

# Advanced SQL Injection

Dump tables



**ZDResearch**

[www.zdresearch.com](http://www.zdresearch.com)

ZDResearch Advanced Web Hacking

# Dump Users table using SQL Injection

- Dump (i.e. download all the records of) the Users table in SQLi Labs

**SQLI DUMB SERIES-2**



# Dump Users table using SQL Injection - Solution

- For dumping data, we need to use a MySQL function called **group\_concat** to concatenate all the result
  - Then the vulnerable app shows it in the output
- So the injected query will something like this:
  - `UNION SELECT 1, ..., group_concat(Column1, 0x3a, Column2, ..) from TABLE`
    - 0x3a is as same as colon
- Here you can see how we dump users table using SQL Injection:

**SQLI DUMB SERIES-2**



Exdemy.com  
Personal property of Keith Samborski  
L\_my69@yahoo.com

ZDRResearch Advanced Web Hacking

***ZDRResearch***

[www.zdresearch.com](http://www.zdresearch.com)

Copyright © Exdemy.com