

Forum:[Hack Forums](#)

Thread: [Sqlmap retrieves empty data. MSSQL + Generic WAF + 414 uri too long](#)

antonio.carrillo78 - February 1, 2019, 3:15 am

Hello guys,

I used sqlmap on a website, it's showing me the Database names but it retrieves empty data for tables names

Microsoft SQL Server 2012
DBms = mssql
WAF detected Generic Unkown

The weird part is that i tried for days on row and finally worked. It showed me the table names, columns, and even data inside the columns such as email, phone numebbers, etc. But now it's not working.

The errors i got were:

- 414 uri too long
- something about unable to decode characters

It detects Generic <unknown> waf. Maybe I should use a --tamper ? Which one ?

It seems strange that it worked before and now it doesn't

I tried

tamper=between,chaencode,charunicodeencode,equaltolike,greatest,multiplespaces,nonrecursiver
eplacement,percentage,randomcase,securesphere,sp_password,space2comment,space2dash,spac
e2mssqlblank,space2mysqldash,space2plus,space2randomblank,unionalltounion,unmagicquotes

but didn't work

Girl With One BallSack - February 2, 2019, 1:06 pm

i can help you look in your private inbox!

smtp.hu - February 16, 2019, 10:24 am

--random-agent will be help you

Kalikou - September 5, 2019, 2:25 pm

(Feb 2, 2019 02:06 PM)Girl With One BallSack Wrote: [\[CITE\]](#) i can help you look in your private inbox!

I have the same problem, can you help me

whitedragonflyer - September 5, 2019, 3:19 pm

(Feb 1, 2019 04:15 AM)antonio.carrillo78 Wrote: [\[CITE\]](#) Hello guys,

I used sqlmap on a website, it's showing me the Database names but it retrieves empty data for tables names

Microsoft SQL Server 2012
DBms = mssql
WAF detected Generic Unknown

The weird part is that i tried for days on row and finally worked. It showed me the table names, columns, and even data inside the columns such as email, phone numebbers, etc. But now it's not working.

The errors i got were:

- 414 uri too long
- something about unable to decode characters

It detects Generic <unknown> waf. Maybe I should use a --tamper ? Which one ?

It seems strange that it worked before and now it doesn't

I tried

tamper=between,charencode,charunicodeencode,equaltolike,greatest,multiplespaces,nonrecursiver
eplacement,percentage,randomcase,securesphere,sp_password,space2comment,space2dash,spac
e2mssqlblank,space2mysqldash,space2plus,space2randomblank,unionalltounion,unmagicquotes

but didn't work

Most likely privilege or waf issue. Should use verbose to see what payload is really being tested. I recommend you to do it manually first in order to understand what tamper script to use. Don't get too dependent on sqlmap, use manual bypass and you will see light. If you can't do it manually then sqlmap won't be of much use to you. And you are using too many tamper scripts which is a bad thing. Basically your payload will become junk. PM me, I'll try to help you with what I know.

Fr33z3 - September 7, 2019, 2:59 am

first of all way to many tamper scipts try using --tamper=modsecurityzeroversioned,charencode or the modsecurity tamper with a --hex or --no-cast switch that should help you too long error and yes --random-agent