

Forum:[Hack Forums](#)

Thread: [I get the vulnerable columns, next step fails?!](#)

LukeRZ - January 6, 2013, 7:24 am

Hi, so I started SQL injection, I'd say 20 minutes ago but I've been trying to figure this out, so a tiny bit longer.

I've done all the steps in every tutorial I've seen, and this is the URL extension at the moment.

+union+select+1,2,3,4,5,6,7,8,9,10,11--

There is a hyphen after ?prodID= and then the product ID also.

I get 3 numbers on the screen like this.

And when I do replace 2, 3 and 5 with @@version, the result is also fine.

At this stage the entire site looks like this, just so you can see the difference of when I try and get the table/column names.

So here's when I replace the @@version's with table_name, column_name has the same effect. I have indeed added rom information_schema.tables-- onto the end, same effect.

What's the problem here?

Also, I'm sort of stuck on what to do now. I've seen something about shells, and I don't honestly understand them overly well, but I believe they're some sort of script that exports content and(or) login information?

I hope someone can help.
Many thanks.

Hepic - January 6, 2013, 7:34 am

You can pm me your site,so to help you faster.

Thank you....

LukeRZ - January 6, 2013, 7:37 am

(Jan 6, 2013 08:34 AM)Hepic Wrote: [\[CITE\]](#) You can pm me your site,so to help you faster.

Thank you....

PM'd, many thanks Hepic.

People, please continue to post your thoughts incase Hepic cannot resolve it. :3

WAMx - January 6, 2013, 7:40 am

Post the "table_name" url you write. You might have done that wrong.

LukeRZ - January 6, 2013, 7:49 am

(Jan 6, 2013 08:40 AM)WAMx Wrote: [\[CITE\]](#) Post the "table_name" url you write. You might have done that wrong.

+union+select+1,table_name,table_name,4,table_name,6,7,8,9,10,11--

or

+union+select+1,table_name,table_name,4,table_name,6,7,8,9,10,11 rom
information_schema.tables--

ajkaro - January 6, 2013, 8:37 am

(Jan 6, 2013 08:49 AM)LukeRZ Wrote: [\[CITE\]](#)

+union+select+1,table_name,table_name,4,table_name,6,7,8,9,10,11--

or

+union+select+1,table_name,table_name,4,table_name,6,7,8,9,10,11 rom
information_schema.tables--
LukeRZ

you should read some SQL tutorial first. There is all this well explained. I suggest you this great collection from ZeroFreak

<https://hackforums.net/showthread.php?tid=2008347>

Code union select 1,group_concat(table_name,0x3c62723e),3,4,5,6,7,8,9,10,11 from
information_schema.tables where table_schema=database()-- -

LukeRZ - January 6, 2013, 8:40 am

(Jan 6, 2013 09:37 AM)ajkaro Wrote: [\[CITE\]](#) LukeTZ

you should read some SQL tutorial first. There is all this well explained. I suggest you this great collection from ZeroFreak

<https://hackforums.net/showthread.php?tid=2008347>

Code union select 1,group_concat(table_name,0x3c62723e),3,4,5,6,7,8,9,10,11 from
information_schema.tables where table_schema=database()-- -

Thanks a bunch dude, love you right now. :3

ajkaro - January 6, 2013, 8:43 am

(Jan 6, 2013 09:40 AM)LukeRZ Wrote: [\[CITE\]](#) Thanks a bunch dude, love you right now. :3

Sorry I wrote your name wrong in my previous post :)