

Information Assurance Group

SQL Injection Attacks

October 3, 2005

The goal behind a SQL injection attack is to gain access to an account that has administrator privileges. Gaining access to these accounts is done by “injecting” SQL commands into text fields, such as the username and password. This will get you initial access to the account to find out information or to make changes. Below, you will find steps that may be taken to gain access.

1. Login
2. Determine Groups
3. Determine who has admin privileges
4. Logout
5. Login with admin username
6. Set password
7. Logout
8. Login as Admin

Good Luck!

-
1. username; ‘ OR 1=1 #
This will log you on as the first user in the user table
 2. Get list of names from messages
 3. Login as an administrator
Change the password and logout
 4. Login as the administrator with the changed password

Anonymous Login

Password: ‘) or ‘? =(‘

Login with only the username

Username: <username>’#