

# Advanced SQL Injection

Read/Write files with SQL Injection



**ZDRResearch**

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

ZDRResearch Advanced Web Hacking

# Read/Write files with SQL Injection

- Upload a backdoor using SQL Injection on Mutillidae
- If you have not installed Mutillidae on your local environment, you can use the online lab

**User Lookup (SQL)**

 Back  Help Me!

 Hints and Videos

 Switch to SOAP Web Service version 

Switch to XPath version

**Authentication Error: Bad user name or password**

**Please enter username and password to view account details**

Name

Password

**View Account Details**

# Read/Write files with SQL Injection - Solution

- If you see the query in the image, you probably notice it is the same SELECT INTO DUMPFILE query we mentioned in the lecture
- If you are looking for the uploaded backdoor to execute, you must first find an insecure folder where MySQL has write access

The screenshot shows a web application interface with a header bar containing 'User Lookup (SQL)', a 'Back' button with a blue arrow icon, and a 'Help Me!' button with a red push-button icon. Below the header is a 'Hints and Videos' section. The main content area features an 'AJAX' logo, a link to 'Switch to SOAP Web Service version', and another link to 'Switch to XPath version'. A red dashed border contains the message 'Authentication Error: Bad user name or password'. Below this is a pink box with the text 'Please enter username and password to view account details'. Underneath are input fields for 'Name' and 'Password', followed by a 'View Account Details' button. At the bottom, a link says 'Dont have an account? Please register here'. A grey box at the very bottom displays the SQL injection result: 'Results for "1" union select 1,2,3,4,"",3,4 INTO DUMPFILE "backdoor.php" -- ".0 records found.'

User Lookup (SQL)

Back Help Me!

Hints and Videos

AJAX Switch to SOAP Web Service version XML

Switch to XPath version

Authentication Error: Bad user name or password

Please enter username and password to view account details

Name

Password

View Account Details

Dont have an account? [Please register here](#)

Results for "1" union select 1,2,3,4,"",3,4 INTO DUMPFILE "backdoor.php" -- ".0 records found.



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