

# Advanced SQL Injection

Authentication Bypass



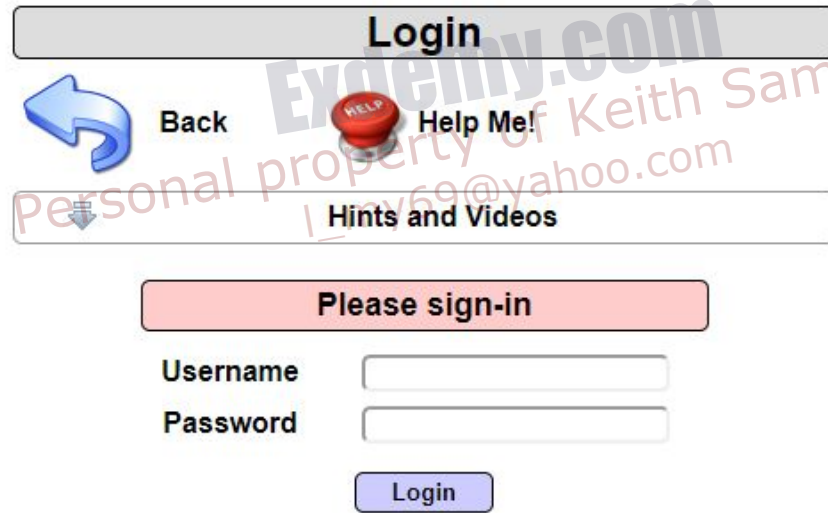
**ZDResearch**

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

ZDResearch Advanced Web Hacking

# Authentication Bypass

- Find a method to log into OWASP Mutillidae as Jeremy (without credentials)



The screenshot shows the OWASP Mutillidae login interface. At the top is a grey bar with the text "Login". Below this bar are two buttons: a blue "Back" button with a left-pointing arrow and a red "Help Me!" button with a red button icon. Below these buttons is a white bar with the text "Hints and Videos" and a small downward-pointing arrow. Below this bar is a pink bar with the text "Please sign-in". Underneath the pink bar are two input fields: "Username" and "Password". Below the input fields is a blue "Login" button. The background of the page is a light orange color with a faint image of a person in a hooded jacket.

Login

Back Help Me!

Hints and Videos

Please sign-in

Username

Password

Login

# Authentication Bypass - Solution

- You can bypass the authentication and then login as any user you want as following:
  - Username : jeremy (or anything else it doesn't matter here)
  - Password : ' or (1=1 and username = 'jeremy') --
- Notice that in the injected query we specify the user we want to log in with, so the username field input doesn't matter here



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