_sub_req_output_filter, pair: (ap_pass_brigade, apr_brig
bug: ap_get_brigade in ap_get_client_block, pair: (ap_get_brigade, apr_brigade_cle
bug: apr_table_unset in ap_set_sub_req_protocol, pair: (apr_table_unset, strlen),
bug: ap_get_conn_socket in ap_start_lingering_close, pair: (ap_get_conn_socket, ap
bug: ap_get_conn_socket in ap_lingering_close, pair: (ap_get_conn_socket, ap_updat
bug: apr_array_push in ap_method_list_add, pair: (apr_array_make, apr_array_push),
bug: ap_get_server_name in log_server_name, pair: (ap_get_server_name, apr_pstrcat
bug: apr_bucket_flush_create in ap_fflush, pair: (apr_brigade_create, apr_bucket_f
bug: apr_bucket_flush_create in ap_fflush, pair: (ap_pass_brigade, apr_bucket_flus
bug: apr_is_empty_table in ap_add_common_vars, pair: (ap_log_rerror_, apr_is_empty
bug: apr_is_empty_table in ap_add_common_vars, pair: (apr_is_empty_table, strlen),
bug: apr_table_addn in ap_add_common_vars, pair: (ap_log_rerror_, apr_table_addn),
bug: apr_array_push in ap_file_walk, pair: (apr_array_make, apr_array_push), suppo
bug: apr_array_make in dirsection, pair: (apr_array_make, apr_hook_debug_show), su
bug: apr_array_make in dirsection, pair: (apr_array_make, apr_hook_sort_register),
bug: ap_exists_config_define in event_pre_config, pair: (ap_exists_config_define,
bug: ap_exists_config_define in event_pre_config, pair: (ap_exists_config_define,
bug: ap_rgetline_core in ap_getline, pair: (ap_rgetline_core, apr_palloc), support
bug: ap_set_config_vectors in ifsection, pair: (ap_check_cmd_context, ap_set_confi
bug: ap_set_config_vectors in ifsection, pair: (ap_pregcomp, ap_set_config_vectors
bug: ap_set_config_vectors in ifsection, pair: (ap_regname, ap_set_config_vectors)
bug: ap_set_config_vectors in ifsection, pair: (ap_set_config_vectors, apr_fnmatch
bug: ap_create_per_dir_config in ifsection, pair: (ap_check_cmd_context, ap_create
bug: ap_create_per_dir_config in ifsection, pair: (ap_create_per_dir_config, apr_f
bug: ap_create_per_dir_config in ifsection, pair: (ap_create_per_dir_config, ap_pr
bug: ap_create_per_dir_config in ifsection, pair: (ap_create_per_dir_config, ap_re
bug: apr_array_make in ifsection, pair: (apr_array_make, apr_hook_debug_show), sup
bug: apr_array_make in ifsection, pair: (apr_array_make, apr_hook_sort_register),
bug: apr_array_push in ap_regname, pair: (apr_array_make, apr_array_push), support
bug: apr_array_make in create_core_server_config, pair: (apr_array_make, apr_hook_
bug: apr_array_make in create_core_server_config, pair: (apr_array_make, apr_hook_
bug: apr_array_make in create_core_server_config, pair: (apr_array_make, apr_array
bug: apr_array_make in ap_byterange_filter, pair: (apr_array_make, apr_hook_debug_
bug: apr_array_make in ap_byterange_filter, pair: (apr_array_make, apr_hook_sort_r
bug: apr_bucket_eos_create in ap_byterange_filter, pair: (ap_pass_brigade, apr_buc
bug: apr_brigade_cleanup in ap_http_chunk_filter, pair: (apr_brigade_cleanup, apr_
bug: apr_brigade_split_ex in ap_http_chunk_filter, pair: (apr_brigade_split_ex, ap
bug: apr_brigade_split_ex in ap_http_chunk_filter, pair: (apr_brigade_create, apr_
bug: apr_array_make in filesection, pair: (apr_array_make, apr_hook_debug_show), s
```

```
bug: apr_array_make in prep_walk_cache, pair: (apr_array_make, apr_array_push), su
bug: apr_brigade_split_ex in ap_core_input_filter, pair: (apr_brigade_cleanup, apr
bug: apr_bucket_eos_create in ap_core_input_filter, pair: (ap_pass_brigade, apr_bu
bug: ap_run_quick_handler in ap_run_sub_req, pair: (ap_process_request_internal, a
bug: ap_invoke_handler in ap_run_sub_req, pair: (ap_invoke_handler, ap_process_req
bug: ap_invoke_handler in ap_run_sub_req, pair: (ap_die_r, ap_invoke_handler), sup
bug: ap_getword_conf in ap_getword_conf2, pair: (ap_getword_conf, apr_pstrcat), su
bug: apr_array_make in ap_select_protocol, pair: (apr_array_make, apr_hook_debug_s
bug: apr_array_make in ap_select_protocol, pair: (apr_array_make, apr_hook_sort_re
bug: ap_run_quick_handler in ap_sub_req_method_uri, pair: (ap_invoke_handler, ap_r
bug: apr_array_make in so_sconf_create, pair: (apr_array_make, apr_hook_debug_show
bug: apr_array_make in so_sconf_create, pair: (apr_array_make, apr_hook_sort_regis
bug: apr_array_make in so_sconf_create, pair: (apr_array_make, apr_array_push), su
bug: apr_array_make in ap_parse_form_data, pair: (apr_array_make, apr_hook_debug_s
bug: apr_array_make in ap_parse_form_data, pair: (apr_array_make, apr_hook_sort_re
bug: apr_array_push in set_server_alias, pair: (apr_array_make, apr_array_push), s
bug: ap_getword_conf in set_server_alias, pair: (ap_getword_conf, apr_pstrcat), su
bug: apr_hash_set in set_cgi_var, pair: (apr_hash_set, apr_palloc), support: 7, co
bug: apr_bucket_alloc in ap_bucket_eoc_create, pair: (apr_bucket_alloc, apr_bucket
bug: apr_array_push in set_define, pair: (apr_array_make, apr_array_push), support
bug: apr_atomic_inc32 in ap_queue_info_push_pool, pair: (apr_atomic_inc32, apr_thr
bug: apr_atomic_inc32 in ap_queue_info_push_pool, pair: (apr_atomic_inc32, apr_thr
```

```
bug: apr_array_push in set_server_alias, pair: (apr_array_make, apr_array_push)
bug: ap_getword_conf in set_server_alias, pair: (ap_getword_conf, apr_pstrcat),
bug: apr_hash_set in set_cgi_var, pair: (apr_hash_set, apr_palloc), support: 7,
bug: apr_bucket_alloc in ap_bucket_eoc_create, pair: (apr_bucket_alloc, apr_buc
bug: apr_array_push in set_define, pair: (apr_array_make, apr_array_push), supp
bug: apr_atomic_inc32 in ap_queue_info_push_pool, pair: (apr_atomic_inc32, apr_
bug: apr_atomic_inc32 in ap_queue_info_push_pool, pair: (apr_atomic_inc32, apr_
```

Figure 6: Support = 3, Confidence = 65, Level = 5, ratio = 40

In Figure 6, the bugs detected by each algorithm are 253, 180, and 165 respectively.



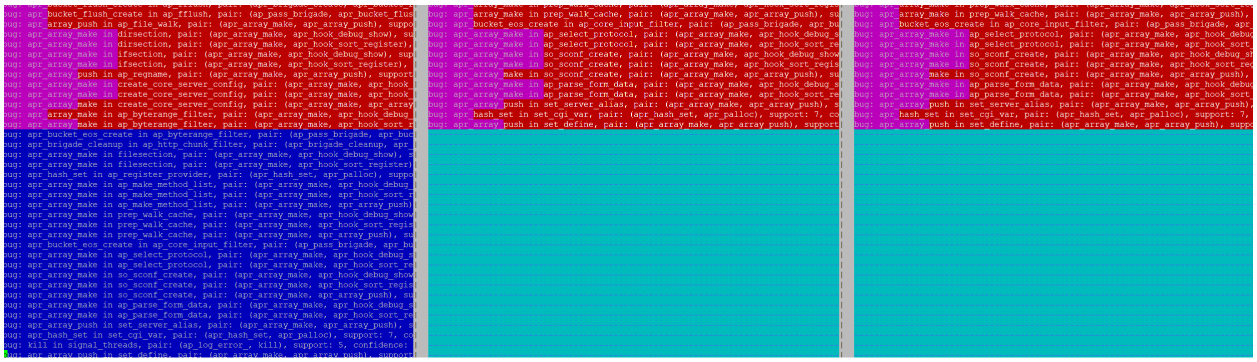
```
bug: apr_array_make in set_errorlog_format, pair: (apr_array_make, apr_hook_sort_r
bug: apr_array_make in ap_list_provider_names, pair: (apr_array_make, apr_hook_deb
bug: apr_array_make in ap_list_provider_names, pair: (apr_array_make, apr_hook_sor
bug: yy_fatal_error in ap_expr_yyset_lineno, pair: (malloc, yy_fatal_error), suppo
bug: apr_hash_set in set_error_document, pair: (apr_hash_set, apr_palloc), support
bug: ap_pass_brigade in ap_http_outerror_filter, pair: (ap_pass_brigade, apr_briga
bug: apr_array_make in ap_parse_token_list_strict, pair: (apr_array_make, apr_hook
bug: apr_array_make in ap_parse_token_list_strict, pair: (apr_array_make, apr_hook
bug: strncmp in core_dump_config, pair: (strlen, strncmp), support: 7, confidence:
bug: apr_hash_set in ap_method_register, pair: (apr_hash_make, apr_hash_set), supp
bug: apr_array_make in main, pair: (apr_array_make, apr_hook_debug_show), support:
bug: apr_array_make in main, pair: (apr_array_make, apr_hook_sort_register), suppo
bug: apr_array_make in ap_list_provider_groups, pair: (apr_array_make, apr_hook_de
bug: apr_array_make in ap_list_provider_groups, pair: (apr_array_make, apr_hook_so
bug: ap_pass_brigade in ap_sub_req_output_filter, pair: (ap_pass_brigade, apr_brig
bug: ap_get_brigade in ap_get_client_block, pair: (ap_get_brigade, apr_brigade_cle
bug: apr_table_unset in ap_set_sub_req_protocol, pair: (apr_table_unset, strlen),
bug: apr_array_push in ap_method_list_add, pair: (apr_array_make, apr_array_push),
bug: apr_bucket_flush_create in ap_fflush, pair: (apr_brigade_create, apr_bucket_f
bug: apr_bucket_flush_create in ap_fflush, pair: (ap_pass_brigade, apr_bucket_flus
bug: apr_array_push in ap_file_walk, pair: (apr_array_make, apr_array_push), suppo
bug: apr_array_make in dirsection, pair: (apr_array_make, apr_hook_debug_show), su
bug: apr_array_make in dirsection, pair: (apr_array_make, apr_hook_sort_register),
bug: apr_array_make in ifsection, pair: (apr_array_make, apr_hook_debug_show), sup
bug: apr_array_make in ifsection, pair: (apr_array_make, apr_hook_sort_register),
bug: apr_array_push in ap_regname, pair: (apr_array_make, apr_array_push), support
bug: apr_array_make in create_core_server_config, pair: (apr_array_make, apr_hook_
bug: apr_array_make in create_core_server_config, pair: (apr_array_make, apr_hook_
bug: apr_array_make in create_core_server_config, pair: (apr_array_make, apr_array
bug: apr_array_make in ap_byterange_filter, pair: (apr_array_make, apr_hook_debug_
bug: apr_array_make in ap_byterange_filter, pair: (apr_array_make, apr_hook_sort_r
bug: apr_bucket_eos_create in ap_byterange_filter, pair: (ap_pass_brigade, apr_buc
bug: apr_brigade_cleanup in ap_http_chunk_filter, pair: (apr_brigade_cleanup, apr_
bug: apr_array_make in filesection, pair: (apr_array_make, apr_hook_debug_show), s
bug: apr_array_make in filesection, pair: (apr_array_make, apr_hook_sort_register)
bug: apr_hash_set in ap_register_provider, pair: (apr_hash_set, apr_palloc), suppo
bug: apr_array_make in ap_make_method_list, pair: (apr_array_make, apr_hook_debug_
bug: apr_array_make in ap_make_method_list, pair: (apr_array_make, apr_hook_sort_r
bug: apr_array_make in ap_make_method_list, pair: (apr_array_make, apr_array_push)
bug: apr_array_make in prep_walk_cache, pair: (apr_array_make, apr_hook_debug_show
bug: apr_array_make in prep_walk_cache, pair: (apr_array_make, apr_hook_sort_regis
bug: apr_array_make in prep_walk_cache, pair: (apr_array_make, apr_array_push), su
bug: apr_bucket_eos_create in ap_core_input_filter, pair: (ap_pass_brigade, apr_bu
bug: apr_array_make in ap_select_protocol, pair: (apr_array_make, apr_hook_debug_s
bug: apr_array_make in ap_select_protocol, pair: (apr_array_make, apr_hook_sort_re
```

```
bug: ap_get_brigade in ap_get_client_block, pair: (ap_get_brigade, apr_brigade_cle
bug: apr_table_unset in ap_set_sub_req_protocol, pair: (apr_table_unset, strlen),
bug: apr_array_push in ap_method_list_add, pair: (apr_array_make, apr_array_push),
bug: apr_bucket_flush_create in ap_fflush, pair: (apr_brigade_create, apr_bucket_f
bug: apr_bucket_flush_create in ap_fflush, pair: (ap_pass_brigade, apr_bucket_flus
bug: apr_array_make in dirsection, pair: (apr_array_make, apr_hook_debug_show), su
bug: apr_array_make in dirsection, pair: (apr_array_make, apr_hook_sort_register),
bug: apr_array_make in ifsection, pair: (apr_array_make, apr_hook_debug_show), sup
bug: apr_array_make in ifsection, pair: (apr_array_make, apr_hook_sort_register),
bug: apr_array_push in ap_regname, pair: (apr_array_make, apr_array_push), support
bug: apr_array_make in create_core_server_config, pair: (apr_array_make, apr_hook_
bug: apr_array_make in create_core_server_config, pair: (apr_array_make, apr_hook_
bug: apr_array_make in create_core_server_config, pair: (apr_array_make, apr_array
bug: apr_array_make in ap_byterange_filter, pair: (apr_array_make, apr_hook_debug_
bug: apr_array_make in ap_byterange_filter, pair: (apr_array_make, apr_hook_sort_r
bug: apr_bucket_eos_create in ap_byterange_filter, pair: (ap_pass_brigade, apr_buc
bug: apr_brigade_cleanup in ap_http_chunk_filter, pair: (apr_brigade_cleanup, apr_
bug: apr_array_make in filesection, pair: (apr_array_make, apr_hook_debug_show), s
bug: apr_array_make in filesection, pair: (apr_array_make, apr_hook_sort_register)
bug: apr_hash_set in ap_register_provider, pair: (apr_hash_set, apr_palloc), suppo
bug: apr_array_make in ap_make_method_list, pair: (apr_array_make, apr_hook_debug_
bug: apr_array_make in ap_make_method_list, pair: (apr_array_make, apr_hook_sort_r
bug: apr_array_make in ap_make_method_list, pair: (apr_array_make, apr_array_push)
bug: apr_array_make in prep_walk_cache, pair: (apr_array_make, apr_hook_debug_show
bug: apr_array_make in prep_walk_cache, pair: (apr_array_make, apr_hook_sort_regis
bug: apr_array_make in prep_walk_cache, pair: (apr_array_make, apr_array_push), su
bug: apr_bucket_eos_create in ap_core_input_filter, pair: (ap_pass_brigade, apr_bu
bug: apr_array_make in ap_select_protocol, pair: (apr_array_make, apr_hook_debug_s
bug: apr_array_make in ap_select_protocol, pair: (apr_array_make, apr_hook_sort_re
bug: apr_array_make in so_sconf_create, pair: (apr_array_make, apr_hook_debug_show
bug: apr_array_make in so_sconf_create, pair: (apr_array_make, apr_hook_sort_regis
bug: apr_array_make in so_sconf_create, pair: (apr_array_make, apr_array_push), su
bug: apr_array_make in ap_parse_form_data, pair: (apr_array_make, apr_hook_debug_s
bug: apr_array_make in ap_parse_form_data, pair: (apr_array_make, apr_hook_sort_re
bug: apr_array_push in set_server_alias, pair: (apr_array_make, apr_array_push), s
bug: apr_hash_set in set_cgi_var, pair: (apr_hash_set, apr_palloc), support: 7, co
bug: apr_array_push in set_define, pair: (apr_array_make, apr_array_push), support
```

```
bug: ap_get_brigade in ap_get_client_block, pair: (ap_get_brigade, apr_brigade_cl
bug: apr_table_unset in ap_set_sub_req_protocol, pair: (apr_table_unset, strlen),
bug: apr_array_push in ap_method_list_add, pair: (apr_array_make, apr_array_push)
bug: apr_bucket_flush_create in ap_fflush, pair: (apr_brigade_create, apr_bucket_
bug: apr_bucket_flush_create in ap_fflush, pair: (ap_pass_brigade, apr_bucket_flu
bug: apr_array_make in dirsection, pair: (apr_array_make, apr_hook_debug_show), s
bug: apr_array_make in dirsection, pair: (apr_array_make, apr_hook_sort_register)
bug: apr_array_make in ifsection, pair: (apr_array_make, apr_hook_debug_show), su
bug: apr_array_make in ifsection, pair: (apr_array_make, apr_hook_sort_register),
bug: apr_array_push in ap_regname, pair: (apr_array_make, apr_array_push), suppor
bug: apr_array_make in create_core_server_config, pair: (apr_array_make, apr_hook
bug: apr_array_make in create_core_server_config, pair: (apr_array_make, apr_hook
bug: apr_array_make in create_core_server_config, pair: (apr_array_make, apr_arra
bug: apr_array_make in ap_byterange_filter, pair: (apr_array_make, apr_hook_debug
bug: apr_array_make in ap_byterange_filter, pair: (apr_array_make, apr_hook_sort_
bug: apr_bucket_eos_create in ap_byterange_filter, pair: (ap_pass_brigade, apr_bu
bug: apr_brigade_cleanup in ap_http_chunk_filter, pair: (apr_brigade_cleanup, apr
bug: apr_array_make in filesection, pair: (apr_array_make, apr_hook_debug_show),
bug: apr_array_make in filesection, pair: (apr_array_make, apr_hook_sort_register
bug: apr_hash_set in ap_register_provider, pair: (apr_hash_set, apr_palloc), supp
bug: apr_array_make in ap_make_method_list, pair: (apr_array_make, apr_hook_debug
bug: apr_array_make in ap_make_method_list, pair: (apr_array_make, apr_hook_sort_
bug: apr_array_make in ap_make_method_list, pair: (apr_array_make, apr_array_push
bug: apr_array_make in prep_walk_cache, pair: (apr_array_make, apr_hook_debug_sho
bug: apr_array_make in prep_walk_cache, pair: (apr_array_make, apr_hook_sort_regi
bug: apr_array_make in prep_walk_cache, pair: (apr_array_make, apr_array_push), s
bug: apr_bucket_eos_create in ap_core_input_filter, pair: (ap_pass_brigade, apr_b
bug: apr_array_make in ap_select_protocol, pair: (apr_array_make, apr_hook_debug_
bug: apr_array_make in ap_select_protocol, pair: (apr_array_make, apr_hook_sort_r
bug: apr_array_make in so_sconf_create, pair: (apr_array_make, apr_hook_debug_sho
bug: apr_array_make in so_sconf_create, pair: (apr_array_make, apr_hook_sort_regi
bug: apr_array_make in so_sconf_create, pair: (apr_array_make, apr_array_push), s
bug: apr_array_make in ap_parse_form_data, pair: (apr_array_make, apr_hook_debug_
bug: apr_array_make in ap_parse_form_data, pair: (apr_array_make, apr_hook_sort_r
bug: apr_array_push in set_server_alias, pair: (apr_array_make, apr_array_push),
bug: apr_hash_set in set_cgi_var, pair: (apr_hash_set, apr_palloc), support: 7, c
bug: apr_array_push in set_define, pair: (apr_array_make, apr_array_push), suppor
```

Figure 7: Support = 5, Confidence = 70, Level = 2, ratio = 40

In Figure 7, the bugs detected by each algorithm are 118, 101, and 101 respectively.



```
bug: apr_bucket_flush_create in ap_fflush, pair: (apr_brigade_create, apr_bucket_f
bug: apr_bucket_flush_create in ap_fflush, pair: (ap_pass_brigade, apr_bucket_flus
bug: apr_array_push in ap_file_walk, pair: (apr_array_make, apr_array_push), suppo
bug: apr_array_make in dirsection, pair: (apr_array_make, apr_hook_debug_show), su
bug: apr_array_make in dirsection, pair: (apr_array_make, apr_hook_sort_register),
bug: apr_array_make in ifsection, pair: (apr_array_make, apr_hook_debug_show), sup
bug: apr_array_make in ifsection, pair: (apr_array_make, apr_hook_sort_register),
bug: apr_array_push in ap_regname, pair: (apr_array_make, apr_array_push), support
bug: apr_array_make in create_core_server_config, pair: (apr_array_make, apr_hook_
bug: apr_array_make in create_core_server_config, pair: (apr_array_make, apr_hook_
bug: apr_array_make in create_core_server_config, pair: (apr_array_make, apr_array
bug: apr_array_make in ap_byterange_filter, pair: (apr_array_make, apr_hook_debug_
bug: apr_array_make in ap_byterange_filter, pair: (apr_array_make, apr_hook_sort_r
bug: apr_bucket_eos_create in ap_byterange_filter, pair: (ap_pass_brigade, apr_buc
bug: apr_brigade_cleanup in ap_http_chunk_filter, pair: (apr_brigade_cleanup, apr_
bug: apr_array_make in filesection, pair: (apr_array_make, apr_hook_debug_show), s
bug: apr_array_make in filesection, pair: (apr_array_make, apr_hook_sort_register)
bug: apr_hash_set in ap_register_provider, pair: (apr_hash_set, apr_palloc), suppo
bug: apr_array_make in ap_make_method_list, pair: (apr_array_make, apr_hook_debug_
bug: apr_array_make in ap_make_method_list, pair: (apr_array_make, apr_hook_sort_r
bug: apr_array_make in ap_make_method_list, pair: (apr_array_make, apr_array_push)
bug: apr_array_make in prep_walk_cache, pair: (apr_array_make, apr_hook_debug_show
bug: apr_array_make in prep_walk_cache, pair: (apr_array_make, apr_hook_sort_regis
bug: apr_array_make in prep_walk_cache, pair: (apr_array_make, apr_array_push), su
bug: apr_bucket_eos_create in ap_core_input_filter, pair: (ap_pass_brigade, apr_bu
bug: apr_array_make in ap_select_protocol, pair: (apr_array_make, apr_hook_debug_s
bug: apr_array_make in ap_select_protocol, pair: (apr_array_make, apr_hook_sort_re
bug: apr_array_make in so_sconf_create, pair: (apr_array_make, apr_hook_debug_show
bug: apr_array_make in so_sconf_create, pair: (apr_array_make, apr_hook_sort_regis
bug: apr_array_make in so_sconf_create, pair: (apr_array_make, apr_array_push), su
bug: apr_array_make in ap_parse_form_data, pair: (apr_array_make, apr_hook_debug_s
bug: apr_array_make in ap_parse_form_data, pair: (apr_array_make, apr_hook_sort_re
bug: apr_array_push in set_server_alias, pair: (apr_array_make, apr_array_push), s
bug: apr_hash_set in set_cgi_var, pair: (apr_hash_set, apr_palloc), support: 7, co
bug: kill in signal_threads, pair: (ap_log_error_, kill), support: 5, confidence:
bug: apr_array_push in set_define, pair: (apr_array_make, apr_array_push), support
```

```
bug: apr_array_make in prep_walk_cache, pair: (apr_array_make, apr_hook_sort_regis
bug: apr_array_make in prep_walk_cache, pair: (apr_array_make, apr_array_push), su
bug: apr_bucket_eos_create in ap_core_input_filter, pair: (ap_pass_brigade, apr_bu
bug: apr_array_make in ap_select_protocol, pair: (apr_array_make, apr_hook_debug_s
bug: apr_array_make in ap_select_protocol, pair: (apr_array_make, apr_hook_sort_re
bug: apr_array_make in so_sconf_create, pair: (apr_array_make, apr_hook_debug_show
bug: apr_array_make in so_sconf_create, pair: (apr_array_make, apr_hook_sort_regis
bug: apr_array_make in so_sconf_create, pair: (apr_array_make, apr_array_push), su
bug: apr_array_make in ap_parse_form_data, pair: (apr_array_make, apr_hook_debug_s
bug: apr_array_make in ap_parse_form_data, pair: (apr_array_make, apr_hook_sort_re
bug: apr_array_push in set_server_alias, pair: (apr_array_make, apr_array_push), s
bug: apr_hash_set in set_cgi_var, pair: (apr_hash_set, apr_palloc), support: 7, co
bug: apr_array_push in set_define, pair: (apr_array_make, apr_array_push), support
```

```
bug: apr_array_make in prep_walk_cache, pair: (apr_array_make, apr_hook_sort_reg
bug: apr_array_make in prep_walk_cache, pair: (apr_array_make, apr_array_push),
bug: apr_bucket_eos_create in ap_core_input_filter, pair: (ap_pass_brigade, apr_
bug: apr_array_make in ap_select_protocol, pair: (apr_array_make, apr_hook_debug
bug: apr_array_make in ap_select_protocol, pair: (apr_array_make, apr_hook_sort_
bug: apr_array_make in so_sconf_create, pair: (apr_array_make, apr_hook_debug_sh
bug: apr_array_make in so_sconf_create, pair: (apr_array_make, apr_hook_sort_reg
bug: apr_array_make in so_sconf_create, pair: (apr_array_make, apr_array_push),
bug: apr_array_make in ap_parse_form_data, pair: (apr_array_make, apr_hook_debug
bug: apr_array_make in ap_parse_form_data, pair: (apr_array_make, apr_hook_sort_
bug: apr_array_push in set_server_alias, pair: (apr_array_make, apr_array_push),
bug: apr_hash_set in set_cgi_var, pair: (apr_hash_set, apr_palloc), support: 7,
bug: apr_array_push in set_define, pair: (apr_array_make, apr_array_push), suppo
```

Figure 8: Support = 5, Confidence = 70, Level = 5, ratio = 40

In Figure 8, the bugs detected by each algorithm are 118, 95, and 95 respectively.

In conclusion, our algorithm, *EILISP*, eliminates some bugs that are highly possible to be false positives in cases with lower support and confidence settings. In addition, with a higher unpaired partner ratio, more false positives are supposed to be eliminated.

Part 2 (a). We provide our classification and explanation toward 18 warnings here.

1. **CID:** 10026 Dereference before null check
   Triage: Bug
   Location: JspDocumentParser.java (line: 1355)

   ```
   int len = attrs.getLength();
   ```

   Explanation:
   Since the developer does null check on *attrs* before derefercning it in function *startElement*,

I believe that the developer forgets to do null check in function $checkPrefixes$, meaning that it is an unintentional bad practice in codes. The fix here is simple that we just need to do null check on $attrs$ in function $checkPrefixes$ before dereferencing it.

2. **CID:** 10102 Dereference null return value
Triage: Intentional
Location: SSIProcessor.java (line: 304)
Explanation:
The developer intentionally initiates a string with null value and rewrite it when $firstLetter$ does not equal -1. There might be a problem because the program may go to false branch, resulting in returning null pointer. To remove the warning, the developer should use other characters to initialize a string or do null check before returning.

3. **CID:** 10148 Resource leak
Triage: Bug
Location: JkMain.java (line: 455)
Explanation:
The developer does not close or reclaim a system resource after creating a $FileInputStream$, which causes to memory leak. A fix here is to store the new stream with an object name. After loading it in try statement, close it with try-catch in finally block.

4. **CID:** 10167 Dereference before null check
Triage: False Positive
Location: DeltaRequest.java (line: 199)
Explanation:
The warning is not really pointing a bug since the null check is just for checking whether the initialization of *action* in line 65 is successful. There is no line fundamentally rewriting *action* pointer before dereferencing it but adding or removing elements in the list. Therefore, the warning is no need.

5. **CID:** 10176 Dereference null return value
Triage: Bug
Location: SimpleTcpReplicationManager.java (line: 416)
Explanation:
Function *readSession* returns null only when an exception is caught within. However, if an exception happens in Function $readSession$, there is no null check after the function returns, causing the program to crash due to dereferencing *session* which is null. A fix here is doing null check before dereferencing it.

6. **CID:** 10231 Resource leak
Triage: Bug
Location: ChannelNioSocket.java (line: 413)
Explanation:

The developer forgets to close *ssc* before returning at line 413. A way to fix it is closing it before returning.

7. **CID:** 10291 Dereference null return value
   Triage: Intentional
   Location: SSIServletExternalResolver.java (line: 358)
   Explanation:
   The developer intentionally returns a null pointer and pass it as an argument to method *startsWith*, which highly make the program to crash. To fix it, the developer should modify function *getContextPath* so it will not always return a null pointer.

8. **CID:** 10351 Dereference after null check
   Triage: False Positive
   Location: SimpleTcpCluster.java (line: 905)
   Explanation:
   By observation, I am sure that the developer wants to exclude the case when message is null. Although I do not really know the return value of $log.isDebugEnabled()$ when object *message* is null, I believe the the developer clearly know it when checking it before derefrencing object *message*. Thus, I consider the warning as false positive.

9. **CID:** 10381 Dereference null return value
   Triage: Bug
   Location: VirtualDirContext.java (line: 193)
   Explanation:
   There is no null check before dereference on *files* which might be null in line 192. To fix it, do null check before between line 192 and 193.

10. **CID:** 10395 Unguarded read
    Triage: False Positive
    Location: StandardWrapper.java (line: 667)
    Explanation:
    By observation, the function *getServlet* which accesses shared value *instance* is just returning it for function *backgroundProcess* to check the current value of it, which has no intention to compete with other threads. Therefore, I think there is no need for this warning.

11. **CID:** 10396 Dereference after null check
    Triage: False Positive
    Location: FarmWarDeployer.java (line: 153)
    Explanation:
    If *econtainer* is null, then the if statement in line 151 will absolutely go to true branch, meaning the program will return instead of dereferencing an object assigned from it. Thus, the warning is no need.

12. **CID:** 10435 Resource leak
    Triage: Bug
    Location: JDTCompiler.java (line: 235)
    Explanation:
    The function *isPackage* returns True or False without closing Inputstream *is*, which causes memory leak. To fix it, do null check and store the result in a variable, then close the stream and return the variable.

13. **CID:** 10453 Dereference after null check
    Triage: Bug
    Location: ChannelUn.java (line: 116)
    Explanation:
    The warning is reasonable since the developer actually does null check before using super with the method, which implies *wEnv* might be null. The developer does nothing to handle a null condition for *wEnv* and just dereferences it in a parent class method, which is dangerous. To remove the risk, the developer should do something to *wEnv* after the null check before dereferencing it in parent class methods.

14. **CID:** 10507 Dereference after null check
    Triage: Intentional
    Location: MessageBytes.java (line: 330)
    Explanation:
    By observation, there are several checks in the following format

    ```
    if(strValue==null && s!=null)
    ```

    showing that the developer just wants to handle this case while ignoring other cases. This is vary dangerous for the latter codes because *strValue* is dereferenced and *s* is passed as an argument in next line. Thus, I think it is a bad practice and should be replaced by

    ```
    if(strValue==null || s==null)
    ```

    to avoid any possible risks.

15. **CID:** 10514 Missing call to superclass
    Triage: False Positive
    Location: ChannelCoordinator.java (line: 88)
    Explanation:
    There is no need to to call superclass if we do not need any actions implemented in superclass method. So, I think the program logic is up to the developer and there is no necessity for this warning.

16. **CID:** 10625 Dereference before null check
    Triage: False Positive

Location: FarmWarDeployer.java (line: 159)
Explanation:
This is the extension of warning 10396. Based on previous analysis, we know that it is not possible to dereference *engine* if it is a null pointer after the check in line 151. Therefore, the warning can be ignored.

17. **CID:** 10654 Dereference after null check
Triage: False Positive
Location: JDBCStore.java (line: 927)
Explanation:
With the if statement in line 669, *preparedRemoveSql* must not be null, meaning it is not possible to dereference *preparedRemoveSql* in function *remove* and encounter NullPointerException. Hence the warning is false positive.

18. **CID:** 10689 Unguarded read
Triage: False Positive
Location: DeltaSession.java (line: 159)
Explanation:
In occurrences block, there are five example pairs of lock and access. In those fire pairs, there are two cases, B and C, accessing *deltaRequest* for null check. One is reported as unguarded read while the other is not, which is nonsense. If accessing *deltaRequest* for null check needs to be locked like other three cases, then there should be two warnings here. Thus, I consider this warning as false positive.

Part 2 (b). There are only two defects detected by Coverity and the causes are the same – retrieving all keys and then accessing the map again to get the value for some of the keys. The warning here is indicating that it is more efficient to use an iterator on the entrySet of the map, avoiding the Map.get(key) lookup. Take CID 10772 for example. Instead of writing codes below

```
for (String caller:callSites.keySet()){
    Set<String> calleeSet = callSites.get(caller);
```

we can do the same thing in another way like below

```
for (Map.Entry<String,Set<String>>entry:callSites.entrySet()){
    Set<String> calleeSet = entry.getValue();
```

Although the program without the defects may probably run faster, there is no considerable impact that we need to care about in the program. Therefore, those defects can be classified as false positive.